BCA

Business Council of Australia

# Australian Cyber Security Strategy: Legislative Reforms

March 2024

# Contents

# 1. Overview

The Business Council of Australia (BCA) supports the ambition and delivery of the Government's Cyber Security Strategy. Becoming the world's most cyber secure nation by 2030 will require concerted effort and cooperation between all parts of Australia, including government, businesses, and the community. The Government's approach – including through the Executive Cyber Council – has supported this type of collaborative approach.

The set of legislative proposals set out in the Consultation Paper reflects both a series of supports and tasks for businesses. We agree with the intention behind many of the proposals, particularly to support greater collaboration through the Limited Use Obligation and the Cyber Incident Review Board.

Other proposals will require further consultation with businesses, to ensure they have a clear scope and deliver practical and positive outcomes – particularly the Consequence Management Powers. Similarly, the changes to the definition of 'business critical' data must be further developed. It will be critical that the Cyber Incident Review Board (CIRB) be developed with and include a strong industry voice.

Getting the balance right will be the key to success. Some proposals – like the ransomware reporting arrangements and the proposed Consequence Management Powers – will increase complexity, risk, and costs. Given the speed at which cyber risks are evolving, having a nimble approach will be critical. Government must weigh these measures carefully and avoid putting in place regulations that create rigidity in responding to cyber threats, and which could result in poorer outcomes for the community.

If Australia is going to remain globally competitive, we should also treat new costs carefully. For this reason, we support Government undertaking a comprehensive cost benefit analysis of these proposals.

Underpinning this, it will be vital that these legislative reforms are interoperable and consistent with key international partners, particularly where they have existing laws in place. Given our close partnership with countries like the US, including through AUKUS, it would be sensible to draw on comparable laws like the US Government's Cybersecurity Information Sharing Act.

More fundamentally for Australia, we need to continue to refine our governance approach to cyber. The establishment of the Cyber Coordinator and the Executive Cyber Council were important milestones for Australia, and they will have a critical role in drawing in industry experts to oversee the delivery of the Strategy.

However there remain some gaps: the Cyber Coordinator needs to be empowered to coordinate agencies in responding to cyber incidents. As it stands, entities still face a barrage of information requests from regulators when responding to major incidents. Resolving this will mean, in part, getting the proposed Limited Use Obligation right: the Cyber Coordinator needs to be empowered to triage government and regulator requests, particularly where they are not critical to the resolution of an ongoing incident.

# 2. Key recommendations

The BCA recommends:

1. Adopting a variety of international standards for IOT devices and aligning with international standards in determining the types of devices these will apply to.
2. For ransomware reporting:
    a. Limit the obligation to reporting on any payments made and relevant information, such as who the payment was made to and technical identifiers.
    b. Ahead of setting any timeframes for reporting, work with businesses to develop the types of information that must be reported.
    c. Provide strong confidentiality protections for any information provided under this scheme.

3. Take forward the Limited Use Obligation, and:
    a. Enact the Obligation through legislation.
    b. Provide clarity on the type and purpose of information the Australian Signals Directorate (ASD), the Cyber Coordinator or the proposed Cyber Incident Review Board require, and expand this group to include information provided to the Australian Federal Police.
    c. Limit the specific purposes information shared can be used for, including prohibiting sharing with regulators entirely.
4. Establish the CIRB, and:
    a. Focus its efforts on providing reports into wider trends or threats, in genuine partnership with businesses.
    b. If legislated, ensure the CIRB has a tight focus, with a statutory prohibition on the further disclosure of any information provided to the Board.
5. Undertake further consultation on the changes proposed to cover 'business critical' data storage systems and focus the definition on where such data vulnerabilities have a direct adverse impact on the operations of critical infrastructure.
6. If the Government wishes to take forward the Consequence Management Powers, these powers should:
    a. Be structured to commence as an 'authorising' power, to enable entities to undertake actions that would otherwise be prohibited. Any directive powers must require an appropriately high threshold of harm to be demonstrated to be used.
    b. Provide clear avenues for appeal and recourse where an entity disagrees with government, particularly if government chooses to take this forward as a directive power, and provide safe harbour for any entities complying in good faith.
7. Any changes to the secrecy provisions under the Security of Critical Infrastructure (SOCI) Act should have strict limits on disclosing protected information to regulators.

# 3. Secure-by-design standards for Internet of Things (IOT) devices

Through the Cyber Security Strategy, the Government committed to adopt international standards for consumer-grade smart devices. Through this consultation paper, the Government is seeking views on mandatory cyber standards for IOT devices, aligning with international standards.

The BCA supports the use of international standards, and we recommend the Government adopt the approach of recognising a variety of standards beyond those developed by the European Telecommunications Standards Institute (ETSI), such as existing frameworks from organisations like the National Institute of Standards (NIST).

We also recommend that international consistency apply in determining which devices these standards will apply to. Consistency with international approaches to the devices which these standards apply to will ensure Australians receive secure devices with minimal additional costs.

# 4. Ransomware reporting for businesses

The Government has committed to working with industry to co-design options for a mandatory no-fault, no-liability ransomware reporting obligation for businesses to report ransomware incidents and payments.

The BCA supports the Government's commitment to working with businesses on this important initiative. It will be a critical enabler to tackling ransomware, and businesses support the Government taking action to tackle ransomware groups. To this end, and for this initiative to be successful, the reporting obligations must have:

- clear thresholds for who must make reports,
- reasonable timeframes for reporting, and
- strong protections in place for entities who report under the scheme.

Fundamentally, we support the approach the Government is taking to this scheme, particularly the recognition that organisations who suffer ransomware attacks are victims and deserving of support rather than criticism.

Confidential mandatory reporting will provide government with the information needed to inform law enforcement and diplomatic efforts and future policy decisions. It also can provide businesses with a better sense of the threat environment they are operating in.

## 4.1 Who is in scope?

There is a risk that this wide scope (particularly given the lack of clarity on what an 'impact' is) will mean the scheme will be unwieldy and create a reporting burden disproportionate to the benefits.

The reporting scheme must have a high threshold. A low threshold, such as a requirement to report all attempted ransomware attacks, is likely to generate such a high reporting burden that the costs will far outweigh any possible benefits, including because it risks creating a high volume of reporting, which may obscure the identification and response to the most serious of cases.

It will also duplicate existing requirements imposed under other reporting regimes. For example, where personal information is lost as a result of a criminal ransomware incident, this would need to be reported as set out under the Privacy Act. Similarly, if a ransomware incident was likely to cause disruption to serious or critical infrastructure, it would need to be reported per the requirements under the SOCI Act.

We acknowledge that removing SMEs will carve the overwhelming majority of businesses in Australia out of the scheme (more than 98 per cent, per the Consultation Paper). These will likely be the most at-risk organisations as well, given their limited capacity to invest in protections.

That said, we do not support the application of reporting requirements to SMEs, given the disproportionate burden this would place on enterprises with limited resources. However, if the intention of the scheme is to understand the overall ransomware threat environment, then the reporting design must be as simple and straightforward as possible.

Consideration should also be given to whether a pure focus on businesses is sensible. Increasingly not-for-profit organisations and entities are facing cyber-attacks. Many of the organisations support vulnerable Australians and therefore have access to highly personal information.

While we do not support imposing unnecessary reporting obligations on these organisations, if we are to fully tackle cyber security, then these key services should be considered, including to ensure government is able to appropriately support these critical service providers.

On that basis, we recommend the scheme should be focused on reporting around the payment itself. This would strike an appropriate balance between allowing law enforcement agencies to pursue criminals and support businesses more widely, while not creating unwieldy or excessive reporting requirements.

## 4.2 Timeframes for reporting

The Consultation Paper suggest that timeframes for reporting of incidents could be aligned with reporting obligations under the SOCI Act (72 hours).

In serious incidents, this timeframe may be appropriate – which is already the case under SOCI.

However, the Government must also weigh up whether imposing reporting requirements will mean that entities – particularly smaller entities who may be facing an existential threat – will be focusing on discharging reporting obligations, rather than recovering and working with their suppliers and customers.

If reporting requirements must be made within a short window, then any reporting requirements should focus on the critical information government needs urgently. Information that is intended to inform a wider threat picture should be requested in slower timeframes.

We recommend the Government continue working with businesses to develop the types of information that must be reported, ahead of setting any timeframes and protocols for reporting.

## 4.3 Protections for reporting entities

How any reported information is used needs to be carefully developed. We strongly support the Government's commitment to prevent the re-victimisation of entities who are the subject of ransomware.

Given this, we support the intention of establishing the scheme under the principles of no-fault and no-liability. Cyber should not be a domain where it is appropriate to re-victimise anyone. Allowing confidential reporting will also build confidence in the scheme. Responding to ransomware and other cyber threats is not an area of competition for businesses, and naming and shaming businesses serves only to harm victims of crime.

To enable this, the reporting scheme must have strong protections in place. Preserving the confidentiality of reporting entities will be key: when the information is shared more broadly it needs to be de-identified and the specific disclosed information would need to be exempt from Freedom of Information requests.

The interactions of any confidential reporting with Australian Stock Exchange reporting requirements or obligations under the Privacy Act (such as the Notifiable Data Breaches scheme) will need to be considered.

Finally, any information reported under the scheme must not be shared with regulators or enforcement agencies beyond the express and limited purpose of pursuing ransomware criminals. Without this, the timeliness of reporting and ability to work with government will be greatly hampered, as entities will have to ensure any reports cannot be misinterpreted by regulators or misunderstood without wider context.

For this reason, getting the Limited Use Obligation right will be critical.

# 5. Limited Use Obligation

The Limited Use Obligation is intended to provide clarity and assurance in how information reported to ASD and the National Cyber Security Coordinator will be used.

This is intended to ensure incident reporting and cooperation between businesses and government can happen in a timely manner. The Consultation Paper notes businesses are increasingly reluctant to share detailed and timely incident information, with an increasing preference to refer inquiries to legal teams.

In many ways this should be seen as a measure of success for the Government: cyber is no longer a lawless domain.

However, we agree that this is having perverse outcomes. Australia is best served where businesses and government can work closely together in a trusted way. But businesses must also have confidence that information provided early in an incident will not be used against them. This is particularly the case with regulators who may not have the full context about information that has been shared and in circumstances where the amount of information known by the business itself at the time of the earliest reporting to ASD will most likely be incomplete and evolving.

As it stands, 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. This significantly impedes disclosure and sharing of threat information.

For this reason, we support the Government's ambition with the Limited Use Obligation as a critical part of ensuring strong government-business collaboration but addressing the safeguards described below.

To deliver on this ambition, the BCA recommends that the Limited Use Obligation should:

- Be enacted through legislation.
- Provide clarity on the type and purpose of information ASD, the Cyber Coordinator or the proposed CIRB require, and expand this group to include the Australian Federal Police.
- Contain specific purposes information shared can be used for, including prohibiting sharing with regulators entirely.

*Types of information requested*

Under the Limited Use Obligation, the Government should provide a clear articulation on the type of information that will be requested and for what purpose.

For example, the US Government's Cybersecurity Information Sharing Act (CISA) provides a clear definition of the type of cyber threat indicators. This approach should be replicated in Australia.

As it stands, however, entities face a plethora of information requests from government. It is often not clear why this information is being requested, even from technical agencies such as ASD. Government should distinguish between information they need:

- Urgently, to support the immediate response to an incident, and
- Less urgently, to build a national threat picture.

Providing this clarity through the Limited Use Obligation will mean entities can focus on providing the information needed to tackle an incident, while providing the wider threat information later.

Further, any Limited Use Obligation should also extend to the Australian Federal Police, who work closely with businesses to support law enforcement responses and, in doing so, frequently request information from affected entities.

*Clarity on purpose of information sharing*

The purpose of the Limited Use Obligation must be specific and clear. The list of permitted uses should not include for 'consequence management'. Permitted use should explicitly exclude any information that is shared being used in actions against organisations (or their personnel) for failure to meet applicable laws or standards, beyond the case of fraud. This approach would better align with CISA.

Moreover, the legislation will need to be clear that disclosure is authorised under law and does not breach confidentiality or any laws by disclosing information or result in a waiver of any privileges. Critically, it should also be protected from FOI disclosure.

Further, the Limited Use Obligation must explicitly prohibit information from being shared for any purpose with regulators, including for enforcement, investigations, or compliance monitoring. Beyond disincentivising information sharing, this is contrary to natural justice. If any regulators require information, they already have substantial powers to request this information.

# 6. A Cyber Incident Review Board

The Government is proposing to establish a Cyber Incident Review Board (CIRB) to conduct no-fault incident reviews, with lessons learned from these reviews shared with the public to strengthen national cyber resilience.

The BCA supports the establishment of a CIRB. We recommend that the CIRB:

- Focus on providing reports into wider trends or threats, in genuine partnership with businesses.
- If legislated, ensure the CIRB has a tight focus, with a statutory prohibition on the disclosure of any information provided to the Board

This would bring it into alignment with the approach taken in the US, which has involved a genuine partnership between government and the private sector reporting on key threats or trends (such as the Lapsus$ and related threat groups, or the Log4j vulnerability).

If the Government looks to establish the CIRB to look at specific incidents, there must be a clear articulation of how this will add additional value beyond existing processes (e.g. reviews through existing government agencies or the appointment of specialist advisers).

Like the underpinning rationale for the Limited Use Obligation, the CIRB must create an environment where all entities are incentivised to cooperate in a timely way.

There would be merit in considering whether lessons could be learned from the Australian Transport Safety Bureau (ATSB). As the ATSB highlights:

> ATSB investigations do not apportion blame or provide a means for determining liability, and we do not investigate for the purposes of taking administrative, regulatory or criminal action.
>
> Our investigations are aimed at determining the factors which led to an accident or safety incident so that lessons can be learned and transport safety improved in the future. Our ability to conduct an investigation would be compromised if we sought to lay blame, as the future free-flow of safety information could not be guaranteed.

For the CIRB, this will mean success will be underpinned by undertaking blameless post-mortems. In practice, this means if the Government seeks to legislate the CIRB it will need to ensure its purposes are tightly scoped and there is a statutory prohibition on the disclosure of information provided to the Board.

# 7. Data storage systems and business critical data

As part of wider reforms to the SOCI Act, the Government is proposing to clarify the application of the Act to cover 'business-critical' data storage systems.

The BCA welcomes further consultation on this change. Any changes must focus the definition on where such data vulnerabilities have a direct adverse impact on the operations of critical infrastructure.

We continue to believe the Privacy Act should be the primary legislative framework regulating personal information. As the consultation paper acknowledges, it will be critical to avoid duplication or overlap.

Given this, the Government may wish to consider amending the definition of 'business critical data' to exclude the reference to the personal information of at least 20,000 individuals. This is an arbitrary number and does not indicate the critical nature of the data.

Fundamentally, if an incident effects a SOCI regulated entity that relates to personal information, the management of this should be done through the relevant legislation: the Privacy Act.

Instead – and given this Act relates to the security of critical infrastructure – any threshold should include a condition where such data vulnerabilities have a direct adverse impact on the operations of critical infrastructure

(i.e. that a cyber attack on such data would impact the ongoing functioning and availability of the critical infrastructure).

It will be critical these amendments are made before data storage systems holding 'business critical data' are included in the definition of an 'asset' under section 5 of the SOCI Act.

# 8. Consequence Management Powers

The Government is proposing to establish a new 'consequence management' power under the SOCI Act. This will allow the government to direct an entity to take actions to manage the consequences of a nationally significant incident.

This will be a major change, and the Government must carefully consider the potential for unintended consequences. This proposed new power would also enable the government to have sweeping powers across the economy, given the SOCI Act is intended to manage all hazards, not just cyber.

Government needs to provide absolute clarity on how these powers would be intended to be used and in what circumstances. To prevent against misuse by future governments, a high threshold must be set – such as after a federal court order, rather than ministerial direction.

We understand that the purpose of these laws is to help manage secondary consequences from incidents affecting critical infrastructure providers by, for example, 'unblocking' entities from sharing information where existing legislative requirements may prevent them from doing so.

Before going ahead with any change of this nature, the Government will need to be very clear about the legislative gap it is filling. There are already broad emergency powers in Commonwealth, state and territory legislation which enable governments to manage crises.

The term 'consequence management' is also very broadly defined. Beyond capturing the 'downstream' consequences of a cyber incident, it may expose any entity involved in a relevant incident (cyber or not) to additional liability.

Instead, we suggest these powers should start as authorising powers. This would allow government to 'authorise' specific entities to take actions they would not otherwise be able to do so (because of, for example, constraints imposed by the Privacy Act or competition law).

This would help businesses work more collaboratively with each other and with government to clear blockers from positive outcomes for Australia. As Australia saw during COVID, the best outcomes were achieved where businesses were able to work *with* government to manage the consequences of an unforeseen and complex emergency, such as ensuring supply chains for groceries were not held back by competition concerns or delivery hour restrictions.

If there are incidents that require directive powers, this should come with a clearly defined (and appropriately high) thresholds, and with clear avenues for appeal and recourse where an entity disagrees with any direction. This may be because a direction would not be in the best interest of the entity (e.g. a direction to allow a threat actor to stay on a network to help with attribution) or may be where an entity disagrees that a direction will have the consequence government intends (e.g. where an entity – as the expert on its operations and networks – believes government's proposed course of action will further harm the provision of critical services). We would welcome further consultation on what form this appeal mechanism should take.

If the Government wishes to create this new direction power, then it must provide any entity receiving a direction under this power with safe harbour from any liability where they are complying in good faith. This could extend on what is provided under section 35AW of the existing SOCI Act.

# 9. Protected information provisions

The Government is seeking views and feedback on proposed changes to the secrecy provisions under the SOCI Act to better support industry and enable a more agile response to attacks.

We support the Government taking steps to improve information sharing. However, we recommend that limits be retained on disclosing protected information to regulators. The current scope of the changes would contradict the good intentions of the Limited Use Obligation.

Further, we recommend the Government first consider whether the existing trusted information sharing networks would facilitate the information sharing requirements government is trying to achieve.

BUSINESS COUNCIL OF AUSTRALIA

GPO Box 1472, Melbourne 3001  T 03 8664 2664  F 03 8664 2666  www.bca.com.au