BCA
Business Council of Australia

Cyber Security Legislative Package 2024: Parliamentary Joint Committee on Intelligence and Security

Submission of the Business Council of Australia

October 2024

Contents

1. Overview

The Business Council of Australia (BCA) represents over 130 of Australia's leading businesses. Our members include some of Australia's largest banking, telecommunications and technology companies. We champion the role that responsible businesses play in generating sustainable economic growth and advocate for policy settings that are in the national interest.

We welcome this opportunity to provide a submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) on the Cyber Security Legislative Package 2024.

The BCA supports improvements to Australia's cyber security settings. Australians deserve cyber protections, and businesses should be supported in their efforts to be cybersecure in an increasingly challenging global environment.

On 11 September 2024, the BCA provided a lengthy submission on the Exposure Draft of the reforms. We are pleased to see many of our recommendations incorporated into the Bill that was introduced into Parliament and is now before the PJCIS for review.

Our current submission will highlight a few remaining issues the BCA considers important to reconsider.

2. Key recommendations

Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill

1. Executing a direction should require explicit consideration of the:
    a. cost burden imposed on the entity in implementing the direction, and whether there are alternative measures that would achieve a similar outcome which are less cost burdensome,
    b. future commercial viability, and
    c. any permanent impact(s) of the short term direction.
2. A direction should be proportionate and adapted to the incident sought to be addressed.
3. The Bill should clarify liability arrangements in the event of negative consequences from executing an explicit direction.
4. The Bill should clarify what 'operated by' means, where a system (such as a cloud hosted platform as a service) is provided by a third party but forms part of a responsible entity's asset.
5. The Bill should more clearly define 'data storage system'.

Cyber Security Bill

6. Australian security standards for smart devices should recognise existing international standards, such as the UK's, and allow entities to satisfy their obligations through existing Statements of Compliance. Alternatively, Australia's security standards should align with existing international standards to minimise the compliance burden on companies.
7. To properly address the extraterritoriality and geographical nexus with Australia, Division 2, Section 26 (1)(c) should be amended to 'the incident has had, is having, or could reasonably be expected to have, a direct or indirect impact on a reporting business entity to the extent that it carries on business in Australia'.
8. The ransomware reporting obligations should extend liability protections from information provided in compliance with the legislation to information reported voluntarily, such as additional contextual information.
9. The Cyber Incident Review Board (CIRB) should be diverse in its membership, including representatives from government, academia and, critically, from industry.
10. The CIRB should not be used to criticise the victims of cyber incidents, and language to that effect should be added to Division 4, Section 62 (2), which already states the Board's functions exclude apportioning blame or liability.
11. Consulting entities on potentially sensitive information should be a mandatory stage of the CIRB's draft review report, rather than an optional stage.
12. The CIRB should align with definitions and policies used by similar Boards in other countries, for example the US Cyber Safety Review Board (CSRB), to help global companies manage their engagements with multiple Boards on international cyber incidents.
13. The Cyber Security Bill should include a clearer statement to the effect that neither initial disclosure by a company, nor its subsequent disclosure to another entity, a Commonwealth body (other than ASD) or a State body will impact a claim of legal professional privilege.

3. Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill

3.1 Ministerial authorisation relating to serious incidents

Amendments to Part 3A shift the language from purely referencing a 'cyber security incident' to an 'incident' more broadly, for information gathering and action directions only, whilst maintaining the criteria that the incident has had, is having, or is likely to have a relevant impact on one or more critical infrastructure assets.[1]

The Explanatory Memorandum notes that:

> *Incidents in scope could be natural or man-made, so long as they impact the availability, integrity and reliability of the critical infrastructure asset. This includes incidents from all types of hazards, such as cyber and information hazards, physical and natural hazards, personnel hazards, and supply chain hazards.*[2]

The BCA has concerns about this scope of directions for non-cyber incidents. Specifically, that an entity could be directed to do something against its commercial interest that is neither proportionate nor adapted to resolving the incident at issue. For example, an entity could be directed to resolve industrial action by agreeing to terms to which it disagrees.

If this provision is to remain in the Bill, the BCA recommends that executing a direction should require explicit consideration of the:

- cost burden imposed on the entity in implementing the direction, and whether there are alternative measures that would achieve a similar outcome which are less cost burdensome,
- future commercial viability, and
- any permanent impact(s) of the short term direction.

The BCA recommends that a direction should be proportionate and adapted to the incident sought to be addressed.

The BCA also recommends that the Bill should clarify liability arrangements in the event of negative consequences from executing an explicit direction.

3.2 Data storage systems that hold business critical data

Amendments in Schedule 1 seek to address cyber incidents impacting non-operational data storage systems held by critical infrastructure entities. Such incidents, while not directly impacting the essential functions of the critical infrastructure asset, demonstrated the risk to the non-operational systems that hold large quantities of both personal information and other business critical data.

The Explanatory Memorandum notes that:

> *As with other critical infrastructure assets, the responsible entity for the primary critical infrastructure asset will be the entity responsible for the data storage system. Where the responsible entity outsources to a third party, then the third party becomes responsible for the data storage system.*[3]

The BCA recommends the Bill should clarify what 'operated by' means where a system (such as a cloud hosted platform as a service) is provided by a third party but forms part of a responsible entity's asset.

The BCA also recommends that the Bill should more clearly define 'data storage system'.

[1] Security Of Critical Infrastructure And Other Legislation Amendment (Enhanced Response And Prevention) Bill 2024 - Explanatory Memorandum, p.11, para 39.
[2] Security Of Critical Infrastructure And Other Legislation Amendment (Enhanced Response And Prevention) Bill 2024 - Explanatory Memorandum, p.11, para 38.
[3] Security Of Critical Infrastructure And Other Legislation Amendment (Enhanced Response And Prevention) Bill 2024 - Explanatory Memorandum, p.8, para 20.

4. Cyber Security Bill

4.1 Security standards for smart devices

The BCA welcomes introducing security standards for smart devices. These standards should be easy for smart devices providers to comply with – there should not be an unnecessary administrative burden.

Ideally, entities that already comply with a recognised international standard or compliance regime should be able to rely on that to streamline compliance with requirements in Australia.

By having the Australian government formally recognise acceptable international security standards, entities would avoid duplicating compliance activities. Australia could permit entities to satisfy their obligations under the Australian regime by using an accepted international Statement of Compliance.

The BCA recommends that Australian security standards for smart devices should recognise existing international standards, such as the UK's, and allow entities to satisfy their obligations through existing Statements of Compliance. Alternatively, Australia's security standards should align with existing international standards to minimise the compliance burden on companies.

4.2 Ransomware reporting obligations

The Bill has extraterritorial effect and is expected to apply to any entity that carries on business in Australia with an annual turnover of $3 million or more. Many global digital businesses would have an annual turnover of $3 million or more – noting that the turnover test is linked to the revenue of the business, not just the Australian revenue of the business.

If the business suffers a cyber incident that is solely confined to, for example, a US business or its US customers, and has no impact on its Australian business, it would still have to report a ransom payment made in relation to that incident. This seems contrary to the intent of the Bill, and the geographical nexus test is not satisfied.[4]

The BCA recommends that to properly address the extraterritoriality and geographical nexus with Australia, Division 2, Section 26 (1)(c) should be amended to 'the incident has had, is having, or could reasonably be expected to have, a direct or indirect impact on a reporting business entity to the extent that it carries on business in Australia'.

The BCA welcomes the protection from liability in relation to the ransomware reporting obligation. In the current drafting of the Bill, entities only get protection if they are providing information that needs to be provided under the Act. This means entities will have to carefully vet the notification to ensure only protected information is included.

However, if entities' provision of voluntary information (such as general contextual information) is also subject to protection, this would encourage collaboration and greater information sharing between industry and government and better cyber security outcomes for Australia.

The BCA recommends that the ransomware reporting obligations should extend liability protections from information provided in compliance with the legislation to information reported voluntarily, such as additional contextual information.

4.3 Cyber Incident Review Board

The establishment of the CIRB—an independent advisory body that reviews major cyber incidents—is another step forward for cybersecurity in Australia, and the BCA welcomes this body.

The BCA strongly recommends the CIRB should be diverse in its membership, including representatives from government, academia and, critically, from industry. We also recommend it should not be just a technical body, but also include members with expertise in legal, organisational and human factors. Membership criteria should be transparent.

For this Board to truly make an impact, it needs to focus on transparency and empathy with victims. It is not just about reviewing what happened—it is about learning from it and ensuring we are better prepared for what comes next. As such, the BCA recommends that the CIRB should not be used to criticise the victims of cyber

[4] Cyber Security Bill 2024 – Explanatory Memorandum, pg. 14, paras 19–21.

incidents, and language to that effect should be added to Division 4, Section 62 (2), which already states the Board's functions exclude apportioning blame or liability.

Further, Division 2, Section 51 (4) ('Draft review reports') notes that

> *(4) The Board may give the draft review report, or an extract of the draft review report, to any other Commonwealth body or a State body or entity:*
>
> *(a) if the Board considers it appropriate to give the body or entity an opportunity to make submissions on the draft review report or the extract; or*
>
> *(b) for the purposes of determining whether information proposed to be included in the final review report is sensitive review information.*[5]

The BCA recommends that consulting entities on potentially sensitive information should be a mandatory stage of the CIRB's draft review report, rather than an optional stage.

The CIRB should be harmonised with other similar entities around the world. The BCA recommends that the CIRB should align with definitions and policies used by similar Boards in other countries, for example the US Cyber Safety Review Board (CSRB), to help global companies manage their engagements with multiple Boards on international cyber incidents.

4.3.1 Legal professional privilege

We support the Cyber Security Bill's express statement that providing information to a designated Commonwealth body in the context of ransomware payment reports (Section 31), to the National Cyber Security Coordinator in the context of voluntary disclosure (Section 41) or to the CIRB in the context of a cyber security incident review (Section 57) does not affect a claim of legal professional privilege.

However, the Cyber Security Bill's Explanatory Memorandum acknowledges that legal professional privilege is considered to be waived if something is done which is inconsistent with the confidentiality which the privilege is intended to protect.[6] Notwithstanding the express statements in Sections 31, 41 and 57 of the Cyber Security Bill, the sharing of information by the designated Commonwealth body, National Cyber Security Coordinator and CIRB to another entity, a Commonwealth body (other than ASD) or a State body, as contemplated by Sections 30, 40 and 56, is potentially inconsistent with the confidential nature of the information and therefore the claim of legal professional privilege.

The BCA recommends that the Bill should include a clearer statement to the effect that neither initial disclosure by the company, nor its subsequent disclosure to another entity, a Commonwealth body (other than ASD) or a State body will impact a claim of legal professional privilege. This is particularly important given that there is not a settled position on whether and when provision of information to government agencies constitutes a waiver of legal professional privilege.[7]

[5] Cyber Security Bill 2024, pg. 58.
[6] Cyber Security Bill 2024 Explanatory Memorandum, paragraphs 254, 329 and 463.
[7] *ASIC v Noumi Ltd* [2024] FCA 349.

BUSINESS COUNCIL OF AUSTRALIA

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

BCA

Business Council of Australia