Insurance Council of Australia

1 March 2024

Department of Home Affairs

By upload

Dear sir/madam

Australian Cyber Security Strategy: Legislative Reforms

The Insurance Council of Australia (the **Insurance Council**) welcomes the opportunity to contribute to the *2023-2030 Australian Cyber Security Strategy's* Legislative Reforms Consultation Paper (the **Paper**). The Insurance Council represents insurers who own and operate critical infrastructure assets under the *Security of Critical Infrastructure Act 2018* (*SOCI Act*). Some of our members also offer cyber insurance, including to businesses in the critical infrastructure supply chain.

Beyond the below general comments on measures outlined in the paper and other considerations important to insurers, responses to the Paper's specific questions are contained at the appendix.

On Measure 4, the Insurance Council supports the adoption of a model imitating, as much as possible, that of the United States of America's Cyber Safety Review Board (CSRB).[1] We recommend the Government consult further on design once a model has been decided and development has begun.

On Measure 5, insurers seek greater clarity on the definition of 'business critical data.' We note the list of examples but a definitive list of business critical data as well as timelines to identify and harden the protection of this data will be important.

On Measure 6, the Insurance Council notes that many critical infrastructure operators use third party providers for some functions such as data storage. We recommend that where a government must exercise a directive regarding such a third party provider's infrastructure and any exploitation is not a result of the critical infrastructure operator's oversight in securing its data, the directive is issued directly to the third party provider.

More generally, and as acknowledged throughout the paper it is important that the Government avoid regulatory duplication or additional unnecessary regulatory burden. Given this, it will be important that before any changes are made to the *SOCI Act* or new cyber security legislation is enacted, consideration is given to the implications for or interactions with other regulatory regimes. For example, insurers have existing obligations around critical infrastructure management under the *Financial Accountability Regime* and the Australian Prudential Regulation Authority's *Prudential Standard CPS 230 Operational Risk Management*. It is important cyber security is approached as a whole-of-government initiative with all agencies and departments working together to ensure businesses do not have multiple, overlapping touch points with the Government.

Fit for purpose regulatory systems are also critical in ensuring businesses in the critical infrastructure supply chain can access appropriate insurance, including for example directors' and officers' insurance

[1] Cybersecurity & Infrastructure Security Agency. *Cyber Safety Review Board*.

Insurance Council of Australia

and cyber insurance. Regulation that is cumbersome, overlapping or otherwise inappropriate creates regulatory risk that can be difficult and expensive to price. This is true adds to the cost of doing business.

The Insurance Council notes the legislative changes discussed in the paper have further development and implementation processes ahead. We, and the insurance industry more broadly, welcome further engagement with the Government to assist with the process. To continue the discussion, please contact Mr Eamon Sloane, Policy Advisor, Regulatory & Consumer Policy, at [redacted].

Regards

[redacted]

Andrew Hall
Executive Director and CEO

Insurance Council of Australia

Appendix: Consultation paper question responses

What mandatory information, if any, should be reported if an entity has been subject to a ransomware of cyber extortion incident?

It is critical that the Government ensure that any information collected and published can be effectively de-identified so that reporting business cannot be publicly identified.

We recommend the Government consider collecting date and time of incident, the identity of the adversary (if known), nature of attack (ransomware variant used and first point of entry), and when and how was a ransom request made.

Reporting should avoid duplicating that which already reportable under the *SOCI Act* or other similar regulatory instruments such as the Australia Prudential Regulation Authority's *Prudential Standard CPS 234.* Already reportable information includes how the incident was discovered; the nature of the incident being reported and what systems the incident is affecting (i.e., information technology, operational technology or consumer data).

We also encourage the Government to consider the implications of legal professional privilege on mandatory reporting.

What additional mandatory information should be reported in a payment is made?

Information such as the payment method (for example, the type of cryptocurrency used), the amount paid and to whom money was paid may be useful in understanding trends and modi operandi among threat actors.

What is the appropriate scope of a ransomware reporting obligation to increase visibility of ransomware and cyber extortion threats, whilst minimising the regulatory burden on entities with less capacity to fulfil these obligations?

We believe it would be beneficial to require more broad but less detailed reporting. This will give the Government the greatest assistance in its goal of establishing a clear threat picture using up-to-date data about cyber incidents as they occur.

The Insurance Council believes further consideration needs to be given to the link between the information to be reported and the timeframe in which it must be disclosed. We are concerned about the quality of information that an organisation can produce in a limited period (i.e., 72 hours), given that internal investigations are usually still in their infancy at this point. A broader but less detailed obligation would help balance these concerns with the need to increase visibility of the ransomware environment.

Should the scope of ransomware reporting obligations be limited to larger businesses, such as those with an annual turnover of more than $10 million per year?

No. We believe that a more universal reporting requirement is key to maximising the national visibility of the ransomware threat.

Further, it is important that corporate entities and businesses operating critical infrastructure understand the risks and threats small businesses, who are among their suppliers and customers, are facing.

Government could partner with small business infrastructure providers such as accounting software providers to deliver an easily accessible reporting capability for small businesses.

Insurance Council of Australia

A broad but less detailed reporting principle would also limit the burden on small businesses.

After an initial period of time, if it were evident that threshold could be raised, the Insurance Council would welcome revisiting the question.

How can the Government ensure that no-fault and no-liability principles balance public expectations that businesses should take accountability for their cyber security?

The Government should provide clear guidance on where an entity will be pursued for doing the wrong thing. The insurance industry supports a proportionate compliance framework, as outlined in the Paper, as a mechanism to help balance public and business expectations.

What is an appropriate enforcement mechanism for a ransomware reporting obligation?

We recommend the Government seek to leverage an existing mechanism rather than establishing a new government touch point for business. This poses challenges for industries with specific regulators and it may be most appropriate for the ACSC to initially collect this information and disseminate to industry-specific regulators such as APRA.

What types of anonymized information about ransomware incidents would be most helpful for industry to receive? How frequently should reporting information be shared, and with whom?

Any information published needs to serve the purpose of helping other organisations avoid falling victims to similar incidents. To this end, information must be timely with publishing dates as short as possible. Information that industry can practically act on to improve their cyber posture will be useful. This will be different for entities in different industries and of different sizes.

In addition to what information should be published, the Insurance Council believes the Government should consider whether information about incidents that have no public effect need to be published. Publishing this information may have unintended consequences that detract from the objective of the slated changes. There may be an effective, more covert mechanism through which relevant information can be shared with the relevant organisation only.

What else can Government do to promote and incentivise entities to share information and collaborate with ASD and the Cyber Coordinator in the aftermath of a cyber incident?

The Government should show industry that in any act of sharing, information will flow both ways. The Insurance Council understand that often information is provided to the Australian Cyber Security Centre by business to no response. This is disconcerting and disincentivising for firms and should be reviewed.

The Insurance Council would welcome measures that embed a culture of genuine partnership and information sharing between industry and relevant public servants. In 2023, the Insurance Council and MinterEllison Consulting hosted an industry roundtable to informally discuss the cyber threat landscape. The Insurance Council would welcome ASD and Cyber Coordinator representation at similar events in the future to build trust and help greater informal collaboration and information sharing.

What factors would make a cyber incident worth reviewing by a CIRB?

Should lessons learnt from a cyber incident be shared publicly, it may be appropriate for CIRB reviews to focus on incidents that have affected the public or are in the public domain. Publicly releasing details of incidents that do not affect the public may have unintended consequences for businesses

Insurance Council of Australia

and critical infrastructure environments. For example, a business may suffer unnecessary reputational damage. It may be appropriate to establish a secondary mechanism that releases lessons learnt from these less public attacks to the business community.

To what extent should the CIRB be covered by a 'limited use obligation', similar to that proposed for ASD and the Cyber Coordinator?

We believe the principles that are applied to ASD and the Cyber Coordinator should also apply to the CIRB, particularly given the similarities in the information each body collects.

The Insurance Council would support formal assurances that information will not be used for other purposes. There should be clarity on how regulators would be able to use documents published by a CIRB.

We also note that it will be important to balance the risk of potential class actions against businesses with the goals of the CIRB.