Insurance Council of Australia

14 April 2023

Department of Home Affairs

By upload

Dear sir/madam

2023-2030 Australian Cyber Security Strategy

The Insurance Council of Australia[1] (Insurance Council) welcomes the opportunity to contribute to the development of the 2023-2030 Australia Cyber Security Strategy (the Strategy). The Insurance Council represents insurers who own and operate critical insurance assets under the *Security of Critical Infrastructure Act 2018* (*SOCI Act*) and are subject to cyber security risk requirements of the Australian Prudential Regulation Authority (APRA), as well as insurers who offer cyber insurance products in the domestic and international markets.

This submission builds on the Insurance Council's previous submissions to the Department of Home Affairs and our *Cyber Insurance: Protecting our way of life, in a digital world* paper.[2] Beyond the below discussion on the important role of cyber insurance, responses to the Strategy's specific questions are contained at the appendix.

Cyber Insurance

The insurance sector is invested in supporting Australian businesses to be more resilient and in turn protecting Australia's physical and digital assets. As the insurance sector has been a stakeholder in developing and advocating for the ongoing improvement of Australia's building standards, the Insurance Council recognises the industry's role in improving cyber standards and practices across the economy. This role is complementary to the Strategy.

Like traditional insurance products, cyber insurance uses price signals and risk selection to incentivise risk mitigation and minimise losses for policy holders. As part of the underwriting process, insurers often examine an organisation's cyber defenses, identify vulnerabilities and provide guidance on how to strengthen cyber security. The ability to mitigate risk allows businesses to innovate, increase productivity and seize opportunities in the digital economy. The Insurance Council would welcome government initiatives that improve firms' cyber risk posture. These initiatives would in turn, likely improve availability of cyber insurance.

The Insurance Council does however note the limitations of the private insurance market in mitigating the risk associated with catastrophic cyber-attacks, particularly those involving state or terrorist actors.

[1] The Insurance Council is the representative body of the general insurance industry in Australia and represents approximately 89% of private sector general insurers. As a foundational component of the Australian economy the general insurance industry employs approximately 60,000 people, generates gross written premium of $59.2 billion per annum and on average pays out $148.7 million in claims each working day ($38.8 billion per year).

[2] Insurance Council of Australia. 2022. *Cyber Insurance: Protecting our way of life, in a digital world.*

Insurance Council of Australia

Given this, we encourage the Government to consider public-private cooperation as is being explored in the US and UK.[3] The industry would welcome the opportunity to discuss this.

As well as improving public-private mechanisms for cyber threat sharing and blocking, the Strategy should consider enhancements to data sharing, from both industry to government and government to industry, to increase understanding and coverage of cyber risk. Where the insurance industry can understand risk, it can engage with customers to mitigate and insure against that risk. While data sharing raises challenges around privacy and commercial-in-confidence requirements, the Insurance Council welcomes the opportunity to further engage with the Government on working through these.

The Insurance Council notes the Strategy has a long development and implementation process ahead. We, and the insurance industry more broadly, welcome further engagement with the Government to assist with the process. To continue this discussion, please contact Mr Eamon Sloane, Policy Advisor, Policy and Regulatory Affairs, at [redacted] or [redacted].

Regards

[redacted]

Andrew Hall
CEO and Managing Director

[3] Ian Smith. 2023. *Financial Times*. Insurers in talks on adding state-backed cyber to UK reinsurance scheme; United States Government Accountability Office. 2022. *Cyber Insurance: Action needed to assess potential federal responses to catastrophic attacks*.

Insurance Council of Australia

Appendix: Strategy question responses

What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?

The Minister's foreword noted that Australia currently operates with a "patchwork of policies, laws and frameworks." The Government should pursue a simplification of this existing patchwork as a matter of urgency, including the regulatory lexicon, reporting timelines and thresholds employed by the various regulatory frameworks.

The Strategy should bring government, industry and other organisations together under a single national approach. Australia's national cyber resilience is only as strong as its weakest link and ensuring the business community, from sole traders to our largest companies, understand and can meet obligations that are proportional to their systemic risk will strengthen the entire ecosystem. As discussed above, cyber insurance can help drive greater cyber hygiene.

Beyond this system-wide uplift in cyber hygiene, the Strategy should seek the harmonise the regulatory environment. The Strategy discussion paper proposes significant changes, such as a new Act, which should aim to simplify the eco-system. However, major changes take time. As discussed in the responses below, the Government should pursue more immediate, non-legislative harmonisation mechanisms while more significant changes are considered. While this will require significant cooperation among financial services and domestic security regulators, it will provide a template for national cooperation and build trust in the Government's agenda among the business community.

The Strategy also needs to consider the interaction of the current framework, as well as any future changes, with other, non-security regulatory systems. For example, there are implications for large firms in their dealings on cyber security with small business suppliers and customers under the unfair contracts regime that security regulators may not have visibility of. For example, where a security agency might believe a large firm can require a small business supplier to meet certain cyber security standards through contractual obligations, this might in fact breach the unfair contract terms regime.

What legislation or regulatory reforms should Government pursue to: enhance cyber resilience across the digital economy?

Currently, some large organisations must meet and report on very similar information security requirements to different regulators. For example, insurance companies have reporting obligations under APRA's *Prudential Standard CPS 234 Information Security* which overlaps with obligations to the Department of Home Affairs under the *SOCI Act* and to the Office of the Australian Information Commissioner (OAIC) under the *Privacy Act 1988*. Some incidents may also need to be reported to the Australian Securities and Investment Commission and Insurance Code of Practice Governance Committee. These multiple requirements do not necessarily increase information security but do add to regulatory complexity and compliance costs.

What is the appropriate mechanism for reforms to improve mandatory operational cyber security standards across the economy (e.g., legislation, regulation, or further regulatory guidance)?

The Insurance Council prefers central, principles-based regulation that ensures a firm's obligations are commensurate with its risk. This includes a single reporting framework that aligns the information requirements of multiple regulators. This also includes the removal of duplicate reporting obligations such as to APRA and the Department of Home Affairs, as discussed above. Beyond this, further government intervention should focus on regulatory guidance and industry support. Avoiding a prescriptive regulatory environment where possible will allow for innovation in the cyber security space.

Insurance Council of Australia

The Insurance Council would support the implementation of minimum standards or similar across the broader economy as well as support for small businesses in meeting these. These initiatives would support the underwriting process for cyber insurance.

Is further reform to the Security of Critical Infrastructure Act required? Should this extend beyond the existing definitions of 'critical assets' so that customer data and 'systems' are included in this definition?

The Insurance Council is not opposed to further reforms to the *SOCI Act*. In particular, we believe further clarity and certainty on definitions is required to ensure application to the general insurance sector is unambiguous. However, we note the Act was only recently amended and further substantive reforms may increase complexity for industry without allowing time to assess the effectiveness of the Act's current requirements.

The Insurance Council would be concerned by the extension of the critical asset regime to cover customer data. Personal data is important and should be held securely, however, is not critical infrastructure. Many smaller firms who hold customer data but do not operate infrastructure that powers Australia may be captured by such an extension at little benefit to Australia in case of a systemic threat. We note the Privacy Act is currently undergoing a significant review and believe protection of data would be better captured there.

Should the obligations of company directors specifically address cyber security risks and consequences?

The Insurance Council does not support specific cyber security obligations for company directors. We note that company directors currently have general duties under Section 180 of the *Corporations Act 2001* and with specific obligations under the *Privacy Act 1988*. Financial services companies also have additional obligations under Section 912A of the *Corporations Act*[4] and APRA *Prudential Standard CPS* 234 *Information Security.* Further obligations would likely only create regulatory complexity and add to compliance costs. The Insurance Council recommends greater regulatory guidance for directors.

Should Australia consider a Cyber Security Act, and what should this include?

The Insurance Council is not opposed to a new Act that centralises regulation and obligations for business. We strongly suggest, however, that any potential legislative reform consider the existing legislative and regulatory requirements, particularly sector-specific regulation such as APRA requirements applicable to financial services entities including insurers. The aim must ultimately be to ensure there is a streamlined and simplified approach. The Government should avoid creating an additional layer of obligations which is likely to create further complexity and a lack of clarity in terms of interactions with existing legislation and regulation. Practically, the insurance industry would be disappointed in the creation of a new Act which duplicated ongoing APRA regulation.

We note any such reform would be a long process with significant consultation required. While the Government considers this, the immediate imperative must remain on harmonising the existing regulatory framework, including multiple and overlapping reporting requirements.

[4] In *Australian Securities and Investments Commission v RI Advice Group Pty Ltd [2022] FCA 496*, the Federal Court found Australian Financial Services licensee, RI Advice, breached its license obligations to act efficiently and fairly when it failed to have adequate risk management systems to manage its cybersecurity risks.

Insurance Council of Australia

How should Government seek to monitor the regulatory burden on businesses as a result of legal obligations to cyber security, and are there opportunities to streamline existing regulatory frameworks?

The Government should open and maintain formal and informal channels with industry. The Insurance Council notes that these channels are effective only when trust is maintained. Monitoring regulatory burden must be matched with the actioning of genuine concerns.

As discussed above, the Insurance Council considers there are several opportunities to streamline existing regulatory frameworks, including reporting requirements. As recognised in the recent *Privacy Act Review Report*, there are likely to be challenges in aligning reporting obligations (such as the Notifiable Data Breach (NDB) scheme and reporting obligations under the *SOCI Act*). It is therefore suggested that further work is needed to better facilitate reporting processes for regulators and reporting entities alike. We suggest similar considerations are required as it relates to cyber incident reporting, including reporting obligations to APRA. Any consolidation of reporting should also consider opportunities to streamline reporting to regulators and appropriate co-ordination across regulators to support a streamlined reporting regime.

Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by: (a) victims of cybercrime; and/or (b) insurers? If so, under what circumstances?

Prohibiting the payments of ransoms is a complex policy issue. The Insurance Council suggests that a broad range of policy responses and actions be considered to counter ransomware, such as strengthening cyber security standards and disclosure regimes (including reporting and sharing of ransomware incidents), tougher penalties and enforcement against cyber criminals, and greater international co-operation and coordination of financial sanctions regimes and information sharing. A multi-faceted approach should aim to reduce the underlying drivers, limit their impact and ensure business resilience.

The Insurance Council notes that the current practice for cyber insurance is that the decision to pay or not pay a ransom is made by the client. Moreover, any ransom payment is made by the victim, not the insurer and may be reimbursed (in part or full), subject to the limits of the policy and compliance with sanction policies. While paying ransoms can contribute to a criminal business model, it must be recognised that no organisation wants to be extorted and the decision to pay a ransom is largely a function of the cost of recovery and remediation being higher than the ransom demand. As such, an outright ban may disproportionally affect smaller entities and may significantly impact their ability and capacity to recover and return to operation. The Insurance Council strongly encourages the Government to consult further with the insurance industry before taking a define position to ban ransom payments. In the meantime, the decision to pay a ransom or not should remain with the victim organisation. Banning ransom payments by businesses and/or reimbursements by insurers may have other unintended consequences which we suggest warrant careful consideration.

Other policy considerations on ransom payments include education and crypto-asset regulation. Business operators, particularly small businesses, need to understand the full implications of a ransomware attack, including that paying a ransom may not mean the retrieval of their data. Protecting a business' cyber assets and backing-up data remain the greatest protection against the loss of data.

Early notification to regulators and government of ransom attacks and information sharing with the wider eco-system help protect against future attacks. Further, as ransom payments are frequently requested in cryptocurrency, greater regulation of crypto assets should be considered as part of the solution to deter attacks.

Insurance Council of Australia

Would expanding the existing regime for notification of cyber security incidents (e.g., to require mandatory reporting of ransomware or extortion demands) improve the public understanding of the nature and scale of ransomware and extortion as a cybercrime type?

As outlined in the Insurance Council's *Cyber Insurance* paper, we consider expansion of reporting and disclosure for ransomware incidents would improve understanding of the nature and scale of ransomware and extortion as a cybercrime type.[5] We also expect there would be additional benefits such as: enabling businesses and insurers to develop a greater understanding of the risk and the opportunity for businesses to therefore enhance their risk mitigation and resilience to combat this threat; opportunities for improvements and innovation in security measures to address the risks; and better targeting of further government policy responses and enforcement.

As noted above however, enhanced reporting requirements should be considered in the context of existing reporting obligations to government departments and regulators with a preference to streamline these where possible.

How can Australia, working with our neighbours, build our regional cyber resilience and better respond to cyber incidents?

Cyber incidents should be viewed through an international framework with cyber-attacks on Australian organisations often originating outside Australia. These attacks can also weaponise supply chain vulnerabilities in third countries as entry points to an Australian organisation's systems. Information exchanges help Australia, and our neighbours in the early identification of and response to systemic risks. Similarly, joint security exercise and formal co-operation agreements with other countries increases our collective defensive capabilities. These actions raise our national and regional cyber capabilities and resilience. The Government should continue these arrangements and seek similar opportunities within and beyond our region.

In encouraging the Government to consider harmonising the domestic lexicon around cyber security above, we note the internationally recognised terms and definitions employed by international bodies such as the International Organisation for Standards and Financial Stability Board. Australia should consider how these might be employed domestically and regionally to increase shared norms.

How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?

The Insurance Council supports government initiatives such as the Hosting Certification Framework which provide assurances to the broader economy about specific providers. The Government should explore expansions of this and similar programs to increase trust across the ecosystem.

What can government do to improve information sharing with industry on cyber threats?

Fundamental to robust incident reporting and information sharing is trust. Without trust, firms are likely to be guarded in terms of what they are willing to share. We therefore encourage authorities to build out mechanisms to strengthen trust. This includes sharing common lessons learnt and information on emerging threats. Informal dialogue opportunities between the public and private sectors to share this non-critical data should be pursued. Information reported to authorities could be aggregated, analysed, and converted into actionable intelligence that is shared with industry to foster near real-time mitigation of future cyber incidents. When authorities share this actionable intelligence with industry, it should be

[5] Insurance Council of Australia. 2022. *Cyber Insurance: Protecting our way of life, in a digital world*. Page 13.

anonymised to avoid identification of the victim firm and done in coordination with the victim firm where possible.

During a cyber incident, would an explicit obligation of confidentiality upon the Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC) improve engagement with organisations that experience a cyber incident so as to allow information to be shared between the organisation and ASD/ACSC without the concern that this will be shared with regulators?

Yes.

Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?

Yes. Australian industry and governments are competing for the same resources among a talent pool that is struggling to meet demand. This drives up wage costs and can crowd organisations out of the ecosystem, creating national weaknesses. A tailored approached is necessary to ease this issue.

How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians?

Government involvement in a cyber incident response should be commensurate the incident's severity. If an incident does not involve critical infrastructure, the Government should seek to limit its involvement to match the assistance requested. It is also important that government limits, as much as possible, re-victimisation of an organisation that has fallen victim to a cyber-attack. Victim blaming erodes trust in the Government among the broader ecosystem.

Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?

In line with the Insurance Council's call for a simplified regulatory regime, the Government should implement a single reporting portal for cyber incidents. Notifying and communicating with multiple government entities, including re-supplying the same information, after a cyber incident take resources away from responding to the incident. By eliminating redundant and conflicting regulations and reducing the need to contact multiple entities, resources can be more effectively allocated. Expansion of the incident reporting regime should be subject to further consultation with industry and implicated regulators.