Insurance Council of Australia

26 August 2021

The Manager
Cyber Security Industry Advisory Committee
Department of Home Affairs
4 National Circuit
Barton ACT 2600

By upload: Department of Home Affairs website consultation submission form

Dear Sir or Madam

Strengthening Australia's cyber security regulations and incentives

The Insurance Council of Australia **(Insurance Council**) welcomes the opportunity to comment on the *Strengthening Australia's cyber security regulations and incentives: An initiative of Australia's Cyber Security Strategy 2020* (**Cyber Security Consultation**).

Overview of the Australian general insurance market

The Insurance Council is the representative body of the general insurance industry in Australia and represents approximately 95 percent 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 $53.9 billion per annum and on average pays out $166.2 million in claims each working day ($41.5 billion per year).

General insurers play a vital role in the Australian economy. They help individuals, households, businesses and communities protect their financial well-being by providing an accessible mechanism to transfer, diversify and pool risk. General insurance not only provides peace of mind it also facilitates economic activity. Access to general insurance enables people and businesses to engage in business initiatives which would otherwise not occur because they are too fraught with risk.

Overview of cyber insurance

Cyber insurance is relatively new to the insurance market, and coverage has developed over recent years to address emerging cyber risks. The increasing digitisation of services and operational technologies, along with the involvement of state actors in cyber-attacks on private sector entities, has fuelled the exploitation of vulnerabilities in organisational security measures.

The cyber insurance market continues to grow, internationally and in Australia, however take-up rates remain relatively low compared to more traditional commercial property and liability insurances.[1] At the same time, cyber-related losses continue to rise in both frequency and severity. Accordingly, insurers constantly monitor and adjust their risk appetite and capacity, together with coverage, limits and pricing, both in Australia and globally.

[1] Organisation for Economic Co-operation and Development (OECD), *Insurance Coverage for Cyber Terrorism in Australia*, February 2020, p13.

Insurance Council of Australia

In Australia, general insurers provide stand-alone cyber insurance policies to businesses to cover a range of losses related to cyber incidents. Coverage is typically available for:

- costs related to the loss of or damage to data;
- content-related claims related to data;
- costs to prevent future breaches;
- fines and penalties imposed by regulators;
- public relations costs;
- liability for denial of service from or access to electronically provided data;
- costs association with cyber extortion reimbursement; and
- compensation to third parties for failure to protect their data.

Of the coverage types listed above, the first seven are 'first-party' as they cover losses incurred directly by the insured, while the final type is 'third-party' as it covers losses incurred by third parties that may subsequently be recouped against the insured. The nature and limits of cover will vary by insurer. Property losses relating to damage or corruption of data are typically excluded.

Cover for cyber exposure may also be available as an additional element of business insurance packages, such as management liability and professional indemnity. In this case, the insured business purchases the primary cover, and elects to include some cyber-specific cover for additional premium. This form of cover is generally more limited than stand-alone cover.

Historically some non-cyber policies may have included some cover for cyber incidents captured under the existing terms of the policy, and not specifically excluded. This is referred to as 'silent cyber'. An example of a cyber incident involving silent cyber losses was the 2017 NotPetya malware attack, which led to claims under property policies. The reinsurance market has tightened silent cyber conditions in recent years and as a result policies are now more likely to explicitly include or exclude cyber cover.

Insurance underwriters place a strong focus on a customer's risk management and security culture when reviewing, assessing and pricing the risk. Effective risk management, including a strong internal security culture, can be the most effective defence against threats.

Capabilities that indicate a strong risk management and security culture may, for instance, include internal data handling and internet usage policies for all employees across the business, adequate prevention, detection, and response security capabilities and internal data breach incident response plans. Guidance and resources that support businesses, especially small businesses, to protect themselves against cyber threats can strengthen risk management and security practices.

Cyber Security Consultation - Specific comments

1. Cyber security regulatory framework and governance arrangements

The Cyber Security Consultation indicates that potential governance standards for large businesses would be principles-based instead of prescriptive. The Insurance Council strongly supports a principles-based approach to regulation. This enables regulation to be 'right-sized' and appropriately applied to businesses in the context of their size, the complexity of their operations, and their risk profile.

We are, however, also conscious that the introduction of new governance standards may contribute to further complexity in the cyber regulatory regime. We note that the Cyber Security Consultation found at least 51 Commonwealth, state and territory laws that create, or could create, some form of cyber security obligation for businesses. Even if the new standards were to be voluntary, there would be a strong expectation that large businesses comply.

Insurance Council of Australia

As highlighted in the Cyber Security Consultation, the financial sector (including insurers) are subject to the Australian Prudential Regulation Authority's (**APRA**'s) *Prudential Standard CPS 234 Information Security* (**CPS 234**). In addition, APRA's Cyber Security Strategy is focused on key areas designed to 'make a step change in Australia's financial system cyber resilience'.[2]

The Insurance Council suggests that CPS 234 and APRA's regulatory approach are appropriate to address cyber security practices and risk management across the insurance sector. We are conscious that any additional standards could be of limited, if any, value while potentially imposing significant additional compliance costs including continual monitoring, review and certification.

Similarly, we suggest that a cyber security code under the *Privacy Act 1988* (**Privacy Act**) is likely not be the most effective way to promote the uptake of cyber security best practices. This is due to the Privacy Act's narrow focus on customer information confidentiality which does not address all the other types of cyber risks, such as, threats to the availability or mission critical IT systems supporting vital business processes, threats to the integrity of business data (e.g. receivables, payables, financial accounts etc.) or threats to life. For large-scale organisations across the economy we note emerging regulatory change in relation to Australia's critical infrastructure, and the opportunity for organisations to adopt International Standards Organisation certifications (e.g., ISO27001 – Information Security Management).

To the extent that a cyber security code is adopted, the Insurance Council recommends appropriate carve-outs are provided for organisations already covered by CPS 234 or who can demonstrate certification to an appropriate International Standard.

More broadly, the Insurance Council suggests that any consideration of new governance standards for other industries and large businesses take account of existing sector-specific legislation and risk profiles, and consider the potential complexities and costs that may arise if current requirements are duplicated.

Ultimately, the Insurance Council considers the regulatory approach which is likely to support most effectively the development of clear expectations, increased transparency and disclosure, and enhance consumer protection is one which encourages regulators and government agencies to focus their energies on communicating to businesses in "easy to understand plain English" information their current legal obligations and current best practice behaviour.

2. Targeted support for small businesses

The Insurance Council supports measures to enable small and medium businesses to better-protect themselves from cyber security incidents. We consider the health checks as proposed in the Cyber Security Consultation may provide positive benefits to a range of such businesses.

The Insurance Council also notes there are existing government resources on small business cyber protection, for example the Australian Cyber Security Centre (**ACSC**) provides information on how small and medium businesses can protect themselves from the most common cyber security threats.[3] The ACSC's Essential Eight Maturity Model provides prioritised mitigation strategies to help organisations to improve their cyber risk management.[4]

---

[2] APRA, "Executive Board Member Geoff Summerhayes - speech to Financial Services Assurance Forum", 26 November 2020. Note, APRA's Cyber Security Strategy "has been informed by extensive consultation with the Department of Home Affairs, as well as Treasury, ASIC and the Reserve Bank of Australia, and is designed to complement Australia's Cyber Security Strategy 2020".

[3] Resources are available at: Small & medium businesses | Cyber.gov.au.

[4] Resources are available at: Essential Eight Maturity Model.

Insurance Council of Australia

3. Clear legal remedies for consumers

Affordability of insurance is an increasing concern across several lines of insurance, including directors and officers (**D&O**) liability and professional indemnity insurance. We urge the Government to approach with caution any measures that would place upwards pressure on these lines of insurance, which have faced significant increases in claims costs, and therefore premiums, in recent years. Constrained D&O affordability and availability, in particular, has been the subject of evidence before parliamentary committees and is an area of focus for the federal government.

For example, the Cyber Security Consultation includes a proposal to amend the Privacy Act. Where a cyber-attack occurs, the amendment would give affected individuals the legal right to sue businesses that hold their personal information. This is likely to increase the associated risk for that business, introduce uncertainty in insurers' risk assessments, and increase claims costs.

We also note that significant cyber-attacks (for example breaches notifiable under the Privacy Act) can require a business to either write to affected individuals and/or post a data breach notice on their website to notify consumers and the market. These already have the effect of enabling consumers to ask questions, request further information in relation to a cyber-attack and seek re-assurance on steps taken by an organisation (or otherwise complain to the business or the Office of the Australian Information Commissioner).

The Insurance Council views these existing remedies available to customers to be sufficient and proportionate and is concerned that calls for additional legal avenues for privacy actions are more reflective of perception rather than a compelling need demonstrated by available evidence.

If implemented these factors could increase premiums for certain insurance products, including D&O insurance, across the Australian economy. The Insurance Council therefore strongly encourages the Department of Home Affairs to consider broader insurance implications of any cyber security changes to Australian regulations.

We trust that our observations are of assistance. If you have any questions or comments in relation to our submission please contact Aparna Reddy, the Insurance Council's General Manager, Policy – Regulatory Affairs, on telephone: 02 9253 5176 or email: areddy@insurancecouncil.com.au.

Yours sincerely

Andrew Hall
Executive Director and CEO