1 March 2024

By Upload.

Dear Sir/Madam

Re: Australian Cyber Security Strategy: Legislative Reforms

AFMA welcomes the opportunity to provide comment on the Australian Cyber Security Strategy: Legislative Reforms.

AFMA would like to commend the Government on its work so far in developing the Australian Cyber Security Strategy.

We see the overall direction of the new cyber security legislation and the amendments to the Security of Critical Infrastructure Act 2018 (SOCI) as constructive, efficient and as likely to support substantial improvements in preparedness for and hardening against cyberattacks, as well as better managing outcomes through its clear focus on enabling information flows and a collaborative engagement with industry.

We suggest below refinements to the requirements around mandatory reporting of ransomware incidents.

AFMA fully supports the 'no fault', 'no liability' and 'limited use' elements of the proposal as critical to the success of the program. We are concerned, however, that the plans to include regulators in the information loop ('limited use is not limited sharing') may, when combined with the statutory obligations of company officers (under Corporations Act 2001 s601FD and elsewhere), fatally compromise the ability of firms to freely share information with the Cyber Coordinator and ASD. As we note below close alignment of the information barriers with the Transport Safety Investigation Act 2003 should address this issue.

AFMA also notes that international firms will often face limitations on the information they can share based on regulatory and other requirements in their home jurisdiction.

In relation to the consequence management and review and remedy powers we understand the need for these powers. Regarding the specific requirements around protecting data storage systems and business critical data, we support the increased clarity in this area.

Australian Financial Markets Association
ABN 69 793 968 987
Level 25, Angel Place, 123 Pitt Street GPO Box 3655 Sydney NSW 2001
Tel: +612 9776 7907 Email: secretariat@afma.com.au Web: www.afma.com.au

The Secure-by-design standards for Internet of Things devices and the telecommunications provisions are not relevant to our industry sector.

We thank you for considering our comments below.

Yours sincerely

Senior Director of Policy

Measure 1: Helping prevent cyber incidents – Secure-by-design standards for Internet of Things devices

Measure 1 questions are not generally relevant to AFMA's industry sectors.

Measure 2: Further understanding cyber incidents – Ransomware reporting for businesses

> 8. What mandatory information, if any, should be reported if an entity has been subject to a ransomware or cyber extortion incident?
> 9. What additional mandatory information should be reported if a payment is made?
> 10. 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?

Answering these questions as a group.

AFMA suggests that the mandatory information reported be limited to the following categories:

- what variant of ransomware was used (if relevant);
- what vulnerabilities in the entity's system were exploited by the attack (if known);
- what quantum of payment has been demanded by the ransomware actor or cybercriminal, and what method of payment has been demanded;
- the nature and timing of any communications between the entity and the ransomware actor or cybercriminal; and
- any other relevant information about the incident or actor that could assist law enforcement and intelligence agencies with mitigating the impact of the incident and preventing future incidents.

Note that AFMA does not think it is useful for the purposes of what this measure is trying to achieve to include information about the assets and data impacted, or the impact generally. These additional categories would also increase the reporting burden.

Another helpful category of information to include would be whether the entity had a cyber insurance policy, and if so, how much could be claimed back.

For global groups, AFMA suggests that the requirement for mandatory reporting be expressly limited to incidents that directly impact or otherwise have a material relevant impact on the Australian business entity. To avoid unnecessary burden, we should avoid a requirement like CPS 234 35(b) which requires entities to report incidents which are reported to other regulators with no express materiality threshold.

Sensible exceptions should be put in place to allow firms to not report ransomware demands that are not likely bona fide, for example those that might be contained in phishing emails.

Regulatory burden can be minimised by recognising and leveraging the existing regulatory reporting obligations that also cover ransomware incidents including SOCI Act requirements and financial sector regulations.

Members report that they do not treat ransomware differently to other cyber attacks and include it in their current reporting.

The sharing of this data from regulatory agencies to the Cyber Coordinator could minimise regulatory costs and duplication. We do not support information sharing in the opposite direction.

> 11. Should the scope of the ransomware reporting obligation be limited to larger businesses, such as those with an annual turnover of more than $10 million per year?

AFMA members are captured under all scenarios.

We note that sensitive data (e.g. Personal Identity Information) can be held by quite small companies and insights into ransomware breaches of these companies may be of benefit.

> 12. What is an appropriate time period to require reports to be provided after an entity experiences a ransomware or cyber extortion attack, or after an entity makes a payment?

AFMA would propose including additional thresholds, e.g. entities with more than a certain number of Australian clients / customers impacted and a risk of harm to those clients or customers, similar to the thresholds in the Privacy Act. Such thresholds may better reflect the intention of the strategy.

AFMA suggests in the initial phases information is often minimal and unclear, and the focus should remain on mitigation measures and other responses. Therefore, in the initial response phase, reporting obligations should be limited to categories of information that will enable the Government to assist the entity to contain or limit the impact of the incident.

In later stages more detailed information is likely to be available and firms will have more time to put together reports.

We recommend the Australian government to align with the Financial Stability Board's Format for Incident Reporting Exchange (FIRE) initiative which seeks to converge incident reporting requirements across the globe.

It would also be helpful to have more clarity about the consequence of making a ransomware report. For example:

- how will the Government respond?
- will Government make suggestions about how the entity should handle the incident; and
- what level of engagement with Government will the entity be expected to maintain following a ransomware report, noting that the entity will need to be expending significant resources on the various aspects of incident response?

> 13. To what extent would the no-fault and no-liability principles provide more confidence for entities reporting a ransomware or cyber extortion incident?

We expect this to be of importance to firm confidence. However, currently we see a drafting conflict between the 'no-fault' and 'no-liability' protection principles. Entities should not be liable for a civil penalty if impact is not disclosed (this would potentially result in double financial impact being ransom payment + penalty). Clarification of the "no-liability" concept suggested.

> 14. How can the Government ensure that no-fault and no-liability principles balance public expectations that businesses should take accountability for their cyber security?

Market forces both from public relations and investor perspectives have demonstrated significant power to exact significant costs and drive relevant change within firms. Firms can also face significant private actions in the courts in the case of large breaches.

In the case of financial firms there are already overlapping regulatory fault and liability obligations that ensure that there are risks of fines and other penalties in the case of cyber breaches. These have been successfully tested in the courts.

These existing mechanisms should be kept separate via the no-fault and no-liability from the clear focus that Home Affairs has on reducing harms to the Australian economy. The public understands the principle of Australian Transport Safety Bureau (ATSB) investigation's clear focus on safety and does not expect these investigations to result in 'accountability'. In aviation as in finance there are other existing mechanisms for this including the Crimes Aviation Act 1991, the Civil Aviation Safety Authority, private legal actions and others. As ATSB notes "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."[1]

A similar clear separation should be maintained by Home Affairs in constructing the mechanisms to respond to cyber incidents.

Financial firms are already covered by regulatory requirements that ensure that in addition to market impacts and costs, and litigation costs, there are multiple regulatory liabilities.

> 15. What is an appropriate enforcement mechanism for a ransomware reporting obligation?

A failure to report a ransomware attack would be a *mala prohibita* type civil offence and therefore enforcement should typically follow Braithwaite's regulatory pyramid. Particularly given the likely wide application there may be the risk of capture of firms that are willing to do the right thing.

The pyramid beings with education and engagements and steps up through increased compliance actions such as cautions, directions, and requests, culminating in enforcement action only for repeated or wilful non-compliance.

> 16. What types of anonymised information about ransomware incidents would be most helpful for industry to receive? How frequently should reporting information be shared, and with whom?

Strategy of incident handling, lessons learned and government advice, via townhall meetings or regular newsletters could be helpful.

Technical information that could help a firm determine if they already have an infiltrator within their network (tactics, techniques, procedures, etc.) would also be of assistance.

Measure 3: Encouraging engagement during cyber incidents – Limited use obligation on the Australian Signals Directorate and the National Cyber Security Coordinator

> 17. What should be included in the 'prescribed cyber security purposes' for a limited use obligation on cyber incident information shared with ASD and the Cyber Coordinator?

[1] https://www.atsb.gov.au/about_atsb/overview

18. What restrictions, if any, should apply to the use or sharing of cyber incident information provided to ASD or the Cyber Coordinator?

19. 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?

Questions answered as a group.

As currently drafted the 'Limited use obligation' is unlikely to be effective as it will not create confidence that information provided will not be used by regulators in the course of their investigations. Information sharing with the industry regulators means that firms will have various obligations not to share information freely with the ASD and Cyber Coordinator.

Firms may be more likely to respond in a compliance-only manner to the sharing of information to the ASD and Cyber Coordinator under the current drafting. This is unlikely to lead to the optimal flows of information appropriate for the national interest in cyber security.

The role of the regulators is to explicate and enforce their relevant Acts. This must be clearly separated from the work of the ASD and Cyber Coordinator as it is in the Transport Safety Investigation Act 2003.

While regulators may put themselves forward as appropriate for inclusion in cyber information flows, AFMA does not see a role for the regulators in technical analysing, or responding to, cyber incidents. The sector regulators are not experts in cyber security or cyber incident response. Their inclusion in information flows will not add to cyber security compared to the Cyber Coordinator communicating directly with relevant firms.

If the regulators are in possession of contact lists or information that would assist targeted communications to reduce systemic cyber risks, then this information should be provided to the Cyber Coordinator and ASD for their use. Provision of high-level information to regulators – for example that an incident is underway, firms should take certain protective measures and the potential for financial system impact should be defined in advance.

Firms should be advised early on if the Act is being used by the Cyber Coordinator, ASD or CIRB.

If information specific to a particular cyber response is shared, *or could be shared,* with the industry regulators then many firms will be required, given their statutory responsibilities, to minimise the sharing of this information with the ASD and Cyber Coordinator. That is, it could compromise the purpose of the Cyber Coordinator and the ASD.

To be effective the 'Limited use' must exclude sharing of information with regulators, as under the Transport Safety Investigation Act 2003.

AFMA suggests the need to ensure the legislation is more prescriptive re "sharing" of information. A purpose that should be expressly excluded is regulatory investigation. If a regulator is going to commence an investigation into an organisation following a cyber incident, material for the investigation should be collected separately using the regulator's distinct information gathering powers.

In order to minimise the risk of confidential data being breached when sharing between agencies AFMA requests that:

- Regulators are not included in general information sharing/war rooms etc.;
- Before any information is shared permission of the financial institution is confirmed and the information is shared on a strict need to know basis;
- A record of how and to whom the reports are distributed is made; and
- Strong security access controls are used;
- Any identifiers in the reports are removed.

The sharing of information should be limited to industry groups which might be considered as they may face the similar threats.

Members note the potential utility of the Traffic Light Protocol (TLP) in relation supporting the appropriate sharing of information by the Cyber Coordinator.

In addition, we note that the Consultation Paper observes that currently companies are sharing limited information and via their lawyers. The reason for this is to ensure that no privileged information is being shared – privileged information generally contains evidence that could be used against companies including by regulators or in litigation. Once privileged information is shared, even if it is for the "limited use" purpose, then privilege is to be waived and would no longer apply which could have a significant negative flow on effect for the company in question.

AFMA suggests that the legislation make clear that any sharing of information under this requirement does not waive legal privilege.

AFMA supports a desktop review exercise following this consultation with the relevant actors including financial firms and agencies. This will help to avoid miscommunication of expectations and ensure we put in place processes to manage the incident beforehand.

Measure 4: Learning lessons after cyber incidents – A Cyber Incident Review Board

20. What should be the purpose and scope of the proposed Cyber Incident Review Board (CIRB)?

The Cyber Incident Review Board should support cyber security and public confidence in cyber services through their independent 'no blame' investigation of cyber breaches; cyber breach data recording, analysis and research; and increasing cyber security awareness and improvement actions. Scope should be on those incidents causing material impact to the industry or in the public interest.

21. What limitations should be imposed on a CIRB to ensure that it does not interfere with law enforcement, national security, intelligence and regulatory activities?

The CIRB should be established as an independent Commonwealth Government statutory agency.

The staffing and governance of the CIRB should be entirely separate from industry sector regulators (including APRA, ACCC, and ASIC).

The application of the TLP protocol to the output of the CIRB may assist minimising the risks to security measures.

22. How should a CIRB ensure that it adopts a 'no-fault' approach when reviewing cyber incidents?

The function of the CIRB should be to improve cyber security in Australia through its review of cyber incidents. A list of allowable functions should be legislated.

Any published CIRB report should contain only best-practice recommendations for dealing with similar incidents in the future.

The functions of the CIRB should explicitly in legislation not include:

- Apportioning blame for cyber incidents;
- Providing the means to determine the liability of any person in respect of a cyber incident;
- To assist in court proceedings;
- To allow any adverse inference to be drawn from the fact that a person was involved in a cyber incident.
- Findings on gaps in the organisation's security measures, as this would not only lead to 'fault' potentially being attributed, but also could expose the organisation to future attacks.

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

The CIRB should prioritize the incidents it reviews based on the potential to increase the cyber security in Australia. A factor relevant to this might include the scale of the incident, or the sensitivity of the information involved, or the level of technical sophistication or complexity of the attack.

In addition, other information might include, incident response and recovery strategy, decision making process for payment and incidents qualifying as 'notifiable data breaches' under the Privacy Act and impacting over a certain number of individuals. Incidents triggering other reporting obligations, e.g., under SOCI or APRA's CPS 234 due to their material impact.

24. Who should be a member of a CIRB? How should these members be appointed?

Members of the CIRB should have technical expertise that can help identify potential improvements from cases and recommend how to frame advice that can be shared with firms so that they can improve their cybersecurity.

25. What level of proven independent expertise should CIRB members bring to reviews? What domains of expertise would need to be represented on the board?

Members should have current knowledge of cyber security and incident response. Members should have the skills and experience to ensure strict adherence to the CIRB enabling legislation. The scope and objectives of each review may have a bearing on the skills required. Similar to other enquiries there should be announcement of what the CIRB will review for a particular incident and there should be some time limits.

26. How should the Government manage issues of personnel security and conflicts of interest?

27. Who should chair a CIRB?

It is important that any CIRB Chair has extensive experience in business running information security. While adherence to the enabling legislation will be critical, we see risks in a Chair being appointed based on their legal knowledge, as this may be less likely to understand the practical realities of information security in a world of limited resources.

A Chair with practical knowledge gained from a credible cybersecurity background and business operations expertise may be more likely to produce practical outcomes.

28. Who should be responsible for initiating reviews to be undertaken by a CIRB?

29. What powers should a CIRB be given to effectively perform its functions?

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

The CIRB should be fully covered by a similar 'limited use obligation'. A partial 'limited use obligation' may be fully discounted by industry, and this result would decrease information flows and the utility of the function.

We are concerned that the proposal to share information with regulators will compromise the effective functioning of the CIRB. Our comments in relation to information sharing and the Cyber Coordinator and ASD also apply to the CIRB.

31. What enforcement mechanism(s) should apply for failure to comply with the information gathering powers of the CIRB?

Firms acting reasonably and in good faith may have to consider conflicting regulatory requirements from multiple jurisdictions. Information may have to be prepared in a way that minimises the risks of negatively impacting global security arrangements.

Enforcement mechanisms should be framed with these considerations in mind and ensure the right balance between the need for firms to provide information and to ensure they remain protected. The regulatory pyramid approach should be applied. Any penalties should be proportionate, and not excessive.

32. What design features are required to ensure that a CIRB remains impartial and maintains credibility when conducting reviews of cyber incidents?

Appropriately independent governance and staffing arrangements will be necessary, along with proven regulatory requirements, such as those from transport safety, that are known to work to protect disclosures.

Staff structures and reports should have systems and processes in place to ensure impartiality and reasonableness. The level of technical knowledge must remain high and completely up to date.

While these design features are necessary, ultimately it will be the track record that is established that will ultimately determine credibility.

33. What design features are required to ensure a CIRB can maintain the integrity of and protection over sensitive information?

AFMA would support legislation being put in place to require CIRB to protect sensitive information.

AFMA suggests that there should not be a power granted to the CIRB to override the protections given to sensitive information. To avoid the inherent conflicts in such an arrangement these type of powers should be given to an independent party with a requirement to consult.

Part 2 – Amendments to the SOCI Act Measure 5: Protecting critical infrastructure – Data storage systems and business critical data

34. How are you currently managing risks to your corporate networks and systems holding business critical data?

35. How can the proposed amendments to the SOCI Act address the risk to data storage systems held by critical infrastructure while balancing regulatory burden?

For the financial markets we request that the SOCI Act continue to recognise the existing extensive requirements that already apply to the sector to avoid duplication in this regard.

AFMA seeks further clarity over the potential increase in scope of the APRA powers under the SOCI Act extension. Understanding what those powers are will help firms ensure there is no conflict with other regulators. It should also be clear what powers can only be executed by the Government.

36. What would be the financial and non-financial impacts of the proposed amendments? To what extent would the proposed obligations impact the ability to effectively use data for business purposes?

Measure 6: Improving our national response to the consequences of significant incidents – Consequence management powers

37. How would the proposed directions power assist you in taking action to address the consequences of an incident, such as a major cyber attack on your critical infrastructure asset?

38. What other legislation or policy frameworks (e.g., at a state and territory level) would interact with the proposed consequence management power and should be considered prior to its use?

In finance there are directions powers associated the financial services licencing regime – these ASIC powers were increased in 2020, and the prudential regulatory regime. These enable the same type of directions as those proposed.

39. What principles, safeguards and oversight mechanisms should Government establish to manage the use of a consequence management power?

Measure 7: Simplifying how government and industry shares information in crisis situations – Protected information provisions 40. How can the current information sharing regime under the SOCI Act be improved?

41. How would a move towards a ‘harm-based’ threshold for information disclosure impact your decision-making?

Would this change make it easier or more difficult to determine if information held by your asset should be disclosed?

Measure 8: Enforcing critical infrastructure risk management obligations – Review and remedy powers

42. How would the proposed review and remedy power impact your approach to preventative risk?