PO Box 248
Deakin West
ACT 2600

info@mdrsecurity.com.au

Our ref: MDR-P060-C004
1 March 2024

MDR Security response to consultation paper on Cyber Security Legislative Reforms

Thank you for the opportunity to provide a response to your consultation paper. MDR Security is a specialised consulting company that combines deep technical expertise with understanding of organizational strategy and operations. This has allowed us to provide strategic policy research and advice for many years. Examples of our published work with ASPI includes a 2019 paper[1] on protecting critical infrastructure which suggested legislation was required to mandate cyber security obligations for critical infrastructure providers. We have been pleased to see Australia implement world-leading legislation through amendments to the Security of Critical Infrastructure Act, introducing positive security obligations, mandatory incident reporting, requirements for risk management plans and designation of systems of national significance. We consider these are a good example of legislation to address market failure, and adopting a risk based approach rather than a "tick-box" compliance approach.

More recently, we published a paper[2] with ASPI in August 2023 discussing what was the right approach to cyber security regulations. Regulation can provide a powerful mechanism to modify incentives and change behaviours. However, securing cyberspace depends on the intersection of many factors—technical, social and economic. Therefore approaches to regulation require careful consideration and analysis.

We are pleased to see that the proposed approach in the consultation paper appears agree that compulsion through regulation is only one option, and often the last resort when other methods such as voluntary codes have failed. We also commend the Government for adopting a consultative co-design process for the proposed legislative changes.

Generally, we recommend for each proposed legislative changes the Government should clearly set out:

1. The purpose of the change:
- What aspect of the cybersecurity problem does the regulation seek to address?
- What's the desired impact on cybersecurity from the regulation?
2. The chosen target of the regulation and the specific behaviours of that target that the regulation seeks to modify
3. The reasons for choosing compulsory legislation as the most appropriate mechanism
4. The metric or measure that the regulation seeks to influence, plans to measure the baseline and impact of this metric, and the target outcome on this metric.
5. Identified risks of unintended consequences and/or effects on third parties, and how these will be monitored and mitigated.

We also recommend that whatever the initial form of the legislation, an iterative approach is taken that measures impact and adjusts approaches to enhance effectiveness, incorporate lessons learned and absorb technological advances needs to be planned from the outset. The incorporation into this

[1] https://www.aspi.org.au/index.php/report/protecting-critical-national-infrastructure-era-it-and-ot-convergence
[2] https://www.aspi.org.au/index.php/report/getting-regulation-right-approaches-improving-australias-cybersecurity

consultation of proposed changes to the SOCI Act based on the experiences of the last two years is a good example of this, which should be maintained.

Specific responses to selected consultation questions are provided below. We have only responded to Part 1, as the Part 2 questions appear to be directed at entities already subject to the SOCI Act. However, the above general commentary and recommendations above could also be applicable to this set of proposed reforms.

Part 1 – New cyber security legislation

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

1. Who in the smart device supply chain should be responsible for complying with a proposed mandatory cyber security standard?
When considering a product or service being offered to end users, options for which the regulation applies could include:
- *the source of supply (the manufacturer or developer of the components used to make the product or perform the service)*
- *the third-party integrator (a service provider who integrates the supply chain to provide the offering to the end user)*
- *the end user.*

When making this choice, consideration should be given to which party is best placed to manage the risk, and where behaviour modification will be most effective. In this instance regulation seeks to target intrinsic properties of the device, hence we suggest the source of supply should be the appropriate target.

2. Are the first three principles of the ETSI EN 303 645 standard an appropriate minimum baseline for consumer-grade IoT devices sold in Australia?
Yes, these are an appropriate starting point, and as they are well aligned with other approaches taken buy other countries, this reduces the burden for device manufacturers to ensure their products are compliant.

4. Should a broad definition, subject to exceptions, be used to define the smart devices that are subject to an Australian mandatory standard? Should this be the same as the definition in the PTSI Act in the UK?
Yes, given the rapidly moving nature of this field, overly narrow technical definitions should not be used. Alignment with the PTSI Act, subject to taking into account any lessons learnt from the UK experience, could be a good approach.

6. What is an appropriate timeframe for industry to adjust to new cyber security requirements for smart devices?
12 months should be the target, although there may need to be provisions to make exceptions for specific products with long lead times to make the required changes.

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

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?

There should definitely be requirements to report if a ransomware or extortion payment is made by an entity. However, any requirements to report incidents involving ransom demands should be carefully scoped to avoid undue burden or complexity. In public discourse, the term "cyber incident" is used very loosely, and can refer to anything from "port scanning" by a researcher (or banks claiming to stop 10,000s of attacks per day) through to a successful major compromise of a system. There is also the risk of "hoax" ransom demands that could be caught up by this. The definitions used in the SOCI Act for mandatory incident reporting could be a good starting point for an appropriate definition that could be used here.

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?
To minimise burdens on small businesses, especially at the time of a cyber incident that may be causing significant stress, it is appropriate to exempt smaller businesses from any obligation to report incidents involving ransom demands even if these are not paid..
However, it would be desirable to minimise any exceptions to the obligation to report any ransomware or extortion payments actually made. While we do not support a prohibition on such payments, mandatory reporting will provide valuable information on the impact on the small business sector, who are often neglected in discussions of the cyber security threat. However, the Government should ensure there is a simple, low effort mechanism to file such reports to reduce the reporting overhead on an entity that will already be under stress.

13. To what extent would the no-fault and no-liability principles provide more confidence for entities reporting a ransomware or cyber extortion incident?
These principles are vital to reassuring entities that the Government does not seek to victim-blame, and to maximise the compliance; this will in turn maximise the benefits gained from these reports in terms of better understanding the threat landscape.

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?
There should be a prohibition on reports under these provisions from being shared with any enforcement authorities for any other legislation. However, filing of reports under this provision should not release the entity from any other reporting obligations they may have with respect to cyber incidents. Nor should an entity filing a report under this provision have any shield from any other enforcement action taken by any other organisation without dependence on the filed report.

15. What is an appropriate enforcement mechanism for a ransomware reporting obligation?
Firstly, the Government should do as much as possible to encourage compliance, eg through the no-fault/no-liability principles, simple low-effort reporting mechanisms etc.
The simple fact of public enforcement action against wilfully non-compliant entities (ie effectively naming-and-shaming) may be a more effective deterrent than the specific quantum of financial penalty when enforcement action is required.

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?
There should be a broad definition to cover responding to the particular incident, remediation and management of the impacts of the incident, investigations and enforcement activities against the

perpetrators, and reducing the risk of recurrence at another Australian victim organisation, either by the same perpetrator, or by the same technique or method.

18. What restrictions, if any, should apply to the use or sharing of cyber incident information provided to ASD or the Cyber Coordinator?
Similar to the ransomware reporting obligations, a no-fault/no-liability approach, prohibiting sharing information with enforcement authorities, but without relief of any other regulatory obligations.

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?
Appropriate mechanisms to share anonymised information back into the relevant community (eg Trusted Information Sharing Network) as soon as possible, particularly in the form of actionable threat intelligence – if entities see the collective benefit from each entity that collaborates and shares information, this will be a strong incentive for all to participate.

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

23. What factors would make a cyber incident worth reviewing by a CIRB?
Incidents with an actual or potential systemic impact on Australia should be the priority.

24. Who should be a member of a CIRB? How should these members be appointed?
Members should have cyber technical expertise as well as understanding of the business and strategic environment. Where possible the appointment process should be as open as possible to avoid the "familiar faces" being appointed by default – for example an open expression of interest process as used by the Department of Finance to appoint Gateway reviewers, or a time-limited process (repeated every couple of years) of inviting applications, as recently used to appoint AAT members.

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?
The focus should be on the required expertise; key skills will include cyber technical expertise, risk management, strategic leadership and business operations experience. Expecting each member to be fully "independent" is unrealistic as it would include the vast majority of suitable experts – anyone with the required level of expertise is likely to be in demand and have some affiliations. However, by appointing a suitable pool of potential members, for each investigation a panel can be formed of individuals that are independent of the entities involved in that particular case.

26. How should the Government manage issues of personnel security and conflicts of interest?
Some investigations are likely to require at least some panel members with security clearances. Adopting an approach of a pool of potential members would provide opportunities for some members without clearances to participate in some reviews where feasible – and also a pipeline to increase the number of cleared reviewers if they are eligible and willing to undergo the process. Also, a pool of potential members should mean investigation a panel can be formed of individuals that avoid conflicts of interest.

27. Who should chair a CIRB?
The chair should be chosen for each investigation from a pool of potential panel members who are considered suitable to act as a chair.

Dr Rajiv Shah