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?

Manufacturers of IoT devices should be responsible for the security of hardware related aspects.

Software manufacturers should be responsible for the security of the applications they develop. In the case where apps are sold or made available through app stores, they should hold some responsibility for security vetting of apps that they make available to customers.

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?

The “no default passwords” should be incorporated into the broadened fifth principle of “communicate securely”, which adds additional measures to securing IoT devices and their communications, rather than just preventing default passwords.

3. What alternative standard, if any, should the Government consider?

The government could consider the IoT Security Compliance Framework, or ISM style controls which can be used to achieve security which can consider OWASP ISVS, ENISA Baseline Security Recommendations for IoT.

NISTIR 8259 series should also be considered.

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, a broad definition of smart devices should be used to define devices covered by an Australian mandatory standard to enable the best way to capture the future devices which may not be considered and to protect the end consumer. Exceptions can be made and added based on the future direction of industry.

5. What types of smart devices should not be covered by a mandatory cyber security standard?

Any “smart” device where the device is able to send and receive communications over the internet, and software installed onto the device should be covered by a cyber security standard.

6. What is an appropriate timeframe for industry to adjust to new cyber security requirements for smart devices?

3-5 years should be adequate for new devices. Legacy devices should have software updated within this timeframe and have mitigations for vulnerabilities in any physical device limitations.

7. Does the Regulatory Powers Act provide a suitable framework for monitoring compliance and enforcement of a mandatory cyber security standard for IoT devices?

The Regulatory Powers Act provides a framework for monitoring compliance, however should be enhanced to consider ways to secure and obtain records which may be held on cloud services which are used.

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?

The nature and scope of the incident, details on how it occurred and the nature of affected systems.

The details of what data and number of records suspected of being compromised.

Any ransom demands including details on the contact received from threat actors, and any communications with them.

9. What additional mandatory information should be reported if a payment is made?

Details of the destination account / information on where payment was made to, and the amount paid. Any other information which was related to the payee's account that was received.

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?

The scope of ransomware reporting should consider the following

- Definition of criteria using a risk-based approach using threshold criteria to determine the level of reporting required. Entities handling sensitive data in high risk industries such as critical infrastructure may have more stringent reporting requirements.
- Standardised reporting formats using automated reporting mechanisms to streamline and simplify the reporting process for entities
- Providing education and support so entities are aware of their obligations and of how and what they are required to report incidents.
- Reporting should be around the spread of the incident (even if suspected) and countermeasures taken. The report should also factor the affected entity's confidence in remediation and any residual risk of left over traces of the ransomware suspected.

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?

No, ransomware reporting obligations should also include smaller and medium sized businesses to both give Government a larger and more thorough view of the threat posed by ransomware actors to Australia.

More onerous obligations should be placed on larger organisations based on their risk as well as their ability to meet the obligations.

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?

The appropriate time period for reporting should consider the time and resources required for an entity to investigate and respond to any attack. As well as allowing the entity to focus on their response, this enables the entity to capture and collate and provide as much accurate information as possible.

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

While the no-fault and no-liability principles provide confidence for entities to report ransomware or cyber extortion incidents, the ease of the reporting is also a large factor in entities compliance with reporting cyber incident requirements.

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?

As well as the no fault and no liability principles, encouraging businesses to report any incidents, the Government should implement enforceable regulations which are enforced by a well-resourced regulator. Giving the regulator the ability to impose meaningful deterrent measures such as fines, or other penalties which are used

Enforcement measures such as regulatory oversight using measures such as independent third-party audits and inspections would assist in ensuring accountability of business for their cyber security.

Public disclosure of incidents or enforcing companies to disclose and incidents would assuage public expectations.

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

Public disclosure of non-compliance with reporting measure or incidents involved in

Fines and penalties for non-reporting of incidents.

The enforcement could be assisted by protections for whistleblowers to encourage people to report where companies may be non-compliant with their reporting obligations.

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?

Details of data and systems that were targeted would be useful to show what information and systems threat actors are targeting and enable others to focus their defensive efforts.

The amount of data / records compromised would give others intelligence into size and scale of the attack.

Reporting should be shared with information security industry to provide threat intelligence as well as other members of the industry of the affected company to enable them to better understand and prepare for the threats posed to their specific industry.

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?

"Prescribed cyber security purposes" for limited use obligation on cyber incident information which is shared with ASD and the Cyber Coordinator should include

- Threat detection and intelligence sharing to enhance threat detection capabilities and facilitate the exchange of actionable threat intelligence between government and private sector to identify emerging threats, trends and attack vectors.
- Incident response and mitigation where applicable to enable timely and effective incident response and mitigation efforts by leveraging shared cyber incident information. This can include identifying affected entities and managing consequences of the incident and remediation activities to minimise the impact of incidents.
- Threat intelligence sharing to enhance collaboration between government and private sector as well as academia and international partners to help inform decision making processes.
- Research and development to analyse trends in the cyber threat landscape and enable partners in academia and industry to research and advance technologies, methodologies and best practices to develop greater resilience against similar threats.
- Law enforcement measures to assist with the identification and capture of the perpetrators of the incident.

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

To promote sharing of information with ASD and cyber coordinators, information shared should not be able to be used by law enforcement or regulators to bring new charges against the sharing entity.

Sharing of incident information with law enforcement both domestically and internationally to attempt to identify, track down and ultimately prosecute the threat actors is extremely

important, and information shared should be available to assist in this process. However, the information shared should not be used against the entity who shared it.

The incident data on attack foot print and methodology should be disclosed to the community so that it will act as knowledge. However, the organisation references and the infrastructure details and any internal vulnerabilities should not be disclosed by ACSC / ASD to others.

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?

Government can promote information sharing and collaboration with ASD and the Cyber Coordinator be engaging with the industry and ensuring that any information shared by industry and entities is used as an input to generate resources and advice which are shared with industry to assist them to enhance their cyber security posture and resilience in a timely manner.

Ensuring that the process of sharing information with ASD and Cyber Coordinator is streamlined, easy to use with clear instructions and processes for entities which minimise duplication of effort is important for entities and their people who are already dealing with the stress, uncertainty and internal damage caused by incident.

Using information provided to provide immediate support to the entity where possible to help manage the incident and fallout to take some of the burden and uncertainty from them by using any information provided by then to provide meaningful assistance would also encourage them to share information.

Government can build trust among communities through confidentiality terms for entities and proactively share knowledge in the form of DR test playbooks for such cyber incidents. The community can be encouraged by the government to plan and perform cyber incident response drills to discover opportunities for improvement in cyber incident response strategies.

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 purpose of the CIRB should include the following key points

- Incident analysis and collaboration
- Information sharing ant threat intelligence to facilitate the exchange of threat intelligence by Government and industry
- Policy advocacy and coordination to identify and advocate for government policy or other regulatory changes to address any systemic challenges.
- Advocate best practise and and lessons learned to develop recommendations for improving resilience and cyber security posture within different sectors.

The scope should include key points

- Sector specific incident analysis to enable focused recommendations and guidance to address unique challenges on different industry sectors such as finance, critical infrastructure, healthcare etc.

- Technical expertise should be used to conduct in depth examinations of incidents, including analysing the forensics of the attack to identify attack patterns and learn from vulnerabilities exploited to improve resilience.
- Engagement with a diverse range of stakeholders including cyber security vendors, academic institutes, industry associations to enhance the review process and gather a broader understanding of the incident and any similar threats.
- Collaboration across sectors to enable lessons from one sector to be shared with others. While incident analysis is focussed to best analyse the incident, lessons should be shared with other sectors to prevent similar incidents.

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?

CIRB should have clearly delineated boundaries to their review activities which limits sharing of sensitive or classified information which could compromise operations or national security interests.

Any CIRB reviews and investigations should not interfere with or prejudice any ongoing law enforcement or legal operations, intelligence operations or regulatory enforcement actions.

Any evidence gathered should be preserved or compromised by any CIRB review, and confidentiality of sensitive data including personally identifiable information, propriety data of data subjects should be safeguarded by adhering to relevant privacy laws and regulations.

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

The CIRB should adopt a no-blame approach similar to ATSB and focus on producing outputs and recommendations which are designed to improve cyber security resilience in the affected industry sector, enable learnings to be shared and strengthen regulatory frameworks and laws.

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

The following factors should be considered when determining whether a cyber incident is worth reviewing

- The nature of the industry the victim operates in, including. Factors such as whether critical infrastructure or services could be affected.
- The amount of data or victims affected. For example, how many PII records were potentially compromised.
- The nature of the attack. For example, the analysis performed by the victim indicates that a new type of attack was carried out

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

Members of the CIRB should come from a cross section of industry sectors, academia and Government to give a broad range of expertise to the CIRB's activities. Each member should bring unique expertise, be that technical or industry sector knowledge which can be used to add value to a CIRB investigation.

Members of a CIRB should be drawn from a pool of members so that consistency across different CIRB reviews is achieved while also allowing different members to be appointed based on their unique knowledge which is more relevant to the nature of a specific incident.

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 of the CIRB should bring a proven experience and expertise in a field or industry which adds value to the board and any investigation in which they participate. This should be demonstratable by proven industry experience and / or qualifications.

Domains of expertise represented should include:

- Industry specific knowledge related to the industry the entity operates in, including relevant legal and regulatory compliance relevant to it. This should include any factors related to critical infrastructure or system protection.
- Cyber security legal and regulatory requirements, privacy and data protection.
- Technical aspects of cyber security, including incident response and crisis management, threat intelligence and analysis.
- Technical experts with a thorough technical knowledge of cyber security domains including network security, endpoint protection among others should be included or available to analyse aspects of the incident and response.

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

To cater for incidents which may occur to entities which handle classified information, some members of the CIRB should have security clearance, or be able to obtain clearance. Enough members should have appropriate clearance to enable the board performing the review to investigate and understand the aspects of the incident affecting the classified information.

27. Who should chair a CIRB?

To guarantee independence and promote engagement and relevance of the review process, a CIRB should be chaired by someone independent, and not a Government representative.

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

Reviews undertaken by a CIRB should be able to be initiated by any of the following, depending on the nature of the incident:

- Minister for Cyber Security
- National Cyber Security Co-ordinator
- The CIRB
- Agreement between Minister for Cyber Security and other ministers relevant to the nature of the review

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

Powers the CIRB will need to effectively perform their function will include

- Authority to access and share sensitive information with authorised stakeholders, potentially including government agencies and industry partners
- Access to classified information related to cyber security threats and incidents
- Authority to enforce compliance with reporting and information sharing requirements.
- Forensic investigation powers to allow CIRB experts to conduct forensic investigations and analysis of cyber incidents to track malicious actors and their activities within the system.
- Powers to make recommendations and provide advisory guidance to government agencies and regulatory bodies to strengthen the cyber resilience and capabilities.

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 would need some limited use obligation to entice them to participate, however should regulations be introduced to compel participation in CIRB reviews, then the limited use obligation could be relaxed.

Limited Use obligation would still be required to protect any protect any data subjects the data of the

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

Failure to comply with information gathering powers or failure to co-operate with a CIRB investigation should depend on the nature of the entity affected. These should include but not be limited to fines or other restriction of ability of an entity to perform its business if assurances cannot be made that security measures or incident response are not adequate.

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

To remain impartial, a CIRB would need to be independent and operate free from conflicts of interest and undue bias or interference.

Credibility comes from having experienced, diverse representation from relevant stakeholders to ensure a balanced perspective. The CIRB should operate a transparent process with transparent criteria for composition of members of a review, including expertise required, qualifications and potential conflicts of interest.

Reviews should ensure strict confidentiality is maintained throughout the entire review process. Standardised review procedures to ensure consistency and fairness in the evaluation of incidents which follow the best practise guidelines for incident review and analysis.

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

Non-disclosure agreements, and strict confidentiality obligations should be adhered to by CIRB members to ensure that sensitive information is protected.

CIRB should be subject to external oversight mechanisms, including independent audits, reviews and oversight by Government to hold it accountable to ensure compliance with statutory requirements.

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?

Information is classified based on the CIA (confidentiality, integrity and availability) and relevant interested party requirements of the data, and systems used to store or transmit this data are identified and segregated where required.

Systems holding business critical data are secured using enhanced security controls including requiring authorisation to access systems and MFA to authenticate access to them, following the least privilege access principles. This helps mitigate risks of unauthorised access to the data.

All software systems accessing business critical and private data are identified and assessments carried out to ensure appropriate security measures are in place. This includes assessing third party providers and their products against data security measures before using them to handle protected data. Assurances can include auditing their products and systems to provide assurance that they are adhering to data security processes and procedures, or by requiring certification to data security standards such as ISO 27001 or other similar data security standards.

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?

Proposed amendments to the SOCI Act can address data security risks for critical infrastructure by implementing an information security management system (ISMS) which covers data security across the supply chain. Independent certification to a data security standard potentially incorporating specific controls similar the Department of Employment and Workplace Relations Right Fit For Risk (RFFR) program can limit the regulatory burden on a company and increase the assurance that data security risks are being mitigated.

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?

It is entirely reasonable to impose more rigorous protection of sensitive data related to critical infrastructure. Entities operating in this market should have conducted a risk analysis and put in place appropriate controls to mitigate risks. Companies should also be responsible for communicating and ensuring appropriate protections are in place throughout their supply chains.

Properly managed there should be no impact on a business to use data for business purposes. Information and assets used in the storage and handling of it should be appropriately categorised and labelled. Appropriate access controls should be in place to manage access to the information and systems which hold or transfer it.

Independent third-party assessments or audits can be used to ensure that the obligations are being met.

Companies unwilling or unable to meet the appropriate steps, as outlined in the amendments to the SOCI Act should not be involved in the operation of critical infrastructure.

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?

As we do not control any critical infrastructure asset, this can only be answered hypothetically. The proposed directions powers would promote planning for consequences to the loss of critical data that was managed by our company and of additional stakeholders relevant to data subjects which exist as a result of handling and storing this data.

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?

Any state privacy or freedom of information acts should be considered, including

- *Privacy and Personal Information Protection Act 1998* (NSW) and *Health Records and Information Privacy Act 2002* (NSW)
- Information Act 2002 (NT)
- Information Privacy Act 2009 (Qld)
- Personal Information and Protection Act 2004 (Tas),
- Privacy and Data Act 2014 (Vic),
- Freedom of Information Act 1992 (WA)

Others related to state critical infrastructure will also need to be considered.

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

Principles:

- Collaboration and cooperation between government agencies, industry partners and stakeholders to identify and manage and to address any consequences quickly and collectively.
- Transparency in the use of the consequence management power, including clear guideline, criteria and process to handle any consequences.

Safeguards:

- Legal safeguards which define the scope of authority, permissible actions and procedural safeguards to protect rights of affected parties.
- Data protection and privacy should be safeguarded, to minimise the collection and retention of personal data to the extent necessary for achieving regulatory obligations, but also considering the prevention of further harm to affected parties.

Oversight Mechanisms

- Independent oversight should be established to monitor the implementation of these powers who have the authority to investigate complaint, conduct reviews and review any enforcement actions taken under the consequence management powers.
- Transparency and accountability of those responsible for managing the consequence management actions by reporting on incidents and actions taken.

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?

The current information sharing regime can be improved by simplifying the provisions to allow for a more timely response during and in the immediate aftermath of an incident. Cyber incidents are often time sensitive, which can quickly become larger and affect more victims and systems if they are not addressed quickly.

In time-critical, high risk incidents, having clear, simple guidelines is vital to minimising the incident.

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?

A harm-based approach to disclosing information provides would provide an approach more like the risk-based approach to data categorisation and handling widely adopted. This simplifies and consolidates the approach to data handling, in this case disclosure, which generates more consistent outcomes. This simplified approach makes it easier to determine the best course of action to determine whether or not to disclose information which is held.

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?

The proposed review and remedy powers would feed extra risks into the risk assessment process, which would then be assessed, with any additional controls or maturity levels potentially implemented to increase the security posture and resilience of the protection of the relevant data.

Measure 9: Consolidating telecommunication security requirements – Telecommunications sector security under the SOCI Act

43. What security standards are most relevant for the development of an RMP?

ISO-27000 family of standards, particularly ISO 27001 and ISO 27002 which define requirements and procedures for a management system for information security using a risk-based approach. Specific standards build on these to cover issues such as ISO 27018 covers cloud computing, ISO 27017 covers protection of personally identifiable information.

Other ISO standards including ISO 31000 — Risk management, ISO 29147 – Security techniques - vulnerability disclosure and related ISO 30111 - Information technology - Security techniques - Vulnerability handling processes are also relevant.

NIST Risk Management Framework (RMF) which provides a risk-based framework for handling cyber security. Control lists to mitigate risks include:

- NIST SP 800-53 which provides a comprehensive list of controls which may be implemented based on the risk assessment.
- NIST SP 800-171 for more generalised and less detailed control set which can be used by contractors within the supply chain who may be smaller

44. How do other state, territory or Commonwealth requirements interact with the development of an RMP?

This is achievable through set up of a special interest group with shared vision and responsibility on the outcome.

45. What are the main barriers to engaging with government through the notification process as it is currently enforced? How can the obligation to notify be clarified?

The current barriers are a cumbersome contact response mechanism with adequate and qualified staffing who can also provide an initial expert advice or suggestion on indent management.

46. How do your procurement and network change management processes align with the existing and proposed notification arrangements? Can you suggest improvements to accommodate industry practice?

This question is not applicable to our business so we do not feel offer an informed response.

47. How can outlining material risks help you adopt a more uniform approach to the notification obligation?

The risk management process could become more objective and metric driven activity that will drive the notification related obligations to any corporation.