NCC Group's response to the consultation on proposed new cyber security legislation and on changes to the Security of Critical Infrastructure Act 2018

March 2024

Introduction

NCC Group welcomes the opportunity to respond to the Department of Home Affairs' consultation and offer our expertise as a global cyber security business.

Through our threat intelligence, incident response and research functions, we are acutely aware of the changing cyber threat landscape, witnessing first-hand the real-world impact cyberattacks have on their victims, communities and ecosystems. **We are therefore pleased that the Government is focused on further strengthening national cyber defences, both through the proposed legislative reforms and the wider delivery of its Cyber Security Strategy.** At a high-level, we support the aims of the changes being consulted on through this consultation, but offer the following observations and recommendations as the Government proceeds with its plans:

- In alignment with global developments such as the EU's Cyber Resilience Act, the Government **should be ambitious in its plans to set security standards for IoT devices**, **covering all hardware sold into Australia** (including enterprise devices), **pursuing all ETSI 303 645 requirements** proportionately, on a phased basis, and **ensuring that manufacturers and developers' compliance is technically validated** by an independent third party where the risk profile necessitates.

- **The proposed mandatory reporting requirement for ransomware attacks should be aligned to existing legislative frameworks** (e.g. SOCI and the Privacy Act), and apply only to **businesses with an annual turnover of more than $10 million per year**. For small to medium sized businesses, the Government should explore what incentives it could provide to encourage reporting, such as in exchange for access to the Government's proposed Small Business Cyber Security Resilience Service.

- **The mandatory reporting requirement, limited use obligation for the Australian Signals Directorate (ASD) and Cyber Coordinator, and the new Cyber Incident Review Board (CIRB) will require clear legal delineations** – backed by a public communications campaign – in order to build trust that the associated powers will not be misused.

- **The Australian Cyber Security Centre (ACSC) and regulators require investment** to ensure they have the capabilities, expertise and skills to effectively enforce the legislative proposals.

We are keen to continue supporting the development and implementation of the Government's plans by sharing our expertise and insights from operating at the 'front line' of cyber security. Below we explore our recommendations in more detail, responding directly to the consultation's questions.

About NCC Group

NCC Group's purpose is to create a more secure digital future**.** As experts in cyber security and risk management, our c.2,200 people worldwide are trusted by our customers to help protect their operations from cyber threats. Each year we dedicate thousands of days of internal research and development enabling us to stay at the forefront of cyber security and ensuring we secure the rapidly evolving and complex technological environment. As a global business operating in 12 countries, we were delighted to open our regional headquarters in Sydney in 2023 amid a rapidly growing footprint across Australia, with around 90 colleagues now based here.

Response to questions

Nb. We have grouped answers to some questions together.

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?

All of the actors the Government has identified should play a part. Indeed, we are pleased to see the Government considering establishing responsibility for complying with the standard throughout the supply chain, including not only manufacturers, but also vendors, software developers and sub-contractors. In doing so, it will be important to clearly establish the roles of the various actors that play a part in the supply chain. Connected technology often comprises many component parts with multiple manufacturers, developers, and vendors. This can blur the lines of responsibility, and often means that no one party takes ownership of the security/risk of a device. It is therefore important that any legal framework provides clarity.

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?

Principally, we support the alignment of the new regime with ETSI 303 645, given that other governments globally have used this standard as a baseline.

That said, we are concerned that simply implementing the first three principles will not provide sufficient levels of cyber security and will quickly become outdated as other regions globally pursue more ambitious approaches such as the EU through its Cyber Resilience Act. While it may be appropriate to implement the three principles in the first instance, we strongly urge the Australian Government to provide a roadmap to full compliance with ETSI 303 645 over time. This could include longer transition periods for the more stringent requirements.

For higher-risk products, manufacturers' and developers' compliance should be technically validated by independent third parties to ensure the requirements have been implemented correctly. This is in line with best practice across other sectors (e.g. smart metering), and will help to ensure a level playing field between those who are taking their security responsibilities seriously and those who may not be.

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

As noted above, we support the alignment of the new regime with ETSI 303 645, given that other governments globally have used this standard as a baseline.

The Government should also establish Memorandums of Understanding with other like for like schemes in core global markets, to ensure mutual recognition of standards and testing.

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

The proposed definition for consumer devices is fine. However, while we understand the focus on consumer devices, given their risk profile, we would urge the Government to extend any standard to all connected devices, including those used in enterprise settings. The UK's PSTI Act was a very

welcome step in the right direction, but its limited scope has meant that enterprise devices (e.g. office booking systems, office phones etc.) continue to go unregulated.

In addition, the separation of standards and Codes of Practices for consumer devices, software and apps and app stores in the UK has created a complex (and often overlapping) landscape for businesses to navigate. Instead, we favour the more holistic and risk-based approach taken by the EU with the Cyber Resilience Act, which covers all hardware and software sold into the region. We'd urge the Australian Government to consider adopting a similarly comprehensive and consistent approach.

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

We agree with the Government that 12 months for compliance with the first three principles of ETSI 303 645 is an appropriate amount of time. However, as outlined under question 2 above, the Government should aim to introduce the remaining principles of ETSI 303 645 over time. This could be implemented on a phased basis.

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

Yes. In addition to powers, the appointed regulator will also require the necessary investment to ensure it has skills, capabilities and resources to effectively enforce the regime.

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

8. **Which entities should be subject to the mandatory ransomware reporting obligation?**
9. **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?**

We agree with the Government that the scope of the reporting obligation should be limited to mid-sized and above businesses (those with an annual turnover of $10 million). Placing the obligation, as outlined in the consultation, on smaller businesses could be disproportionate and create unfair and unmanageable administrative burdens. Instead, we would recommend that the Government explore whether there was a less burdensome obligation that could be placed on smaller businesses, or what incentives it could provide. This could include encouraging reporting in exchange for access to the Government's proposed Small Business Cyber Security Resilience Service.

10. **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 notification timelines should be aligned to Australia's existing cyber reporting regulatory regimes such as SOCI. Creating differing reporting timelines is likely to create confusion and additional administrative burdens for regulated entities.

11. **To what extent would the no-fault and no-liability principles provide more confidence for entities reporting a ransomware or cyber extortion incident to Government?**
12. **How can the Government ensure that the no-fault and no-liability principles balance public expectations that businesses should take accountability for their cyber security?**

Getting the balance right between ensuring reporting is genuinely no-fault and no-liability while meeting public expectations will be difficult. Principally, the obligation must be designed in a way that does not force entities to 'go underground' should they be in fear of legal repercussions. Existing regulatory frameworks such as SOCI and the Privacy Act are intended to ensure that critical entities and businesses handling personal data are accountable to Government (and ultimately the public) for

their cyber and data security. Conflating this reporting obligation with these frameworks could risk undermining its main purpose of encouraging greater information sharing. We therefore would recommend that the Government focus on creating a genuinely no-fault, no-liability reporting obligation, distinct from existing regulatory frameworks, with legal clarity on how reporting information should and should not be used.

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

The proposed civil penalty provision seems appropriate, but must be implemented proportionately.

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

NCC Group's Threat Intelligence practice would welcome monthly round ups from ACSC, summarising key trends across sectors, covering variants, ransomware demands and attack vectors. This will support our work with clients to enhance their resilience against emerging malicious actors and cyber attacks. These reports should be anonymised as much as possible, so as to build trust in the reporting obligation.

The Government must also ensure that they invest in ACSC so that it is equipped with sufficient resources, capabilities and skills to manage and analyse the reports. This may need to include drawing in additional external expertise to plug the skills gap.

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

15. 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?

Broadly speaking, we support the proposals and agree with the prescribed cyber security purposes.

16. What restrictions, if any, should apply to the sharing of cyber incident information?
17. 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?

A clear public communications campaign detailing how cyber incident information is (and is not) being used will be critical to building trust.

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

18. What should be the purpose and scope of the proposed CIRB?

While we understand the drive for an independent CIRB to review cyber incidents, we would caution that such a body could draw resources and expertise from the ACSC. We think that it would be better for the ACSC to continue to be promoted as the independent source of knowledge and voice of expertise for learning lessons after cyber incidents.

That said, should the Government move forward with forming the CIRB, it must be clear how the Board would interact with the mandatory ransomware reporting obligation. Any sense (however untrue) that reporting an incident could lead to a very public investigation is likely to disincentivise information sharing.

The Government should also ensure that the CIRB does not score or rank attacks, as this could "gamify" attacks for attackers seeking ever higher scores and rankings.

19. **What limitations should be imposed on the CIRB to ensure that it does not interfere with law enforcement, national security, intelligence and regulatory activities?**
20. **How should the CIRB ensure that it adopts a 'no-fault' approach when reviewing cyber incidents?**

The Government must carefully consider and define how such a Board would interact with, and be separate from, civil court proceedings, law enforcement investigations and regulatory activities. These legal delineations should be consulted on with industry to ensure trust in the CIRB as a truly independent body is built.

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

The proposed factors are sensible and would provide a proportionate threshold.

22. **Who should be a member of a CIRB? How should these members be appointed?**
23. **What level of proven independent expertise should CIRB members bring to reviews? What domains of expertise would need to be represented on the board?**
24. **How should the Government manage issues of personnel security and conflicts of interest?**
25. **Who should chair a CIRB?**

We agree that a CIRB should include representation from across the Australian cyber ecosystem, including industry and academia. That said, as the Government rightly identifies, conflicts of interest need to be carefully managed (e.g. if a CIRB member works for, or is affiliated to, an organisation that has been subject to a significant cyber attack and might be under investigation).

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

We believe that the CIRB should be subject to a limited use obligation to encourage organisations subject to a Review to share information.

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

In addition to ensuring a balanced membership from across the cyber ecosystem, there should also be procedures put in place for managing any conflicts of interest that arise.

Measure 5: Protecting critical infrastructure – Data storage systems and 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?

We broadly support the proposed amendments and overarching aim to ensure critical infrastructure entities are protecting all relevant data storage systems.

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

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

We would caution that any power to allow the sharing of protected information must be balanced against other national security and data privacy considerations. Safeguards should include limiting the sharing of protected information with those organisations who have proven strong data handling practices.

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?

We broadly support the proposed provisions.

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?

We broadly support the introduction of the review and remedy power. Clarity on the remediation process, including standardised timings will be needed. Given regulators' and the ACSC's limited resources, the Government may need to work with trusted industry partners to support remediation.

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?

We broadly support the proposals to align telecoms providers to the same standards as other SOCI-regulated entities. In doing so, providers must be held to equivalent or greater standards than they currently are. Indeed, we would caution against any steps which could weaken requirements.

When considering an RMP for the sector, we recommend the Government look to best practice standards globally, including the implementation of the Telecoms Security Framework in the UK. In our experience, the UK Regulations, and underpinning Code of Practice, have greatly improved telecoms operators' awareness of their security environments, what they need to address as security best practice in telecoms and this is already driving up resilience, despite only being in the early stages of implementation.