THE UNIVERSITY OF QUEENSLAND
AUSTRALIA

CREATE CHANGE

The University of Queensland's submission to the 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms consultation paper

This submission to the 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation Paper compiles feedback from academic and professional staff from the University of Queensland, and includes UQ Cyber, AusCERT, UQ School of Mathematics and Physics, T.C. Beirne School of Law, and UQ Information Technology Services division (ITS).

This document focuses on specific questions relating to Measures 1, 2, and 4 in the Consultation Paper.

A summary of our recommendations is provided below. Our detailed responses to the three measures are provided in the remainder of the document. Where applicable, our responses relate to specific questions or, in some circumstances, our responses address entire measures.

Recommendation 1: We recommend all entities involved in developing, selling and related miscellaneous processes relating to parts and components should be included in the scope of a standard to ensure that the end-user device or parts are secure-by-design.

Recommendation 2: We consider that only “No Default Password” from ETSI EN 303 645 is suitable from a regulatory perspective.

Recommendation 3: We recommend that a statement about the purpose of information collection is shared, who is collecting the information and used in determining the scope of information collection relating to ransomware reporting.

Recommendation 4: We recommend that there should be two report types: (1) A simple report to be completed within 72 hours indicating that an attack has happened, and (2) A longer report with additional information provided within 60 days of the attack.

Recommendation 5: We suggest a number of categories of information that could be required (see below section).

Recommendation 6: We recommend that, with any reports, there should be a reasonable test that the information is as reasonable as the circumstances allow the organisation.

Recommendation 7: We recommend a step-by-step approach with the end-result of all organisations included in scope.

Recommendation 8: We suggest the threshold of scope of >$10 million should be lower.

Recommendation 9: We recommend a no-fault and no-liability approach where reported information is not treated as an admission of liability while not absolving entities of legal liability.

Recommendation 10: We suggest that the proposed legislation could introduce statutory damages and presumptions in favour of members of the public whose information was accessed by the criminal.

Recommendation 11: We recommend all information provided should be anonymised but published promptly online.

Recommendation 12: We suggest that the CIRB should be forward-looking, consolidating lessons from cyber-incidents in a safe way.

Recommendation 13: We suggest that the CIRB should maintain operational independence between from law enforcement/national security agencies.

Recommendation 14: We suggest a number of factors may be used to determine if an incident is relevant (see below section).

Recommendation 15: We suggest that the selection process should prioritise diversity, considering a broad range of perspectives, backgrounds, and expertise enabling a well-rounded analysis of cyber incidents. r.

Recommendation 16: We suggest that independent advisers, such as representatives from other countries who are collaborating or coordinating cybersecurity efforts with Australia, should be included.

Recommendation 17: We recommend that the CIRB should be provided with the power of access to information and subpoena power.

Recommendation 18: We recommend that CIRB should not use information collected for purposes beyond those for which it was intended, except if the information reveals an immediate threat to public safety or national security.

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?

- An effective secure-by-design approach should involve the whole supply chain from component suppliers, application developers, vendors to the market, organisations as a responsibility entity, and government and regulatory bodies.
- All these entities, within a supply chain, are pivotal in the design process. There is not a single part that should be overlooked, from the supply of the components that make up the smart device to the application developers that make the software that brings functionality to the smart device. Also, there are other parts of the supply chain that need to be considered, such as the device source, or the place of acquisition of the device.
- For example, vendors, alternative suppliers and organisations buying smart devices in large quantities should bear responsibility. Vendors directly interacting with users should ensure that they only source devices and similar options that satisfy the same base standard. Alternative suppliers of similar smart devices should also either comply or be prevented from selling these devices to users. Organisations that purchase quantities of the smart devices for distribution to staff/clients should also bear responsibility to ensure they source compliant smart devices.
- **Recommendation 1:** All entities involved in developing, selling and related miscellaneous processes relating to parts and components should be included in the scope of a standard to ensure that the end-user device or parts are secure-by-design. We recommend considering these entities when defining the scope of the proposed mandatory cyber security standard.

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?

- **Recommendation 2:** In view of the secure-by-design approach and the scope of the Consultation Paper limited to the first three principles of ETSI EN 303 645, we consider that only “No Default Password” is suitable from a regulatory perspective. We recommend that this principle should be applied.
- The other principles (“Vulnerability Disclosure Policy” and “Keep the Software Updated”) are relevant but difficult to regulate as they relate to the usage of the device. It is difficult to then ensure that these principles are implemented during the design phase of the device.
- However, we do recognise that it is desirable to enable automatic software updates by design where feasible, as users typically fail to perform software updates on IoT devices. These usage controls will also be monitored and acted upon by the market as smart devices come to be available and consumers give preference to devices that are kept up to date.
- If, additional principles from ETSI EN 303 645 are to be considered, we support “Validate Input Data” and “Securely Store Sensitive Security Parameters”. The former principle addresses the occurrence of buffer overflows, SQL injection vulnerabilities and other vectors that can be limited by correct validation of inputs. The latter principle will provide a layer of protection over security parameters stored on the device.

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

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?

- Any definitions, alternative standards or approaches to mandatory requirements adopted should align with international efforts. Adoption should be a rapid process to impose pressure on manufacturers and vendors to source conforming devices.
- However, government and regulatory bodies need to ensure that the minimum level for smart devices balances the competing needs of security and creative freedom. A standard needs to embed a degree of freedom in the manufacturing, component sourcing, retailing, installation and use of the smart device to enable the maximum amount of competitive advantage when using the smart device. Simply put, additional cyber security controls increase costs creating a barrier for those sourcing and using smart devices. This may lessen the positive impact of the capabilities of the new smart device.

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

8. What mandatory information 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?

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?

- We support a ransomware reporting scheme, however, further clarification is needed about the purpose of information collection, who will be collecting the information and how will the information be stored/anonymised. Specifically, we consider that the mandatory information collected should be scoped to align with the purpose of information collection.
- For instance, if information is for governmental or research purposes, the scope of information to be collected may be wider. If the information is for whether ransoms are being paid may mean that the information collection could be narrower in scope.
- In addition, whether the information is anonymised prior to being stored is important to understand as this may affect how much entities disclose about a cyber incident.
- **Recommendation 3:** We recommend that a statement about the purpose of information collection is shared, who is collecting the information and used in determining the scope of information collection.
- The information collection process should not be onerous nor divert resources from incident response.
- **Recommendation 4:** We recommend that there should be two report types:
    - A simple report to be completed within 72 hours indicating that an attack has happened, and
    - A longer report with additional information provided within 60 days of the attack.
- This recommendation is based on our belief that it is more important for entities to focus on dealing with the issue than reporting to the government. The reports are mostly not time critical, and it is unlikely that there will be a need for the government to act immediately on what is reported.

Accordingly, the selected time requirements for the two reports are an appropriate period to lodge such reports.

- This latter report can be important in sharing insights into lessons learned and any identified preventative measures that may have helped with the incident. These insights can be invaluable for the entity and other entities in preventing future incidents.
- For the first report, the use of a simple survey-questions style report is suggested. The scope of the information reported may also need to be proportional to the size of the business.
- **Recommendation 5:** The type of information that could be required for either report include:
    - Involvement of third-parties;
    - Affected systems/individuals;
    - Types of data accessed or encrypted including whether any sensitive or personal information was involved etc.,
    - Networks affected;
    - How the incident has affected the entity's operations, services or business continuity;
    - The communications with the perpetrators
    - The entity of the request; and,
    - All information deemed relevant to help with investigations, response, and recovery.
- Specifically, the second report could also include, for entities that pay a ransom:
    - the amount of payment,
    - the date of payments,
    - the method by which payment was made,
    - to whom the payment was made,
    - whether the payee negotiated the payment amount and if the savings made from negotiation,
    - whether the payment was funded by an insurance policy, and
    - whether the payee had professional legal or technical advice in relation to the cyber incident and payment.
- If an entity decides not to pay a ransom, the entity should report this in the second report as well as the amount of the demand and who made the demand.
- **Recommendation 6:** With any reports, there should be a reasonable test that the information is as reasonable as the circumstances allow the organisation. This means that information may be discovered contradicting previous information reported.
- We also suggest that a central reporting platform may be useful, such as extending the existing Australian Cyber Security Centre (ACSC) page[1]. To support the two report types, a reporting organisation can report an incident within the 72 hours and mark the incident as ongoing and save the incident. By marking it as ongoing, the organisation can continue adding information to it for their second report even though ACSC would be notified of the incident. After completing the second report, the organisation can then mark the incident as complete. Regulators could acknowledge the occurrence of timely reporting with leniency relating to penalties and fines if necessary.

[1] https://www.cyber.gov.au/report-and-recover/report

10. Which entities should be subject to the mandatory ransomware reporting obligations?

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?

- Determining the appropriate scope for a ransomware reporting obligation is a challenging task and requires a concerted approach by all relevant stakeholders. It is suggested the government singles out this particular matter, consults with relevant entities (e.g., other government organisations, corporations, small and medium-sized businesses, academia) at regular intervals, and establishes the scope.
- **Recommendation 7:** Given the criticality of this subject, we recommend a step-by-step approach. As a starting point, to strike a balance between effectiveness of the measures and feasibility of the same, it is suggested to utilise current scoping offered by the SOCI Act, e.g., 11 critical infrastructure categories. A second stage could see the scoping expand to include organisations from all sectors, with an annual turnover > $ 3 million, similar to the Privacy Act. A final stage could include all organisations aligning with **Recommendation 8** (see below).
- This staged approach would require the ransomware reporting obligations to be accessible to all businesses, which may be met by applying our earlier recommendations.
- Ensuring the process is accessible is essential in providing Government with greater granularity in terms of, for example, whether small businesses are targeted more often or disproportionately compared to larger organisations. This may include having the scope of the first report from **Recommendation 4** be proportional to the size of the business, based on the number of employees and contractors (not revenue).
- Further, we believe ransomware reporting to be an effective way to raise awareness on the issue and to be a potentially significant measure to uplift the capabilities of less than large businesses. As a consequence, we believe the threshold of $10 million per year to be too high to produce significant outcomes. **Recommendation 8:** We suggest the threshold should be lower.
- Many ransomware incidents are aimed at small and medium-sized businesses (SMEs), and accordingly, to the extent that reporting is useful for society, it should include SME incidents, which are the vast majority of incidents.
- Excluding SMEs from the reporting obligation may be detrimental to research and incident response efforts. For instance, responses to the WannaCry attack benefited from cyber attack information sharing[2]. Further, pattern identification across cyber incidents may be harmed by excluding businesses from the reporting obligation, i.e. it may be difficult to answer whether many businesses had been attacked in a similar way recently.
- In the recent Privacy Act review, there was strong support for removing the small business exemptions to the application of the Privacy Act. It would seem inconsistent to have a small business exemption to the reporting obligations here. We do recognise that smaller business should not be required to report to the same level of detail as a large business. However, it is important to collect information such as the cause of the breach so that lessons can be learnt as to the cause of the breach so that breaches in the future can be minimized.

[2] https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf

13. 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?

- Entities that have broken the law or breached legal obligations should be responsible for losses caused as a result. Nothing in the proposed legislation should absolve such entities of legal liability.
- It is appropriate to have a presumption that the fact of reporting and the contents of the report is not an admission of liability. But it should not absolve the entity of liability that they would otherwise be subject to. This is essential to ensure that these principles do not inadvertently encourage lax security practices or remove all incentives for entities to maintain robust cyber security measures.
- Information that is reported by an entity should be able to be accessed by victims or litigants, from the reporting entity, in response to usual legal process, such as discovery and a subpoena. If the reports are shielded from disclosure, then entities may be able to game the system and place all information in the reports (and nowhere else) thus shielding this information from disclosure via the usual legal process.
- Having said this, we maintain that the main goal of ransomware reporting obligations is not to enforce the law, but to increase the visibility of this matter, in order to help organisations 'up' their game in cybersecurity. Based on this, for cases in which legal liability is not at stake, we recommend solid no-fault no-liability principles for organisations that have demonstrated willingness to collaborate with government, for the common goal of improved awareness. At the same time, secrecy of reporting details will be of utmost importance, to prevent the creation of a 'public ranking' of mostly affected organisations, which would simply give more power to cyber-criminals.
- A corollary to this no-faults and no-liability approach is the safe harbour provisions in tax where any false and misleading statements may not lead to liability if the client provides all the relevant information and does not act with deliberate malice.
- There should a reasonable test that the information is as reasonable as the circumstances allow the organisation. This means that information may be discovered contradicting previous information. The no-faults and no-liability approach should not be limited in scope even if additional information is discovered after the time period for reporting has ended.
- **Recommendation 9:** A no-fault and no-liability approach where reported information is not treated as an admission of liability while not absolving entities of legal liability.

14. 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?

- **Recommendation 10:** The proposed legislation could introduce statutory damages and presumptions in favour of members of the public whose information was accessed by the criminal. This is similar to the California Consumer Privacy Act, which allows individuals affected by a data breach to be entitled to statutory damages, without proof of loss, unless proven that the entity has made improvements to their systems to prevent future violations[3].
- We suggest that a similar approach is implemented where an entity can report the incident with individuals affected automatically being entitled to a defined statutory damage. As the information reported under this reporting obligation cannot be used to admit liability, this scheme

[3]https://www.foxrothschild.com/california-consumer-privacy-act/ccpa-class-action-defense#:~:text=Under%20CCPA%2C%20companies%20that%20handle,actual%20damages%2C%20whichever%20are%20greater.

may reduce the likelihood of subsequent legal actions by victims as the victims would already have been compensated under this scheme. Liability imposed from non-compliance with legislation or contractual agreements is and should be unavoidable.

- The scheme reduces the incentive to not disclose incidents caused by fears of further legal action.
- To recognise the differing value of information, additional tiers of payments may need to be introduced. In addition, a fixed statutory damage may be inappropriate considering different organisational sizes and may discourage SMEs reporting incidents. Instead, a statutory damage schedule proportionate to resources may be appropriate. This may include applying the General Data Protection Regulation approach where the statutory damage total is capped at the higher of a dollar value or percentage of turnover.

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

- It is fundamental to strike the right balance between enforcement and support to encourage organizations to report incidents promptly. **Recommendation 12:** We recommend that an appropriate reporting mechanism requires a balance of the following components:
    - Regulations:
        - 1) Oversight by ad hoc agencies responsible for enforcing ransomware reporting obligations. These agencies can audit organizations and impose sanctions for non-compliance.
        - 2) Structured audit: conduct regular audits of organizations to ensure they are reporting incidents appropriately.
    - Fines: Penalties should be created that affect organisations who fail to report ransomware incidents. The severity of the fines should be proportionate to the scale and impact of the incident. Legal repercussions should be clarified in case of liability.
    - Insurance: Insurance premiums should be proportionate to organisations' track-record in appropriately reporting ransomware incidents with the authorities. Legal Consequences: Establish legal consequences for non-compliance, including potential criminal charges for intentional or repeated failures to report.
    - Training: conduct regular training programs for organisations willing to better understand 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, with whom and in what format?

- **Recommendation 11:** All information provided in relation to Question 8 and 9 should be anonymised but published promptly online. Anonymising information is important and should include removing any information that may identify the victim. In addition, information that may be used by bad actors should not be published.
- We suggest that for technical aspects of the information, e.g. attack vectors, information could be shared with the industry using an industry accepted format, such as MITRE's ATT&CK framework[4]. This may allow incident information to be overlayed to provide a heat map of which tools and

[4] https://attack.mitre.org

techniques are relevant. This is similar to what Thailand's Electronic Transaction Data Agency has implemented[5].

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)?

- **Recommendation 12:** The CIRB should aim at raising visibility around cyber-incidents and spreading best practices in prevention, mitigation, response, and recovery. The CIRB should consolidate lessons from cyber-incidents in a safe way (e.g., not for liability purposes towards the affected organisations) and have in place the appropriate mechanisms to ensure confidentiality (e.g., anonymity). Learnings from cyber-incidents should be disseminated widely, and explored in ad hoc workshops and events, for the betterment of baseline cybersecurity.
- This may include:
    - recommending adoption of new technologies (in a vendor agnostic manner), security standards, and best practices to mitigate future cyber risks.
    - analysing international cyber incidents that may have implications for national security or could affect domestic entities.
    - evaluating the effectiveness of incident response and recovery efforts, identifying areas for improvement, and recommending enhancements to incident response frameworks.
    - facilitating improved information sharing mechanisms between the public and private sectors to enhance collective defence against cyber threats.
- There should be a consideration to extend the scope of the CIRB to ascertained incidents, but also major 'near misses'. The inclusion of 'near misses' can be uplifting for entities and is similar to the model of what is done in other industries (e.g., civil aviation).
- Information collected by the CIRB should align with the ransomware reporting obligations determined in Measure 2.

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

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

- The CIRB may need to, at any indication of criminality, refer the matter to the police. This is dependent largely on the incidents that are reported.
- **Recommendation 13:** We suggest that the CIRB should maintain operational independence between from law enforcement/national security agencies. While the CIRB can receive briefings and insights from these entities, it should not be involved in operational decisions or actions related to law enforcement or intelligence gathering.
- This should be supported by positioning the CIRB primarily in an advisory role, focusing on policy recommendations, best practices, and strategic insights rather than on enforcement actions or regulatory compliance.

[5] https://apt.etda.or.th/cgi-bin/listgroups.cgi?c=&v=Australia&s=Education&m=&x=)

- This is supported by having the CIRB not make determinations of fault or backward-looking conclusions. The CIRB's reports should focus on forward looking recommendations that can be implemented by business in general to reduce the risk or effect of future incidents.
- Further, it should be clearly stated that any findings of the CIRB cannot and do not constitute comprehensive evidence of fault or liability.

23. What factors would make a cyber incident worth reviewing by a CIRB?
24. Who should be responsible for initiating reviews to be undertaken by a CIRB?

- **Recommendation 14:** An incident may be deemed relevant depending on the following factors:
    - Scale and Scope (# users) e.g. the number of Australians who are impacted by the incident;
    - the size of the demanded ransom payment;
    - whether the data disclosed, published, locked or deleted was personal information;
    - whether the data disclosed, published, locked or deleted was sensitive personal information;
    - whether the entity is listed on a stock exchange;
    - National Security Implications;
    - Impact on Public Safety;
    - Economic Impact;
    - Novelty of tactics, techniques, or procedures;
    - Breach of High-Value Targets (e.g. those in scope of SOCI);
    - Legal and Regulatory Implications; and
    - The ability of the company to recover from the attack in a timely manner;
    - The intentions of the ransomware attacker to go beyond double extortion. e.g. contact suppliers, DDoS threats and the likes, beyond the denial of access to local data and the threat of publication.
- Besides these above factors, there should also be a process to allow for requests for reviews from key stakeholders, such as government agencies, critical infrastructure sectors, or congressional oversight committees.

24. Who should be a member of a CIRB? How should these members be appointed?
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?
26. How should the Government manage issues of personnel security and conflicts of interest?
27. Who should chair a CIRB?
28. What powers should a CIRB be given to effectively perform its functions?

- **Recommendation 15:** The selection process should prioritise diversity, considering a broad range of perspectives, backgrounds, and expertise enabling a well-rounded analysis of cyber incidents. Selected members should be made in consideration of background checks, security clearance and conflict of interests. These conflicts of interests should be disclosed and made publicly available in a conflict of interest register.

- Primarily, members should be technical cyber security and IT experts. Other members should be GRC experts and experts in organisational learning (e.g., risk managers). It may be useful to have members with awareness of the ethical and social implications of cyber incidents and cyber security practices. This includes understanding the balance between security and privacy, and the broader impact of cyber incidents on society.
- Lawyers, judges, accountants, bureaucrats, and politicians should not be appointed. To avoid conflicts, current and former partners of law firms, accounting firms and management consulting firms should not be appointed.
- **Recommendation 16:** We suggest that independent advisers, such as representatives from other countries who are collaborating or coordinating cybersecurity efforts with Australia, should be included.
- After selection, we recommend that members undergo training to prepare them for their role in the CIRB.
- The chair of the CIRB should be a member of the CIRB, as decided by vote of the members of the CIRB and should rotate every 2 years.
- **Recommendation 17:** The CIRB should be provided with the power of access to information and subpoena power.
- It may be appropriate to provide the CIRB with the ability to provide information to the regulator about the type of controls that could be required, including alternative controls. For instance, this may be in the form of reports of recommendations after incident reviews.

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

- **Recommendation 18:** The CIRB should not use information collected for purposes beyond those for which it was intended. Having said that, if information reveals an immediate threat to public safety or national security, they should be able to share this information with relevant authorities.

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

- Refer to our response to Q28 where the CIRB should be provided with the power of access to information and/or subpoena power.
- Any mechanisms should be balanced with efforts to build a collaborative relationship between the CIRB, and entities involved in cyber incidents.
- However, in cases of non-compliance, the CIRB should have the authority to seek court orders to access information. This must be used as a last resort when all other attempts at voluntary compliance have failed.

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

- The CIRB could have the following features to support their impartiality and credibility:
    - Diverse membership in experts;
    - Term limits;

- Well defined scope;
- Code of Ethics and Conflict of Interest register;
- Unbiased funding; and
- Independent advisors.

Contributors' List (Alphabetical Order)

Sasenka Abeysooriya, Senior Strategic Adviser – UQ Information Technology Services

Ivano Bongiovanni, Lecturer in Information Security Governance, Policy, and Leadership - UQ Business School and UQ Cyber

Daniele Celoria, Lecturer – UQ School of Mathematics and Physics

Joseph Grotowski, Head of School – UQ School of Mathematics and Physics

Ryan Ko, Professor, Chair of Cyber Security and Director of UQ Cyber

John Swinson, Professor – UQ TC Beirne School of Law and UQ Cyber

Geoffroy Thonon, Senior Analyst - AusCERT

Elinor Tsen, Postdoctoral Research Fellow, UQ Cyber

Mark Utting, Associate Professor in Software Engineering, UQ ITEE and UQ Cyber

Brendan Walker-Munro, Senior Research Fellow, UQ TC Beirne School of Law and UQ Cyber

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA

CREATE CHANGE

Contact details

uq.edu.au

cyber.uq.edu.au

auscert.org.au

CRICOS Provider 00025B •