CyberCX

Australian Cyber Security Strategy: Legislative Reforms

Response to Public Consultation Paper

Public Submission

MARCH 2024

Table of Contents

1 Executive Summary

The legislative reforms proposed in the Australian Cyber Security Strategy 2023-2030 represent a historic effort by the Australian Government to modernise Commonwealth statute to match the technological disruption and malicious threats that will continue to characterise the digital environment of our communities. Writing in response to the Consultation Paper released by the Department of Home Affairs (the Department), CyberCX welcomes this opportunity to engage with the government to shape and inform these proposals. Our submission is informed by the extensive direct experience CyberCX has had helping Australian organisations manage complex cyber risk, improve their preparedness and resilience, and protect themselves from current and emerging cyber threats.

CyberCX has reviewed the measures proposed in the Consultation Paper and this submission outlines our observations and suggested recommendations for improvement. CyberCX's views are summarised as follows:

New Cyber Security Legislation

- Measure 1 – Secure-by-Design Standards for IoT Devices

  Supportive, with suggestions concerning industry OT and addressing related issues of technology supply chain risk.

- Measure 2 – Mandatory Ransomware Reporting

  Supportive, with suggestions concerning how to improve the ease of reporting; how to make reporting insights as useful as possible; and how the efficacy of such reporting could be regularly evaluated.

- Measure 3 – Limited Use Obligations

  Supportive, with suggestions concerning the protection of information shared with government and mitigating the potential for unfair or inadvertent impacts on reporting entities.

- Measure 4 – Cyber Incident Review Board

  CyberCX believes a more effective model would be a Board comprising relevant regulators, intelligence agencies, and law enforcement bodies, with non-government advisors drawn in on a case-by-case basis. We also believe there are existing entities that could be leveraged to perform the desired purpose of reviewing "the root cause of cyber incidents and assess[ing] the effectiveness of post-incident response".

Amendments to the SOCI Act

- Measure 5 – Protecting Data Storage and Business Critical Data

  Supportive.

- Measure 6 – Consequence Management Powers

  Supportive, while suggesting a need to clarify intended scope as it may be impractical to confine the powers as described to only SOCI Act critical infrastructure entities.

- Measure 7 – Protected Information Provisions; Measure 8 – Enforcing Critical Infrastructure Risk Management Obligations; Measure 9 – Consolidating Security Provisions of Telco Act and SOCI Act

  Supportive.

2 Response to Proposed New Cyber Security Legislation

2.1 Measure 1: Secure-by-design standards for IoT devices

CyberCX supports the proposal to mandate that consumer IoT devices for sale on the Australian market are compliant with relevant international standards. This is a logical measure that should have the effect of better protecting users from attacks exploiting fundamental design weaknesses in consumer IoT devices. It will bring Australia in line with standards regulation occurring in other leading markets, namely the EU and the United States. Regulations mandating the adoption of IoT device standards should focus on consumer products as a means to protect end users, households, and businesses as IoT devices become ever more ubiquitous and integrated into our way of life. For this reason, the proposed regulations should be crafted to mitigate unintentionally impacting industrial, medical, or government operational technology (OT) as well as research and experimental technologies.

Standards play a useful role in setting baseline expectations for consumers and the market concerning the quality and safety of products. However, with regards to IoT and other digital products, applying standards alone is insufficient in protecting against malicious efforts by state and non-state actors to poison the supply chain of certain technologies, especially by exploiting comparatively insecure foreign vendor equipment and services. Hardware and software supply chains are intricate and highly globalised, with the production of most devices and digital products involving numerous internationally dispersed entities. This complex, globalised technology supply chain has already been exploited on numerous occasions by malicious state and non-state actors seeking to exfiltrate stored data; collect and share data; disrupt services; disable or degrade devices; and otherwise establish unauthorised remote connections and access. Methods for doing so includes targeting frailties or sabotaging end-user-equipment (which would be partially mitigated by mandating standards); network infrastructure, IT and OT components; unmanned and remote systems; and surveillance devices and sensors. CyberCX assesses that threats to Australia’s technology supply chain security will only increase. This is because it is anticipated that societies will become more digitally interconnected and that geopolitical tensions will continue to incentivise state actors to sabotage and subvert adversaries’ technology as an alternative to, or in tandem with, conventional warfare.

Technology supply chain risk (TSCR) will vary in complexity and severity across industrial and other sectors, but for those entities encapsulated by the SOCI Act, addressing these risks will become more urgent as they seek to protect and sustain their business operations in the face of more capable and determined threat actors. The Government may wish to consider working with CI and SONS entities to establish Technology Supply Chain Risk Management Plans, which could be a tool for helping entities and the government to: better understand their exposure to TSCR; identify their risk appetite for TSCR; and establish proportionate mitigation strategies for addressing TSCR over time.

2.2 Measure 2: Mandatory Ransomware Reporting

CyberCX welcomes the government's prioritisation of measures that will improve the understanding and visibility of the cyber security landscape available to government and industry. Mandating entities to report when they have experienced a ransomware attack or when a ransom has been paid should improve the granularity and fidelity of information concerning ransomware attacks available to government and industry, especially if aggregated insights from these reports are made highly accessible and actionable for targeted entities.

The proposal that reporting requirements apply to all businesses with a turnover of over $10 million per annum would appear to encompass many of the businesses typically most victimised by ransomware attacks. Small to medium enterprises (SMEs) are more likely to be subjected to a cyber attack than a large business, whether due to cyber criminal opportunism or a deliberate attempt to 'island hop' a large entity's supply chain through SME systems. Attacks on SMEs can have even more devastating consequences than those on larger organisations (which usually have redundancy and resilience measures in place, such as preparatory backups and emergency response procedures).

To support entities impacted by ransomware attacks, CyberCX created a Ransomware and Cyber Extortion Guide to provide clear advice for organisations in taking practical steps to prevent, respond to, and recover from cyber extortion attacks.[1] The Guide draws on key learnings from our considerable operational experience and advisory expertise, including our Digital Forensics & Incident Response practice, CyberCX Intelligence, which is our unique Indo-Pacific intelligence capability, and our Cyber Strategic Communications team, which advises leaders in many of our region's most high-profile incidents. CyberCX is willing to freely offer the government the intellectual property associated with our Guide in order to help the broadest possible range of organisations to manage the risks of ransomware attacks.

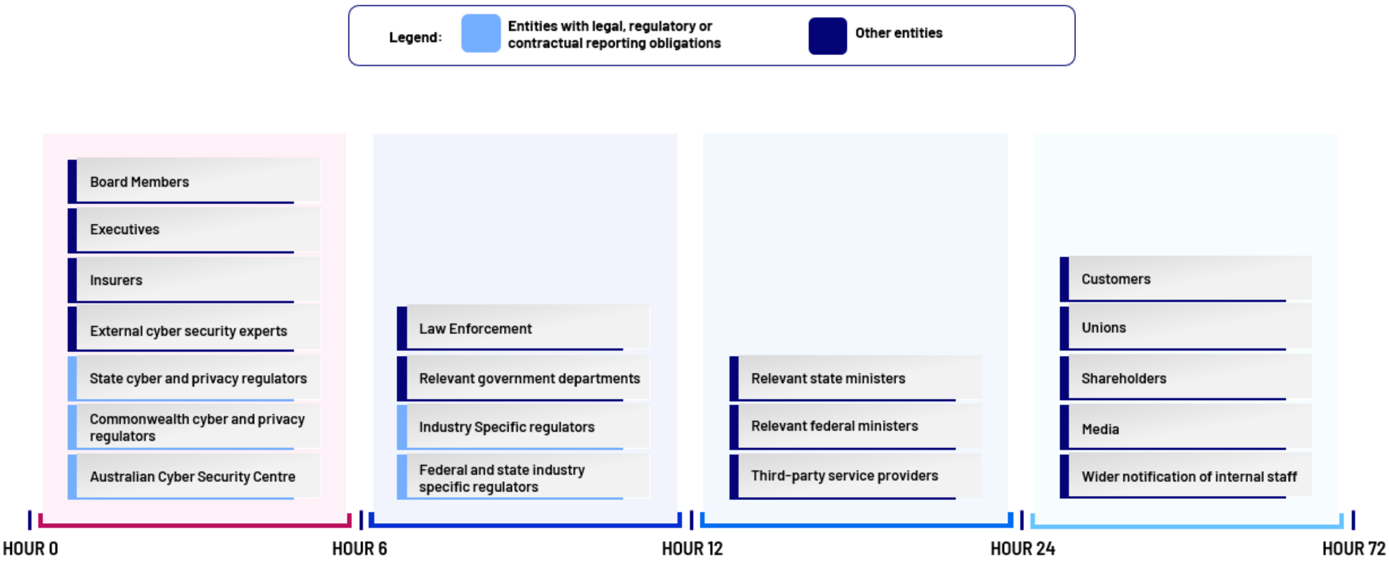
CyberCX suggests that the Government may wish to also consider additional criteria for capturing some non-commercial entities that might not have a $10 million per annum turnover, but otherwise undertake operations of significant community or national interest, such that the government would want to be aware of ransomware attacks on these entities. Examples could include civil society groups, think tanks and research institutions, political groups, and other non-profit entities. The merit of ensuring these nationally significant entities undertake ransomware reporting is intuitive, however we note that for non-commercial entities in particular, mandatory reporting requirements could be a significant impost on their operations. CyberCX therefore suggests the government making funding available to these entities so they are able to uplift their systems and staff to support mandatory reporting requirements.

While we believe these reporting requirements are warranted, CyberCX would like to stress the importance of aligning any new reporting requirements with existing obligations and ensuring that the procedures for reporting are as user-friendly as possible, for example by leveraging existing reporting systems such as *ReportCyber.* Insofar as possible, duplicative information requests should be eliminated and reporting timeframes consolidated. A Ransomware Information Sharing Platform which mirrors the existing technical reporting structures of the ACSC's CTIS, but is tailored to the

[1] **https://cybercx.com.au/resource/ransomware-guide/**

needs of the broader business ecosystem, would provide the most effective means of enabling community driven ransomware information sharing. It should also be inclusive of small and medium enterprises, which may not be able to ingest complex machine-to-machine threat information products. Such a platform would allow the Department to become a 'broker' of ransomware information for a broad range of relevant stakeholders.

The government's suggested 72hr timeframe for reporting should be matched by assurances from relevant agencies to industry that their reports will be assessed – and relevant insights shared – with a similar degree of urgency. Quarterly sharing of aggregated insights drawn from mandatory ransomware reporting may therefore be too infrequent. To aid the government's consideration of these details, CyberCX outlines below an indicative reporting sequence experienced by Australian entities in the immediate wake of an incident. This is informed by our extensive experience working with all types of entities. This figure should be taken as indicative only, and does not account for industry-specific notification requirements.


Legend:
Entities with legal, regulatory or contractual reporting obligations
Other entities
Board Members
Executives
Insurers
External cyber security experts
State cyber and privacy regulators
Commonwealth cyber and privacy regulators
Australian Cyber Security Centre
Law Enforcement
Relevant government departments
Industry Specific regulators
Federal and state industry specific regulators
Relevant state ministers
Relevant federal ministers
Third-party service providers
Customers
Unions
Shareholders
Media
Wider notification of internal staff
HOUR 0
HOUR 6
HOUR 12
HOUR 24
HOUR 72

Indicative Incident Reporting & Notification Timeline

Additionally, to aid the creation of uniquely valuable insights based on this new reporting regime, the government may wish to consider creating a third, voluntary reporting criteria for entities that have identified unsuccessful attempted ransomware attacks. While it is not practical or proportionate to mandate entities to report attempted ransomware attacks, giving entities the option to provide this information – for example if they feel they have experienced a particularly unique attempted incident – could improve the overall value of the aggregated assessments that will be generated by the new reporting regime. CyberCX also believes that providing easy avenues for entities to voluntarily report attempted incidents will help create a strong reporting culture as well as a regular cadence of reporting to government.

CyberCX also believes it would be prudent for the government to include sunsetting provisions in the legislation that will give effect to these new reporting requirements, for example a period of 24 months. This would ensure the parliament is afforded the opportunity to closely scrutinise the effectiveness of these reporting requirements and hear from the government and affected entities about whether the reporting regime is achieving intended outcomes, how it can be refined, and whether it remains a proportionate measure, especially in the context of existing reporting obligations already placed on industry. The inclusion of sunsetting provisions would also focus responsible departments and agencies, as well as industry, on operationalising the regime and the assessments it will produce in a timely manner.

2.3 Measure 3: New Limited-Use Reporting to ASD, ACSC and National Cyber Security Coordinator

As a means to encourage greater information sharing from industry, CyberCX supports the proposal to place explicit limitations on how voluntarily reported cyber incident information can be used by ASD and the National Cyber Security Coordinator. The government's consultation paper explained that ASD and the Coordinator would not be able to share information obtained under this voluntary regime with regulators for the purpose of compliance or enforcement, but that limitations would not be applied on how the information could be used for intelligence or law enforcement investigations, nor would immunities from legal liability be offered.

CyberCX suggests that some additional constraints should be placed on the use of this information to better encourage industry participation and avoid unintended consequences that could be unfairly harmful to businesses. In particular, more attention should be paid to ensuring that information voluntarily shared by a business with ASD or the Coordinator does not adversely impact that business' reputation nor its commercial relationship with the Commonwealth or other governments. For this reason, the model adopted should be one that applies a general prohibition on sharing with specific exemptions for prescribed purposes, such as for law enforcement and intelligence investigations. Such an approach would also be consistent with other sensitive information collection, usage and sharing regimes, such as electronic surveillance, where targeted exemptions are applied to general prohibitions.

In particular, the sharing of system information, telemetry and other technical data can be highly sensitive to reporting entities, but potentially very useful for ASD, law enforcement and intelligence agencies. Encouraging entities to share this valuable information will require giving them confidence that its distribution will remain tightly controlled.

Proper constraints in this area will also be important for reassuring business that information shared with ASD or the Coordinator under this scheme will not be used to inform future commercial decisions by the government nor passed on beyond Commonwealth agencies (i.e. interstate or overseas).

At a practical level, voluntary reporting to ASD or the Coordinator under this measure should be a low-friction user experience where online reporting can take place alongside other reporting processes and using existing platforms, such as *ReportCyber.*

2.4 Measure 4: Cyber Incident Review Board

CyberCX is circumspect about the value and efficacy of the proposed Cyber Incident Review Board (CIRB). CyberCX does not accept the assertion that there is “no national mechanism to review the root cause of cyber incidents and assess the effectiveness of post-incident response”. CyberCX believes the following entities are examples of those that already have existing mechanisms that could be used for this purpose:

- **ASD/ACSC** have the remit to work with law enforcement and other agencies to investigate cyber incidents affecting Australia, including their provenance and impact. ASD and ACSC can generate assessments concerning these incidents which could include lessons for industry and government. Both already produce reporting and other material that is accessible to industry. The prioritisation of resources from these agencies to support post facto incident response evaluations is likely the key obstacle to performing this function, rather than an absence of remit.
- **The National Emergency Management Agency** was initially established to improve Australia’s capacity to prevent, prepare, respond, and recover from natural disasters, however the agency has acknowledged the need to address hazard convergence, including the impacts of cyber incidents, and possesses the remit to shape policy across the emergency management continuum. Conceivably, the NEMA could evaluate nationally significant cyber incidents in the context of its existing capabilities for informing national emergency prevention and hazard reduction.
- **The Minister for Home Affairs**, the Prime Minister, and the Cabinet have various mechanisms available to them to appoint independent reviewers to undertake evaluations into cyber incident response effectiveness. This includes making recommendations to the Governor-General for vice-regal appointments that can carry significant powers.
- **The parliament** can establish dedicated inquiries into any issue, with powers to compel witnesses to appear, hear testimony in-camera, and extend parliamentary privilege to witnesses. The parliament can also pass laws to empower committees with special, additional powers. The government of the day, or individual members of parliament, could seek to use these existing powers to set up inquiries to evaluate lessons from recent cyber security incidents.

Should the government believe a new entity should be formed, CyberCX believes the optimum pathway would be one that convenes established regulators and affected agencies to strategically coordinate their existing powers and capabilities. This entity would not need to be legislated. For example, the CIRB could comprise representatives from organisations including, but not limited to, ASD/ACSC, the Office of the Information Commissioner, the National Cyber Security Coordinator, the Australian Communications and Media Authority, Australian Securities and Investments Commission, AUSTRAC, the Australian Federal Police, the Australian Criminal Intelligence Commission, the Australian Security Intelligence Organisation, as well as relevant State or Territory agencies. This joint model has been a long-standing approach in other national security areas as it allows agencies to use their distinct powers to undertake operations within their discreet remits but in a manner that serves the larger shared objective.

A CIRB that comprises these regulators and agencies should of course invite non-government entities or experts to participate on a case-by-case basis. However, the standing responsibility to produce actionable recommendations informed by lessons from past incidents should rest with government agencies who have the remit and independence from affected industries. The recommendations of the CIRB should also be informed by the work of dedicated investigative professionals who can undertake sensitive examinations of affected entities using consistent methodologies, while be accountable to established oversight bodies. Having agencies jointly deploy existing investigative staff from law enforcement agencies and regulators would be the best path for achieving this without the need for new legislation.

3 Response to Proposed Amendments to the *Security of Critical Infrastructure Act 2018*

3.1 Measure 5: Protecting Data Storage Systems and Business Critical Data

CyberCX supports the proposal to amend the SOCI Act to include 'business critical data' in the Act's definition of 'asset'. This is a practical and logical initiative to ensure businesses are safeguarding their data storage systems, including those managed by third parties, in line with other critical assets. CyberCX suggests that the government may also wish to evaluate current processes surrounding entities' critical infrastructure risk management plans (CIRMPs) to ensure they properly capture where risks have been delegated to third party data service providers. Similarly, the government will want to be confident that procedures are in place for ensuring that third party data service providers are aware of when they are interacting with business critical data and have therefore become subject to the SOCI regime.

3.2 Measure 6: Introduction of Consequence Management Powers

CyberCX agrees with the principle that the Commonwealth should, in extremis, be able to step-in to aid entities affected by nationally significant cyber security incidents where they are unable or unwilling to manage the cascading impacts of the incident. This is particularly important when it comes to protecting or restoring the operations of critical infrastructure entities or systems of national significance. CyberCX therefore supports the legislation of powers for the government to mitigate post-incident consequences by directing entities to undertake certain activities. However, CyberCX notes that the proposed consequence management powers represent potentially one of the most expansive pieces of national security legislation since the *National Security Act 1939.* CyberCX therefore suggests that the government should consider the following observations should it wish to proceed with these reforms:

- We note that the proposed powers as described in the Consultation Paper are not confined to solely managing the consequences of cyber security incidents, but rather they have an 'all hazards' application. This means the powers could logically be used as part of the government's response to the full spectrum of potential emergencies, from bush fires to military attacks. Further, while it is conceivable that the entities most likely to be impacted by these consequence management powers will be critical infrastructure entities as described under the SOCI Act, it is entirely possible that, in the course of mitigating the consequences of an incident, it becomes impractical to only apply these powers to critical infrastructure entities.
- For example, if a cyber incident were to impact a major Australian bank in a manner that prevents its customers making payments, the government could need to direct certain retailers, such as pharmacies or GPs, to forestall requiring payment for essential medical products and services. It may therefore be useful to couch these powers elsewhere, such as in the *National Emergency Declaration Act 2020,* where the activation of consequence management powers can be directly linked to the declaration of a national emergency. The drafting of the declaration itself could also be used as the means for describing which types of entities will be subject to the consequence management powers and why.

- The scope and severity of these powers should mean they are accompanied by sunsetting provisions that will ensure the parliament is able to regularly evaluate their proportionality and efficacy and allow industry to make representations on the impact these powers have on their operations. CyberCX would also like to see ample scope for affected entities to have the government's decisions to invoke these powers reviewed to ensure the utmost proportionality.

3.3 Other Proposed Measures

The other proposed measures to be actualised in a reformed SOCI Act include:

- Simplifying information sharing between government and industry during a crisis by amending the protected information provisions of the Act;
- Providing the Secretary of the Department, or a similar regulator, with the ability to direct entities to address deficiencies in their critical infrastructure risk management plans;
- Rationalising security requirements of the Telco Act and SOCI Act to clarify obligations for telco entities and simplify the application of each Act.

CyberCX supports these initiatives as practical improvements that will support the proper functioning of the regimes articulated within the SOCI Act.

4 Conclusion

CyberCX thanks the government for the opportunity to engage with the policy development process surrounding these important and timely legislative reforms. We support the objectives of the Australian Cyber Security Strategy 2023-2030 and these legislative proposals to improve Australia's national cyber resilience. As an Australian founded organisation that has established itself as a sovereign capability for protecting our communities, CyberCX looks forward to continuing to work with the government to ensure Australia can be one of the most cyber secure nations in the world.

About CyberCX

CyberCX is the leading provider of professional cyber security and cloud services across Australia and New Zealand. With a workforce of over 1,400 professionals, we are a trusted partner to private and public sector organisations helping our customers confidently manage cyber risk, respond to incidents and build resilience in an increasingly complex and challenging threat environment.

Through our end-to-end range of cyber and cloud capabilities, CyberCX empowers our customers to securely accelerate opportunities in the digital economy.

Our expertise is represented across 12 cyber security and cloud practices:

- Strategy and Consulting
- Governance, Risk and Compliance
- Security Testing and Assurance
- Privacy Advisory
- Identity and Access Management
- Network and Infrastructure Solutions
- Cloud Security and Solutions
- Managed Security Services
- Cyber Capability, Training and Education
- Cyber Intelligence
- Digital Forensics and Incident Response
- Cyber Strategic Communications

Contact us to find out how CyberCX can boost the cyber security skills of your entire organisation.

cybercx.com.au ☎ 1300 031 274

CyberCX

PUBLIC