2023–2030 Australian Cyber Security Strategy: Legislative Reforms

Submission to the Department of Home Affairs
1 March 2024

Thank you for the opportunity to comment on the proposed changes to cyber security regulation and legislation emanating from the *2023-2030 Australian Cyber Security Strategy* (the Strategy).

This submission has been prepared in the context of our work at Geomastery Advisory Pty Ltd and our experience working with legislation, regulation, technology, and cyber security both within and external to government (in small and large enterprise). It does not reflect the view of clients or other bodies with which we are associated.

We make the following observations, some of which may be echoed in responses to the individual measures. We look forward to the opportunity to discuss these issues further with the Department.

The purpose of the legislative changes

Both the Strategy and consultation paper argue there are gaps in the legislative and regulatory framework. However, sometimes what may be construed as a 'gap', exists for good reason—for example, to enable flexibility on the part of business operators, to minimise regulatory burden or to uphold and strengthen individual choice and freedoms. Alternatively, what is a 'gap' is a matter of interpretation, which could be resolved through definitions, or contradictory and/ or conflicting sets of legislation.

Legislative change too often becomes a matter of accretion rather than clarification. As a result, it can simply add to the increasing complexity of legislation and regulatory burden, while diminishing clarity, trust, freedoms and, ironically, security.

Thus, the consultation to better inform debate and consideration, would have benefitted from clearly identifying where those gaps are, why they exist, and the potential consequences in terms of their 'closure', including the transfer of cost and risk.

It's worth noting that legislative clarity may be gained through subtraction, rather than relying on accretion—just as a garden benefits from pruning and weeding. Careful subtraction would be needed and would astutely recognise the horizontal role of cyber security and cyber technologies; that could be achieved through a more holistic view of legislation that affects the cyber posture of Australia, its critical infrastructure, and organisations, while preserving democratic values and norms.

Moreover, gaps are features, not necessarily bugs, in a fast-moving, often disrupted environment. Care needs to be taken not to over-specify, especially in legislation, which is a slow-moving artefact—or to legislate for past conditions. There's a strong case, on complex systems principles, for providing guidance and agency to entities and individuals, while retaining legislation for slow-moving aspects or the broader societal and technological systems where surety is needed.

We are concerned that discussions of privacy have been separated out and not addressed. This is a fundamental characteristic and value of democratic societies, and as such is need of stronger protection and assurance. It is also, in the digital world in which we live, indivisible from security concerns—that's inherently recognised in the 28 February 2024 Presidential Executive Order on prevention of access to American personal and sensitive data by countries of concern.

The personal data and privacy of individual Australians are no less important. We note that security concerns motivate the proposed regulation of smart devices. But in principle, better privacy helps ensure better security; security is now fundamental for privacy. The separation of the two is a gap that is left unaddressed; tackling in in a coherent manner has been called for by a wide-range of industry and academic actors.

A theme running through our comments is that of transparency and accountability. Trust must be earned, not demanded. How government engages with the private sector and community, including the handling and use of confidential information provided by external parties, including during incidents, is key. Transparency similarly works bi-directionally. Authorities must be willing to listen authentically, provide feedback, and issue timely reports. Accountability measures must be robust and sustained, with sufficient information to verify that their actions have been in the public interest.

There is the question of resourcing. Legislation is in danger of being a paper tiger, or causing undue risk and burden, if its provisions are not sufficiently and sustainably resourced. Measures that are the due responsibility, and accountability, of government should not be transferred onto others, either through risk or cost.

There is also the question of whether the proposed regulatory authorities have the requisite knowledge, skills and understanding of the technologies, industry business models and market conditions in fast-changing environments.

Last, in terms of how the government might approach implementation of the cyber security strategy, including any mandatory reporting regime, we strongly encourage the Department to be mindful of the journey industry has been on with this topic at the request of government. Incorporating the co-design contributions and feedback from those processes will no doubt help facilitate a smoother introduction and evolution of supporting infrastructures.

PART 1

Measure 1: Secure by design standards for IoT devices

We agree that IoT devices extend substantially the threat surface of organisations and are sources of exploitable vulnerabilities. As such, it is good to see the government wanting to address the problem.

However, we consider the issue to be more complicated than that inferred by the consultation paper.

Australia is a majority taker of technologies—and thus of standards—rather than a maker and to a lesser extent, a shaper. Alignment with the standards of others aligned with our interests and democratic norms makes sense. It is worth noting there is a progressive shift towards security-by-default.

The nature of the devices being targeted for this measure. The definitions are overly broad and neglect the nature of the market mechanisms that define their uptake and use—and disposal.

- For example, the consumer market is characterised by breadth, variety, and consumables/ disposables with fast development cycle times, short life spans and (comparatively) low cost per item. On a per item basis, there's little value-add to companies in ensuring better security. That's less the case on a market level, but Australia is obviously not the size of market in the United States, Europe or Asia.
    - The ACSC guidance states that security (and we add, privacy) should not be a luxury item. Yet one consequence may be Australia becomes less attractive as a market, and potentially to test innovative new products.

- There is a second category of IoT/ smart devices. Those include medical devices, operationally critical devices, and other devices that capture critical personal and identifiable information. The per-item cost for security by design/ default tends to be lower on a per unit basis.
    - As a problem set, these are more likely to be targeted by attackers, and as such provide better returns in terms of protection, and signalling to fellow countries, nations and adversaries.
- Third, the devices themselves may function simply as sensors or collectors of data. The devices themselves may be secure by design/ default. But such measures may not be sufficient for the security, let alone privacy of the information collected and passed through to other devices, systems, or applications.
    - That raises the question of the extent we should be abstracting up and looking at ecosystems of devices and systems to afford improved protection—especially as consumer devices and sensors are being embedded in organisational systems and everyday life.

A security (and privacy) by default setting will strengthen security through the full lifecycle of devices and applications, from conception, design, development, implementation, maintenance, closure, and disposal.

- Security by design implies the only time consideration, including by users, has been done in the design/ development phase.

Security-by-default and full-life cycle approach recognises that there is no single point of absolute assurance of security: there is 'no compliance badge or logo for products meeting a set of requirements.'

- Use of artefacts such as logos or badges may infer unwarranted confidence, potentially increasing risk-taking behaviour on the part of users and their customers.
- It's worth noting the log4j vulnerability would likely have passed any such badged-focussed effort to assure security. Moreover, it required many and ongoing efforts to patch the vulnerability.

As the UK's NCSC says, security by default is an ethos or philosophy. There are no silver bullets here. Software development alone is hard work; its complexity means that 'master builders' in charge of applications and programs are quickly overwhelmed.

- While some may argue the advent of AI will help such assurance, it is worth noting that AI itself is hardly without flaw, bias, or assured security. Moreover, research suggests that AI co-built code may be less secure due to over-confidence on the part of programmers.
- AI itself will generate changes in the nature and use of smart devices, and especially device ecosystems.

Consequently, a better approach is to encourage the use of security by default philosophies — again, set out by the UK's NCSC—not simply for developers, but throughout the life cycle.

- Developers tend to prioritise the efficiency of code, and there is a constant tension between performance and design. These concepts extend into the operation of the systems driven by code, such that how systems are implemented, managed and support can weaken security posture.

Last, the use of other mechanisms to help consumers understand and make decisions about their IoT devices should be considered. Perhaps the best example is Sweden and Estonia, which have linked device security to their recycling programs, giving consumers a view of the device life cycle from purchase, but also encouraging them to think more carefully about data retention and disposal.

Measure 2: Ransomware reporting for businesses

To achieve the desired outcome from mandatory reporting—described in the discussion paper as greater visibility and understanding of how ransomware attacks and cyber extortion impact Australia's economy and society—the context of *where* in the economy/society an incident has occurred is likely as important as the *how* and *when*.

Notwithstanding privacy considerations on the information mandated for inclusion for a reported incident, the characteristics of the victim's organisation, such as sector (using the ANZSIC codes plus an 'other' option for self-identification) and customer orientation (G2G, B2G, B2B, B2C, C2C etc.), will be important to help, in the first instance, civil society and smaller organisations to better understand the breadth and scope of cybercriminal use of ransomware and extortion. And, over time, such information will enable, among other benefits:

- deeper pattern analysis of possible intent;
- understanding how malicious actor tactics and techniques are adjusted (or not) for different sectoral and market segment targeting as well as early-warning information to be shared more widely among CSOs, CISOs, CROs and business managers;
- finetuning of deterrence options; and,
- more adaptive mechanisms to prevent repeat attacks on individual victims.

We consider that <u>all organisations</u>, public (including all levels of government) and private, should be required to report under a mandatory scheme. Such comprehensiveness is needed to meet the desired outcome described; else,

- otherwise out-of-scope organisations may become more attractive targets for cybercriminals, either for their direct benefit or for supply and value chain access to others; and,
- out-of-scope organisations may be inclined to greater risk-taking behaviour.

It is incumbent on government to streamline the reporting mechanism as much as possible, including with other concurrent reporting requirements such as the Notifiable Data Breach Scheme and privacy breaches, to guard against regulatory burden.

- Other governmental experiences provide templates (such as the United Kingdom) and relevant, fit for purpose, secure software has long been available that puts the user context and experience first.

Related, it will also be critical to harmonise the underpinning regulatory instruments with international efforts in this arena, such as those in the European Union and North America,

- for data comparison and analysis and threat identification;
- to ensure interoperability with insurances, legal advisory and post incident court proceedings (domestic and international); and
- to facilitate adjustment of the instruments to keep pace with technological and process change, including in preparation for a post AI-enabled quantum computing world.

Harmonisation is also a domestic consideration, an integral part of the overall picture of cyber security regulatory reform.

- How a mandatory ransomware and extortion reporting regime operates with State/Territory voluntary and mandated requirements around data protection, incident management and privacy is important in this specific instance and needs careful consideration.
- The same is true for concurrent federal legislation and regulation such as those applying to critical infrastructure collectively and banking and finance, telecommunications and health specifically.

Publicly funded resourcing of the reporting regime is critical. Australia does not deserve another underfunded regime—the compounded effect of the underfunding of the Office of the Australian Information Commissioner (OAIC) has in turn undermined comprehensive civil society and organisational education on privacy and data breaches and thus confidence in government's commitment to these issues.

- We observe internationally, in likeminded nations, the security, economic and societal benefits that accrue to regimes resourced proportionately to both population size and need as well as scale and reach of the challenge.

Appropriate and sustainable funding of the regime increases the likelihood that economic agents and civil society will see and experience the benefits of meeting the requirements of reporting, including the (as streamlined as possible) time invested to comply with the type of information required, and come to trust the regime's aggregated data and insights.

Measure 3: Limited use obligation on Australian Signals Directorate and National Cyber Security Coordinator

For myriad operational and legal reasons that have been the subject of discussion for over a decade in Australia, it has been a struggle to build and sustain trust between industry and government that would facilitate the needed open and frank dialogue on why (as opposed to how and when) non-federal government entities and the private sector are reluctant, and in some instances refuse, to share cyber incident information with government.

At its core, this is an issue of trust—across people, process and technology. On the process and technology aspects, it is indeed the role of government to meet the higher standard of compartmenting information shared for a prescribed purpose.

Government is also expected to ensure relevant and appropriate permissions are sought from the information owner(s) and/ or custodians (noting most data breached or compromised is not owned by the organisations suffering the breach or compromise) on how the information is handled in government systems once the immediate trigger for the information to be shared has passed.

- For example, organisations—or those whose data has been shared—should be able to ask for and receive certification as to the destruction of the data.
- Government could also consider a 'right to be forgotten' in the aftermath of an incident.

We support the notion of a limited-use obligation as described. We support the clarity around the important distinction between safe harbour and limited use. However, we caution against its introduction at the exclusion of legal safe harbour where and when it is most applicable.

- Due to the highly contextual nature of each individual cyber incident, together with the asymmetric nature of the cyber-physical landscape as a vector for large scale and significant harm, it is becoming more and more critical for the practice of cyber incident response to be treated far more holistically.

The role of individual and institutional researchers in understanding incidents, as well as their role in discovery and tactics, techniques, and procedures analysis, is obviously a key, and valued, part of cyber incident lifecycles and value chains.
Current provisions, and fear of prosecution, mitigate against those intellectual assets and insights being available to the benefits of the Australian community, organisation and government systems.

- Other nations such as the United States have successfully introduced safe harbour provisions for researchers that have had measurable impact on incident prevention, response and recovery.

Time-limited safe harbour provisions in a defined instance of crisis, applied without legal prejudice, should also be explored as another use case—perhaps more relevant for circumstances where law enforcement agencies are involved, but therefore still relevant for the design of a limited-use obligation for ASD and the Cyber Coordinator

Specific safe harbour provisions and a limited-use obligation working in tandem, within a holistic view of incident lifecycles, could present a powerful set of levers for government and industry if used in a more trusted partnership, as well as supporting deterrence and resilience.

- It also has a less discussed benefit of minimising financial and reputational harm to victims in their future for any longer-term issues arising from a cyber incident, including matters of insurance and legal precedence.

Measure 4: Cyber Incident Review Board

We welcome the opportunities for improving cyber security through a review and lessons learned mechanism. There is real value in the understanding the specifics of incidents, but as importantly, learning from how including how organisations have adapted and learnt from the experience.

First, language matters. We suggest strongly that the proposed Cyber Incident Review Board (CIRB) be renamed, as in the United States, the Cyber Safety Review Board (CSRB).

- ‘Incident review’ implies more of a tactical response; ‘safety’ suggests purpose and broader outcomes, lessening the chance of victim blaming, helping to support the ‘no fault’ premise of reviews, and be more in line with the Minister for Home Affairs’s own framing of cyber.

Second, while the Australian Transport Safety Bureau is used as the measure of a new cyber-related Board, more could be done by drawing on the experience gained since the US CSRB was established in 2022.

- Like the CSRB, the new Board should do in-depth reviews and look to draw significantly consequential, pragmatic conclusions and recommendations from them.
    - For example, the two reviews undertaken by the CSRB thus, on log4j and Lapsus$ are robust and well-written, with a range of observations and recommendations.
- There has been some criticism within the US cyber community that the CSRB’s review has not provided the detailed analysis sought by experts (with concerns registered regarding potential conflicts of interest—addressed below).
- We need to bear in mind the audience served by such boards include the broader public, and decision and policymakers, not simply focussed on the cyber tech community. That argues for potentially different means of communicating and fora to ensure analysis is robust and lessons fully understood.

Third: trust, reputation, and independence. The key benefit of a CSRB is the non-attributable investigation and analytical reporting of cyber incidents, with recommendation for improved practices. That’s critical for building capability, national resilience, and public trust of both government and industry. The rigour of the approach will be as important as a regulated ‘no fault’ approach in enabling both value to the community, appropriately targeted lessons, and trust.

If a premium is placed on building trustworthiness, reputation, and community, and both government and industry see value in the Board’s analysis and reporting and because of their own data’s protection and integrity in government or the Board’s custody, then there will likely be less need for coercive information collection powers.

- Before the Board is awarded such powers, we need assurance around its transparency: how the Board manages information, the integrity of its approach, will be key.

That suggests there needs to be an enforceable provision enabling the Board to hold such material confidential including, potentially, from the intelligence and law enforcement communities.

- There is a European precedent for such practice. The Hybrid CoE, based in Finland, is protected under specific Finnish law, ensuring its independence and the inviolability of the information it receives from partners in pursuit of the larger objective of building community and trust, and sharing information and lessons.
- Government reluctance to fully protect confidentiality of material presented to a CSRB may compromise companies' willingness to participate, therefore the Board's value.

The need for trust means, too, that the Board will need to comprise reputable and trusted members who are able to undertake reviews in an independent, objective, and professional manner, motivated by learning from past incidents.

Fourth, membership. The CSRB is staffed by both established government and industry experts and those with the capability to enact change in their organisations—including CIOs and CISOs. The consultation paper posits a standing membership, a pool of potential members, or a combination of the two. We would suggest refinements to the latter:

- standing members have set terms of two years, with the possibility of an extension to a third to enable closure of investigations where needed;
- both standing committee and pool members should have 50:50 representation in terms of public sector and private sector;
- both standing members and the broader pool include 'next adjacent' expertise—that is, from users and experts, for example in usability design, AI, quantum computation and privacy and ethics. We consider that important from the perspective of diversity, but important when the Board shapes observation and recommendations; and,
- the Board be supported by a sufficiently sized and funded secretariat that comprises knowledgeable, capable, cyber-savvy, and industry-versed staff, who can write.

Fifth, decision-making. Both perceptions and the reality of independence will be critical to the Board. That has three implications:

- The Minister for Home Affairs and/or Cyber Coordinator may recommend to the Board an investigation. The Board, however, makes the decision, and may choose to vary the scale and scope of an investigation and consult with other relevant mechanisms such as the Foreign Investment Review Board. The Board itself may also decide to pursue a particular investigation.
    - We do not expect rampant investigation as a result: the Board will be constrained by time and the availability of its members. That should also lead to Board to favour consequence, a more strategic approach (e.g. rather than an individual incident, consider a trend, set of behaviours or broader type of attack/ vulnerability) and thus weightier recommendations.
    - The Board's chair may be from government; the deputy should be from industry.
- Board reports must be open and available on completion to the public. It should not be 'massaged' by the intelligence agencies or Home Affairs or proxied via a press release.
- Perceptions of conflict must be carefully—and visibly—managed. Where the perception of conflict may arise, including between industry competitors or potentially by government agencies, members step aside.

Sixth, scope. It is also notable the CSRB's Charter includes consideration of cyber incidents involving federal government systems. The same provision should apply in Australia, not least the nature of material held, including the personal information of Australian citizens: the federal government has a duty of care above and beyond that of corporates, and that should be reflected in the government's willingness, and accountability, to open its own systems for such reviews.

A subject of focus should not simply be the compromise of infrastructure, but the compromise of data. For example, compromised Medicare data may be replicated, through matter-of-course, machine-to-machine data exchange, into Medicare. The question for a Board may be: how does a breach, leakage, compromise or corruption of personal or critical operational data in one entity affect the privacy, operations and the integrity of data in the broader ecosystem?

Last, it's worth noting the key attributes of the US CSRB, essential for its trust, integrity and effectiveness:

- ethics—the US CSRB has a strong ethical requirement, including around purpose and conflicts of interest—no mention is made of ethics in the consultation paper;
- capability—members are expected to bring their personal cyber expertise, not the equities of current or past employers—this needs to be explicit for the Australian Board;
- confidentiality—security clearances and non-disclosure agreements are required, and reports and related materials are protected under Presidential Communications Privileges—we have no equivalent in Australia;
- impartiality—appointments are made regardless of political affiliation—this needs to be explicit in the Australian case; and,
- practicality—with a focus on understanding what happened during incidents and generating pragmatic recommendations for improving cyber security.

While the government is clearly observing Biden Administration cyber initiatives, we recognise that such an American construct will translate imperfectly to an Australian setting. It's not simply filling a 20-person board, it needs the support of a quality, resourced secretariat. Australian mechanisms and capability are arguably more limited than its American contemporary.

Likewise, the new Board must be sufficiently resourced. Too often such pronouncements are made, departments and agencies then scrabble to find funding and staff for the task, and as is typically in the Department of the Prime Minister and Cabinet's 'tiger teams' resourcing is inadequate, continuity and capability is erodes, and agility is lost.

PART 2

Measure 5: Data storage systems and business critical data

We defer to others on to comment on this measure substantively. We note our observations and perspectives on privacy reflected elsewhere in this submission.

Measure 6: Consequence management powers

We defer to others on to comment on this measure substantively.

We note, however, that any last resort power provided to the Minister for Home Affairs would need to take account of concurrent requirements in the existing powers of most other federal Ministers whose portfolios are impacted by a major incident's consequences. There are further, potentially complicating requirements and obligations under intergovernmental agreements.

Measure 7: Protected information provisions

We defer to others on to comment on this measure substantively. We note our observations and perspectives on privacy reflected elsewhere in this submission.

Measure 8: Review and remedy powers

The concept of and principles underpinning the ‘double lock’ review mechanism of the United Kingdom’s Investigatory Powers Commissioner is a likely effective model to consider for this measure.

As noted above, the highly contextual nature of both the practice of cyber security and the ways and impacts a malicious cyber incident are executed (or nearly executed) means there is a disproportionate impost on fairness and the ability of any given organisation to comply relative to their cyber risk posture and maturity.

It is less about the process of applying the double lock that is applicable (issuing warrants etc.), but more what is considered in the process and the design of the actual mechanism in action, including the use of a Technical Advisory Panel comprising vetted industry experts.

Measure 9: Telecommunications sector security under the SOCI Act

We defer to others on to comment on this measure substantively.