IBM Australia Limited
259 George Street
Sydney, NSW 2000

IBM Australia
28 Sydney Ave
Forrest, ACT 2603

Cyber Security Reform
Department of Home Affairs

-- By Email --

To whom it may concern,

Re: IBM Response to DHA's Australia's Cyber Security Regulations & Incentives thinking

IBM is pleased to provide input into the Department of Home Affairs (DHA) consultation process on the cyber security regulations and incentives that will support the proposed legislation.

As a professional services firm focused on hybrid cloud, digital transformation, AI and security, IBM recognises that Australia's digital economy must have a well-established cyber security capability and be highly resilient to all cyber security threats both foreign and domestic, the Government is revising legislation to ensure all citizens can be secure in this digital environment and we look forward to contributing to this dialogue to create a robust and useful discussion on Cyber Security regulations and incentives.

Drawn from our significant experience protecting critical infrastructure and enterprise IT systems, which includes systems such as Internet of Things (IoT) networks, critical infrastructure (OT) networks, , software and networking systems, for over 17,000 clients in more than 130 countries, it also builds on our past work in Australia to support government initiatives to build cyber resilience including sharing perspectives on a Federalised Digital Identity and in highlighting vulnerabilities in Australia's global supply chains.

As the Government seeks to advance their mission with a recognition that no one can fully predict future requirements, our responses, specifically to chapters 4, 5 and 8 aim to share our industry experience and learnings so the Government can reward commercial enterprises that have already begun to embrace cyber security strategies and encourage others to commence.

In summary, our response intends to enable organisations to treat cyber risk as a standard practice, to assess the effectiveness and financial impact of cyber spending, whilst encouraging the government to drive greater adoption of a quantitative approach. Through the Privacy Act, the legislative drivers exist to encourage this approach, however, need to consider the approach beyond just legislative compliance and more towards a proactive and effective method of understanding and managing risk.

Chapter 4: Governance Standards for large businesses

IBM recommends that voluntary standards are more appropriate than mandatory ones being enforced. This is due to the complex range of standards for large businesses, which already vary widely depending on the industry, location, customer base, etc and are already immensely complex.

Local and multinational corporations already comply with a collection of different cybersecurity regulations such as NIST, PSPF, ISM (E8), ISO 27001, ISO 27002, APRA Telecommunications Act or the Privacy Act to name a few; where the overlap of these risk-based governance standards provide prescriptive guidance.

As no organisation is the same, an approach to strengthening corporate governance of cyber security risk is to:

1. provide additional material and guidance to raise awareness directed to all Board and executive-level audiences in Australia.
2. guide the integration of cyber security risk into existing enterprise risk governance forums charters which all different sizes of organisations have in place already.

Adding additional layers of governance expectations through legislation in an aspiration to streamline adherence to the same cyber frameworks and codes, would likely end up driving a checkbox culture. In saying that, ASD's Essential 8 are a strong foundation and when considered in conjunction with other regulatory frameworks and should still be promoted as a minimum baseline to help reduce the risk of cybersecurity incidents from occurring.

Organisations always seek to minimize their risk, but often lack the information and skilled workers needed for appropriate action within their budgets. Designing governance that assists to quantify the level of cyber risk that organisations carry will drive better cyber risk awareness and decisions at the Board and management levels.

Security risk quantification is a common framework that is used to unite C-suite on security, making security strategy consumable to upper management including board executives for buy-in. Board executives gain insight into estimated dollar amounts of the potential financial loss facing their business if they fail to implement recommended security controls. By quantifying security risk, executives will receive additional clarity, assisting strategic cyber investment decisions where board members can:

- Make more informed decisions in less time under conditions of uncertainty
- Understand the true monetary impact of potential threats
- Prioritize risks in a contextually relevant manner
- Enable decision support with risk aggregation
- Convey the return on security investment

In 2020, IBM increased its Australian investment into cyber security services where we have learned through our engagements that clients typically make decisions from an area of uncertainty on how to increase their commitment to prioritise their cybersecurity capability. This is a key concern where voluntary adoption of principles based upon best practice and nationalised standards will enhance self-management of cyber risk. Notwithstanding the costs incurred if mandatory governance standards are implemented, we believe a prescriptive cyber regime may only erode trust between government and industry.

When comparing this to similar international bodies, Israel's national cybersecurity policy today reflects a distinctive approach to become a proactive and long-term approach, focused not on potential attackers but potential threats (and the assets requiring protection) and on organisations as the first line of defence. When compared to the United States, another approach is seen through public-private partnerships with leading risk management and insurance firms to implement best practices and certification to reduce liabilities incurred through risk mitigation and improve the performance of cyber-related outcomes. This is furthered by the government through tax relief to small businesses without the fear of being unable to achieve a level of cyber maturity that may commercially be unfeasible.

While a wholly mandatory structure might yield far greater compliance, the costs to businesses and regulators could be high, which is likely to trickle down to consumers. It is also difficult to see how a wholly mandatory, compliance-based framework will be appropriate for all businesses and can be updated on a regular basis in the context of a threat landscape that is both highly dynamic and rapidly expanding.

Chapter 8: Responsible Disclosure Policies

Responsible disclosure policies should be included alongside mechanisms to incentivise adherence through something like an accreditation scheme (in line with current badging mechanisms burgeoned through industry) with an independent industry body.

Developed in consultation with industry and industry bodies any policy needs to be valuable to the organisation, as well as easy to implement. It should not merely be a policy document, but take the form of tools, playbooks, or checklists that the relevant personnel can refer to at any time. Guidance should aim to make disclosure easier for the businesses, as well as customisable according to their industry and needs. This would make its implementation much more desirable to Australian businesses. Disclosure and reporting will assist government agencies to prioritise affected organisations highlight trends and predict attack patterns, beneficial to entire industries. However, these benefits are only possible if the businesses are encouraged and incentivised to implement responsible disclosure policies.

As communication today is widely understood as applying to both spoken and written word, written code needs to be included too. For developers, testers or customer-facing staff, a higher degree of awareness needs to be present, highlighting their influence. The provision of services online need to be held to a higher standard of ethics and expectations as the proliferation of their work can be global. In the areas of automation and AI, organisations need to make clear when and why AI is being applied, how it is trained, and the rights in terms of IP and data. This may also include the need to regulate the use of results found by AI and the measures in place to ensure they are and remain secure, accurate and not open to manipulation.

The government should clearly define its expectations for the minimum standard, however, permit the industry to establish the education, management, and delivery to obtain the relevant training. Education and training that accredits this aptitude may be needed to ensure common practice but also be flexible depending on their industry as it is reasonable to expect critical infrastructure to have stricter protections.

Any training and certification will also need to be readily accessible to encourage adoption and be delivered by an accredited body at an affordable price. This could be in the form of a star or badge system that would give the recipients an industry advantage. This creates a sense of trust with customers as well as incentivises businesses to operate at a higher standard. A governing body such as the Australian Computer Society (ACS) or Australian Information Security Association (AISA) could endorse obtaining this certification and hold the accreditations, as they already have established education delivery platforms and methods as well as having built trust with corporations. The accreditation will not be able to guarantee cyber security. However, it does provide a baseline level of risk-based security knowledge and skills in place to establish controls and security measures.

Looking at the government's response to the Productivity Commission's Inquiry into Data Availability and Use, which resulted in the Data Sharing and Release Act, the Government legitimised the importance of maintaining public trust in the system to facilitate the economic and social benefits of increased data use. The response emphasised that data openness is a continuum, and that legislation needs to clearly outline accountability of all actors to create and maintain trust. Funding and education were also highlighted to ensure a secure environment is created and the correct behavioural transformation is achieved.

Chapter 5: Minimum Standards for Personal Information

There is universal recognition of the fundamental importance, and enduring relevance, of the right to privacy and protection of personal information, and of the need to ensure that it is safeguarded, in law and in practice. IBM understands that the Privacy Act is currently under review and believes that further clarity about how to meet existing obligations under the Privacy Act would be beneficial.

We appreciate DHAs consultative approach on this area of concern and are happy to address any of our points in greater depth if you have any questions.

Yours sincerely,

Kylie Watson
Partner, Head of Cyber Security[1]
Global Business Services
[redacted]

Chris Hockings
CTO
IBM Security
[redacted]

[1] Major contributors to this response include: *Anu Kukar, Deanna Gibbs, Zuben Rustomjee, Akira Singh and Tayla Payne*