Strengthening Australia’s cyber security regulations and incentives

Amazon Web Services Submission

27 August 2021

27 August 2021

Technology Policy Branch
Department of Home Affairs
Commonwealth of Australia

(Submission lodged via DHA website)

RE: Strengthening Australia's cyber security regulations and incentives

Amazon Web Services (AWS) welcomes the opportunity to comment on the Department of Home Affairs (Home Affairs) discussion paper, *Strengthening Australia's cyber security regulations and incentives* (the Discussion Paper).

As a global hyperscale cloud service provider, security is our top priority. AWS customers trust us to handle their data securely, and we honour our commitment to build and operate infrastructure that satisfies the requirements of all organisations from small startups to the most security-sensitive corporations and governments.

The case for Government's ongoing interest and investment in cybersecurity is clear. Cybersecurity is a pressing economic and societal challenge that impacts all facets of modern life; as noted in the Discussion Paper, the World Economic Forum's *Global Risk Report 2021* listed cybersecurity failure the ninth highest risk by likelihood. As stated in the Discussion Paper, estimates on the annual cost of cybercrime in Australia range in the tens of billions. For individuals, the psychological toll of falling victim to cybercrime is only beginning to be understood, especially at a time where online communication has become the primary means of staying connected and doing business.

The complexity and scale of the cybersecurity challenge demands a clear, cohesive, and comprehensive approach that simplifies cybersecurity issues and increases the ease and success of implementation. To achieve this, AWS supports policies that:

- Strengthen a country's cybersecurity ecosystem, reinforce the benefits of the digital economy, and promote trust;
- Balance the need for additional regulations with market-based approaches that encourage, rather than inhibit, innovation and digitisation. We agree with the Office of Best Practice Regulation that the introduction of new regulations should not be the default, with a preference for alternatives such as voluntary compliance and guidance on best practice;
- Support boards in understanding how to engage with cybersecurity risks, rather than imposing new and highly specific obligations on directors;
- Provide small and medium businesses (SMB) with practical and scalable guidance not just for implementing security controls, but for the promotion of operational excellence and performance efficiencies;
- Encourage genuine collaboration with Government and industry, with Government leveraging the expertise, experience, and reach of large enterprises to promote and support strong national cybersecurity outcomes; and
- Set clear milestones and measures for success, built on an evidence-based approach to cyber policy that considers more than numbers of reported incidents or compliance with prescriptive frameworks.

As recognised in the discussion paper, there are substantial cybersecurity challenges that the Australian Government has a crucial role in addressing. Choosing when and how to act are consequential policy decisions for all governments in avoiding the unintended consequences of overlapping, contradictory, or overly prescriptive reforms. While there is no doubt that cybersecurity requires urgent action, proposed actions should be carefully considered, planned and sequenced. This will allow all businesses the opportunity to effectively boost their cybersecurity while reaping the full benefits of the digital economy and minimising unnecessary regulatory burdens.

There are important steps the Australian Government can take now that meet these needs and the intent of this Discussion Paper. In our submission, we don't seek to address every question posed by the Discussion Paper; rather, we offer recommendations for how the Australian Government can help strengthen cybersecurity through simplification.

We welcome ongoing engagement with Government as it seeks to address this important economic and societal challenge.

Best Regards,

[redacted]

Roger Somerville [redacted]
Head of Public Policy, Australia and New Zealand
Amazon Web Services.

Avoiding the Implementation Gap

The Australian Government's *Cyber Security Strategy 2020* (Cyber Strategy) laid out an ambitious program of activities impacting across the Australian economy. AWS supports these endeavours and agrees that security, safety and trust are fundamental to building confidence in the digital economy. However, we caution against the introduction of additional measures – predicated on the assumption that businesses are not making the 'right' investments in cybersecurity – before existing reforms have been properly implemented, matured and evaluated. This process is critical for ensuring that any new policies are based on evidence; consistent and complementary to existing policies; and are addressing a genuine policy gap.

Many of the initiatives introduced as part of the Cyber Strategy are in their formative stages, and some of these – including the *Security Legislation Amendment (Critical Infrastructure) Bill 2020* – have serious implications for the entire Australian economy. Among the reforms that have been announced or implemented in the 12 months since the release of the Cyber Strategy, many have or will introduce major changes to the nation's cybersecurity. These include:

- The drafting of the *Security Legislation Amendment (Critical Infrastructure) Bill 2020*, which significantly expands the scope of industries and entities captured under existing security legislation and introduces civil penalties, offences and infringement notices for non-compliance.
- Announcing a comprehensive review of the *Privacy Act 1988* intended to modernise and strengthen the Australian privacy regime;
- Passage of the *Online Safety Act 2021*, which significantly strengthens the powers of the eSafety Commissioner and introduces new measures to help Australians experiencing harm online;
- The introduction of the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020*, creating new powers and warrant classes to aid the Australian Federal Police and Australian Criminal Intelligence Commission to help counter cyber-enabled crime; and
- The release of the Hosting Certification Framework, a landmark policy intended to provide assurance to Government on the secure management of government systems and data.

By any measure, these reforms are substantial and meaningful. AWS expects they will have a significant impact on building Australia's cybersecurity and boosting confidence in the digital economy, at a time where digitisation is fundamental to Australia's post-pandemic economic recovery. However, these reforms need time to take effect – and impacted entities allowed sufficient time for implementation – before the introduction of any new regulatory instruments or initiatives.

To ensure consistency, avoid confusion and maintain a common language and understanding of cybersecurity expectations, a harmonisation and simplification of the regulatory environment would be beneficial to both business and Government. As noted in the Discussion Paper, at least 51 Commonwealth state and territory laws that create, or could create, some form of cybersecurity obligation. Consequently, the risk of confusion, conflicting or overlapping regulations is high. As we discuss later in this paper, simplification and consolidation of cybersecurity regulations and messaging should be an important element of the Australian Government's ongoing efforts to support cybersecurity across the Australian economy.

Recommendation 1. Existing reforms, frameworks and programs should be allowed space to be implemented, matured and evaluated before the introduction of additional regulatory measures or compliance programs.

Recommendation 2. The existing regulatory environment should be simplified and harmonised.

Educating Boards and Senior Executives

Many of the proposed reforms under the Cyber Strategy almost entirely impact large businesses – and among these large businesses, many will soon be subject to significant new regulations under the *Security Legislation Amendment* and upcoming *Privacy Act* review. This is a disproportionate regulatory burden, especially considering larger entities are already more likely to have made substantial investments in their cybersecurity. For example, with security as the bedrock of our services, AWS has been externally assessed as compliant with 23 international security standards, including global standards such as ISO27001 and SOC1-3.

Not all entities have the resources or need for security to this scale, but it is incorrect to assume that those businesses and business leaders simply fail to recognise the importance of cybersecurity. Indeed, the World Economic Forum's *Global Risk Report 2021* ranking of business risks are based on perception surveys informed by an extensive network of business, government, civil society, and thought leaders. Similarly, PwC found that 95% of Australian CEOs identify cyber hazards as a key threat to organisational growth, with 78% also reporting increased long-term investments in cybersecurity and privacy[1]. The pandemic, in addition to accelerating the pace of digitisation, also saw a doubling in CEOs globally who were more likely to consider cybersecurity and privacy as part of every business decision – an increase from 25% to 50% in just one year[2].

Nevertheless, knowing that there is a risk and knowing how to address that risk are two separate issues. The same PwC global survey found that more than half of respondents (55%) lacked confidence that their current budgeting processes sufficiently linked cybersecurity spending to their most significant risks[3]. As technologies continue to evolve and digitisation accelerates, cybersecurity investments will necessarily need to become more dynamic and integrated into all business decisions.

Mandatory cybersecurity governance standards or specific director's duties will do little to improve this knowledge gap. At its core, cybersecurity is a business risk and is already part of a director's existing duties. Instead, we believe company directors, senior executives, and other responsible office holders need education and support to understand how to effectively manage their cybersecurity risks.

This was acknowledged by the Australian Securities and Investments Commission (ASIC) in 2015's *Report 429: Cyber Resilience*, which clearly articulated that Australian directors are responsible for building and maintaining cyber resilience and offered guidance on resilience practices[4]. In the same report, ASIC also acknowledged that many regulated entities already had proactive and sophisticated risk management practices to address cyber risks – but that even then, it was not possible to protect against all cyber risks:

> As cyber attacks continue to increase in complexity and sophistication, invariably you may be subject to an attack. However, you can seek to improve your overall cyber resilience so you can survive and recover from an attack as quickly as possible[5].

A voluntary code may assist directors in making more informed investment decisions, but we caution against overly prescriptive codes that emphasise compliance with prescriptive technical controls at the expense of a holistic risk management strategy. Any guidance should be principles-based and recognise that each organisation's risks, priorities, and systems are unique. This will allow organisations the flexibility to choose appropriate cybersecurity approaches with a clear view of business-drivers and technology-use, and prevent the shift of resources to reporting and compliance requirements. While we acknowledge that principles-based approaches may lack consistency, prescriptive approaches can be difficult and expensive to implement and ultimately ineffective.

As indicated by PwC's findings, effectively integrating cybersecurity into all business decisions will take time – and, in many cases, will necessitate a rethink of well-worn investment processes. Industry, academia and professional associations are well-placed to partner with government for the development of practical, risk-based cybersecurity guidance and outreach programs for boards and senior executives that assists in making those long-term investment decisions. We encourage the Australian Government to partner with industry, academia and professional associations to develop a risk and resilience culture within Australia's boards that also encourages, rather than inhibits, innovation and digitisation.

Recommendation 3. Government should partner with industry, academia and professional associations to develop guidance that helps boards and senior executives understand how to engage with and manage cyber risks.

[1] https://www.pwc.com.au/ceo-agenda/ceo-survey/cybersecurity-threats-data-privacy.html
[2] PwC Global Digital Trust Insights Survey
[3] Ibid
[4] https://asic.gov.au/media/3062900/rep429-published-19-march-2015-1.pdf
[5] Report 429 p. 31

Supporting Small and Medium Enterprises

Due to the Australian Government's focus on larger enterprises, Australia's already complex regulatory environment, and the multitude of cybersecurity initiatives underway, we are concerned that SMBs are not receiving the clear messaging and support needed to help boost their cybersecurity while also maximising the advantages of digitisation. We are also concerned that rhetoric surrounding cybersecurity may have the unintended consequence of discouraging smaller entities from undergoing digital transformation or engaging with the digital marketplace. As stories of high profile organisations suffering from sophisticated cyber breaches reach the news, smaller entities may feel an overwhelming sense of helplessness and confusion at their prospects for managing cyber risks.

This is not a new phenomenon, or unique to Australia. Dr. Ian Levy, technical director of the UK's National Cyber Security Centre (NCSC), said in 2016 that "The biggest future threat we have is to keep talking about cyber security the way we do today"[6]. As noted by Microsoft, the language used by the cybersecurity industry – often opaque, highly technical and sensationalistic – only serves to create a barrier of understanding at a time when cybersecurity must become more inclusive[7]. Industry shares the responsibility of shifting away from alarmist and overly technical rhetoric to help SMBs feel empowered to manage their cyber risks effectively. AWS sees an important role for Government in leading this change.

In its 2016 cyber security strategy, the NCSC made a deliberate effort to avoid alarmist rhetoric and put in place consistent, actionable guidance on a single resource. By contrast, while there is an abundance of cybersecurity information available via Australian federal and state government websites, this information is spread across multiple departments and is inconsistent in style and substance[8]. This is reflected in the ACSC's own research. In a study commissioned by the ACSC and released in August 2020, only 36% of respondents were aware of and knew something about Scam Watch. The ACSC had a similarly low awareness rate at 31% of respondents[9]. The level of awareness for Stay Smart Online was even lower, at just 18%. A 2018 study by the MITRE Corporation, commissioned by AustCyber, found that:

> [T]he abundance of standards and guidelines available to Australian organizations at both the federal and state/territory level caused confusion around what advice should be adopted. "Cyberaware" organizations are overregulating, doing nothing, or applying a mixture of domestic and international standards for guidelines. The result is inefficient and is a barrier to improving Australia's cyber resilience. The Australian government can begin to address this issue by taking steps to harmonize the guidelines it provides to industry and other levels of Australian government.[10]

With the ACSC study also finding that there is a significant unmet demand for more information about cybersecurity, simplifying and consolidating cybersecurity messaging for SMBs is a substantial and meaningful contribution Government can make to improving Australia's cybersecurity. While we welcome the Government's suggestion of a program in the vein of the UK's Cyber Essentials certification scheme, we again caution against the introduction of new programs before existing initiatives have been properly implemented and assessed. Even with the success of Cyber Essentials, which has been in place since 2014, knowledge of Cyber Essentials as of 2020 among micro and small firms was just 10% and 23% respectively (compared to 40% for medium and large firms)[11]. On the basis of ongoing research and surveys to the effectiveness of the scheme, changes have been incrementally introduced over time.

[6] https://www.proofpoint.com/au/corporate-blog/post/three-goals-uk-new-cyber-security-strategy

[7] https://www.microsoft.com/security/blog/2019/04/08/the-language-of-infosec/

[8] https://www.aspistrategist.org.au/small-businesses-on-the-front-line-as-australias-cybersecurity-strategy-released/

[9] https://www.cyber.gov.au/sites/default/files/2020-12/ASD%20Cyber%20Security%20Research%20Report.pdf

[10] https://www.mitre.org/publications/technical-papers/analysis-of-nist-mds-practice-guide-for-australia

[11] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/893399/Cyber_Security_Breaches_Survey_2020_Statistical_Release_180620.pdf

We encourage the Australian Government to similarly take a long-term, evidence-based view to maximising the impact of existing programs. Having only been released in March and April of this year, the Cyber Security Assessment Tool and Cyber Security Business Connect and Protect Program are in their infancy and require the Government's commitment to implementing, maturing and supporting these initiatives over the longer term. The introduction of additional initiatives threatens to dilute the potential positive impacts of these programs.

Recommendation 4. Government should consolidate and simplify cybersecurity messaging and advice for SMBs.

Strengthening Cybersecurity Through Simplification

An important tool of government is conveying complex topics in a language and format readily accessible to non-experts, and we believe the Australian Government can make a substantial impact on cybersecurity in Australia through an approach that streamlines, simplifies, and effectively scales existing programs. As acknowledged earlier in this submission, regulation and corporate governance play a vital role in ensuring risks are appropriately managed and transparency is maintained, but these take time to implement and achieve their desired outcomes. We believe the Australian Government should allow ongoing regulatory reforms to take effect before the introduction of additional measures; concurrently, we believe there are steps Government can take to improve community and businesses engagement in cybersecurity:

1. The development of a 'single door' for cybersecurity advice and guidance. Although cyber.gov.au is ostensibly intended to be this resource, advice relating to cybersecurity can be found across multiple government departments or agencies. Consistent, clear, and 'plain language' messaging pointing to a single well-structured resource would be hugely beneficial to SMBs in particular.
2. Government could also use the existence of this single resource to clearly delineate the responsibilities for cybersecurity between departments and agencies. Assisting individuals and entities in knowing when, how and with whom to engage would be a significant step forward in establishing a strong public-private trusted partnership model.
3. A single platform would also allow Government to more effectively amplify the existence of ongoing programs and initiatives. As noted in the ACSC report cited earlier, awareness of existing initiatives is quite low. Consolidating these resources and communicating the existence of a single source should see an increase in that awareness.
4. We believe that guidance helping SMBs make more informed technology investment decisions that will open them to the advantages of the digital economy, while reducing their cybersecurity risks, would also be a beneficial and welcome resource for these entities.
5. As part of a holistic program, we also see an opportunity to integrate cybersecurity education and training to schools and non-cybersecurity programs. While addressing the cybersecurity skills gap is important, we believe that having a cybersecurity literate society and broader workforce is equally – if not more – important for reducing cybersecurity risk over time. The need for a cybersecurity literate workforce is reinforced by findings from a recent report commissioned by AWS and prepared by AlphaBeta, which found that 64% of Australian workers already apply digital skills in their jobs[12].

Investing in digital skills will remain an important initiative for the Australian Government, with the same study finding that Australia will require an additional 6.5 million digital workers by 2025 to keep pace with technological change. Of those, cloud architecture design and cybersecurity are anticipated to be two of the top five in-demand digital skills in Australia. We encourage Government to continue supporting and promoting the Cyber Security Skills Partnership Innovation Fund, and look forward to partnering with Government on developing Australia's digital workforce.

[12] https://alphabeta.com/our-news/australias-need-for-65m-digital-workers-in-the-next-four-years/