Amstelveen

What Australia and its Six Cyber Shields must get right

Following the 2023-2030 Australian Cyber Security Strategy Discussion Paper and anticipating the official release towards the end of 2023, the Minister for Home Affairs and Cyber Security, the Hon. Clare O'Neil MP, recently outlined Australia's cyber posture through six "shields". The strategy outlines how we will remain resilient amidst a malicious cyber environment. This article summarises the proposed strategy and outlines the key risk considerations in its implementation.

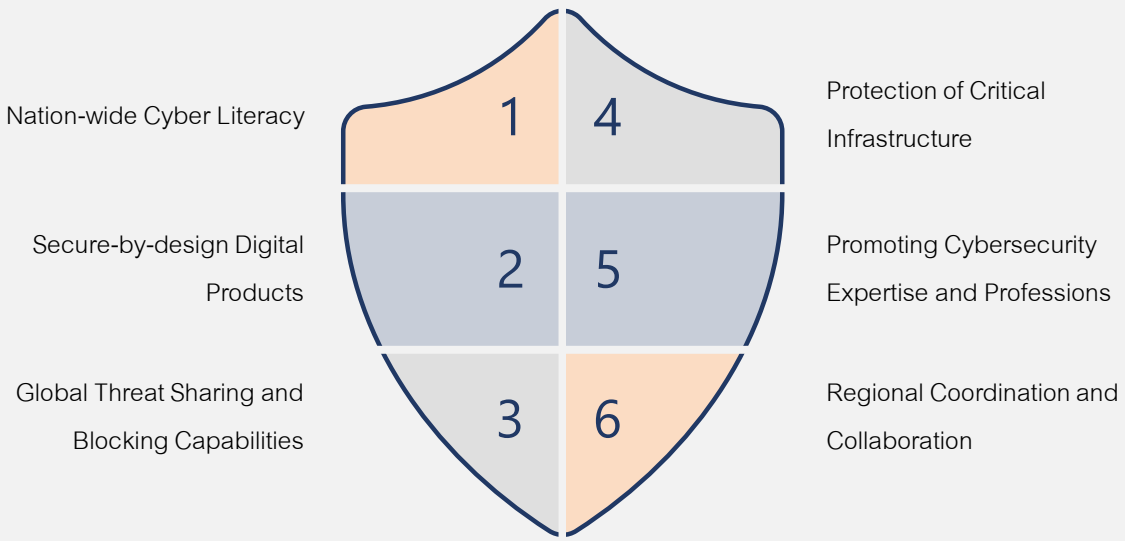
BY ANDREW MILLWARD, OBED OEI & JAYASHRI SOOD

Introduction

We have been anticipating the 2023-2030 Australian Cyber Security Strategy since its development was first announced late 2022 by the Hon. Clare O'Neil MP, Minister for Home Affairs and Minister for Cyber Security. The topic has since evolved through a discussion paper, inviting industry experts and organisations to respond, before its final release expected at the end of 2023. The July appointment of Air Marshal Darren Goldie as Australia's national cyber security coordinator was also welcomed with high expectations, as it revealed a systematic and operational shift in how Australia will respond to cyber incidents. To round it all up, and as the topic of this article, the Minister recently presented at the 2023 AFR Cyber Summit (18th September 2023), revealing the **first plans for how the cyber strategy will be executed**, motivated by a heightened push for a government-led and coordinated capability, in the wake of Australia's recent cyber-attacks. These developments come at a time where the national cyber threat grows exponentially year on year, in-line with the rapid evolution of smart technologies and the increasing number of internet-connected devices circulating personal data.

What do the first plans of the Cyber Strategy look like?

The uplifted national cybersecurity strategy centres on six shields (key areas) that Australia must get right, from now up until 2030 and beyond, to ensure we are equipped for a constantly changing and malicious cyber environment. The six cyber shields are designed with the aim of better protecting both citizens and organisations, through the following:



1. Nation-wide Cyber Literacy

Uplifting and empowering Australians and businesses of all sizes to understand the cyber threat and feel empowered to take the necessary actions when they fall victim to cyber-attacks. The two-pronged approach consists of establishing the right support networks and a long-term education plan.

We will be very interested to see how training and education programs will be executed. Appreciating differing levels of cyber literacy across individuals and businesses, education must be simple, yet effective. We also expect increased promotional material surrounding the Australian Government's cyber support networks, such as the Cyber Security Hotline, and heightened involvement from the Australian Federal Police in responding to higher frequency reported cyber-crime. Much like how Australians know to instinctively call '000' or the poisons hotline in emergencies, it will be extremely useful to know what the process is and which hotlines to contact should they fall victim to cyber-crime. As a side note, regulators are also interested in the topic. ASIC will be placing greater accountability for senior management and Board members regarding cyber literacy and involvement in incident response and testing.

2. Secure-by-design Digital Products

Digital software and their providers will have to abide by minimum global security standards in the development and release of their solutions, such that these products can be used by everyday consumers confidently and safely.

Consistent with an earlier April announcement from Australia, Canada, Germany, the Netherlands, New Zealand, the UK and the US, these 'global' standards will be formulated, tried and tested collaboratively. Australia's track record in setting global standards (via 'Standards Australia' and being a founding member of ISO) will place us in a capable light. We expect that the standard(s) should align to pre-existing, well-known standards (e.g., ISO 27k), and/or replace disparate existing ones to avoid compliance burden. A balancing act will also likely happen between geopolitical actors, to achieve a truly global stance.

3. Global Threat Sharing and Blocking Capabilities

Threat Intelligence will be another core factor for fulfilling the Cyber Strategy. This will consist of near real-time monitoring and communication capabilities between key government and business agencies on and offshore to ensure threats are blocked before they cause any harm.

Investment into this area will likely fall into areas such as centralising and automating the services that support citizens and businesses in responding to, managing and recovering from cyber crime. As attackers utilise disruptive technologies (e.g., Artificial Intelligence and robotics) to expedite offensive capabilities, it is critical that the government also invests in innovating processes related to collating, validating and sharing threat intelligence, to accelerate response times. In doing so, we will naturally see an uptake in reported cases of cyber crime, as escalation processes and mechanisms are streamlined. This will be a positive indicator and a contrast to the past where many organisations have had to navigate up to 30 different agencies and entities when coordinating their major breach response.

4. Protection of Critical Infrastructure

Another key aspect of the national strategy proposes increased restrictions to critical government infrastructure. The intended approach includes the uplift of foundational security controls within both government departments and public agencies.

We expect these minimum controls to have elements of governance (including risk assessments and profiling), prevention (e.g., firewalls and appropriate access restrictions), monitoring (threat intelligence) and (incident) response. These foundational security controls are pivotal in:

- Understanding how to identify and continuously assess the risk profile of critical infrastructure (Governance);
- Restricting physical and logical access to these assets (Preventive controls);
- Ensuring we are vigilant on all angles and threat vectors (Monitoring via threat intelligence); and
- Ensuring we are ready to respond at any time (Incident response).

SME discussions further indicate that a big focus also remains on the Security of Critical Infrastructure (SOCI) Act to uplift practices and processes across the industry given, disruption of critical assets is a major risk for government.

5. Promoting Cybersecurity Expertise and Professions

A pivotal component of Australia's cybersecurity response plan also revolves around increased promotion from government and organisations to grow and nurture interest in the cybersecurity profession from a grassroots level.

We anticipate an evolving focus for organisational talent attraction and retention campaigns to ensure that technology roles, particularly security and innovation related roles, are sponsored adequately. This will ensure organisations are continuing to not only build out security SMEs but also security capabilities and education across younger and newer team members. A critical indicator for success will be that every technologist becomes a cyber security expert. Much like law and medical programs make ethics compulsory, so should privacy and cyber security be within every technology degree or diploma.

6. Regional Coordination and Collaboration

The final pillar of the government's cybersecurity approach includes boosting regional inter-country coordination and collaboration to share key learnings with friendly neighbours and dissipate silo mentality.

Australia's reputation as one of APAC's core leaders means that there will be high expectations for our security posture and how we will lead the broader region towards secure capabilities. We will be leaned upon by our neighbours to drive coordinated and collaborative responses to cyber security incidents across and within our sovereign borders and the development of a joint strategy from the Minister will likely be in the works – to be presented and discussed at regional summits. At minimum, we would expect the following to be carefully considered in the development of the joint strategy:

- How participating nation-states collaborate despite varying security priorities and resources;
- Expectations onto actors in midst of varying capacity and capability; and
- Varying adequacies, appropriateness and baseline security of infrastructure across the region.

Conclusion

The cyber landscape is hostile and the rate and impact of malicious cyber attacks across and within sovereign geopolitical borders will continue to increase. Australia is not unique in this plight, but it is encouraging to see that our government has chosen to take the matter seriously through the establishment of its 2023-2030 Cyber Security Strategy, among other initiatives. This cohesive government-led strategy will be Australia's best shot at minimising our exposure to digital risks and to protect our most critical infrastructure. However, it requires duality of effort between the government and its people (and businesses), such that all must continue to uplift proficiency and commit resources to security initiatives, in alignment with the broader principles of this national strategy. Moving cross-border, there is further merit in prioritising international collaboration with other governments and non-government actors to tackle what is in essence a global risk. Australia will do this first through its presence in the APAC region, but will only continue to evolve, hopefully matching the evolution of the topic.

Our Authors

Andrew Millward
Director

Andrew is a technology risk and information security professional with ten years of experience in risk management, internal audit and information security. He has worked in a variety of roles advising and supporting risk management functions, internal audit, project teams, steering committees and project sponsors of large Australian corporations.

Obed Oei
Senior Manager

Obed has over seven years of experience in technology and operational risk, business analysis, and cyber assurance. He has supported clients across many industries through external/internal audit of their system and business processes, and has delivered risk and controls transformation programs, as well as GRC implementation projects.

Jayashri Sood
Senior Consultant

Jay is a Senior Consultant with over three years of experience in technology risk, assurance, contract risk and business analysis. As part of her work with Amstelveen and major consulting firms, Jay has been involved in end-to-end internal and external IT audits, including software licensing and cyber security reviews, across the financial services industry and a range of other industries.

Amstelveen

Amstelveen equips organisations to identify, assess and mitigate their most significant risks. Our risk, compliance and technology professionals support clients to improve the governance of their organisations. We provide specialist support to the largest public and private organisations in Australia and New Zealand.