Australian Chamber of Commerce and Industry

Charting New Horizons: Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy

ACCI Submission

29 August 2025

Australian Chamber of Commerce and Industry

Working for business.
Working for Australia.

Telephone [redacted] | Email [redacted] | Website www.acci.com.au

Media Enquiries
Telephone [redacted] | Email [redacted]

Canberra Office
[redacted]

ABN 85 008 391 795

Australian Chamber of Commerce and Industry

Table of Contents

Australian Chamber of Commerce and Industry

Introduction

Developing our vision for Horizon 2

2.1 Outlook for Horizon 2

What trends or technology developments will shape the outlook over the next few years and what other strategic factors should Government be exploring for cyber security under Horizon 2?

There has been a marked increase in cyber-attacks and fraud (via technology) on SMEs, as larger businesses are typically more mature in their cyber resilience, as evidenced by ACSC statistics. Nevertheless, larger corporations remain targets, and high-profile cyber-attacks remain a risk for business. One crucial area of concern is the reduced barriers to create mis- and disinformation, enabled by artificial intelligence technologies. To combat this, the government needs to build mechanisms that support the integrity of communication, which can include supporting and encouraging the adoption of technologies.

2.2 Collaborating across all levels of Australian Government

Are there initiatives or programs led by State or Territory governments you would like to see expanded or replicated across other levels of government?

On the whole, cyber security is an issue of national and international importance: harmonising approaches to cyber security uplift should be undertaken first and foremost at the Commonwealth level, to ensure uniformity of approach.

There are many initiatives at State and Territory level which are delivering important work related to cyber security, particularly in respect to upskilling: Victoria's SummerTech Live connects SMEs with university students, with the objective of uplifting their use of technology, however the participation linked to cyber was limited. South Australia's Cyber Uplift Step Program attempted to raise the cyber capability of SMEs.

Victoria's *Digital Jobs* program re-skilled over 5,000 mid-career Victorians for jobs in the digital economy – this program was well received, and some companies permanently hired staff they received through the initiative.

2.3 Monitoring progress in a changing world – a conceptual framework for evaluating cyber security outcomes

Does the high-level Model resonate, and do you have any suggestions for its refinement?

On the whole, the high-level model is a good approach: it is focused on concrete and outcomes-based actions, and takes the whole of economy into consideration, showing clear roles for government and industry. The topic remains very challenging, to the extent that we need a set of metrics to measure the cyber uplift capability of SMEs. This is typically very difficult to measure, as businesses tend to be secretive about their cyber situation.

Australian Chamber of Commerce and Industry

Shield-level focus for Horizon 2

3.1 Shield 1: Strong businesses and citizens

What could government to do better target and consolidate its cyber awareness message?

Government publicity initiatives under the Cyber Security Strategy have been useful in so far as they have been presented in clear and easy-to-understand language, with clear, actionable points to raise the standard of cyber security among businesses and individuals. The *Act Now, Stay Secure* campaign, now in its second year, is a good foundation for getting the message out to Australians. However, it remains unclear to what degree the campaign has markedly raised cyber awareness.

Targeted campaigns can be helpful, to the extent that they include nuances relevant for specific sectors or groups, e.g. small business, NFPs. One such example is the *Stop the Hack* campaign delivered under the Executive Cyber Council's Working Group on Small and Medium Business.

How can Government encourage SMBs and NFPs to uptake existing cyber resources (i.e. Small Business Cyber Resilience Service, Cyber Wardens, ACNC guidance etc.)?

One of the main hurdles to raising the cyber security levels in SMBs and NFPs is awareness of the seriousness of cyber risk. On top of this, burdensome red tape and the high cost of doing business push cyber risk and cyber security down the list of priorities for SMBs and NFPs in Australia today.

Government could leverage the position of industry associations to communicate and support SMBs in protecting their business from cyber threats, building on existing networks and using existing materials. The use of simple guidance on cyber security steps, or interactive checklists, can be useful in this regard. Furthermore, tangible incentives to participation can help, e.g. grants for investing in cyber security products and consultations, or tax breaks for upskilling programmes. In the context of cyber security, which is built on trust, SMEs need to find entities and providers whom they trust: trusted institutions such as universities offering internships with SMEs can help uplift their cyber resilience.

What existing or developing cyber security standards, could be used to assist cyber uplift for SMBs and NFP's?

There are already many resources available to support business in raising their level of cyber security, including the ASD's Essential Eight. International standards are also available and widely used in Australia, e.g. ISO/IEC 27001 (information security and management systems). The issue is not with the existence of standards, but their availability to industry, especially SMBs and NFPs. More work should be done to communicate these standards to business.

In addition to this, cyber security in medium and large enterprises is a board governance responsibility. Unlike accounting standards, there is no standard framework for Boards on cybersecurity and elements like Penetration Testing. Accounting standards, and Annual Reports with Financial Statements, have been agreed over decades, whereas cyber lacks that maturity – if Boards had agreed standards, they could enforce those standards through their supply chain as well, uplifting the whole of economy including small businesses. There may be some merit to investing in standards that Boards could adopt. There are also some private sector initiatives for SMEs that could be adopted, e.g. SMB1001:2025.

Australian Chamber of Commerce and Industry

Do you consider cyber insurance products to be affordable and accessible, particularly for small entities? If not, what factors are holding back uptake of cyber insurance?

Low awareness of cyber insurance and limited understanding of cyber risk continue to constrain uptake among SMBs. Many operators struggle to assess the value of cyber insurance, especially when they lack clarity around their digital risk exposure. First-time buyers may also be unaware of the support insurers provide across the incident lifecycle, including threat intelligence, security assessments, and access to expert resources.

Cyber insurance should be viewed as one element of a broader cyber defence strategy, not a standalone solution. SMBs need to balance insurance costs with investment in preventive measures, which can also help reduce premiums. Improving cyber literacy will support more informed decisions around purchasing and claims.

Pricing is influenced by the business's risk profile, industry, data sensitivity, supply chain exposure, and claims history, as well as broader market dynamics such as rising ransomware incidents and competitive pressures.

A deeper understanding of SMB awareness and adoption of cyber insurance would help identify opportunities to strengthen resilience and improve coverage across the sector.

How well do you consider you understand the threat of ransomware, particularly for individuals and small entities? How is this threat evolving or changing?

It is typically very difficult to get data from businesses on ransomware, and justifiably so. There is a perception that ransomware seems to be less of a focus, with extortion of personal identifiable information (PII) becoming more of a priority.

How could the government further support businesses and individuals to protect themselves from ransomware attacks?

As with other cyber threats, a major issue with ransomware attacks is awareness of what to do when such a situation arises. The government introduced and passed legislation on ransomware attacks and struck a good balance between the threshold for reporting ($3 million turnover) and the trigger to report (payment actually made).

However, more support is needed for businesses at the critical point in time when a ransomware attack is received, and before a payment is made. Clear and accessible guidance can help a business make the right decisions, understand their obligations, and know what support is available. This guidance could come in the form of a step-by-step playbook on 'what to do in the case of an attack', tailored to SMBs.

Which regulations do you consider most important in reducing overall cyber risk in Australia?

In addition to the reforms to cyber security legislation passed in the previous Parliament, long-awaited reforms to the Privacy Act are necessary. Updating the Privacy Act should uplift data protection obligations and practices in Australia. It is critical that a balance is struck between the necessary steps to ensure personal data is treated correctly and protected (including by technical and organisational means, i.e.

cyber security measures), and the need to avoid overburdening SMBs. To this end, a cascading approach could be considered, whereby smaller businesses would be required to comply with commensurately lesser obligations than larger businesses.

Have regulatory/compliance requirements negatively impacted the cyber maturity of your organisation? How are you currently managing these issues?

From a general perspective, increasingly burdensome regulation and compliance obligations reduce a business' time and resources which could be spent on upgrading systems and investing in cyber awareness and protections (e.g. data protection software). Where possible, obligations and reporting requirements (e.g. in the case of an incident) should be streamlined, and compliance toolkits / checklists could be a useful support.

3.3 Shield 3: World-class threat sharing and blocking

What could government do to support and empower industry to take a more proactive cyber security posture to ensure the resilience of our cyber security ecosystem? What do you think Australia's proactive cyber security posture should look like for industry?

Increasing industry access to threat intelligence, as well as actionable steps to be taken to protect against new developments, should be considered as a way in which to bring business up to speed with the most prescient developments in cyber threats, and how to protect against them. This is part of building relationships and an environment of trust between all stakeholders, which is a prerequisite for a mature cyber secure ecosystem.

Practically, timely and brief reports provided to impacted sector peak bodies could be useful for the dissemination of information through existing networks along with public quarterly reports which also monitor trends over time.

3.4 Shield 4: Protected critical infrastructure

How effective do you consider the SOCI Act at protecting Australia's critical infrastructure? Are the current obligations proportionate, well-understood, and enforceable?

The SOCI Act was subject to major changes in the 2024 Cyber Security Legislative Package, including expanding the scope of application. The new legislative changes are too recent to be able to undergo a thorough assessment.

Is the regulatory burden on industry proportionate to the risk and outcomes being sought?

The main issue with dealing with cyber security incidents as a SOCI entity remains the overlapping and duplication of reporting obligations, including timelines, required information, and public bodies to whom information should be provided. The Government's **Single Reporting Portal** (provided by the ASD) is a useful tool for all types of business to know their respective obligations in case of a cyber-attack or data

breach – however it is not clear if the broad business community is aware of this resource. Further publicity would help make this important tool more widely known and used.

3.5 Shield 5: Sovereign capabilities

What role should government play in supporting the development and growth of Australia's cyber workforce? What initiatives, pilots or policy ideas do you think would best support industry to grow?

Considerable work is already underway to raise the standard of Australia's cyber workforce, both in the tertiary education and VET sectors. Initiatives developed by the Jobs and Skills Councils (e.g. Future Skills Organisation) are critical to direct training needs as defined by industry and government.

Nevertheless, the disciplines related to cyber security are diverse, disparate and constantly evolving in respect of technical skills: hundreds of pathways representing numerous specialisations and levels of expertise exist and are certified by hundreds of professional organisations and bodies. An individual can specialise in, among others, communication and network security, security architecture and engineering, security and risk management, security operations, testing etc. As such, there is no clear picture of what is meant by a cyber security expert or professional. Greater understanding of the specialisations and the present and future needs of the economy is required.

What have been the most successful initiatives and programs that support mid-career transitions into the cyber workforce and greater diversity in technology or STEM-fields more broadly?

Two initiatives (one at Commonwealth level, another in Victoria) are particularly pertinent examples:

- Federal Government's mid-Career CheckPoint was a welcome program for mid-career reskilling
- Victoria's *Digital Jobs* program re-skilled over 5,000 mid-career Victorians for jobs in the digital economy

What are some of the industries with highly transferrable skill sets that could be leveraged to surge into the cyber workforce? Is there any existing research/data that could support these efforts?

There is often a misunderstanding of IT, and specifically cyber, skills. Typically, the skills required take a number of years to develop.

How can industry, academia, think tanks and government best work together to set research priorities and drive innovation to further our strategic, economic and community interests and achieve our common goals?

Building on the model of the Executive Cyber Council, roundtables could be established to bring together academia, industry and government to identify and fund the most relevant and impactful research projects.

About ACCI

The Australian Chamber of Commerce and Industry represents hundreds of thousands of businesses in every state and territory and across all industries. Ranging from small and medium enterprises to the largest companies, our network employs millions of people.

ACCI strives to make Australia the best place in the world to do business – so that Australians have the jobs, living standards and opportunities to which they aspire.

We seek to create an environment in which businesspeople, employees and independent contractors can achieve their potential as part of a dynamic private sector. We encourage entrepreneurship and innovation to achieve prosperity, economic growth, and jobs.

We focus on issues that impact on business, including economics, trade, workplace relations, work health and safety, and employment, education, and training.

We advocate for Australian business in public debate and to policy decision-makers, including ministers, shadow ministers, other members of parliament, ministerial policy advisors, public servants, regulators and other national agencies. We represent Australian business in international forums.

We represent the broad interests of the private sector rather than individual clients or a narrow sectional interest.

ACCI Members

State and Territory Chambers

Industry Associations

Australian
Chamber of Commerce
and Industry