AiGROUP

2023-2030 Australian Cyber Security Strategy

SUBMISSION - April 2023

Building cyber capability in Australian industry

Ai Group welcomes the opportunity to respond to the 2023-2030 Australian Cyber Security Strategy Discussion Paper.

Below is a summary of key themes and recommendations as they relate to the *2023-2030 Australian Cyber Security Strategy Discussion Paper*.

Key points:

- Australian industry is engaged with and actively investing in cyber security, however there is a wide range of cyber capabilities between businesses. Gaps remain particularly for smaller enterprises and more traditional industry subsectors.
- There are major opportunities for Australia to become a leading cyber capable nation, but it will require targeted investments. Developing the cyber capability and digital skills of the workforce – both for specialist and generalist roles – will be critical, as will building the depth of the national cyber ecosystem.
- Regulatory measures should consider the balance of security and business innovation. Businesses facing cyber-attacks are victims and should be treated as such. Regulation should be designed in a way that is practical for widespread uptake amongst industry and supports broader digital upgrading.
- Collaborative government support is also needed to help uplift cyber capability, particularly for smaller businesses. Investments in informational resources, skills, incident recovery and ecosystem development will all augment current efforts by industry.

Cyber capability development in Australian industry

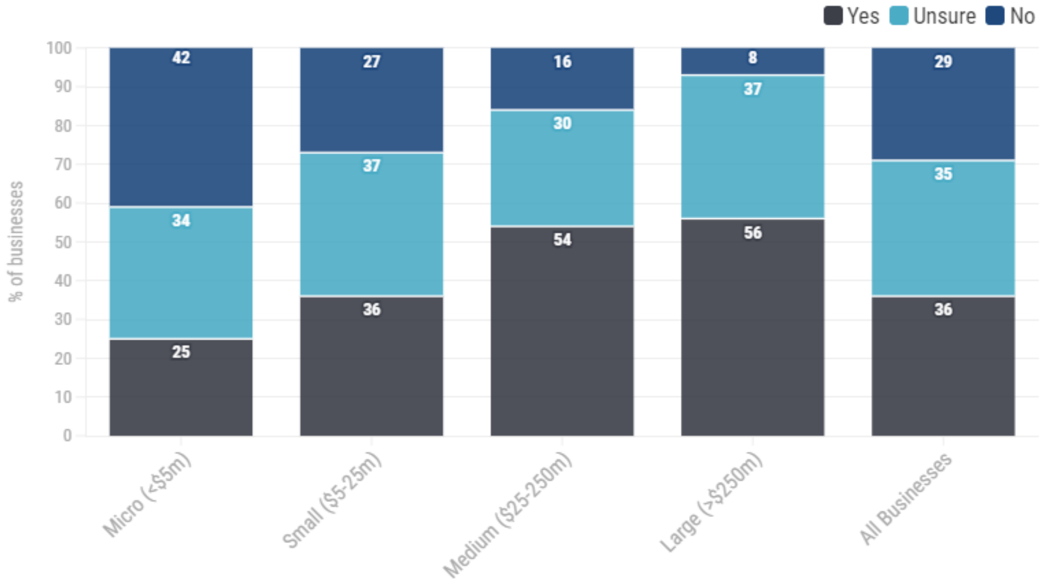
Cyber capability is an essential requirement for contemporary business, and awareness of cyber issues is well developed in industry. Even so, there is a wide range of digital maturity across these businesses in the approaches to assessing, learning, implementing and improving digital capabilities. While cyber capability already has traction in Australian industry, there is considerable room for growth.

Data on the uptake of cyber capabilities in industry is available from Ai Group's futuremap® platform, a business diagnostic designed to assist manufacturers and related industries to adopt Industry 4.0 practices. Since its launch in 2018 by the Innovative Manufacturing Cooperative Research Centre (imcrc), nearly 1200 Australian businesses have completed the futuremap® tool.

Utilising the data gathered through futuremap®, Figure 1 below provides an assessment of cybersecurity in the manufacturing and related industrial sectors. It shows that:

- 36% of Australian industrial businesses report having effective cybersecurity systems and technology, and 29% report not having effective cybersecurity.
- Cybersecurity effectiveness increases with business size. Only 25% of micro-businesses report effective security, while over half of medium and large businesses do.
- For all business sizes, approximately one-third of businesses are unsure if their cybersecurity systems and technology are effective.

Figure 1: Businesses with effective cybersecurity technology and systems

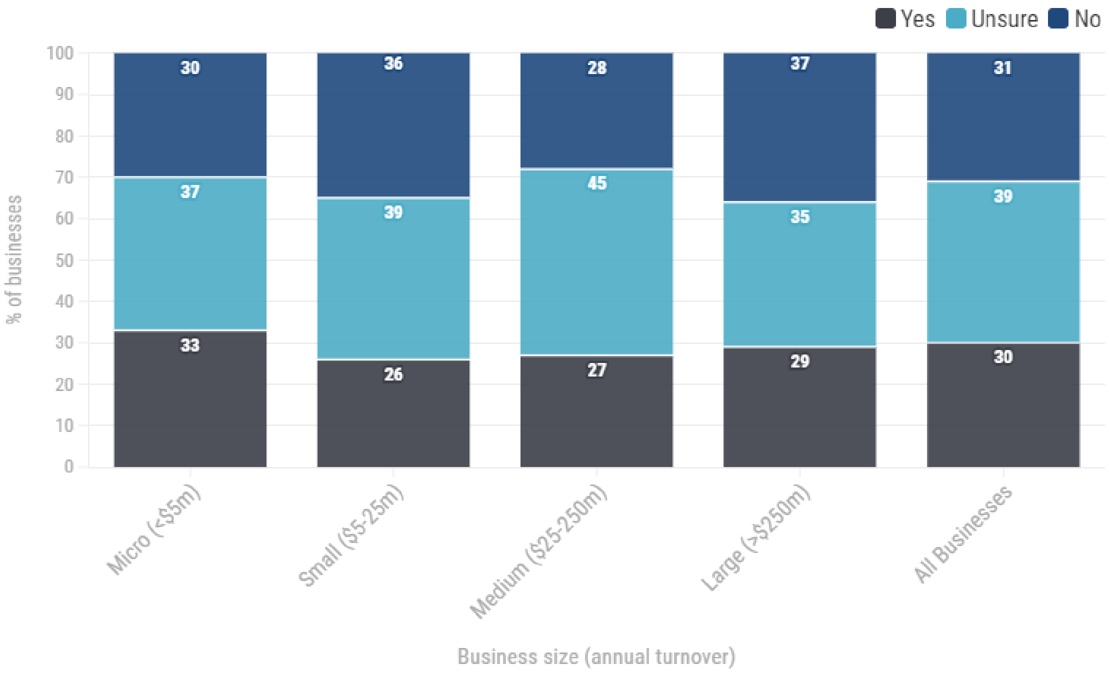


Source: Ai Group imcrc futuremap

The basis of strong business cyber capability lies within the digital skills of the workforce. Digital skills comprise both those required in technical roles as well as broader digital literacy across the workforce. Just under one-third (30%) of industrial businesses report that they have the needed digital skills embedded within their organisation (Figure 2). Another third report they do have embedded skills, and a further third are unsure.

Businesses of all sizes report similar levels of digital skills embeddedness. This suggests that digital skills gaps are a generalised problem in the Australian economy, affecting businesses of all sizes relatively equally.

Figure 2: Businesses with digital skills embedded across the organisation

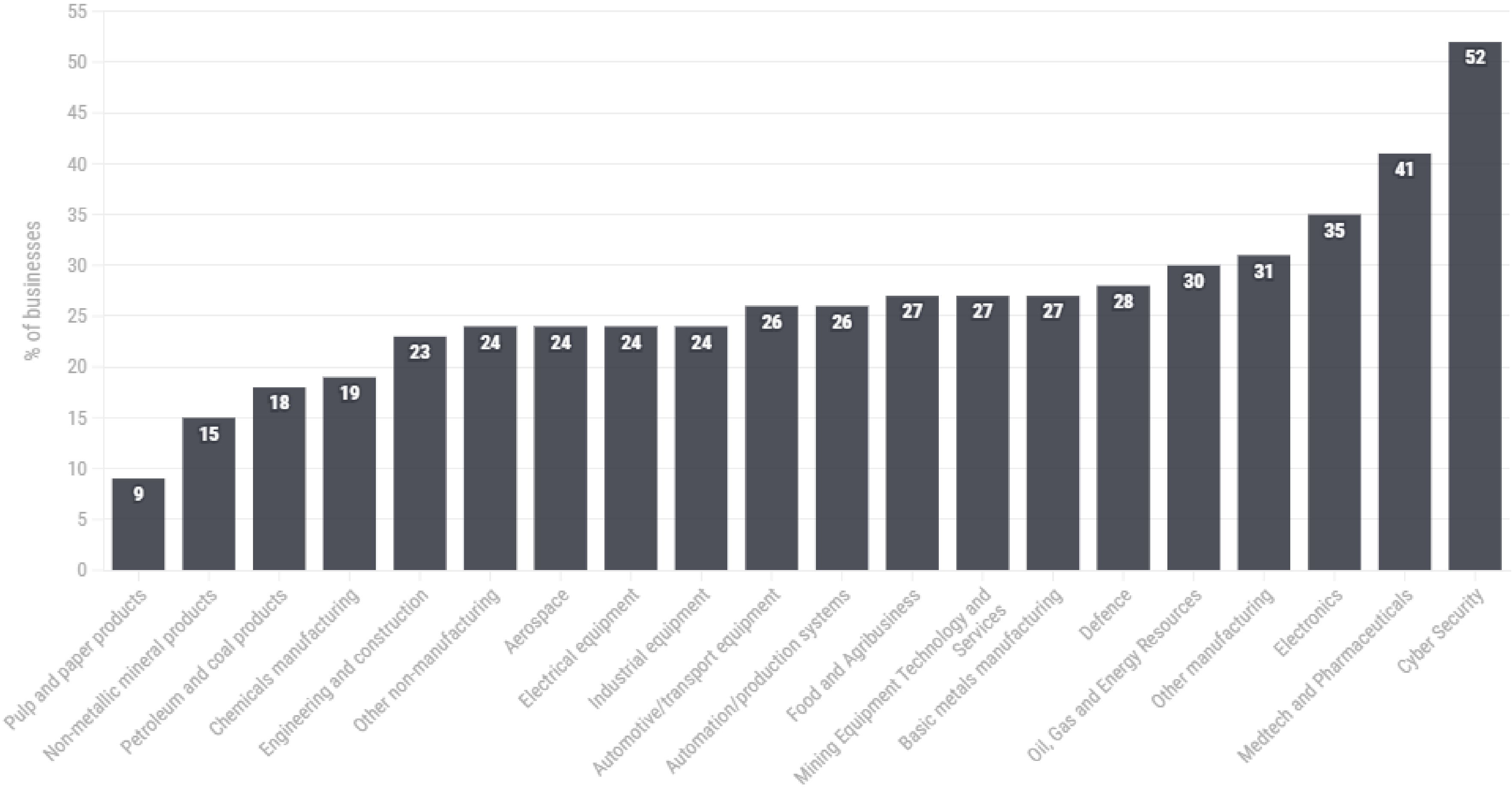


Source: Ai Group imcrc futuremap

There are significant variations in the effectiveness of cybersecurity practices between industry subsectors (Figure 3). According to Ai Group's futuremap® data, the cybersecurity industry itself is the strongest, with 52% of businesses reporting effective technology and systems. There is a clear relationship between an industry's technology-intensiveness and cybersecurity effectiveness. Those which report higher scores – such as medtech, electronics, energy and defence – are all technology-intensive industries. Those reporting lower scores tend to be in simpler materials processing, construction and basic equipment industries.

This indicates that cybersecurity effectiveness is correlated to the technological sophistication of business, with greater need for uplift in more traditional sectors of the economy.

Figure 3: Businesses with effective cybersecurity technology and systems, by industrial subsector



Source: Ai Group imcrc futuremap

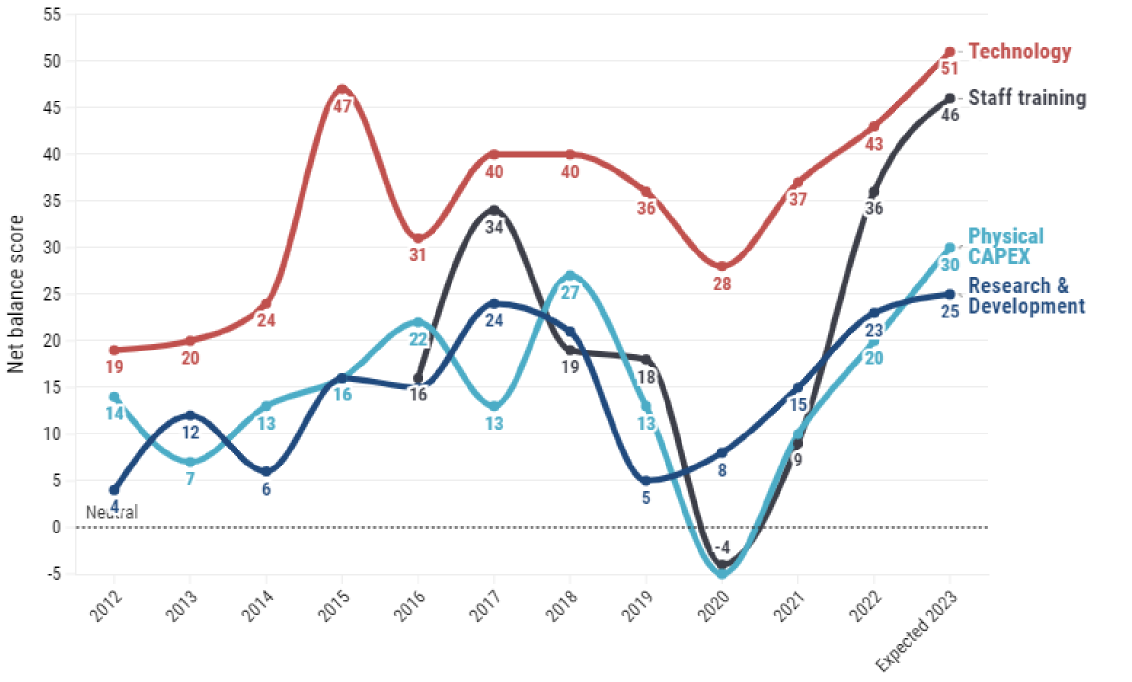
Business investment in digital and cyber capabilities

Australian industry recognises the challenges posed by cybersecurity, and business is investing aggressively in building cyber capabilities. Data collected in the most recent Ai Group CEO Outlook Report provides an indication of how business leaders rank digital investment priorities in 2023. According to the survey data:

The majority of Australian business intend to increase their technology investments in 2023, with 56% of intending to raise their spend and only 5% planning to reduce. Technology remains the top business investment intention for 2023, and the indicator is currently at the highest level in the decade since the survey has been conducted.

Half (50%) of Australian businesses intend to increase their staff training investment in 2023, and only 4% will reduce it. Staff training is ranked a close second behind technology as an investment priority, and is also at an all-time high. It has leapt ahead of more conventional investment intentions such as physical CAPEX and R&D.

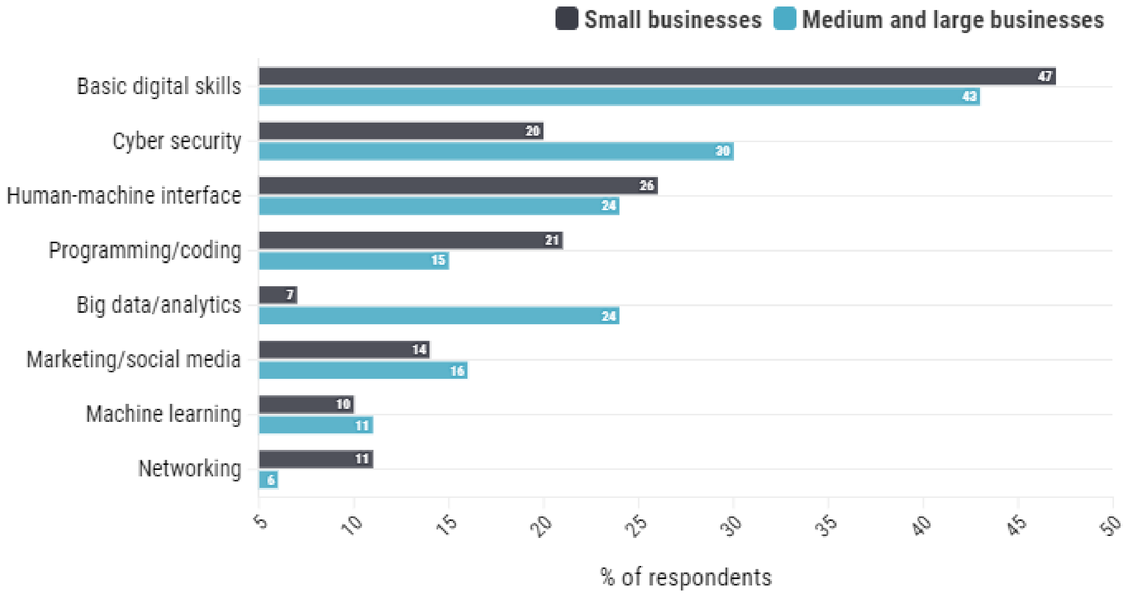
Figure 4: Business investment indicators 2012-2023



Source: Ai Group CEO Survey

Within the domain of staff training, cyber security also ranks highly as a business investment priority. According to data from the Ai Group Skills Survey in 2022, basic digital skills were the primary digital skill need identified by business leaders (Figure 5). However, cyber security skills ranked a close second, identified as a top workforce skills priority by 20% of small and 30% of medium and large businesses. Basic and cyber digital skills are also closely linked, as a business's cyber capability relies both on improving cyber-specific skills in specialist roles, and ensuring basic digital skills are in place across the broader workforce.

Figure 5: Top ranked digital skills investment priorities of business



Source: Ai Group Skills Survey 2022

This recent increase in investment intentions for technology and digital skills provides an opportunity for a significant cyber capability uplift in Australian industry. As businesses increase their digital investments, cyber capabilities will clearly rank at the top of the list.

Feedback from Ai Group members suggests that the type of capability targeted will vary between businesses based on their size:

- **Small and medium enterprises** often rely on commercial providers for their cybersecurity technology and systems. They are seeking effective, affordable and trusted cyber advice and services from specialised providers. They will have relatively few in-house IT specialists, and the digital skills uplift required for their workforce will focus on basic digital skills to utilise cyber technology and practice appropriate digital hygiene. They may find it challenging to determine what cybersecurity services they require, and decide the appropriate size and scope of cyber investments.
- **Larger enterprises** typically have a greater share of their cybersecurity capabilities in-house. They are seeking a supply of skilled cyber professionals to manage technology and systems, augmented by commercial services in more advanced areas of enterprise-specific need. They will need to manage the interaction of enterprise platforms with external services, and address the human dimensions of cybersecurity across a large and diffuse workforce. They may find it challenging

to recruit and retain cyber professionals, and map their systems' exposure to current and emerging threats.

Ensuring regulation helps augment industry cyber capability uplift

Ai Group agrees there is a need to update Australia's digital and cyber regulations as part of the National Cyber Security Strategy. Increases in the frequency, severity and sophistication of cyber incidents warrant the development of more contemporary regulatory frameworks. The increasing digitalisation of the economy – across both consumer and industrial sectors – will bring transformative opportunities for Australia while also posing greater cyber exposure. Keeping cyber regulation up to date with this evolving landscape is critical for national economic security.

However, all regulation inherently involves striking a balance between security and efficiency. While under-regulation leaves Australia exposed to cyber risk, over-regulation will stifle innovation and new opportunities in the digital economy. It is especially important that regulation be supportive of the efforts by industry to augment its cyber capabilities, as the practices of business are one of the front lines of national cyber security.

Ai Group makes the following recommendations regarding principles for the updating of Australia's various regulatory frameworks for cyber security:

Legislative vs collaborative policy instruments: There is an appropriate place for legislative instruments to set national cyber security standards, particularly in mandating core operational practices. However, legislative instruments can date too quickly in the face of evolving technologies, and can be difficult to define and enforce.

Government should complement legislative instruments with other collaborative policy measures that guide, support and collaborate with businesses to improve enterprise capability. Government should give proper consideration to non-regulatory options to address inhibitors that reduce the incentive for business to invest in digitalisation and cyber security. Where legislation is used, language should be clear, direct and practical for implementation by industry.

Obligations upon company directors: Ai Group does not support making cyber security risks and consequences a specific obligation of company directors.

Companies face a range of risks (including but well beyond cyber), and the nature of cyber risks varies widely between businesses and industries. Existing obligations of company directors already appropriately recognise risk in the 'duty of care and diligence' (per s180(1) of the *Corporations Act).* The creation of an additional and distinct obligation upon directors would not create additional incentives for cyber capability uplift, while potentially exposing directors to liability in cyber incident situations where the company is a victim of a crime.

It should also be noted that digitalisation is both an opportunity for Australian companies (in terms of innovation in products and processes) and a risk (in terms of cyber security concerns). Company boards should be encouraged to take a holistic view of digital transformation, which embraces the opportunities it presents while appropriately managing new risks posed. A specific obligation on company directors regarding cyber security risks would improperly pose digitalisation as a negative factor, and potentially deter the digital innovations necessary for national economic advancement.

Explicit obligations of confidentiality upon Commonwealth agencies: During a cyber incident an explicit obligation of confidentiality upon the ASD and ACSC is essential. Businesses need to be confident that they are not subjected to unnecessary reputational damage while they are victims of cyber threats. Government needs to ensure a level of trust in the organisations designed to work with business. Language around cyber incidents needs to be collaborative and supportive, not accusatory.

Expansion of mandatory cyber incident reporting: The purpose of mandatory cyber incident reporting is to manage threats which are potentially large-scale, complex, and/or affecting critical infrastructure. Mandatory incident reporting is not designed, nor should be used, to improve public understanding of the nature of cybercrime. This objective should be pursued through appropriate public education campaigns. The scope of mandatory incident reporting should be determined principally based on the consideration of systemic risk management and compliance costs for business.

Regulation of business data collection: There are some businesses for whom the collection of customer data is the business model, and others where it is a result of usual business interactions. There is no one size fits all solution to managing cyber security and data collection, and needs to be treated differently depending on its function within a business.

For those collecting and storing data as a consequence of usual business, there is a reasonable expectation that businesses should engage in data minimisation for consumer protection. Reducing information that can be collected, how long it can be stored for and how it is stored, is useful in limiting the volume of data that can be exposed during cyber incidents.

However, in many industries, innovative business models require the use of customer data to make business decisions more effectively. The ability to do so currently and into the future is a legitimate international competitiveness and innovation requirement and should be considered when holding and using consumer data. Consideration should be given to future innovation using data collected as a part of normal business, and whether it should be discarded or held for future use.

Privacy and data stewardship: Ai Group supports the need to provide the public with confidence that their privacy and their data is being handled safely and responsibly. We advocate for the principle of Data Stewardship, which reflects the obligations and responsibilities of business of all sizes and industries in managing data collected in the usual course of business or as part of the business model. It reflects both the governance requirements and responsible utilisation of data and covers technological and behavioural strategies. It also addresses the safe disposal of data at the end of its usefulness.

Consideration should be given to the impact of multiple forms of regulation in this area such as Consumer Data Right and industry specific regulations. Over-regulation has the potential to chill innovation in digitalisation, add costs to business, and reduce Australia's attractiveness as an investment destination.

Data localisation requirements: Ai Group does not support data localisation as a means for ensuring cyber security. Data localisation does not fundamentally increase cyber security, as locally stored data is not necessarily more secure than that stored overseas. Indeed, if data localisation requires that businesses storing data in multiple places, it increases the risk and likelihood of a data breach. Businesses should be required to maintain appropriate data security wherever data is stored. Over regulation and directives regarding data storage increases the risk that Australian businesses become less attractive for investment, and less able to compete in international markets.

International collaboration: The digital economy transcends borders, and Australia's cyber security is inherently interdependent with that of our economic partners. Government should not limit is cyber security efforts to Australia, and place a high priority on working internationally to ensure as secure a global cyber ecosystem as possible.

International cyber collaboration already takes many forms, and is likely to expand in scope and depth over the coming decade. However, three areas of high immediate priority for international collaboration include:

- Increased security for international financial transactions through appropriate international mechanisms and platforms
- Pursue local prosecution of identified threat actors in collaboration with international agencies
- Greater work on cross-border cyber challenges - collaborate with foreign governments to reduce state-sponsored interference and pursue prosecutions overseas of non-state bad actors.

Support from government for cyber capability uplift in industry

Ai Group argues that as Australia's cyber regulations are updated, complementary efforts to support cyber capability uplift in Australian industry must be undertaken. National cyber security is a function of both *regulation* (which determines the behaviours businesses must undertake) and *industry capability* (which determines their ability to meet these behaviours). An increase in regulation without a corresponding increase in business capability will not genuinely improve Australia's cyber resilience.

As noted in prior sections, Australian industry is already investing in technology and skills capabilities, with digital and cyber very high on the list of priorities. But with only a third of industrial businesses confident in the effectiveness of their cyber security systems, and another third lacking confidence, there is a clear and pressing need to accelerate these efforts.

Government should also recognise that while businesses are committed to cyber uplift, they also face many uncertainties about cyber security. They often lack knowledge and/or information on:

- How to assess the effectiveness of their capabilities in an evolving risk landscape
- Which cyber products and services in the market are most appropriate for their business and risk
- How much invest in security and technology products and services, versus how much to invest in staff training
- What to do during a cyber incident
- How to recover from a cyber incident
- How to prevent a subsequent incident that may be different to the first.

These cyber uncertainties affect all businesses but are most pronounced in SMEs. SMEs have limited specialist cyber capabilities in house, and often rely on external providers for advice, technology and services. Some businesses report they are deliberately investing in new cyber capabilities, but remain unsure of whether they are investing in the right mix of technology and services appropriate for their situation. Helping business develop the capability to address these cyber uncertainties will be critical in ensuring business investment in cyber uplift is focused and effective.

Government can support business to improve cyber capabilities by:

Collaborative government-business approach: Government and industry can work together to improve cyber security best practice. A collaborative relationship that recognises uncertainty and works together to identify and understand risk will produce the best results. Language regarding cyber security in policy should not be punitive and accusatory but rather collaborative and supportive.

Resources and support for cyber uplift: Businesses require practical and easy use advice to be able to target their cyber investments effectively. Government can aid in this process by providing resources, platforms and support for businesses to assess their cyber security (with a particular focus on SMEs). They would also benefit from better information to assess available products and services with respect to their own distinctive cyber needs.

Support for improved incident recovery: While there is a prominent focus on incident prevention and response in current regulations, less attention is paid to promoting recovery efforts. Businesses who suffer a cyber-attack are the victims of a crime, and need support in assessing options and take-up of disaster recovery services. Effort needs to be dedicated to ensuring that the Australian cyber services ecosystem contains an appropriate mix of prevention, response and recovery services. And where prevention efforts are promoted, recovery should be made an integral part of the information mix (such as in the ACSC's 'Essential Eight' package).

Skills investment: While an increase in STEM skills is essential for the workforce generally, particular consideration needs to be given to uplifting the cyber skills of the current workforce beyond the broader national STEM agenda.

Basic digital workforce skills, a capability concern for a large proportion of businesses, can be improved faster and separately to lifting STEM skills more broadly and in the longer term. All employees, not only those in technical roles, need to be able to recognise what cyber risk looks like and how to maintain appropriate digital practices.

Specialist cyber security skills, a concern for cyber security vendors and companies with in-house capabilities, also requires investment. There is a need to increase the training pipeline for cyber security specialist in aggregate, as well as provide mechanisms for the updating of the existing workforce. Cyber-attacks and defences will continuously evolve as technology evolves, requiring resources for existing cyber specialists to update their skills and capabilities. Education and training platforms that allow for 'lifelong learning' in the cyber professional community will be essential in ensuring these skills are available.

Tailored responses for SMEs and large businesses: There are major differences in the cyber risk profile, resources, and cyber security approaches of smaller and larger companies. SMEs principally need practical information and access to affordable commercial solutions; whereas larger businesses need more advanced capabilities and a supply of cyber specialists with up-to-date skills. One-size-fits-all approaches to regulation and business support are likely to are likely to meet the needs of neither.

Use government as a lever for upgrading the national cyber security ecosystem: Whether directly or indirectly, all businesses rely on the national ecosystem of cyber professionals, skills, educational resources and commercial providers. Government has the capability to shape this ecosystem in two ways. First, practices used in government agencies as de facto best-practice benchmarks that attract wider commercial adoption. Second, government procurement activities can provide a lever to develop the market for advanced and emerging cyber capabilities needed by broader businesses. Beyond their role in providing the security of government-held data, government practices should be used as an 'ecosystem maker' that can offer positive spillovers for private business.

About the Australian Industry Group

The Australian Industry Group (Ai Group®) is a peak employer organisation representing traditional, innovative and emerging industry sectors. We are a truly national organisation which has been supporting businesses across Australia for more than 140 years.

Ai Group is genuinely representative of Australian industry. Together with partner organisations we represent the interests of more than 60,000 businesses employing more than 1 million staff. Our members are small and large businesses in sectors including manufacturing, construction, engineering, transport & logistics, labour hire, mining services, the defence industry, civil airlines and ICT.

Our vision is for a thriving industry and a prosperous community. We offer our membership strong advocacy and an effective voice at all levels of government underpinned by our respected position of policy leadership and political non-partisanship.

With more than 250 staff and networks of relationships that extend beyond borders (domestic and international) we have the resources and the expertise to meet the changing needs of our membership. We provide the practical information, advice and assistance you need to run your business. Our deep experience of industrial relations and workplace law positions Ai Group as Australia's leading industrial advocate.

We listen and we support our members in facing their challenges by remaining at the cutting edge of policy debate and legislative change. We provide solution-driven advice to address business opportunities and risks.

Australian Industry Group contacts for this submission

Louise McGrath – Head of Industry Development and Policy
[redacted]

Colleen Dowling – Senior Research Analyst
[redacted]

www.aigroup.com.au