Australian Chamber of Commerce and Industry

2023-2030 Australian Cyber Security Strategy Discussion Paper

ACCI Submission

21 April 2023

Australian Chamber of Commerce and Industry

Working for business.
Working for Australia

Telephone 02 6270 8000 | Email info@acci.com.au | Website www.acci.com.au

Media Enquiries
Telephone 02 6270 8020 | Email media@acci.com.au

Canberra Office
Commerce House
Level 3, 24 Brisbane Avenue
Barton ACT 2600
PO BOX 6005
Kingston ACT 2604

Melbourne Office
Level 3, 150 Collins Street
Melbourne VIC 3000

Sydney Office
Level 7, 8 Chifley Square
Sydney NSW 2000
Locked Bag 938
North Sydney NSW 2059

Perth Office
Bishops See
Level 5, 235 St Georges Terrace
Perth WA 6000

ABN 85 008 391 795

Australian Chamber of Commerce and Industry

Table of Contents

Introduction

ACCI welcomes the opportunity to provide feedback on the Australian Cyber Security Strategy Discussion Paper for 2023-2030.

With cybercrime costing the Australian economy approximately $42 billion a year, cyber security is an essential component of doing business in the digital age[1]. ACCI welcomes the Australian government's efforts to strengthen the nation's cyber security posture and asserts that a collaborative approach between government, industry, and the community is essential to achieving this goal.

In our members' experience many Australian businesses have rapidly increased their cyber resilience, posture, and awareness in recent years. This has been particularly apparent since the COVID-19 pandemic which has contributed to an overall rise in digital services and led to a greater use and reliance on technology and online interactions. Boards and directors of Australian companies across industries and of varying sizes are increasingly aware of cyber security, data protection, privacy, and related issues.

ACCI and members note that the current cyber security obligations are confusing and difficult to follow, both from an operational perspective and as company directors. The government needs to ensure that cyber security regulatory frameworks avoid regulatory overlap and are cohesive in nature, with enforcement activities overseen by a single agency with appropriate and adequate expertise and resourcing.

ACCI and members encourage government to simplify what is at present a complicated web of interconnected legislation and department responsibilities relating to cyber security by creating consolidated legislation, and clearly defining boundaries of agencies to prevent business confusion and overlap. Ongoing monitoring and review should be prioritised to ensure any unforeseen impacts on businesses are identified and addressed.

Any new cybersecurity requirements should be developed in consultation with industry stakeholders and subject to a rigorous cost-benefit analysis. This will help to ensure that any new regulations are effective, efficient, and do not create unforeseen and unnecessary compliance costs for businesses.

[1] Phair, Nigel (2021) Cybercrime in Australia: 20 years of in-action, Independently published.

Regulatory Reforms

Principle-based regulatory approach

Responds to

Q2a. *What is the appropriate mechanism for reforms to improve mandatory operational cyber security standards across the economy (e.g., legislation, regulation, or further regulatory guidance)?*

Q2e. *How should Government seek to monitor the regulatory burden on businesses as a result of legal obligations to cyber security, and are there opportunities to streamline existing regulatory frameworks?*

Given the pace of technological change and adaptation of organisations, ACCI and members discourage the government from taking a prescriptive approach through introduction of enforceable codes requiring organisations to implement particular governance, risk management or cyber security systems and controls. The current principles-based regulatory approach should be retained.

While ACCI is aware of the importance of cybersecurity standards in protecting against cyber threats, we believe that if any new or mandatory standards were to be introduced, they should be risk-based and proportionate to the size and complexity of the business. The Office of the Australian Information Commissioner's (OAIC) Guidance on Privacy Impact Assessments is a good example of this type of guidance[2]. Many small and medium-sized enterprises (SMEs) may not have the resources to comply with extensive cybersecurity requirements and would be disproportionately impacted by any new obligations.

ACCI members have raised several issues with existing standards and mandatory requirements that should look to be addressed prior to any new obligations. These include current procurement and contract requirements for engaging with government services and service delivery. The threats are moving extremely quickly, and there is concern that prescriptive legal frameworks will most likely fail to fully encompass the future threats unless the regulation is flexible, or principles based.

Examples of current complexities and possible solutions

One example of the current complexities is seen where each government department is creating its own standard. With one of the most onerous compliance programs being created by the Department of Employment and Workplace Relations (DEWR) that involves not only ISO27001, but the full scope of the Information Security Manual (ISM) involving over 900 controls that must be assessed. At this scale, it is not enhancing cyber security, it is compliance, and in most cases the well-meaning program is diverting limited resources away from cyber security uplift initiatives and into compliance.

Members have suggested further exploring how procurement and government contract complexities could be overcome. One area is Vendor Risk Assessments for suppliers where each company is creating their own questionnaire. This could be simplified to mirror Australian Cyber Security Centre's (ACSC) *Essential 8* model where Levels are defined against controls for the level of data help by a business, so only 50 controls are applicable at Level 1, whilst 300 controls exist at Level 2, and the full 800 become in scope at Level 3. This would allow each company to certify to a level, and for that to be used across Australian businesses and government rather than needing to respond individually, and for organisations to be holding detailed information on each other's cyber security posture.

Similarly, organisations that hold sensitive data are required to adhere to strict privacy controls by DEWR and must ensure obligations are accurately passed on and met by providers. This creates a

[2] OAIC, (2020), Guide to undertaking privacy impact assessments.

significant administrative burden. The government should explore opportunities for whole sections of control requirements to be automatically assessed as met by citing use of specific software such as Power BI which gets assessed to Infosec Registered Assessors Program (IRAP) standards.

State and federal government departments should not be creating their own schemes, rather there should be a standardised model across government departments. Similar to other 'tell-us-once' government initiatives, the collection of detailed information on business cyber posture should be limited to a singular agency (as described further below) which has appropriate high security standards and protections in place. Every entity collecting information creates and increases the risk of data exposure in case of a breach.

ACCI members note that monitoring regulatory burdens is a key step to ensure businesses are able to keep up with the various compliance changes and costs. In monitoring regulatory burden, different categories of stakeholders and risk levels should be articulated and mapped. There are clear distinctions in risk between individual businesses directly holding any sensitive/critical information to businesses engaging third-party service providers and the associated compliance requirements of each. Each category of business may have different mandatory requirements. This is particularly evident when considering the overlay of Privacy Act requirements and possible changes.

ACCI provides further detail on our concerns with compliance requirements for different businesses in relation to data in the Privacy Act Review Report submission[3].

Recommendations

- The government should review current contract and procurement requirements to ensure they are fit for purpose and not increasing the administration and compliance burden unnecessarily.
- Any proposed regulatory changes should first be presented to businesses and their respective peak bodies for comment to ensure all views on the proposed changes are consulted on well before implementation.

Obligations of company directors

Responds to Q2c. *Should the obligations of company directors specifically address cyber security risks and consequences?*

Our members note that the range of existing directors' duties and obligations under the Corporations Act, the common law and company constitutions (where applicable) are sufficiently broad to adequately cover care and diligence obligations relating to cyber security.

The Australian Securities and Investments Commission (ASIC) in its role as the national corporate regulator has been proactively promoting the importance of cyber resilience to Australian companies and has successfully prosecuted an Australian financial services licence holder for failure to manage cybersecurity risks as part of its licence obligations. The standard expected of directors of Australian entities is already high by international comparison and there is a noticeable trend towards imposing greater personal liability on directors.

Our members also note that the cost of Directors' and Officers' (D&O) insurance has increased substantially in recent years in all sectors and the scope of coverage has decreased.

[3] ACCI (2023), Privacy Act Review Report submission

Expansion of director liability may risk additional cost escalation in the D&O insurance market and may deter individuals from taking up senior positions if there is uncertainty as to their accountability and coverage, further feeding into the cyber skills shortage problem. Hence, **the existing obligations of company directors are adequate to address cyber security risks and consequences**.

SOCI and Cyber Security Acts

Responds to

Q2b. *Is further reform to the Security of Critical Infrastructure Act required? Should this extend beyond the existing definitions of 'critical assets' so that customer data and 'systems' are included in this definition?*

Q2d. *Should Australia consider a Cyber Security Act, and what should this include?*

Amendments to the Security of Critical Infrastructure (SOCI) Act have only recently come into effect (February 2023), with the risk management program rules commencement.

Industry members are of the view that further time should be granted in order to sufficiently embed the amendments into everyday business practices and then undertake a review evaluating how the extension of the SOCI Regime is operating before further extending the regime to cover areas such as customer data and systems.

The current review of the Privacy Act is also likely to impact on customer data in a range of ways. It will be important to consider the Privacy Act Review and any extension of the SOCI regime to customer data in tandem.

ACCI notes that if the proposed Cyber Security Act is purely meant to consolidate all existing cyber requirements, then we would support its creation, otherwise, we do not support introducing new regulatory requirements at this stage. At present, there is no one clear problem that requires further regulatory intervention by the government.

Additionally, the need and scope of a new Cyber Security Act must be the subject of extensive consultation to ensure that any new legislation serves to simplify the current cyber security legislative regime rather than add to the current complex web of legislations and standards.

Recommendations

- A new Cyber Security Act should only be introduced if the purpose is to consolidate existing cyber legislations. For example, the government should look to eventually consolidate the SOCI Act under any overarching Cyber Security Act (if there were to be one) after a period of ensuring that the SOCI Act is embedded followed by another round of consultation prior to consolidation.
- The government should consult further on any proposal to introduce such an Act.

Ransomware attacks

Responds to

Q2f. *Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by: (a) victims of cybercrime; and/or (b) insurers? If so, under what circumstances?*

i) *What impact would a strict prohibition of payment of ransoms and extortion demands by cyber criminals have on victims of cybercrime, companies, and insurers?*

Q2g. *Should Government clarify its position with respect to payment or non-payment of ransoms by companies, and the circumstances in which this may constitute a breach of Australian law?*

Malicious software deployed by criminal groups to deny access to an organisation's Information Technology (IT) systems and data until a ransom is paid is now the biggest cyber threat facing Australian businesses and government. Ransomware attacks have increased by nearly 500 per cent since the start of the COVID-19 pandemic[4].

Sophisticated ransomware crews have innovated new methods of maximising pressure on targets to pay, including 'double extortion' schemes, that combines traditional IT system ransoms with an additional threat to publish an organisation's confidential information online if payment is not forthcoming. This double extortion ransomware model is particularly threatening of professional services firms whose business relies on their ability to protect confidentiality of client data.

Roughly one third of Australian businesses that are hit with a ransomware attack choose to pay the ransom – for an average amount of roughly $1.25 million, according to a survey conducted by Crowdstrike in 2020[5]. Businesses that do pay ransoms may put other Australian businesses in danger by creating a revenue stream for attackers who are likely to continue to perpetuate these crimes.

ACCI and members note that without the government clarifying its position on payment of ransoms by companies, and the circumstances in which this may constitute a breach of Australian law, it is difficult for industry to provide relevant commentary or recommendations.

From the information available and initial member discussions, **our members are inclined to support a prohibition on the payment of ransoms, however, ACCI notes that there are a range of potential practical issues that warrant further consideration**.

One member notes that in almost all cases, cyber criminals reside overseas, well beyond the reach of Australian law enforcement. There is a concern that even if a ransom payment is prohibited under Australian law, it is unlikely to have any real impact on these cyber criminals who may even increase the scale and ferocity of their activities. Whereas, if Australia is known as a location where ransoms are never paid, then we may become less of a target.

If businesses are permitted to pay ransom, it will likely result in a continued decline in the number of providers offering cyber insurance services with ransom coverage. This is a more pronounced issue for SMEs who already struggle to find insurance providers to provide coverage at an affordable price. Permitting ransom payments would result in increased insurance costs or force a decision by a business whether to forego any cyber risk mitigation strategies available.

Were a ban on ransom payments to be introduced, there may also need to be consideration of a carve out for situations where personal safety is involved.

Our international colleagues – the US Chamber of Commerce who are also engaged in cyber security consultations have recommended that end users first need to be educated on simple concepts such as social engineering and what to look for in emails[6]. The government needs to encourage SMEs to ensure that their endpoint protections and email security backups are up to date with centralised management, logs of assets, and a resilient firewall policy in place.

[4] ACSC, (2021-2022), Annual Cyber Threat Report, ASD
[5] Small Business Association of Australia, (2022), The cost of ransomware: should you pay the ransom?
[6] D. Roberti, Christopher (2022), How businesses can be prepared this cybersecurity awareness month, U.S. Chamber of Commerce

We would support this position, emphasising that the baseline awareness and capabilities of SMEs need to be lifted first before any more complicated activities are introduced.

Recommendations

- If a prohibition on ransomware payments is broadly supported, further targeted consultation needs to then occur to fully explore the range of practical implications this would have in order to minimise any unintended consequences.
- Part of developing a Cyber Security Strategy should contemplate how best to lift the baseline capability of SMEs to protect from ransomware attacks in the first instance before looking to implement more complex or onerous requirements.
- A secondary element should then look to address action following a threat or attack. The government should encourage businesses to report ransomware or extortion threats/demands and then provide sufficient support, guidance, and a plan of action.

National Office for Cyber Security

Central coordination and reporting

Responds to:

Q13. *How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians?*

- ***a.*** *Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?*

Q7. *What can government do to improve information sharing with industry on cyber threats?*

The prevailing sentiment of the strategy and related media is that although Australia has experienced several significant and high-profile cyber-attacks like Medibank, Optus and Latitude Financial, the action taken by the government in response, the lessons learnt from these, and the various agencies erected provide a level of confidence that we can sufficiently deal with future incidents. However, the business community does not share this belief.

This false confidence downplays the fact that Australia continues to report one incident of cybercrime every seven minutes[7], with the majority targeted towards SMEs. Our members have stated that there is a perception of "buck-passing" between various businesses and law enforcement, state, and government agencies resulting in confusion within the industry on the appropriate government contact for various cyber security concerns.

ACCI recognises that with cyber threats constantly evolving, a comprehensive and collaborative approach is needed to ensure resilience in the digital economy that benefits all Australians. The government needs to provide clear and streamlined guidance to regulated entities in this fast-moving threat-environment. ACCI supports the government's decision to appoint a 'Coordinator for Cyber Security' supported by a 'National Office for Cyber Security' within the Department of Home Affairs to improve communication between government departments and manage cyber incidents. ACCI believes that for this position to be successful, it needs to be high-profile, in the public domain and well understood to be the 'cop-on-the-beat' for cyber security issues. The establishment of a high-profile position would give clarity and accountability and build confidence with the public that the issue is being taken seriously.

However, despite being established to improve coordination, ACCI notes that the lack of reporting arrangements with other agencies like the Australian Signals Directorate (ASD) will make it difficult for the national office to successfully undertake the very functions it was established for.

ACCI is also concerned about the lack of additional funding to establish the national office and encourages the government to appropriate funds to ensure that the agency is able to carry out it functions effectively.

Centralised platform for incident reporting and information sharing

There has also been no clear indication on whether this body would be responsible for industry engagement and partnership, or function as a central platform for information sharing for business, organisations, and individuals when it is not in relation to a specific cyber-attack incident.

[7] ACSC, (2021-2022), Annual Cyber Threat Report, ASD

Currently, organisations are required to report cyber incidents to multiple regulators, including the ACSC, the OAIC, and the Australian Federal Police (AFP). This can be a time-consuming and complicated process, especially for SMEs with limited resources and capacity.

ACCI is supportive of the government's proposal of harmonising existing reporting requirements and having a single reporting portal for businesses who come under cyber-attack.

ACCI would propose the consolidation of several existing reporting mechanisms into one central reporting portal that is managed by the national office as it will allow for customised action plans for businesses under attack. **ACCI recommends that the national office functions as the single point of contact for not just reporting a cyber-attack, but also to get information on cyber security concerns**. A single agency, or a centralised platform functioning as a **one-stop-shop** for all of industry is needed for two main purposes: information sharing, and functioning as a single entry point for all cyber incidents.

ACCI is supportive of the national office outsourcing handling IT systems of private companies who are under attack to only the ASD on three conditions: one, if the business under attack asks for help, two, if there is demonstrated need and proof that the data of Australians is being compromised, and finally, as long as they report findings and action plans to the national office, which will function as the one and only point of contact for these businesses. Consolidation of several existing reporting mechanisms into one central reporting portal that is managed by the national office will allow for clear, customised action plans for businesses under attack. Consideration should be given to the ACSC working with the national office to relocate its resources into this centralised platform.

A single reporting portal would enable organisations to report cyber incidents in one place, reducing duplication of effort and streamlining the reporting process. This would also help to ensure that all relevant information is reported promptly on the same platform, improving the government's ability to respond to cyber incidents, put out accurate media and resources, and protect Australia's cybersecurity.

Such a platform will allow industry and government to share information on cyber threats and attacks, vulnerabilities, and best practices, increasing cyber-awareness to prevent and better manage cyber risks and attacks. This would help to improve cybersecurity awareness and enable organisations to take proactive measures to protect themselves against cyber threats.

Recommendations

- ACCI supports the government's proposal of the national office functioning as a national body responsible to coordinate cyber security efforts across government and encourages funding allocation or reappropriation to ensure this.
- Existing and future agencies with cyber security functions should report to the national office to ensure that all efforts are centralised and coordinated at all times. Power to commandeer IT systems of private companies under attack may be outsourced to ASD only under special circumstances.
- The national office should have a two-fold role: function as a single point of contact for reporting a cyber threat/incident, and function as a centralised hub for information sharing and industry engagement.
    - Ongoing evaluation measures such as regular reports on trends and good practices would function as a good means of supporting public transparency and input.
    - Consideration should be given to this centralised function having a 24x7 information hotline, similar to the current ACSC cyber hotline, however, not merely for reporting cyber-attacks and counselling services, but also for businesses and individuals to speedily obtain information and guidance on cyber security threats and concerns.
- The national office should conduct regular briefings with industry association representatives to keep them informed about the latest cyber threats, vulnerabilities, and attack methods. This information can then be disseminated through industry networks to help businesses stay up to date on the latest threats and information and to take proactive measures to protect their systems.

- The national office should work with industry to develop a threat intelligence framework that is easily understood by businesses (e.g., similar to the smart traveller warning system) that standardizes how cyber threat information is shared between government and industry. This framework should include guidelines for sharing information, classification of threats and significant impacts.

Cyber security skills, workforce and migration

Responds to:

Q11. *Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?*

Q12. *What more can Government do to support Australia's cyber security workforce through education, immigration, and accreditation?*

A strong and abundant cyber security workforce is crucial to address emerging threats and new challenges, and to maximise the benefits of the global economy's shift online. ACCI supports the government's focus on boosting the cybersecurity workforce to meet the challenges of the digital age. Investing in cybersecurity skills and training programs will not only boost digital literacy helping to address the skills gap, but also foster a culture of cybersecurity awareness across all sectors of the economy.

Training and education

Data, digitisation, and cyber security skills offer businesses of all sizes and in all sectors of the Australian economy commercial opportunities to increase productivity, enabling them to grow, create jobs, and provide an improved work-life balance. It is increasingly important for businesses, particularly SMEs, to look to the adoption of digital technologies within a trusted ecosystem secured by design that is both robust and resilient.

Currently, the adoption and productive use of technology in businesses is limited by the digital, data and cyber security skills a business has at their disposal.

It is estimated that close to half a million Australian SMEs have no or little engagement with digital tools[8]. They are more vulnerable to cyber-attacks because they lack the necessary infrastructure and knowledge to manage cybersecurity risks. The Technology Investment Boost and Skills and Training Boost Measures announced in the 2022-23 federal budget was a step in the right direction to assist small businesses in improving their digital capabilities. However, the time frame for these measures may not be sufficient for small businesses to take advantage of them fully. ACCI recommends extending this incentive until 30 June 2025 to enable more small businesses to take advantage of it, thereby enhancing their digital capabilities and improving their cybersecurity posture.

Digital and Tech skills Working Group

ACCI is a member of the Digital and Tech Skills Working Group which has been established by ministers O'Connor and Husic as the key practical mechanism to take forward the Digital and Tech Skills Compact.

The working group has been exploring the drivers of the current digital and tech skills shortages (which includes cyber security skills) and is working to develop a model scheme to support workers to take on entry-level tech roles through a blend of employment and training.

Through the working group, underlying problems relating to 'earn while you learn models' and wider system issues have been identified that are causing 'symptoms' relating to attraction, retention and outcomes. These issues include:

[8] Myob, (2022), Australia's SMEs: A Snapshot

- Skills identification: businesses, particularly SMEs are often unable to identify or articulate the specific skills that they need and don't have effective frameworks or systems for identifying skill needs in an ongoing capacity.
- Attraction and recruitment: the current system does not support opportunities for a diverse range of learner groups (e.g., getting younger generations into the IT sector as there are no IT role models encouraging these roles as an attractive future job, mature-aged works reskilling), nor does it attract and support employers that are prepared to invest in employees undertaking employment-based learning.
- Education: higher education and vocational education and training (VET) sector regulatory systems are contributing to an education bottleneck as accreditation of qualifications is slow and burdensome and regulators may be risk averse to new, innovative approaches to designing qualifications to keep up with the pace of change.
- Work supervision and training: industries are looking for skilled people but are also not generally willing to employ university graduates as a means to tackle labour shortages as they lack experience. Employers also often lack the capacity and capability to effectively support worked-based learning and so recruiting graduates and providing on-the-job-training is not an option.
- Assessment and accreditation: There is no clear framework for effective and consistent assessment of learning, which leads to inconsistent assessment quality.

The working group is currently considering potential 'earn while you learn' models to scale up or fund further as well as other system-level actions that government and industry can take to address digital, including cyber security skills needs.

Accreditation

It has been noted that most SMEs do not have the resources to maintain an in-house IT department, and as a result, they rely on external IT providers to manage their cybersecurity needs. However, they often lack the knowledge and expertise to assess what particular services they require and whether the provider has done enough to secure their systems adequately. This puts them at significant risk of cyber-attacks.

A voluntary cybersecurity services accreditation scheme for IT providers may provide a certification process that would enable businesses to identify IT providers with the necessary skills and expertise to provide adequate cybersecurity services. The accreditation would also help providers market their services as legitimate and help to eliminate the risk posed by unqualified providers. This will significantly help businesses to identify qualified and competent IT providers, provide assurance that they have taken reasonable steps to secure their systems, and reduce the risk of cyber-attacks. The scheme would also help to promote the development of a cybersecurity workforce with the necessary skills and expertise to meet the growing demand for cybersecurity services. A structured scheme would also significantly increase trust that businesses are dealing with certified professionals.

Skilled Migration

Alongside the important outputs from Australia's education and training sectors, skilled migration is a vital tool that assists businesses who experience skills gaps, as well as filling skills shortages in the wider economy. Noting the shortage of skilled cyber security professionals in Australia and the urgent need to address it, migration needs to form a part of the solution.

The increase to the permanent migration program, as well as the increase in funding for the Department of Home Affairs to allow for faster visa processing times were welcome developments. However, there

are additional changes that need to be made to ensure Australia's migration system is responsive to the changing environment and can meet the challenges and opportunities that lie ahead. In particular, ACCI recommends that employer sponsored skilled migration, both permanent and temporary, should again have access to all occupations that are classified as 'skilled' and should not be limited to a restricted list that is not sufficiently responsive to changing needs. This would ensure the system is responsive to all skill needs, not just national skill shortages.

In addition, all occupations are experiencing technological progress and the nature of work and job roles are constantly changing. This is particularly the case in the cyber security space, where new jobs are being created every year, and there may not be an "easy fit" in the Australia New Zealand Standard Classification of Occupations (ANZSCO) system. For example, for many years data scientists were not included, or classified as "software developers". ANZSCO not only needs to identify new jobs, but also needs to regularly appraise the duties within their job and assign or adjust an appropriate skill level. An out-of-date ANZSCO denies fair access to important migration programs and unreasonably complicates the regulation of the program due to the need for work-around style caveats in order to meet business' needs.

Recommendations

- Extend the Technology Investment Boost and Skills and Training Boost Measures announced in the 2022-23 federal budget until 30 June 2025 to encourage a greater uptake and allow more small businesses to digitalise and grow.
- The Cyber Security National Workforce Growth Program needs to be strengthened. Grants and funds like the Cyber Security Skills Partnership Innovation Fund should be expanded to provide industry and education providers the necessary funding to continue to deliver innovative projects and train cyber security workforce.
- Governments should look to further invest in promoting cyber security courses and job opportunities in primary school, high school, and tertiary studies with the aim of increased take-up of careers in cyber related fields.
- The government should undertake consultation on the option of a voluntary cybersecurity services accreditation scheme for IT providers with a minimum-security standard that providers must meet to attain accreditation. The accreditation process should involve a rigorous evaluation of the provider's capabilities, including penetration testing, vulnerability assessments, and audits, to ensure that they meet required standards.
- Employer sponsored skilled migration should have access to all occupations that are classified as 'skilled'.
- A regular review of major statistical infrastructure such as the ANZSCO needs to be built into the normal operating budget of the ABS to ensure there is fair and ongoing access to migration programs.

Further industry support to increase cyber resilience

The increasing uptake of digital technology needs to be complemented with cyber resilience building activities to protect business and national security assets from the risk of cyber-attacks.

Additional support for SMEs

***Responds to Q15a**. What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?*

Cyber-resilience is a particular challenge for resource-constrained small businesses and individuals. SMEs are not just cybercrime targets; they are the *principal* target due to their lack of resources to detect and defend themselves from attacks as compared to larger businesses. According to Melbourne-based cyber security firm Kaine Mathrick Tech, 43 per cent of cyber-attacks target SMEs and only 5 per cent of SME data folders are protected[9].

"Naming and shaming" organisations for data breaches may deter other businesses from reporting incidents, even in spite of fines. This is especially relevant for SMEs on an existential level as more than half of small businesses close after a cyber-attack or data breach[10] and thus require additional safeguards and support.

Many small businesses in regional areas are not aware of the risks and consequences of cyber-attacks and may not have the necessary resources or knowledge to protect their businesses from these threats. First, they may not be aware of or able to identify what cyber-security needs they have based on their business activities. Second, they typically have limited resources to invest in cybersecurity measures or may not have access to cybersecurity expertise. Thirdly, they may not regularly review or update their software or security systems, leaving them exposed to known vulnerabilities that can be exploited by attackers. Many small businesses are using outdated technology (computers and software) and may not be aware they are the target of a cybercrime until weeks, months or even years later. Finally, they are more likely to rely on third-party service providers for their IT needs, such as internet service providers, which may not have the required expertise or robust security measures in place.

One member has noted that SMEs may benefit from a voluntary certification program that can be used to demonstrate their commitment to cyber security, similar to the Heart Foundation tick program for nutritional standards.

Equipping small business owners and the community with the information and tools they need to protect themselves will encourage greater adoption of cyber secure products and cyber smart decision-making.

Recommendations

- Government and industry should collaborate on public awareness campaigns to educate individuals and organisations about the true nature of cyber threats, best practices, and how to avoid becoming a victim of cybercrime.
- The government should work with industry associations, large businesses and service providers to provide SMEs within critical supply chains with cyber security information and tools delivered as a 'bundle' of secure services (such as threat blocking, antivirus, and cyber security awareness training).

9 Mybusiness, (2022), Almost half of Australian cyber attacks hit SMEs
10 Mybusiness, (2022), More than half of small businesses close after a cyber attack

- Governments at all levels should work in partnership with chambers of commerce to develop programs to boost regional engagement with SMEs.
- The government should further consult on how they might incorporate quality assurance programs and minimum cybersecurity requirements being embedded within programs they deliver, for example in community pharmacy programs.

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