2023 – 2030 Australian Cyber Security Strategy Discussion Paper

-Accenture Australia Response

accenture | Australian Government Department of Home Affairs

Letter of Thanks

Dear Home Affairs and the Cyber Strategy Task Force,

Accenture values the opportunity to share our perspectives on the 2023-2030 Australia Cyber Security Strategy Discussion Paper.

We commend the government on its focus on cyber security and its aspirational vision in this regard. We believe there are significant opportunities for Australia to collaborate across government, industry, and community groups to improve cyber security practices within Australia, and to contribute to the cyber security capabilities that enable and safeguard the global economy.

Accenture has more than 16,000 cyber security professionals around the world. We are a leading provider of end-to-end cybersecurity services, including strategy, protection, resilience and industry-specific cyber services. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Cyber Fusion Centres. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence.

We have expressed various ideas drawn from this experience in our response below and follows from our comprehensive response to the 2020 cyber strategy. We welcome the opportunity to provide any support needed or answer any questions you may have moving forward.

Kind regards,

[redacted]

Angelo Friggieri
Managing Director
Accenture Security - Health and Public Sector
[redacted]

Accenture's response

1. What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?

From our perspective, the following themes should be considered as the foundation for the policy.

- **Clarity of obligations** of government and of industry. Apply clear and objective criteria when imposing cyber security obligations on organisations, working with industry to establish and adopt objective reference standards that are specific and actionable. We recommend comprehensively reviewing legislative requirements to reduce the scope and duration of all data retention obligations, while balancing legitimate auditability and assurance objectives.
- **Consistency in compliance frameworks**, policy, and procedures. There is currently inconsistency in approach between federal departments, state government, and private sector generating confusion, fostering a compliance rather than resilience culture, and impeding collaboration / data exchange. Additionally, consistency and alignment in frameworks and standards across the FVEY or the OECD would help multi-national companies attempting to comply with differing regulations.
- **Framework to foster collaboration**. Industry is self-organising in pockets, putting competitive tension aside for the greater good. However, there is more that could be done in collaboration without the fear of persecution, or repercussion (government stepping in) where there is good intent shown to collaborate for the purpose of cyber security uplift. Disclosure obligations in the event of a data breach should be streamlined, while still retaining the ability for a disclosing party to tailor such communications to the relevant audience.
- **Don't forget the carrot with your stick**. Consider how fines for non-compliance and not performing reasonable steps to prevent a breach would generate revenue to potentially support tax relief for organisations exceeding obligations and seen to be lifting the posture of cyber security for the nation. Similarly, reduce the stigma associated with notification of a security incident and support organisations who do experience an incident to prioritise mitigation and remediation activities.
- **Education and Awareness.** Through education and public awareness campaigns, reposition cyber security away from full risk elimination (which is not possible or practical) and compliance driven, to a more comprehensive cyber resilience and agile risk management approach, giving appropriate weight to the value of personal information. Seek to standardise training and certification across institutions across the country. The minimum standard to a Cyber certification, diploma or degree, and the minimum base cyber security curriculum that is included from Primary School through to High School.
- **Emerging Technology Division.** Stand-up an Emerging Technology division that is supported by industry and instils an agile approach to policy and regulation for emerging technology (such as, Quantum, metaverse, and AI). We are unfortunately in a state of continuous catchup. We need broad themes with potential threat assessments and subsequent adjustment to obligations, and compliance readiness, working with industry to help accelerate and enable a comprehensive view and approach. Specifically, we encourage government to urgently address the risk that credible 'deep fake' technology poses in the absence of truth in political advertising laws.
- **Clarify the application of implied warranties** in the Australian Consumer Law with respect to cyber security controls. Consider adopting explicit cyber security standards for consumer IoT and home automation products that pose a higher risk, allowing for full release from such obligations at the end of the product's lifecycle (cease support).
- **Mental Health.** Support a voluntary framework to address mental health impacts experienced by cyber security professionals, particularly those involved in incident response activities.

2. What legislative or regulatory reforms should Government pursue to enhance cyber resilience across the digital economy?

Cyber security impacts upon the full spectrum of Australian society, and the many and varied industries that operate in our global economy. As such, the scope of legislation and regulation that interacts with cyber security is extremely broad.

We recommend prioritising reform in the following areas:

1. Data retention obligations are directly and indirectly imposed by numerous industry specific regulations. We recommend the committee conduct a comprehensive review of regulations that require an organisation to retain personal data, applying the following principles:
    a. *Minimise the scope and duration of retention* – the less data an organisation holds, the less data can be exposed by a breach.
    b. *Maintain audit and assurance objectives*.
    c. *Define specific datasets where practical* – in our experience, where there is ambiguity, most organisations opt to retain excess data (which can increase the severity of a breach), to reduce their risk of non-compliance and associated reputational and regulatory penalties.
    d. *Strengthen existing data protection laws,* such as the Privacy Act and align to learnings from the UK and EU.
2. The *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* imposes a significant barrier to the export of cyber security services from Australia. For example, a service provider may be issued a Technical Assistance Notice (TAN) or Technical Capability Notice (TCN) without judicial oversight or timely transparency, undermining the security controls of an organisation. New vulnerabilities do not need to be 'systemic' to pose a security risk to the organisation (or those whose data is held). We encourage the government to act on the recommendations of the various reviews of this legislation conducted to date (e.g. by the PJCIS and INSLM) to improve the independent oversight and proportionality of these laws.
3. Physical and electronic security activities (e.g. locksmiths, alarm and CCTV design & installation) are currently regulated differently between states, including multiple organisation and individual level licensing regimes. We recommend consolidating these regulations into a single national regime, and clarifying their application to activities where physical, electronic, and cyber security converge - for example: OT security, physical penetration testing, and advice/installation of digital identity access management systems. We recommend against imposing a licensing requirement to perform cyber security activities, as this would create an unnecessary barrier and may impact Australia's ability to attract cyber security talent in competitive global market.

(a) 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)?

We do not consider a 'one size fits all' approach to be suitable to improve and drive adoption of operational cyber security standards.

We believe the following areas are better addressed by amendment to legislation / regulations:

- Clarifying the duties of company officers in relation to security controls and processes adopted by their organisation;
- Streamlining and aligning regulatory reporting obligations in the event of a security incident;
- Consolidating the various state-based licensing regimes for 'security' providers (intended to regulate physical / electronic security) to clarify their application to cyber security activities, and address convergence between physical, electronic, and cyber risks;

- Enacting previously recommended reforms to the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* to improve the independent oversight and proportionality of these laws; and
- Adopting explicit cyber security standards for high-risk consumer products (such as consumer IoT and home automation) within the *Competition and Consumer Regulations*.

We believe the following areas are better addressed through guidance, education and awareness activities, and other engagement with industry (for example a voluntary code of practice):

- Establishing objective and actionable reference standards for cyber security controls, including education as to the purposes and limitations of existing frameworks such as the Essential 8 and ISM;
- Updating government procurement guidance and standard form contracts (as further discussed in Questions 6 & 18 below); and
- Clarifying the application of implied warranties in the Australian Consumer Law with respect to cyber security standards. E.g. when does an organisation's cyber security hygiene impact whether their consumer goods or services are of acceptable quality or fit for purpose?

(b) 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?

We do not recommend extending the definition of 'critical assets' to customer data or systems generally. The obligations imposed by SOCI are significant, and we believe a broader definition will make it significantly more challenging for a responsible entity to identify the assets that are truly critical and prioritise their security investments accordingly without a material gain in cyber resilience.

In our view SOCI already addresses the scenario where a system or (more rarely) customer data forms part of a critical asset, such that its absence, damage, or compromise would prevent or cause significant damage to the critical asset.

We do however recommend that the SOCI Act provide greater clarity regarding scenarios where third-party service providers are engaged in connection with a critical asset, for example an outsourced service provider engaged to perform a specific function of the asset. While various operational requirements of the act may flow down to such providers, we consider the registration and reporting obligations and overall accountability for the asset should expressly remain with the asset owner to avoid potential duplication and confusion.

(c) Should the obligations of company directors specifically address cyber security risks and consequences?

We recommend providing further clarity as to the application of the duties of directors and company officers in adopting cyber security controls and processes for their organisation, and their disclosure to impacted organisations and individuals in the event of security incident.

When strictly interpreted, existing director's duties can conflict with desired cyber security outcomes – for example the obligation to act in the best interests of their company may incentivise reduced disclosures in the event of a breach.

Note that in the current threat landscape, an organisation may implement extensive cyber security mitigations and still experience a security incident. Any reform to director's duties should consider the wider context in which decisions are made as to processes and controls adopted. We recommend against reforms that stigmatise forthright disclosure, or unfairly punish an organisation or company officer for the actions of a threat actor.

(d) Should Australia consider a Cyber Security Act, and what should this include?

A Cyber Security Act is a worthwhile consideration to bridge the gap between the Privacy Act, the Crimes Act, and organisations not subject to the SOCI Act.

The Act could be used as a basis to standardise the compliance landscape in Australia. The Act should include reporting requirements, penalties and enforcement, continuous education and skill uplift.

(e) How should Government seek to monitor the regulatory burden on business as a result of legal obligations to cyber security, and are their opportunities to streamline existing regulatory frameworks?

Streamlining the regulatory frameworks between federal government, state government, and private sector would go a long way to reducing the so called "burden". However, we need to change the narrative on regulation and compliance in the sector. It's a matter of national security, a matter of citizen safety, health, and wellbeing. Being secure by design and taking the regulatory expectations on within that journey makes compliance a simpler exercise.

It is not necessarily government's responsibility to reduce the burden, however, apart from streamlining regulation, another element is the pivot of responsibility of compliance. Placing more pressure and obligation on the manufacturer rather than the end user for compliance. Why is security functionality still a paid optional extra when procuring a SaaS service? Why is the compliance and security function an end user and not the manufacturer's responsibility? These are concepts to consider while refining regulation for the sector.

(f) 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?
(f)(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?

Accenture discourages the payment of ransoms and extortion demands. However full prohibition may be a step we as a society, economy, and maturity of industry is not quite ready for.

In practice, making a ransom payment provides an impacted organisation with little to no assurance against further extortion or impact to their business. A broad prohibition may assist organisations responding to a breach by 'taking the decision out of their hands, however, there will be exceptions where a total prohibition may place organisations in extremely difficult situations where lives or national security is at risk.

In principle, a commercially motivated threat actor will find little value in making a demand that their target simply cannot meet. We anticipate threat actors will respond with various attempts to circumvent a prohibition if put in place (possibly including a short-term increase in incident volume as the prohibition is tested), and assuming these attempts are unsuccessful, followed by a general long-term reduction in the use of ransomware for commercial purposes as threat actors move to more attractive / viable vectors.

(g) 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?

Yes – a clear position will assist organisations who experience a breach to understand their options. We encourage the government to produce clear guidance addressing common scenarios and key edge cases.

3. How can Australia, working with our neighbours, build our regional cyber resilience and better response to cyber incidents?

Like other forms of aid Australia provides to the region, cyber needs to be an area of focus for education and capability uplift across the region. We have seen and commend actions from the Australian Government

represented by the Department of Foreign Affairs and Trade and Australian Aid in increasing cyber capability in the Pacific. This should continue, however, we have to remember that cyber doesn't see geographic boundaries, so strengthening the region may not yield an uplift in resilience for Australia. What it will achieve, is greater protection of Australian citizen data as they travel to countries within our region. It would also help combat the silent but active state-based threats using the vulnerable smaller nations as launch pads for economic chaos and disruption to the Australia and the West.

4. What opportunities exist for Australia to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective?

Accenture believes other respondents may have a more focused view point to this question.

5. How should Australia better contribute to international standard-setting processes in relation to cyber security and shape laws, norms and standards that uphold responsible state behaviour in cyberspace?

Australia can better contribute to international standard-setting processes in relation to cybersecurity by actively participating in existing international forums and engaging with organisations that address cybersecurity issues, such as the UN and OECD.

Through this dialogue, Australia has the opportunity to lead the charge on multi-national collaboration in threat intelligence, threat hunting and assessments, that build a better posture and understanding of resilience leading to a greater understanding of priority of focus on legislation adoption and alignment domestically.

6. How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?

There are significant opportunities for the Commonwealth Government to model and contribute to exemplary cyber security practices:

- Simplifying government control frameworks and ensuring relevant departments and positions have a good understanding of said frameworks and their role in it. Government could also work collaboratively with industry to develop an objective reference standard of technical and organisational controls with various levels of risk profile organisations can adopt. While guidelines like Essential 8 have proven a valuable resource, it does not provide the desired level of detail that an organisation would want in a reference standard.
- Government can use the way they interact with other organisations to show how a model organisation should implement cybersecurity principals. We recommend avoiding imposing imprecise cybersecurity obligations, such as requirements to 'take all reasonable steps'. This language leaves the specific controls that are expected to be vague and up to interpretation, when this is a perfect opportunity to demonstrate to other organisations what proper controls look like and lead by example. It can lead to a false sense of security where controls are assumed but explicitly laid out. And such obligations are easy to reinterpret in hindsight, contributing to post-incident disputes (e.g. 'an incident has occurred, therefore the steps were not 'reasonable', regardless of investment level').
- Another example of this could be implemented by a modification of government procurement frameworks to explicitly include a suppliers current cybersecurity capability as well as its ability to provide maintenance for said capability. This brings the benefit of creating a competitive environment where security is forced from being a priority for the IT department to being a business priority.
- Participate in information sharing and collaboration: Commonwealth Government departments and agencies should participate in information sharing and collaboration initiatives with other government entities, private sector organizations, and international partners. This includes sharing

threat intelligence, collaborating on incident response, and developing common cybersecurity standards and best practices.

- Additionally, fostering a culture of embedded security across government departments is critical. Including the roles and functions of security throughout a department and the continuous awareness and training for all resources. As an example, the most senior responsible officer for Security reports to the CIO in most government organisations. Elevating this role to the Assistant Secretary level with a remit of security across the enterprise and the ability to advise and manage risk holistically would set an example for private enterprise.

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

To improve information sharing with industry on cyber threats, the government could take the following steps:

1. Develop clear guidelines and protocols for information sharing: we recommend that the Federal government develops clear guidelines and protocols for information sharing that define what information can be shared, with whom, and under what conditions. This should include guidance on how to protect sensitive information and ensure confidentiality. This is largely covered in the PSPF, however, the adoption of this at the state and local levels is inconsistent. A single approach is needed.
2. Establish a trusted platform for information sharing: The government should establish a trusted platform for information sharing between government agencies and industry.
3. Provide regular threat intelligence briefings: The government should provide regular threat intelligence briefings to industry on emerging cyber threats and trends. These briefings should include actionable information that can help industry organizations to protect their networks and systems. Industry would contribute to these via initiatives such as Cyber Threat Intelligence Sharing (CTIS) being developed by the ACSC.
4. Encourage industry participation in cyber threat exercises: The government should encourage industry participation in cyber threat exercises to help them prepare for potential cyber attacks. These exercises should simulate real-world cyber attack scenarios and provide opportunities for industry and government to work together to test their response capabilities.
5. Foster a culture of information sharing: The government should foster a culture of information sharing between government agencies and industry by promoting collaboration, communication, and trust. This includes regular engagement with industry organizations and building relationships with key stakeholders.

8. During a cyber incident, would an explicit obligation of confidentiality upon the Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC) improve engagement with organisations that experience a cyber incident so as to allow information to be shared between the organisation and ASD/ACSC without the concern that this will be shared with regulators?

An explicit obligation of confidentiality may assist to improve information sharing with ASD / ACSC. To further encourage such information sharing we also recommend that such a mechanism:

- Allow for no-names basis voluntary information sharing by intermediaries such as law firms and incident response service providers;

- Provide the impacted organisation with limited relief from confidentiality obligations it owes to third parties (such as implementing the mechanism in a way that it falls cleanly within the '…as required by law' exception to confidentiality found in many contracts); and

- Consider enabling ASD / ACSC to facilitate information sharing with relevant third-party providers on a confidential basis for risk mitigation purposes, noting that such a mechanism should also clarify the application of regulatory and market disclosure obligations, both in Australia and overseas, that may arise from information received in confidence via ASD / ACSC.

9. Would expanding the existing regime for notification of cyber security incidents (e.g. to require mandatory reporting of ransomware or extortion demands) improve the public understanding of the nature and scale of ransomware and extortion as a cybercrime type?

An expansion but simplification of the current notification regime would in our opinion improve public understanding, but the scheme would also need to show the impact of the incidents, simply showing the number rise will not give the public the full idea of how these incidents effect government and industry systems and subsequent impact to our way of life in Australia or the region. It should be noted that any expansion of regime should come with clarification on the obligations of service provider and impacted organisations, and the obligations of organisations based overseas that are storing Australians data.

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

A more tailored approach is required for general growth in Australia's cybersecurity. The reality is that Australia is not alone in the talent crunch. The demand of cyber skills exceeds the supply globally. Even with recent economic downturn and significant redundancies in the Technology sector, demand for cyber security talent has remained steady. Therefore, initiatives to equally attract talent, retain talent, and grow talent are needed. Initiatives that generate innovation locally with incentive and encouragement for sovereign industry would be encouraged.

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

In looking to support Australia's cyber security workforce we believe there are some changes that could be made to cyber security education throughout this country. Firstly, it would be advantageous for cyber security education across the country to have some sort of standardisation of the content taught. By ensuring a minimum standard in the content taught we can ensure that most of the people entering the workforce are coming in with a similar level of knowledge that can then be built upon as professionals undergo additional training and education. We see this both for Cyber specialisations (consistency in cyber professionals) but also the minimum standard of cyber security education included through general education in schools. How are we equipping the next generation to operate safely in a digital world?

Additionally, an issue for Australian cyber security is that many of those leaving higher education often lack the practical experience to get into the cyber security workforce and get into the cybersecurity field, we propose firstly that an incentive to businesses to work with educational institutions to provide practical work experience as part of the curriculum could help to provide a steady supply of new cybersecurity professionals who are entering the workforce with a high level education meeting a minimum standard but also bring practical experience to the role. The skills and education pillar may actually require a separate strategy and policy alongside this primary Cyber Security strategy. This is a broader challenge for Australia.

Another point to bring to this conversation is the role that mental health can have in causing burnout and stress in cybersecurity, it would be beneficial for the government to play an active role making sure that mental health services are readily available, and possibly advocating for cooling off periods for professionals in the aftermath of security incidents which could help reduce burnout caused by work related stress.

From an immigration perspective, this is a very thin needle to thread. Relaxing or accelerating visa processes for cyber skills to help remediate demand may result in adverse effects to National Security with the injection of state-based actors into the critical infrastructure organisations. Regardless, as highlighted in our answer to question 11, with the current demand challenges globally, relaxing visas may not actually generate a net capacity uplift unless paired with significant incentives in terms of life in Australia.

An area to consider, to help solve for the global talent crunch while also solving for early warning and collaboration on threat intelligence, is increased use of shared services across Five Eye (AUS | CAN | NZ | UKI | US) government and industry. As an example, Accenture's Five Eye network of Cyber Security innovation Centres and Security Operating Centres provides an ability to support managed detection, incident response, threat intelligence, and other security remediation and maintenance activities as a shared service. The service includes leveraging continuous improvement and automation models to effectively reduce the volume of human tasks to enable more effective coverage and net resilience for Accenture internally and our customers.

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

Beyond existing law enforcement and operational responses there would be value in considering the following:

1. Developing a national cyber incident response plan: The government could develop a national cyber incident response plan that outlines the roles and responsibilities of different agencies and stakeholders in responding to major cyber incidents. Make this publicly available and provided to all organisations (perhaps as a mail out as part of the next Business Activity Statement (BAS) to the ATO, or in the company's Notice of Assessment from the ATO). This plan can also include procedures for coordinating the response to cyber incidents across different levels of government, as well as with the private sector and international partners where relevant.
2. A portal to provide status and communication to the public on the incident. The media frenzy surrounding these incidents is not helping. We need a single trusted source. The government can provide timely and accurate information to the public about major cyber incidents, including the nature and scope of the incident, the potential impact on individuals and organizations, and steps that can be taken to mitigate the risk of harm. This can help to reduce confusion and panic, and empower individuals and organizations to take appropriate action to protect themselves.
3. Via the same portal, provide a mechanism for access to support to affected individuals and organisations, including counselling, financial assistance, and technical assistance to restore systems and data. This can help to mitigate the impact of the incident and support the recovery of affected individuals and organisations.
4. A lessons learned portal or collaboration mechanism. Encourage organisations that suffer a breach to speak up, where they had a gap, how they resolved it, how other organisations can prevent similar breaches.

The announcement by Hon Claire O'Neil on 14th April 2023 on "bringing together Australia's most critical services across the whole economy together to conduct exercises to test and better prepare for potential cyber-attacks" is exactly the coordinated effort we believe that could generate a step change in Australia's resilience. The exercises should continue and if conducted effectively, should generate awareness, learning, and a rapid sourcing of ideas to increase resilience. This pivot from compliance focus to deep understanding of the threat and agile adjustment in protection mechanisms is a step in the right direction. The sharing of the results of these exercise sessions with actions for small to medium enterprises to take on would be seen as highly valuable also.

13(a) Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators

Absolutely, as per our recommendation above.

14. What would an effective post-incident review and consequence management model with industry involve?

A post-incident review with industry should be conducted on a foundation and principle of continuous learning and future prevention. Yes, there should be material consequences if an organisation is seen at fault in not

doing what is industry recognised as reasonable and minimum standard to prevent a breach or incident, however, we know that compliance does not equal protection. When considering a post-incident review, we recommend the following:

1. Appointment of an ACSC accredited cyber service provider as the Cyber Incident and Forensic Response (CFIR) lead to operate as the impartial third party to chair and support the review. A model could be put in place where the CFIR service provider is co-retained by government and the impacted industry organisation.

2. A debrief from the appointed CFIR lead on the route cause, the indicators of compromise, the resulting impact to the organisation. The ACSC should also provide information (where appropriate for the purpose of National Security) on the threat actor assessment – was this state based? Is this one step in an attack chain across other organisations. To better understand the next potential target.

3. An assessment on how the incident could have been prevented. Was the organisation compliant against the relevant framework? If so, how does the framework need to be adjusted?

4. An industry specific CISO forum where relevant share learnings and potential warning. E.g. if there was a breach on a hospital, let's get all the hospital CISOs together so they are well informed. They are not there to weigh in, this is about industry collaboration for prevention and resilience.

5. A publicly releasable briefing of the findings, actions, and recommendations for both personal data protection, but also future breach prevention.

6. The process should also inform consequence management actions based on a pre-determined framework (which would also come out of this strategy). This would include financial penalties, regulatory changes and compliance framework changes.

An effective post-incident review and consequence management model with industry should be collaborative, transparent, and focused on continuous improvement to ensure that cyber incidents are effectively managed and future incidents are prevented

15. How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime?

Beyond the current work from the ACSC with Essential 8, the following steps are examples of joint government and industry initiatives to support the adoption of best practice, increase knowledge and support victims of cybercrime.

1. Education and awareness: Government and industry could work together to provide education and awareness programs on cyber security best practices, including safe online behaviours, password management, and how to identify and respond to cyber threats. These programs can be tailored to different audiences, including employees, students, and the general public;
2. Victim support services: Government and industry can work together to provide victim support services to individuals and organizations affected by cybercrime. This can include counselling, financial assistance, and technical support to help victims recover from cyber incidents; and
3. Collaboration and information sharing: Government and industry can collaborate and share information on cyber threats, vulnerabilities, and incidents to improve incident response and prevention. This can include sharing threat intelligence, coordinating incident response activities, and sharing best practices.

16. What opportunities are available for government to enhance Australia's cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia?

The cybersecurity technology ecosystem is extensive, and new technologies are surfacing every week. It has become a challenge for governments and organisations to navigate and determine what they actually need and the value (efficiency, resilience, protection) that the tool or technology would provide.

There are three main barriers for the adoption of cyber technologies in Australia at present:

1. Australia's small market size and therefore a company's footprint (data holding, volume of users) resulting in a higher price per unit for the technology when compared to US or EU markets;
2. Access to technical skills in country in the various technologies to effectively design, implement and most importantly, maintain; and
3. The heavy focus on IRAP and sovereignty in Federal government, which is also being adopted by state governments.

Although obtaining and maintaining IRAP is a critical long-term need to support consistency in application and data security, however, how could Government co-invest and or provide an alternative path to test the value of a cyber security technology and the potential upside before an IRAP is required? A purist view would be that if the technology vendor was truly secure-by-design then they would have met the IRAP requirement prior to coming to market. However, this is a significant investment for a small market (Australia) with a lower barrier to entry in other jurisdictions. How could the Australian government recognise five eye equivalent certifications in place of an IRAP for certain technologies? The reality is that cyber doesn't discriminate between geographical borders, so having solutions that treat it as such is a false positive.

Since the transition of the Australian Signals Directorate (ASD) no longer being the sole arbiter of an IRAP for a SaaS platform, we have slowed down the uptake of newer technologies. The new approach from ASD was to remove themselves as the bottleneck and provide more choice to government departments to take up technology based on their need. However, as a result we now have government departments fearful of being first, each one looking at the next on who is going to certify their XYX SaaS platform to PROTECTED first so they can follow suit. As a result, we as a country are falling further behind.

17. How should we approach future proofing for cyber security technologies out to 2030?

We recommend starting with the principle that the strategy will never be static. It needs to be flexible and a guideline, rather than prescriptive and tactical. The pace of technological change and threat landscape evolution would place any tactical policy out of date before the ink is dry.

With this understanding, we can start to determine how to build in flexibility and the horizons of change we predict so we can prepare for them.

1. Establish a focus / task force / section dedicated to Emerging Technology. Do not do this alone. Industry have invested heavily and is ahead of government. Lean on that fact. Maintain a working group with a mandate of being a horizon ahead to maintain greater pace with technology evolution;
2. We need to fight back the urge that we can't invest in emerging technology now, because it's not being adopted at scale, i.e., budgeting for the here and now. By investing heavier in year one on the next horizon, you will start to get an economic return on investment where we as a society and economy are better prepared for the emerging threat and therefore are not as impacted when the next breach occurs;
3. Maintain the government and industry collaboration during the life of the strategy with a focus on tweaks and updates to pivot for technology change;
4. Start to look at cyber as a global challenge, not just a sovereign one. Work with Five Eye nations as a tier one, NATO nations as tier two collaborators (as an example). Not just government, but industry players too. Run international threat modelling and cyber games to get different perspectives and

also see your own threat surface from a new vantage point, discovering vulnerabilities you never considered; and

5. Push industry further with regulations on their come to market for technologies and their inherent secure by design.

18. Are there opportunities for government to better use procurement as a lever to support and encourage the Australian cyber security ecosystem and ensure that there is a viable path to market for Australian cyber security firms?

There are opportunities through government procurement to leverage Australian industry and encourage and support Australian based cyber capabilities:

1. Leveraging existing models for sovereign participation like the Australian Industry Capability program to enforce a percentage of sovereign and Australian business participation in major procurements;

2. Standardising Australian control frameworks to widen the market for the sovereign capability to participate in and reduce the cost or barrier to entry;

3. Tax incentives for Australian innovation and capability along with government support in taking Australian capability to friendly global markets through diplomatic relations;

4. Education subsidy (like what Australia has done in the past for nursing and teaching degrees) in cyber security, with a commitment to work in Australia for Australian companies or government for a period of time (like the Australian Defence Force Academy with the University of NSW where a four-year engineering degree is paid back via five years of military service).

In adoption this approach, while we agree that it is vital for Australia to develop domestic capabilities, given that cybersecurity threats have a tendency to be global issues it will be important for these efforts to grow Australia's domestic cybersecurity capabilities to include opportunities for international firms to grow in Australia bringing easier access to resources all over the globe that will aid in the combating of cyber threats.

19. How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?

As technology advances it will be important for strategy to be revisited as technology changes, with recent advanced technologies such as artificial intelligence and cryptography, and quantum computing on the horizon, government must keep track of these technologies and the creative ways people will employ them in order to make sure that the strategy does not fall behind and Australia is left vulnerable to potential malicious use of the technologies. Some considerations:

1. Collaboration with industry and academia: The Strategy should promote greater collaboration with industry and academia to develop and promote best practices for securing emerging technologies. This can include partnering with technology companies and research institutions to identify emerging cyber security risks and develop solutions to address them.

2. Regulatory frameworks: The Strategy should work to develop regulatory frameworks that encourage the adoption of security by design in new technologies. This can include setting minimum security standards and requirements for emerging technologies, and providing incentives for companies that prioritise security in their product development.

3. Education and awareness: The Strategy should prioritize education and awareness initiatives that promote cyber security best practices and increase public awareness of the cyber security risks associated with emerging technologies. This can include promoting cyber security education and training programs for technology professionals, as well as public awareness campaigns to raise awareness of emerging cyber threats and how to mitigate them.

20. How should government measure its impact in uplifting national cyber resilience?

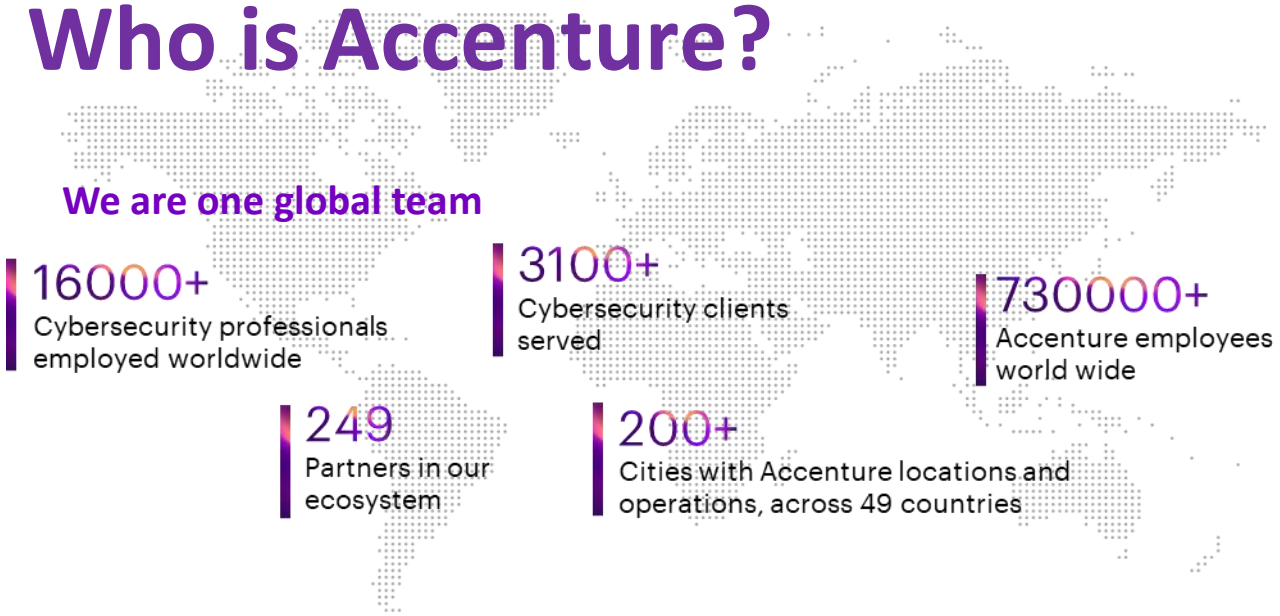
We need to consider that the term cyber resilience is just as much about the ability to pivot and *survive* a cyber incident as it is about protecting against or preventing them in the first place. Measures on volume of incidents is probably redundant, as the volume will increase. However, there are fringe elements to measure and consider the generational impact of the strategy.

1. Volume of certifications (standardised) in security in Australia;
2. Reduction in impact to cyber incidents (volume of citizen personally identifiable information impacted, number of citizen records impacted); and
3. Volume of industry and government collaboration with the uptake of threat intelligence sharing and resilience measures

21. What evaluation measures would support ongoing public transparency and input regarding the implementation of the Strategy?

Government should consider that the implementation of the strategy will continue to evolve over the next seven years to 2030. An open but clear communication with the public is necessarily in line with education and awareness measures. Because cyber is such an evolving threat, the general population would expect a static solution, and a solution immediately. Helping the public understand how cyber evolves and that advice will continue to evolve to keep pace will be positive for public perception.

Who is Accenture?



Who we are?

Accenture is a professional services company with a presence in over 120 countries, and over 730,000 employees globally. Accenture's purpose is to deliver on the promise of technology and human ingenuity by **unleashing creativity, inventiveness and limitless imagination**. We embrace the power of change to create 360° value for our clients, people, shareholders and partners. At the heart of every great change is a great human who has ideas, ingenuity and a passion for making a difference.

Locally, Accenture Australia has partnered with the Australian government for more than 30 years. Delivering some of the most complex transformations for both State and Federal governments.

Who Is Accenture Security?

Accenture is one of the largest cybersecurity service providers with 16,000 security professionals globally. Our service catalogue spans from Cyber Strategy and Risk services – helping you prepare and make the shift from defence and compliance to resilience, through to Cyber Protection – allowing you to accelerate your transformation journey with cloud, platform, data, and AI security, along with digital identity services; and Cyber Resilience – forensic and incident response, threat hunting, threat intelligence and threat assessment services. All supported by our network of security operating centres and cyber fusion centres globally to provide managed security offerings.