Submission in Response to the 2023-2030 Australian Cyber Security Strategy Discussion Paper

School of Computing and Information Systems
University of Melbourne

Contributors (in alphabetical order): Atif Ahmad, Shaanan Cohney, Suelette Dreyfus, Sarah Erfani, Liam Harding, Christopher Leckie, Sean Maynard, Toby Murray, Olga Ohrimenko, Adrian Pearce, Benjamin I P Rubinstein.

Executive Summary

We are grateful for the opportunity to provide input to the 2030 Australian Cyber Security Strategy currently under development. Our response makes some key recommendations, chiefly:

- Government should invest in research and development on future cyber threats enabled by advancing digital technologies, including AI, as well as on producing a body of evidence based organisational cybersecurity practices rather than those based solely on expert opinion.
- Strict prohibitions on ransom payments should not be pursued and in many cases are likely to be counter-productive for cybersecurity overall.
- Universities have a unique role to play in uplifting cybersecurity capability in the Indo-Pacific region and further investment here would be beneficial.
- Sufficient evidence does not currently exist for the benefits of mandatory cybersecurity education accreditation, beyond existing education accreditation regimes. Indeed, empirical survey evidence suggests that mandatory accreditation regimes could be counter-productive and reduce workforce diversity. Any accreditation regime must be informed by all stakeholders and recognise the distinct value of the various education providers.
- Efforts to uplift cyber skills and capability within Australia must extend beyond the traditional technology domains to include other professions that support cybersecurity activities (e.g., law, policy, executive management, etc.) as well as the public. Universities of course can and should play a vital role in these efforts.
- Australia should invest in risk-taking cybersecurity innovation to create an innovation pipeline to support sovereign cybersecurity capabilities, from inception at our universities and research institutions, through to commercialisation and productization, leveraging Australia's myriad unique home-grown commercial providers.

The Government released the *2030 Australian Cyber Security Strategy* discussion paper in February, and is calling for responses by April 15. This consultation process is part of the formation of the 2023 Cyber Security Strategy that the government is currently leading.

This response was prepared by a diverse group of academics from the University of Melbourne's School of Computing and Information Systems, whose combined expertise is unmatched in Australia, in terms of its breadth and depth across all aspects of cybersecurity. In 2017, University of Melbourne was selected as one of two Centres of Excellence in Cybersecurity; our recent work with the Department of Foreign Affairs and Trade (DFAT) resulted in us being selected as a preferred provider for cybersecurity skills training by DFAT. Our expertise spans deeply technical cyber domains like vulnerability discovery and assurance, data privacy and machine learning, through to information security management and executive education.

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?

We support introducing programs that will innovate and standardise practices for defending against vulnerabilities that arise out of digital technology, not least those relying on AI. Such programs should involve Universities, which house world-class research and expertise on emerging threats, in collaboration with government and industry. The government should also make use of its universities to develop empirical evidence about which cybersecurity practices are most effective, rather than relying on expert opinion and industry norms.

The need for such programs is due to Cybersecurity threats continuously evolving and leveraging modern technology[1]. The rapid evolution of digital technology, especially AI, means that vulnerability defence technologies created today are unlikely to be fit for purpose in 2030. With the rise of reliance on AI and its rapid development, we call upon government to develop programs to innovate and standardise practices to defend against vulnerabilities that future technology will undoubtedly face, especially those technologies relying on AI.

Universities and research providers have long played an important role in looking ahead to new threats and defensive capabilities and innovating at early technology readiness levels. The nation's cybersecurity strategy should seek to make the best use of our universities' world-class research and education capabilities, in partnership with government and industry.

We submit that the practice of cybersecurity in Australian organizations is heavily influenced by 'expert opinion' rather than empirical evidence. This expert opinion is sourced from consulting firms, product vendors, and 'best practice' industry standards. This is not surprising as cybersecurity is a rapidly evolving area which is driven by practice needs and solutions. However, given the considerable advancement in cybersecurity research at Australia's leading universities, there is an opportunity for Australia to develop a body of empirical evidence that provides a stronger basis for cybersecurity practices in organizations. This evidence-based practice would be a direct outcome of genuine collaboration between government, industry, and university research. This type of partnership exists in the domain of medical research and has led to invaluable outcomes such as the COVID-19 vaccine.[2].

[1] Tom Williams, 'Experts say AI Scams are on the rise as criminals use voice cloning, phishing and technologies like ChatGPT to trick people' *ABC* (online, 12 April 2023) https://www.abc.net.au/news/2023-04-12/artificial-intelligence-ai-scams-voice-cloning-phishing-chatgpt/102064086.

[2] See eg, 'Doherty Institute secures landmark agreement with Moderna to expedite vaccine research for infectious diseases' *University of Melbourne* (Media Release, 24 March 2022) https://www.unimelb.edu.au/newsroom/news/2022/march/doherty-institute-secures-landmark-agreement-with-moderna-to-expedite-vaccine-research-for-infectious-diseases; 'Moderna to build manufacturing facility at Monash' *Monash University* (Media Release, 15 August 2022) (noting this research hub is parly funded by the State Government) https://www.monash.edu/news/articles/moderna-to-build-manufacturing-facility-at-monash.

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

There will undoubtedly be a need for further legislative and regulatory reform to enhance cyber resilience across the digital economy. We submit that in pursuing these reforms, it is important than in the efforts to improve Australia's cybersecurity we do not lose important Australian democratic values, including transparency, accountability, a respect for individual privacy rights and worker rights.

By nature, many automated cybersecurity programs gather data on end-users, whether they be customers or employees. AI is accelerating this trend. The potential for this information to be repurposed is of concern. For example, data collected while a worker sits working at their desk may be gathered in the first instance automatically simply to look for anomalies which might suggest an intruder. However, this data might then be reused for a different reason for which it was gathered, for example an employer misusing it to determine if the worker took too many rest breaks, or perhaps didn't spend enough time on certain work activities. The employer might then draw conclusions (which may not be accurate if data is misinterpreted) about the worker, and potentially sell some data/conclusions about work habits/activities to international online job providers, en masse, as a source of revenue. This might all happen without the worker's knowledge.

Indeed, we note there have been various initiatives[3] within the past 20 years to investigate reform of laws regulating workplace surveillance; unfortunately, none of these have resulted in any substantial action.[4]

It is therefore important to establish protections for privacy and human rights in the context of a society where cybersecurity must increase. These protections should be embedded in law, and should bring together thought leaders in this space, with unions (since it will very likely affect workers across industries), privacy experts, NGOs, and academic researchers.

It must include diverse voices, including those with expertise outside the industry and those who know about and care deeply about digital privacy and human rights, and those who may be at times critical of the industry on privacy grounds. Without being inclusive, the outcome will not be robust. The time to do this now – not as an afterthought. Cybersecurity does not have to clash with digital rights for Australians, but the rapid expansion may do so if firm and thoughtful guardrails are not put in place as a matter of priority.

2.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?

2.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?

We do not support strict prohibitions on payment of ransom demands. The impact of a prohibition on ransom payments depends on the nature of the demand, which we submit should be distinguished as 'leak' or 'cripple' demands.

[3] 'Workplace Privacy' *Victorian Law Reform Commission* (Project Summary, 5 May 2005); 'Uniform workplace surveillance laws' *Australian Law Reform Commission* (Discussion Paper proposals, 27 March 2014); The former Standing Committee of Attorneys-General also convened a working party on the matter in 2008, arising out of the VLRC's work in 2005. Unfortunately the work was

In a 'leak' scenario, attackers steal sensitive information and demand a ransom payment in exchange for not leaking that information (whether publicly or to other parties, including selling it on the dark web). On the other hand, in a 'cripple' scenario, attackers instead encrypt critical business systems and data, effectively crippling an organisation, and demand a ransom in exchange for the decryption key (thereby restoring the organisation's access it its own systems and data).

'Leak' scenario

Paying the former is generally inadvisable as the benefits are too unclear. It is not possible for an organisation to verify whether their information has indeed been leaked privately (e.g., sold privately on the dark web to another party). Strong norms around not paying these kinds of ransom demands are already emerging, and we submit that this trend is likely to continue in the wake of high-profile instances in which Australian businesses opted publicly not to pay ransom demands even for significant volumes of highly sensitive information (such as in the case of the Optus and Medibank incidents in 2022). Therefore, outlawing this kind of payment is likely to have little impact.

'Cripple' scenario

We submit that 'cripple' scenarios are quite different, but that prohibiting ransom payments for those would be counter-productive overall for cybersecurity defence efforts in Australia. For Small and Medium Sized Entities (SMEs), these incidents are known to be crippling and paying such ransoms may be the only way to keep their businesses operating. Prohibiting such payments therefore forces a business to have to choose between staying afloat or breaking the law. Ransom payments are, by nature, difficult to detect.

We submit that enforcing a prohibition is likely to be very difficult. Prohibiting payments for 'cripple' scenarios would therefore induce a strong incentive for businesses to quietly pay such ransom demands, forcing them to keep quiet about cybersecurity incidents and exacerbating the existing culture of sharing too little information about cybersecurity incidents (with government, other businesses or the public). That would be incredibly unfortunate given the positive benefit of information sharing (e.g., to help improve cybersecurity practices across industries, or to enable government to assist in the event of large-scale breaches, etc.)

Finally, we note that if ransom payments are outlawed then companies who choose to pay ransoms open themselves up to further extortion attempts (since a criminal organisation now has evidence that the company has acted illegally and may threaten to expose the company to law enforcement). Thus, outlawing ransom payments may create additional opportunities for attackers.

2.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?

We submit the government should not have a position here. What they should do is provide guidance to Australian businesses about situations in which ransom payments have and have not been effective, and how to pay ransoms safely. We submit that government should also work with cyber insurance firms to strengthen norms around ransom payments since ransoms are often paid by making a claim against an organisation's cyber insurance policy. Therefore, cyber insurance firms are a key lever by which norms around ransom payments can be established.

---

subsequently abandoned in 2010. For summary of this initiative, see: Murray Brown and Normann Witzleb, 'Big Brother at Work – Workplace Surveillance and Employee Privacy in Australia' (2021) 34 *Australian Journal of Labour Law* 170, 189-90.

[4] Brown and Wizleb, (n 3) 'Big Brother at Work'.

We further recommend that the government provide formal guidance as to how payment of ransoms can be made in adherence with existing law. Specifically, sanctions regimes play a complicating role and the lack of guidance makes it more challenging for CISOs, boards, (and their associated entities) to determine the best course of action.

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

Australia can play a leading role in building cyber resilience in the Indo-Pacific region. Key strategies include (1) assisting in the development of cyber response and crisis management capability of critical infrastructure organizations in partner countries, (2) promoting information and intelligence sharing among key stakeholders in government, industry and academia to enhance collaboration and cooperation in the face of the complex and evolving threat landscape, (3) establishing standards to promote a common language and common standards of practice, and (4) providing cyber training programs to stakeholders in government, industry and academia.

Universities can play a key role in building regional cyber resilience. For example, Australian universities have been training high quality cybersecurity professionals for many years. Offering such training across the region through subsidized award and non-award programs (such as micro credentials) can rapidly advance the capability of nation-states while promoting standardization in knowledge and capability. Australian universities can train professionals in a range of cyber-related areas from strategy (e.g., in cyber leadership, risk management) to operations (e.g., in penetration testing, vulnerability patching) to law (e.g., law and ethics in cybersecurity).

There is a unique opportunity to build genuine cooperation and collaboration between cybersecurity researchers across the region. Such collaboration can lead to the transfer of cybersecurity knowledge sparking innovation in cybersecurity technologies and organizational practices. As an example of such an initiative, we point to a DFAT-sponsored project at the University of Melbourne that is developing Malaysia's cyber resilience and response capability.[5] An international team of researchers from the University of Melbourne and the National University of Malaysia are benchmarking the cyber response capability of three Malaysian critical infrastructure organizations against the leading purveyor of cyber practice in Australia. This exercise will lead to (1) a maturity model by which cyber response can be measured and improved, and (2) the training of one hundred Malaysian cyber executives on how to understand, measure and improve cyber resilience in their organizations. In addition to the industry outcomes, the project seeks to replicate the University of Melbourne's unique capability in conducting practice research in cybersecurity within the National University of Malaysia.

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

The research networks at Australian Universities present numerous opportunities to elevate the bilateral relationships between Australian and its regional partners from a cybersecurity perspective. At the core of this objective is mutual trust and a willingness to work together. With trust comes the sharing of information, knowledge, capability, and genuine partnerships by which mutual capability can be advanced to benefit the region.

[5] 'Developing Malaysia's Cyber Incident Response Capability' *University of Melbourne* (Research Project, 2022-24) https://findanexpert.unimelb.edu.au/project/107440-developing-malaysia%E2%80%99s-cyber-incident-response-capability

Universities form a natural network of knowledge centres across the region that can be leveraged as a trusted platform for promoting information and intelligence sharing among government, industry, and academia. Knowledge sharing can be conducted through training as well as research. Regional conferences and forums can be the hub for such sharing leading to partnerships on a range of new and exciting initiatives.

Further, as previously mentioned, Australian researchers have pioneered methods to produce empirical evidence that can provide a stronger basis for cybersecurity practices in organizations. This kind of research becomes particularly valuable when it is applied in different cultural and organizational contexts leading to a higher order understanding of commonalities and distinctions (e.g. due to national culture) in the practice of cybersecurity in organizations.

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?

We submit that any measures introduced to create incentives or mandates for organisations who have suffered a breach to share information with the ASD and ACSC need to be very carefully considered and should be based on empirical evidence about their effectiveness and need.

However, binding commitments that prevent intelligence services from further sharing company data obtained in aid of protecting Australian interests would likely strengthen trust and increase willingness to share.

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?

We submit that there should be expanded incentives for organisations to disclose cyber security incidents and that doing so would be beneficial overall for cybersecurity in Australia. Disclosure of incidents improves information sharing between different organisations about best practices and their effectiveness.

We agree that it may also help to improve public awareness about cybercrime; however, awareness through public disclosures of incidents alone is insufficient. Government should continue to invest in public cybersecurity education initiatives, which universities are ideally placed to aid.

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

We submit that a tailored approach could be helpful. We also submit that cyber skills uplift must happen across a range of professions well beyond the traditional technology workforce. For example, key stakeholders in improving Australia's cyber resilience include not only businesses executives, who must make informed choices about cyber security investment and response, but also those who investigate, prosecute, and adjudicate cybercrime in Australia. Again, universities have a key role to play in uplifting cyber skills including in these diverse domains. University of Melbourne is already active in this area but we contend that government should invest more in aiding training organisations to develop and deliver cybersecurity education tailored to non-technical professions (e.g. executive education, law, etc.)

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

We do not believe that sufficient evidence exists currently for the benefits of mandatory cybersecurity education accreditation, beyond existing education accreditation regimes. Indeed, the Australian Information Security Association (AISA) conducted a national survey of its members in 2022 found only mixed support from industry for introducing an accreditation scheme[6].

Perhaps most critically, surveyed employers did not support strict cybersecurity education accreditation. Employers valued aptitude (ability to learn), work experience and attitude well above all others, including industry certification. A university education that enhances students' ability to learn is therefore an important contribution to industry needs. This is doubly so in an environment that moves as quickly as cybersecurity, and agility requires more than just knowing the latest specific technology in a narrow area.

The AISA report, based on a national survey and on qualitative feedback from over 50 industry experts and executives from Australia's leading companies (such as CISOs, CSOs and CIOs) who form AISA's Executive Advisory Board, concluded that there was no single door of entry into the cyber security profession, and that accreditation was unnecessary, as it 'would need to be complex to be inclusive, and acts as a potential hurdle to new entrants to the industry'.[7] Thus, the risk is that a rigid accreditation system might impede flexible entry to the cyber workforce, forcing industry to hire what they could view as less suitable candidates who 'ticked boxes' but lacked the main criteria industry says it needs.

Further, the report noted a concerning aspect of certificate-based accreditation: females would be disadvantaged from such a scheme. The report identified that only 25.6% of female cyber security professionals have such certifications. This compares to males where 42.4% have them.

Employers in the AISA industry study were reported to significantly value a candidate's work experience, with two out of three students doing a placement transitioning into full time staff at their host organisation. While industry placements are highly valued, the process to enable them is often bespoke and difficult to streamline. Commissioning insights from the tertiary education community in how to streamline these processes might accelerate closing the labour skills gap in this area. The goal should be finding ways to provide work placements at scale. Incentive structures for this may need rethinking.

We submit that any accreditation regime must be informed by perspectives gathered from all major stakeholders (tertiary education providers including universities, commercial training providers, business consumers, and education accreditation organisations) and must be evidence-backed. Adopting an accreditation regime that is too narrowly informed or scoped will do more harm than good.

In addition, government must recognise the value provided by diverse players in the cybersecurity education market. For instance, universities provide principles-driven education, designed to last the lifetime of a career, and to be supplemented by on-the-job and continuing professional development activities. This model has served extremely well across all the professions. On the other hand, industry training provides a quicker entry into the workforce but requires more frequent retraining, because it does not provide the foundational underpinnings necessary for knowledge and skills transfer. Each has a vital role to play in the cybersecurity education market and any accreditation regime should not prioritise one over the other.

The government should invest in reducing the cost of cybersecurity training to students, especially those from underrepresented backgrounds. Education investment should go beyond the traditional technical skillset to encompass

---

[6] AISA, *Research Into Cyber Security Accreditation in Australia* (Report, September 2022) https://www.aisa.org.au/public/News_and_Media/News/2022/AISA-Accreditation-Survey-Report-2022.aspx

[7] AISA (n 6) 2.

executive education and those from diverse fields like business management, legal and policy. Further resources should also be invested in public education, recognising the key role that universities can play in this area as independent, unbiased experts.

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 future of cybersecurity in Australia relies on educating future specialists, their integration into the industry sector and ongoing conversations between industry and the education sector. The government should further invest into programs encouraging collaboration between universities and industry, as well as facilitation of international collaborations. Such programs can create a two-way stream that translates best practices to industry and informs the universities about the most prominent problems faced by industry. This ongoing relationship can ensure that new applications or technology developed in the industry is communicated to security experts and emerging technology goes through an analysis for potential cyber threats.

Government should invest in and support sovereign cybersecurity capabilities, throughout the entire lifecycle from research and conception through to productization and commercialisation. Australia has myriad unique areas of cybersecurity expertise unmatched elsewhere in the world, from world-leading research groups at its universities through to commercial providers of cybersecurity education and services. Investment that stimulates an innovation pipeline from the former to the latter would help to strengthen our sovereign capabilities.

Specific key opportunities for government include financial support for practical experimentation on bringing together user-focussed design expertise with cybersecurity functionality. Understanding how end-users accept or reject a technology, based on how easy it is to use, needs to be applied more successfully to cybersecurity tools and processes. Some grant funding that open-sourced findings from this work could aid the entire ecosystem in Australia, rather than making findings proprietary and limiting the usefulness to Australian society as a whole. Given that cybersecurity is increasingly a public good, much like clean air or water, and that it largely depends on a critical mass of the ecosystem being secured (rather than just a few players in it), there is a real role for government to support research and application that is open source here.

Further, government also has a role to play in encouraging risk-taking innovation. Aspects of the industry are, quite reasonably by nature, risk averse and risk mitigating. However, Australia cannot 'stay ahead of the game' by incrementalism in this space. The rest of the world is moving too quickly. Funding bold pilots and experimentation is crucial. That means not punishing innovations–or innovators–who fail.

Of course, the nature of politics can make this difficult to stomach. Thus, such a program should be purposefully designed, with the intent to fund small-cost experimentations some of which will fail.

Finally, government-supported public outreach that is aimed at grass-roots education and adoption will be important to any widespread societal adoption. Through public events and media outreach by independent experts, such as academics, it is possible to nudge the dial on population awareness and action. Provocative traveling art exhibits that are interactive and engage in public spaces are also a good way to bring cybersecurity messages to a population of young people who may ignore traditional promotional marketing.

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

The emergence of new technologies and platforms is creating the potential for a new generation of advanced cyber threats. For example, the rapid evolution of off-the-shelf artificial intelligence and machine learning services is creating

the potential for adversaries to create new types of AI-enabled attacks that are highly automated and stealthy. Agencies such as Europol have already reported the first signs of such attacks.[8] However, the resources of Australian industry are stretched just trying to meet the challenges posed by existing cyber security threats. Future defences using artificial intelligence may be vulnerable to attack themselves, with classifier "poisoning attacks" similar to incidents observed in the wild targeting consumer anti-virus.[9] It is vital for Australia to understand how these attacks of the future are likely to operate, so that we can proactively anticipate the threat and devise appropriate countermeasures, rather than reactively relying on our over-stretched cyber security teams to play catch-up once these new threats have emerged. Key steps to future-proof our cyber security capabilities to meet these emerging threats include:

- Government has a key role to play in developing a focused agenda and funding research and development programs to identify and prepare for these attacks of the future.
- Universities and other research providers can provide the capability to conduct research into these attacks of the future and help devise appropriate responses.
- Universities, as centres of teaching, can train future industry leaders on the emerging digital technologies relevant to tomorrow's attacks and mitigations.
- Given the sensitive nature of this research, it is vital that there be a trusted information sharing network between appropriate government agencies, universities and industry partners, so that emerging threats, their potential impact and appropriate countermeasures can be rapidly identified and shared.

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

The Australian government should prioritize the effectiveness of cyber security technologies above the promotion of local industry. The promotion of local industry is a worthwhile goal, and where proposals from two entities provide *otherwise equivalent security* it is worthwhile to tie-break in favour of Australian enterprises. However, "not invented here syndrome" too often is the cause of insecure deployments and systems. Concurrently, there are strong national security grounds to favour solutions operated and developed in jurisdictions that are closely aligned with Australian values and national interests. This principally incorporates Australia and our five-eyes allies.

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

To ensure the strategy stays abreast of cybersecurity issues arising out of emerging technologies, we submit the strategy should encourage partnerships between the University sector, industry and government to leverage the world-class research expertise available in Australian universities.

The strategy might encourage industry, government and the University research sector to partner to identify emerging digital technologies, and how these might impact the future cyber security landscape. For example, while AI might be weaponised by attackers to scale and amplify their capabilities, AI that is adopted in defensive systems might itself be susceptible to attack.

---

[8] Trend Micro Research, United Nations Interregional Crime and Justice Research Institute (UNICRI), Europol's European Cybercrime Centre (EC3), 'Malicious Uses and Abuses of Artificial Intelligence' (Report, 7 December 2021)https://www.europol.europa.eu/publications-events/publications/malicious-uses-and-abuses-of-artificial-intelligence.

[9] Joseph Menn, 'Exclusive: Russian antivirus firm faked malware to harm rivals – Ex-employees', *Reuters* (London, 14 August 2015).

Such partnership can be facilitated by funding programs to support high-risk high-reward basic research, and initiatives supporting information sharing.