MACQUARIE
University

Discussion Submission to the 2023-2030 Australian Cyber Security Strategy

Macquarie University Cyber Security Hub

TABLE OF CONTENTS

Discussion Submission to the 2023-2030 Australian Cyber Security Strategy ... 1

Foreword ... 3

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? ... 4

2. What legislative or regulatory reforms should Government pursue to: enhance cyber resilience across the digital economy? ... 6

2.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)? ... 6

2.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? ... 6

2.c. Should the obligations of company directors specifically address cyber security risks and consequences? ... 7

2.d. Should Australia consider a Cyber Security Act, and what should this include? ... 7

2.f. What impact would a strict prohibition of payment of ransoms and extortion demands by cyber criminals have on victims of cybercrime, companies and insurers? ... 8

6. How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities? ... 8

7. What can the government do to improve information sharing with industry on cyber threats? ... 9

10. What best practice models are available for automated threat-blocking at scale? ... 9

11. Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda? ... 9

12. What more can government do to support Australia's cyber security workforce through education, immigration, and accreditation? ... 10

14. What would an effective post-incident review and consequence management model with industry involve? ... 11

17. How should we approach future proofing for cyber security technologies out to 2030? ... 11

19. How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies? ... 12

FOREWORD

Thank you for the opportunity provided by the discussion paper to contribute our views to shape the Australian Government's approach to domestic and international cyber strategy. The following represents views and comments by several academics and cyber security experts from the Macquarie University Cyber Security Hub. They are:

Academics and Cyber Security Experts	
Name	**Title**
Professor Dali Kaafar	Executive Director of the MQ Cyber Security Hub, Faculty of Science and Engineering Director of Cyber Curriculum NSW Institute of Applied Technology Digital
Professor Niloufer Selvadurai	Director of Research and Innovation, Macquarie Law School
Associate Professor Babak Abedin	Head of the Department of Actuarial Studies and Business Analytics, Macquarie Business School
Dr. Dinusha Vatsalan	Senior Lecturer, Faculty of Science and Engineering
Dr. Hassan Asghar	Senior Lecturer, Faculty of Science and Engineering
Dr. Muhammad Ikram	Senior Lecturer, Faculty of Science and Engineering
Dr. Benjamin Zhao	Postdoctoral researcher, Faculty of Science and Engineering
Michael Chen	Senior Cyber Project Manager, NSW Institute of Applied Technology Digital, Faculty of Science and Engineering

We have selected a set of questions provided in the discussion paper, and address them below.

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 Dali Kaafar

The need for regulation that enforces formal and provable cyber security processes. If it is probably secure, it probably isn't.

For a nation to be cyber secure, it crucially needs to strengthen data Collection regulatory constraints and most importantly to enforce formal methods and provably secure processes for data storage and data analytics within public and private organisations alike. The Cyber Security Strategy has to ensure Australia is pro-actively and provably secure against data breaches. Formal and provable techniques to protect data include well documented and industry-grade use of cryptographic methods for storing data in an encrypted form while still allowing data analytics.

Australia requires a more ambitious, innovative and firmer strategy for data collection and storage. We need to regulate in an explicit way how organisations collect, retain, store and use data (including individuals data). There is clearly a need to formalise the processes by which organisations collect and store customers data. Very often data is only required for one-off processes (e.g. for identification purposes) in which cases data is not needed to be retained. Similarly, governments should legislate on transparent data management and data workflows within organisations. These could include the need to enforce specific privacy preserving frameworks (e.g., Differential privacy or secure multi-party computation) to quantify the level of privacy risks of data stored within organisations or the enforcement of the encryption of data at rest or data processes only at government-certified data analytics secure enclaves by organisations. In other words, encryption and provable preserving technologies should become the norm in Australian organisations, public and private alike.

From Babak Abedin

The need to include cyber education in primary and high school education: Much of attention to cyber security has been focused on organisations and professional workers and senior decision makers. However, younger people and even children have often been ignored in cyber plans. Cyber education needs to be included in primary schools and continued all the way to high school and tertiary education so as to build a resilient cyber culture in the society. Given the dynamic nature of cyber-attacks, Australia needs to build fundamental cyber knowledge and awareness across different cohorts of digital users in all states and regions.

From Benjamin Zhao

The need for protections for proactive vulnerability mitigation: Many of the current ideas within the Strategy take on a post-cyber event stance, mitigating the subsequent impact on individuals and businesses following such a breach. We urge the consideration of proactive approaches to supplement the existing post-event state of thought. For example, inroads are made to bring awareness to harden a system against security vulnerabilities through findings by security researchers on high-level risks to systems, or specific deployed weaknesses in current systems through penetration testing by internal or external contractors. Beyond these two groups, there also exists the ability for non-affiliated persons, 'white-hat hackers', to perform tests against company systems. Each of these entities should be provided accommodations in the search for vulnerabilities without fear of legal ramifications, provided diligent disclosure of found vulnerabilities are performed. The ACSC has provided guidelines to businesses about Vulnerability Disclosure Programs, however there remains real examples whereby individuals disclosing vulnerabilities continue to be legally pursued by the vulnerable company/organisation, to force the cessation of their actions, often to suppress the existence of their findings (https://threats.disclose.io/). Such actions discourage benevolent actors from finding system flaws, leaving potential flaws intact for malicious actors.

From Niloufer Selvadurai

The need for an integrated multidisciplinary approach: We recommend the adoption of a multidisciplinary approach to cyber security policy and practice, integrating understandings from computer science, data science and engineering, as well as law and regulation. In addition, domain specific expertise, such as from finance, education and energy, should be incorporated as needed. Such a holistic approach is critical to ensuring that cyber security initiatives are both technically sound and address wider socio-economic considerations. Legal expertise is necessary to design effective laws and regulations, and also ensure that effective monitoring and enforcement mechanisms are implemented to support compliance.

From Muhammad Ikram

The need for user awareness and informed decisions via empirical analysis. The empirical analysis of systems and applications is essential for informed decisions and awareness regarding the security and privacy risks associated with web and mobile platforms that play a critical role in our daily lives. Despite the convenience offered by these platforms, the lack of privacy and security protections in many mobile apps is a growing concern. Research has shown that the majority of mobile health apps fail to comply with laws and regulations related to privacy protections, which can lead to serious privacy breaches and violations.

To ensure the protection of user data, it is essential that mobile app developers meet minimum security standards and keep up-to-date with the latest security measures. This includes combining multiple security features and employing binary protection techniques to prevent reverse-engineering of app binaries.

Efficient attributions of privacy and security risks are proposed to enable timely and effective mitigations of potential cyber attacks on mission-critical platforms, sensitive enterprise networks, and the Australian digital infrastructure. Rapid risk triage is necessary to assess the coverage and costs of potential breaches within heterogeneous environments. The project addresses cyber security, protective security, and offensive cyber challenges, with a focus on automating at-scale response to ensure comprehensive protection against cyber threats.

2. WHAT LEGISLATIVE OR REGULATORY REFORMS SHOULD GOVERNMENT PURSUE TO: ENHANCE CYBER RESILIENCE ACROSS THE DIGITAL ECONOMY?

2.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)?

From Dali Kaafar

Regulation mandating provable and transparent cyber security defence mechanisms and data security processes both pre and post cyber breaches. Regulation should also include mandatory disclosure of breaches as soon as such breach becomes known to the organisations regardless of the nature of the data and independently from the impact assessment of the coverage, impact or persistence of the threat or lack thereof. Regulation should also Impose penalties and fines on organisations that fail to prove they implement adequate cybersecurity measures, including but not limited to the Essential 8 Maturity model.

From Niloufer Selvadurai

There are a few matters to be considered. Firstly, it is important to identify relevant stakeholders and consult as to what is needed to support cyber security. This should not be limited to industry peak bodies but should also involve consultation with the sectors at high cyber security risk, such as transport, telecommunications, health and energy. Secondly, it is important that the consultation process is not limited to the substantive content of new laws (or revisions of existing laws) but extends to how we develop effective enforcement mechanisms. It is necessary to get buy-in from high-risk sectors and ensure that they are able to effectively comply with the legal requirements and support law enforcement agencies as required. The best laws in the world will do little to deter cyber security attacks if the enforcement mechanisms (as distinct from the laws) are ineffective. Finally, enforceable legislation and regulation should be supported by appropriate Guidelines and Practice Notes, further supported by community-wide education through public campaigns. At present the public is highly cognisant of the dangers of privacy breaches (due to the publicised Cambridge Analytica and other scandals) but not sufficiently aware of the cyber security risks they face on a daily basis, including through online banking and shopping.

2.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?

From Dali Kaafar

Yes, customer data regardless of the (potentially subjective and not quantified) appreciation of sensitivity of such data is to be included in an extended definition of “critical assets”. Research has demonstrated that it is extremely challenging to assess whether a piece of data can be considered as potentially personally identifiable or not, in particular with advances in machine learning and AI capabilities that extend the capabilities of adversaries to exploit seemingly harmless and non identifiable information.

From Niloufer Selvadurai

Yes. The Security of Critical Infrastructure Act 2018 (Cth) (SOCI) was based on traditional understandings of critical infrastructure – electricity, gas, water and ports. Subsequent legislation, the Security Legislation Amendment (Critical Infrastructure) Act 2021, passed in December 2021, and the Security Legislation Amendment (Critical Infrastructure Protection) Act 2022, passed in March 2022, expanded the sectors deemed to be critical. However the notion of 'assets' remains central to the protections provided. It would be useful to extend the protection of the SOCI regime to 'critical systems' so as to make the legislation more easily applicable to critical networks and systems.

2.C. SHOULD THE OBLIGATIONS OF COMPANY DIRECTORS SPECIFICALLY ADDRESS CYBER SECURITY RISKS AND CONSEQUENCES?

From Dali Kaafar

Yes, with accountability and responsibility of the company directors being articulated and tied to a regulatory framework that mandates the implementation of provable security mechanisms and explicit processes to protect customer data within the organisation.

2.D. SHOULD AUSTRALIA CONSIDER A CYBER SECURITY ACT, AND WHAT SHOULD THIS INCLUDE?

From Niloufer Selvadurai

It is not clear that a whole new *Cyber Security Act* is required. Many existing criminal and civil laws apply to cyber security. Notable examples include the cybercrime provisions in federal and State criminal legislation, as well as the offences in the *Telecommunications Act* 1997 (Cth). Other examples include State civil liability statutes (e.g in NSW, liability for negligence is based on a notion of duty of care that derives from the evolving common law, enabling it to potentially expand to encompass cyber security related breaches and ransomware etc), and the federal *Australian Consumer Law* (e.g. product safety laws that apply to devices). A separate new *Cyber Security Act* may create areas of overlap and confusion. Before any such Act is enacted, it would be useful to carefully map the operation of existing laws and identify clear gaps in the legislation that need to be addressed. Specifically, this would require: (a) Identifying gaps in present laws; (b) Analysing whether and to what extent existing laws can be reformed and/or expanded to address such gaps; and (c) designing new laws as necessary, with close regard to other existing laws. In such a way it would be possible to develop a clear and harmonious Cyber Security legislative scheme. It is relevant to note that in the area of AI liability, the European Commission's September 2022 *AI Liability Directive* does not propose a new AI act but rather suggests refinements to existing laws to broaden their scope of operation. It is however early days, and it would be useful to carefully consider all options – A whole new *Cyber Security Act,* expansion of existing law and/or new targeted specific cyber security provisions.

2.F. WHAT IMPACT WOULD A STRICT PROHIBITION OF PAYMENT OF RANSOMS AND EXTORTION DEMANDS BY CYBER CRIMINALS HAVE ON VICTIMS OF CYBERCRIME, COMPANIES AND INSURERS?

From Dinusha Vatsalan

Prohibition of ransom payment shifts focus of cybercriminals: The legitimate users (victims of cybercrime and companies) would lose trust with the cyber governance and cyber security law and regulations. It could also create a precarious situation for the legitimate users as they will be in the pressure of losing their data, while not being able to legally make the ransom payment. Implementing laws for strict prohibition of ransom payment could also shift the focus of cybercriminals to most vulnerable organisations, especially small and medium-sized businesses.

6. HOW CAN COMMONWEALTH GOVERNMENT DEPARTMENTS AND AGENCIES BETTER DEMONSTRATE AND DELIVER CYBER SECURITY BEST PRACTICE AND SERVE AS A MODEL FOR OTHER ENTITIES?

From Hassan Asghar

Cybersecurity as a service. Small companies and startups may not have the resources to implement state-of-the-art cyber security protections into their products. Such companies should be given access to cost-effective cyber security services that makes it easier for them to integrate security in their products from the beginning. This is similar to provision of compute resources to startups by online cloud service providers like Amazon AWS, and email services through web-based email service providers like Google's Gmail. Of course, such a cyber-security service needs to be developed and constantly updated with the latest cybersecurity best practices. The Government can help initiate and steer such a project which should include industries, agencies and Australian universities.

From Babak Abedin

Mandatory on-going in-job staff and management training: Over 80% of cyber attacks and risks are human related and hence human-related measures must be given the top priority in a cyber mitigation plan. For Government Departments to better demonstrate cyber practices, Government staff need to receive generic on-going mandatory in-job cyber training as well as domain specific field specific cyber education in their role. This needs to become embedded in hiring and job training as well as performance review processes similar to other mandatory courses such as respect at work and work safety training.

7. WHAT CAN THE GOVERNMENT DO TO IMPROVE INFORMATION SHARING WITH INDUSTRY ON CYBER THREATS?

From Dali Kaafar

By mandating the use of provably private technologies for data sharing, data storage and data analytics, the government would enable the potential for data sharing without the concern of information leakage, privacy violation or loss of competitive advantage. Several mathematically proven frameworks (as opposed to ad-hoc techniques) such as Differential privacy or homomorphic encryption based techniques have been already applied in several domains (mobility data, health related data, etc.) and can be generalised to the wider context of organisations-owned data and in particular threat intelligence data.

The government should consider setting up a national provably confidential platform for threat intelligence sharing to be developed as a joint partnership between the department of Home Affairs, Australian Department of defence and Australian organisations including Australian universities and researchers who have a demonstrated world class track record in research and development in privacy preserving data sharing.

10. WHAT BEST PRACTICE MODELS ARE AVAILABLE FOR AUTOMATED THREAT-BLOCKING AT SCALE?

From Dinusha Vatsalan

Threat intelligence gateways: Taking actions for threat-blocking still relies heavily on human intervention. For example, intrusion detection systems identify any unusual patterns in the network and alerts the system administrator to take any actions. One of the main hurdles of automating threat-blocking with most of the existing cyber security techniques is the inability to handle threat intelligence at scale. Threat Intelligence gateways have emerged as a new category of cyber security technologies enabling organisations to block threats in real-time analysing and predicting using massive volumes of threat intelligence data/indicators. Threat Intelligence Gateways are highly efficient (around 10Gbps+ performance) and scalable (around 4+ million Indicators processing in memory) in blocking of known threats at the perimeter, such that those known threats can be filtered out automatically in the first-pass triage and resources can be freely used to tackle unknown or more complex threats in the second-pass triage.

11. DOES AUSTRALIA REQUIRE A TAILORED APPROACH TO UPLIFTING CYBER SKILLS BEYOND THE GOVERNMENT’S BROADER STEM AGENDA?

From Michael Chen

STEM education is important for developing foundational technical capabilities for Cyber Security. However Cyber Security as a major challenge is intrinsically a multi-disciplinary problem to tackle, that requires a cross pollination of cyber skills training from the technical to the governance and compliance facets of cyber security across intelligence, data science and legal and ethics. These skills can be developed in micro-skills and micro-credentials such as cyber breach simulation and crisis management simulation, digital forensics, AI for cyber security, penetration testing, ethical hacking and offensive security, system and network attack simulation, security management leadership, cyber governance and planning, legal obligations and compliance, and data privacy in legal perspective and technical cross-perspectives.

To address these specific cybersecurity skills, Australia requires a tailored approach that overlaps with the broader STEM agenda to uplift cyber skills. This may include targeted cybersecurity education programs co-designed and co-delivered by the industry and academia for new-skilling, up-skilling and re-skilling, development of Australian cybersecurity framework, and cyber range training facilities for real-world simulated and emulated cyber-attack scenarios for practising cyber skills. The government could also partner with industry and education providers to develop a cybersecurity career pathway, including apprenticeships, internships, and work experience opportunities, as well as career development and mentoring programs for different focus groups including women, and aboriginals.

12. WHAT MORE CAN GOVERNMENT DO TO SUPPORT AUSTRALIA’S CYBER SECURITY WORKFORCE THROUGH EDUCATION, IMMIGRATION, AND ACCREDITATION?

From Benjamin Zhao

Australia has enacted policies to encourage the update of STEM subjects from Primary, Secondary and Tertiary education. However, specifically in relation to the development of cyber skills to safeguard Australia’s cyber security workforce, and ability to develop new technologies for the sector, there is a deficiency in the number of individuals seeking to undertake postgraduate studies, to push the envelope of knowledge in the cyber security space.

Particularly for domestic postgraduate research in Computer Science and Engineering, which cyber falls under, many potential candidates are dissuaded from pursuing further study due to uncompetitive stipends of the Research Training Program. A graduate moving directly into industry can expect multiples of what is offered from pursuing research. This places a handbrake on the capacity in which research organisations can train new talent, and consequently the number of highly trained individuals contributing to sensitive areas of research. I would recommend additional financial support for prospective postgraduate researchers to bolster the available talent in projects for emerging cyber threats, and more broadly lift the attractiveness of the Research Training Program (RTP) stipends in light of major challenges in attracting domestic students to postgraduate studies in the general area of STEM and cyber security in particular.

From Michael Chen

The field of cyber attacks is constantly evolving and getting more sophisticated, as cyber criminals come up with new methods and techniques to target individuals, organisations, and governments. There is growing demand for cybersecurity professionals in the workforce. More support from the Government through education and accreditation is essential for helping Australia’s cyber security workforce protect critical infrastructure, reduce the impact of cyber attacks, promote innovation and competitiveness, and protect national security. A range of initiatives include focused cybersecurity education programs, cybersecurity-specific training, industry-led certification and cyber range training facilities.

14. WHAT WOULD AN EFFECTIVE POST-INCIDENT REVIEW AND CONSEQUENCE MANAGEMENT MODEL WITH INDUSTRY INVOLVE?

From Hassan Asghar

Knowledge sharing of data breach instances. At present organisations and agencies are required to notify OAIC about cyber security incidents especially data breach incidents. However, these notifications are generally of a declarative nature and seldom release any details about the technical causes of such incidents. In some cases, one can make educated guesses on the possible cause of data breaches through information scattered on the news web, e.g., the use of an unauthenticated public facing API in the case of Optus, and the misuse of employee credentials at Latitude Financial. But even in these rare instances, disclosed information is not enough to paint a complete picture of the hack. For instance, what caused the employee credentials to be leaked to the attackers in the case of Latitude Financial? We strongly believe that the lack of transparency surrounding the cause of such data breaches is hampering Australia's efforts to improve cybersecurity best practices across its organisations and agencies. The victim organisation, by virtue of experiencing the cybersecurity breach firsthand, and having full knowledge of the cause of the breach, can improve its cyber security toolkit to avoid recurrences. However, other organisations may still be vulnerable to such attacks unaware of the practices that may be causing such data breaches. Lack of transparency is also a significant hindrance to the possible collaboration between cybersecurity practitioners and academia which can advance technologies that mitigate instances of breaches in the future. Secrecy around exact causes of data breaches is understandably attributable to reputation concerns. A suggestion is for this information to be available per-need-basis to cybersecurity researchers and practitioners in a way that does not adversely impact organisational reputation, while simultaneously helps everyone get a clearer idea of cybersecurity mistakes commonly leveraged by cyber attackers.

17. HOW SHOULD WE APPROACH FUTURE PROOFING FOR CYBER SECURITY TECHNOLOGIES OUT TO 2030?

From Dinusha Vatsalan

A zero trust approach: Future proofing for cyber security technologies should be following a 'zero trust' approach. Cybercriminals continue to evolve and cyber threats are growing increasingly sophisticated, hence legacy cyber security techniques may no longer be enough. A zero trust and end-to-end security approach should be enforced throughout the whole digital economy.

A good offence is the best defence: Future proofing of cyber security technologies should be prioritised based on proactive solutions rather than reactive solutions (e.g. intrusion prevention systems over intrusion detection systems). Proactive solutions, such as intrusion prevention systems, take automated actions when events that are likely to cause damage are detected, whereas reactive solutions address issues only after they have become problematic. Prevention is the best form of defence that proactively identifies and prevents an attack before it impacts the systems and network. In order to build proactive solutions, the businesses or organisations implementing or using cyber security solutions should be focusing more on the offensive side rather than on the defensive side. A holistic approach that combines a blue/defensive team, who will be building secure solutions, and a red/offensive team, who will be evaluating vulnerabilities and breaking through cyber security defences, through the use of a hybrid/purple team for developing and future proofing cyber security technologies need to be practised and followed in the industries.

19. HOW SHOULD THE STRATEGY EVOLVE TO ADDRESS THE CYBER SECURITY OF EMERGING TECHNOLOGIES AND PROMOTE SECURITY BY DESIGN IN NEW TECHNOLOGIES?

From Dinusha Vatsalan

Mandatory basic cyber hygiene features: Cyber security has evolved from being post-development consideration to design-phase consideration in new technologies development, and hence the emerging technologies, such as using Blockchain technology, quantum computing, serverless computing, and AI assistants, need to be built as secure by default. Similar to how airbags were introduced in cars as options, but later made as mandatory safety equipment in all cars, basic cyber hygiene protections need to be built into the emerging technologies by design as mandatory features. For example, cyber security protections like multi-factor authentication, mandatory backup features, and prohibitions on non-encrypted connections, need to be designed in any new technologies or systems as mandatory featur

MACQUARIE
University

Macquarie University is a vibrant hub of intellectual thinkers, all working towards a brighter future for our communities and our planet.

A PLACE OF INSPIRATION

Macquarie is uniquely located in the heart of Australia's largest high-tech precinct, a thriving locale which is predicted to double in size in the next 20 years to become the fourth largest CBD in Australia.

Our campus spans 126 hectares, with open green space that gives our community the freedom to think and grow. We are home to fantastic facilities with excellent transport links to the city and suburbs, supported by an on-campus train station.

RENOWNED FOR EXCELLENCE

We are ranked among the top two per cent of universities in the world, and with a 5-star QS rating, we are renowned for producing graduates that are among the most sought after professionals in the world.

A PROUD TRADITION OF DISCOVERY

Our enviable research efforts are brought to life by renowned researchers whose audacious solutions to issues of global significance are benefiting the world we live in.

BUILDING SUCCESSFUL GRADUATES

Our pioneering approach to teaching and learning is built around a connected learning community: our students are considered partners and co-creators in their learning experience.

FIND OUT MORE

Macquarie University NSW 2109 Australia
T: +61 (2) 9850 7111
mq.edu.au

ABN 90 952 801 237
CRICOS Provider 00002J