CHECK POINT RESPONSE TO 2023-2030 AUSTRALIAN CYBER STRATEGY DISCUSSION PAPER

PREPARED BY:
ASHWIN RAM | SECURITY EVANGELIST
VIVEK GULLAPALLI | FIELD CISO
PETER NICOLETTI | FIELD CISO

April 2023

CHECK POINT RESPONSE TO 2023-2030 AUSTRALIAN CYBER STRATEGY DISCUSSION PAPER

> "THE MOST PRESSING NEED FOR SAFEGUARDING AUSTRALIANS LIES IN ROBUST POLICIES THAT ADDRESS THE EVER-EVOLVING AI THREAT LANDSCAPE, ENSURING OUR NATION'S SECURITY AND RESILIENCE."

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?

- National-level Cyber Strategy Framework: Develop a straightforward and comprehensible framework for strategy, execution, and evaluation. The framework ought to concentrate on CIIs and concentration risk that may impact the functioning of the government and affect citizens' lives. The framework should hold Boards & C-Levels personally accountable & responsible, not merely the organisations. The focus is on having robust governance with "safety and soundness" while ensuring business continuity.

- A resilient critical infrastructure environment: Establish a first layer of self-healing/adaptive preventative security controls provided by the government, with frameworks that encourage organisations to concentrate on attack prevention.

- Cyber awareness training: Incorporate cyber awareness education into primary school curricula and provide multilingual resources to ensure all community members understand cyber risks and online safety.

- State Level Cyber Security Ministers: Appoint a Cyber Security Minister at the state government level for every state and territory in Australia.

- Cybersecurity Legislation: Implement legislation outlining essential security controls and practices.

- Mandatory Incident Response Testing: Mandate organisations with over 1,000 employees or those handling/processing Personal Identifiable Information (PII) to conduct regular incident response testing and reporting.

- Collaboration: Encourage cooperation across government, industry, and academia.

- Research and Development (R&D): Foster an R&D culture centred on emerging cybersecurity research.

- Cyber Strategy Framework: Develop a clear and easily understood framework for strategy implementation and evaluation.

- Accountability: Call out cyber security controls from vendors that are not effective or have a track record of being exploited due to vulnerabilities within the security vendors product.

- Leverage international security grading reports that rank countries and industry verticals against ISO (and NIST) compliance as well as number of incidents and costs to ensure Australia gains against the rest of world.

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

Privacy and Cybersecurity are interlinked, and thus harmonisation of laws across all of Australia will enable companies to operate easily (without regulatory burden) whilst ensuring safety and soundness. Integrate cybersecurity and privacy into a single law across various States and Territories.

Bringing cybercriminals to justice, particularly those outside the jurisdiction of Australia. Hence, international treaties to expedite justice, as well as the ability to issue "cease and desist" orders for malicious websites and applications that impersonate or scam Australian citizens, businesses, and governments.

Having cybersecurity expertise on the board and having a dedicated CISO who reports to the board and CEO would provide accountability and drive execution.

In addition, maintain uniformity in legislation and regulations across Australia. Ensuring consistency in cyber and privacy laws throughout various States and Territories within the nation is crucial for standardisation. Disparate legal frameworks can lead to difficulties in achieving a coherent and unified approach to these critical issues.

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)?

Tighten the existing Security Legislation Amendment (Critical Infrastructure Protection) Act 2022. As cybersecurity is an evolving discipline, enhance the cybersecurity ecosystem that fosters collaboration between government, academia, organisations, talent and security product vendors.

Create a certification scheme that recognises security vendors to build confidence for organisations that purchase the product or services.

Adopt international standards like ISO to encourage interoperability and collaboration.

Look at the leading laws for consumer privacy protection and overall security programs and ensure that Australia leads.

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?

Yes, any organisation that transfers, processes or stores customer data in electronic format must be subjected to the Critical Infrastructure Act.

It should be mandated that all organisations defined as Critical Infrastructure must:

- Establish comprehensive cybersecurity incident response strategies that encompass all relevant departments, legal contacts, and reporting obligations.

- Execute cybersecurity tabletop exercises on a quarterly basis to ensure preparedness.

- Regularly perform vulnerability assessments and implement necessary remediations to maintain a secure environment.

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

Yes, the obligations of company directors must address cybersecurity risks and consequences. They have a fiduciary responsibility to safeguard their organisation's assets, reputation, customers and stakeholders. Addressing cybersecurity risks is crucial to fulfilling this duty. Given directors are responsible for establishing their company's risk management strategy, incorporating cybersecurity risks will ensure a comprehensive approach to risk mitigation.

The failure of directors to address risks and issues should have fines and other legal consequences.

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

Yes.

- Mandate organisations to establish a cybersecurity charter that clearly delineates roles and responsibilities. Ensure that employees and customers can effortlessly identify the parties responsible and accountable for cybersecurity, as well as those who must be informed and consulted regarding cyber-related tasks and initiatives.

- All Critical Infrastructure entities, not solely Systems of National Significance (SoNs), should be subject to Enhanced Cyber Security Obligations. Australian organisations of a certain size, or those handling, processing, or transferring significant data, must be obliged to:
    - Develop cybersecurity incident response plans to adequately prepare for cyber incidents.
    - Conduct cybersecurity exercises to enhance cyber preparedness.
    - Undertake vulnerability assessments to identify and remediate potential weaknesses.

- Vulnerability assessments should be conducted by independent third-party evaluators. Moreover, it must be mandatory for C-suite executives to attend cybersecurity exercises, such as tabletop simulations, to ensure their engagement in and understanding of cybersecurity matters.

We recommend incorporating the following measures into the cybersecurity act to enhance the cyber literacy of boards of directors:

- Prioritise the inclusion of a cyber expert on the board to ensure awareness and understanding of current and emerging cyber threats.

- Encourage boards to engage external cyber experts to expedite the development of cyber literacy within the organisation.

- Emphasise the importance of cyber literacy for all board members, including understanding current company risks, cyber insurance requirements and costs, foundational knowledge of top attack vectors, incidents at peer organisations, and factors that significantly impact the cost of cyberattacks.

- By adopting these recommendations, boards of directors will be better equipped to make informed decisions and effectively address cybersecurity challenges.

- Provide and promote cyber security frameworks that go beyond ASDs Essential 8, so that organisation have a chance at address current and emerging cyber threats.

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

Depending on the size of a business (measured by the number of employees), tax incentives should be provided to encourage the implementation of cybersecurity controls and processes. This approach would promote a secure digital environment while also supporting businesses in their efforts to protect sensitive information and systems.

f. Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by:

a) victims of cybercrime; and/or

Yes, that is the approach some States in the U.S have taken. Denying the threat actors ransom payments can go a long way in curbing their business model. To ensure this approach has the best chance of success, it is imperative organisations regularly:

- Practice incident response.
- Test and validate the restoration process of their offline backups.
- Leverage security tools that prevent email threats, cloud misconfiguration threats and other vectors that can be routinely exploited by hackers.

b) insurers?

Yes, the government should prohibit the payment of ransom by insurers too. A current trend has arisen in which ransomware perpetrators seek victims' cyberinsurance policies to customise ransom demands based on policy limits. This approach enables threat actors to optimise profits while reducing payment rejections. However, the escalating frequency and intensity of ransomware attacks place considerable pressure on the cyberinsurance industry, potentially resulting in increased premiums, limited coverage, and market exits.

Governments, regulators, and the private sector must cooperate to tackle the ransomware menace, striking a balance between providing financial safeguards for organisations and curbing the growth of ransomware attacks.

If so, under what circumstances?

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

In the worst case, with companies that have poor backups that are not able to be restored, the company will suffer with an outage until restoration occurs.

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

Yes, transparency and clarity regarding what is permitted and what is not under Australian law are crucial, particularly when decisions must be made swiftly and under pressure.

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

- Joint Cybersecurity Exercises: Australia should conduct and host joint cybersecurity exercises and simulations to assess Pacific CERT (PacCERT) readiness, identify gaps, and improve incident response capabilities across borders.

- Confidential Threat Intelligence Sharing: Facilitate the sharing of cyber threat intelligence, best practices, and vulnerability information among regional partners (Pacific Islands, NZ, Japan) to enhance collective defense and proactive response.

- Establish a joint or regional Computer Emergency Response Teams (CERTs) working group to enable coordinated and efficient response to cross-border cyber incidents. Our CERTs should work closely with PacCERT to help upskill their capabilities.

- Collaborate closely with universities and tertiary education institutions in the Pacific region to advance cybersecurity programs and address the existing skills gap. Furthermore, Australia may offer remote employment opportunities within the cybersecurity sector to Pacific Islanders, ensuring their skill levels align with global benchmarks.

- The Australian government could consider providing financial support and management for cybersecurity awareness campaigns targeting the Pacific Islands.

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

We should consider extending invitations to additional members for the Quad Senior Cyber Group (QSCG), such as New Zealand, Singapore, and the Pacific Islands.

One of the primary objectives of multilateral partnerships should be to advocate for the safe and responsible use of Artificial Intelligence technologies. Additionally, it is imperative to formulate policies that hold big tech companies and AI technology owners accountable, responsible, and liable for AI-related harm.

Multilateral partnerships should be considered to implement policies that prevent the misuse of AI generated cyber-attacks, as well as limit the spread of misinformation and disinformation.

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

From an emerging threat perspective, Australia should consider enacting new legislation to protect its citizens from novel risks introduced by technologies such as artificial intelligence (AI).

We need laws that hold AI technology owners and users accountable when harm occurs, as well as regulations that inform citizens when they are interacting with AI and how their personal and private data is being utilised.

It is essential to implement legislation that ensures data is not collected and stored without consent, and that prevents organisations from retaining personal and private data for longer than necessary.

Australia should strive to be at the forefront of developing new regulations and actively collaborate with international bodies to drive change, ensuring the protection of human values in the face of advancing technology.

Australia should evaluate and leverage the leading international laws and guidance from US-NIST, ISO and EU privacy laws.

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

Adopt a prevention-focused approach, utilising tools that safeguard all vectors, including email, cloud resources, network, endpoints and employees. Implement industry-leading practices and frameworks to maintain a robust security posture.

Exhibit thought leadership in the field.

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

The Australian government could develop a centralised threat intelligence platform, enhanced by third-party threat feeds, to be utilised as a standard across all government agencies. Encourage international collaboration and threat intelligence sharing among government agencies from different countries. Cybersecurity is a global concern transcending local and regional boundaries; therefore, fostering partnerships across international borders is essential for collective learning and progress.

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?

Yes, the initial time taken to engage incident responders in the event of a cyber incident is of paramount importance. Rapid response can significantly mitigate the potential impact, reduce the likelihood of further damage, and facilitate a swift recovery process.

This is a similar approach that the US uses that is managed by CISA.GOV and the FBI.GOV.

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?

Yes, enhancing public understanding of the various types and magnitudes of cyber-attacks is essential. To achieve this, a consistent reporting framework should be established, enabling the public to easily understand the attack's characteristics, implications, sophistication, execution methods, detection process, attack signatures, and potential preventive measures. Such measures encompass specific security controls and processes that organisations and individuals can employ to prevent or limit the impact of cyber-attacks.

Making this incident notification information readily accessible is crucial for fostering a better understanding of cyber threats and promoting proactive measures to safeguard against them. By using a concise approach, it should be possible to facilitate clear communication, that ultimately contributes to improved cybersecurity awareness.

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

The best practice models for automated threat-blocking at scale involve utilising threat intelligence platforms, such as those offered by established security vendors like Check Point, which are capable of real-time updates, continuous enrichment with exclusive threat intelligence, and AI-driven analysis. A key aspect of this real-time response is demonstrated when a malicious link is detected and blocked during a zero-day attack in the US; the threat data should be immediately shared across all attack vectors, updating protections and allowing the same malicious link to be blocked in a similar attack in Australia in less than 2 seconds.

Essential features also include API integration for seamless communication and coordination between security tools and systems, enabling efficient response to threats across an organisation's entire security infrastructure. By combining these elements, a robust and adaptable defence against cyber threats can be achieved, ensuring the protection of valuable data and resources.

Australia should consider choking the malicious traffic at major internet entry points such as telcos and cloud service providers. Thus, protecting the nation and its citizens.

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

There must be a focus on cultivating the next generation of cyber warriors to protect Australia, extending beyond simply examining cyber security through the lens of STEM. We require a targeted and focused curriculum that fosters the development of cyber security defence, leveraging Artificial Intelligence. So, our emphasis must be on AI skill sets as well as cyber security. We should promote diversity to ensure that bias and ethical considerations remain at the forefront.

The cyber security talent should focus on all levels including leadership level talent e.g., CISO or educating the board on mandatory cybersecurity.

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

- Establish and finance Cybersecurity Centres of Excellence that provide specialised research and education centres concentrating on cybersecurity, fostering innovation and collaboration among academics, researchers, industry professionals, and security vendors.
- Promote gender and diversity inclusion in the technology and cybersecurity workforce by implementing targeted initiatives, scholarships, and mentorship programmes that encourage underrepresented groups to pursue careers in fields like Artificial Intelligence.

- Facilitate the transition of military/defence personnel into civilian cyber roles, capitalising on their experience and skills for the benefit of the broader cybersecurity workforce.
- Organise national or international cybersecurity competitions and challenges to help identify and nurture talent.
- Encourage companies to fund and support universities and training schools to help fill job openings.

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

Equip Australians for a potential cyber pandemic by ensuring organisations comprehend the necessary steps to prepare and withstand catastrophic cyber-attacks. Key aspects include:

- Raising awareness
- Promoting cyber hygiene
- Implementing best practices (segmentation, MFA, encryption, etc.)
- Facilitating real-time prevention
- Cultivating a prevention mindset
- Conducting crisis simulations
- Promoting business continuity tests
- Encouraging threat intelligence sharing
- Focusing on containment and isolation strategies
- Employing orchestration and automation for breach containment

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

Yes, implementing a single portal can help minimise confusion. Employ stringent authentication and authorisation measures to ensure optimal security.

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

- One that involves root cause analysis that takes into account people, process and technology.
- It should have an element of threat intelligence sharing, lessons learnt and processes that must be finetuned to prevent future attacks.
- Post incident response should be done in a consistent manner.

- All incident failures and issues need to be addressed and repaired in short time frames to prevent a repeat issue.

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

To assist crime victims, the Australian government could initiate awareness campaigns, informing the public about available support and assistance channels. Streamlining this process ensures easy access and fosters a more seamless experience.

a) What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?

Incentivise local Managed Security Service Providers (MSSPs) to offer tailored expertise and services for small businesses, addressing the current scarcity in this market segment. Encourage security vendors to develop accessible platforms for MSSPs to efficiently deliver these services.

The Australian government could provide easy to understand security guidelines for small and mid-size businesses. This could include short videos that explain the various attack surfaces and attack vectors so that small businesses can make informed decisions about their cyber investments. These videos could be used to educate small business owners on the importance of offline backups, encryption, MFA, advanced endpoint security such as endpoint detection and response, etc.

Consider offering tax breaks to small businesses, fostering cyber investment, and establish 'cyber hubs' where entrepreneurs and business owners can seek guidance and support in implementing appropriate security measures.

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 Australian government should strive to establish the nation as a hub for cyber security start-ups. This can be achieved by fostering a culture that promotes cyber security entrepreneurship from high school through to universities and other tertiary education institutions, such as TAFE, similar to the start-up ecosystem in Israel. It is essential to develop programs that encourage innovative and disruptive solutions in the field of cyber security.

Incentives should be provided for start-ups to concentrate on the following key areas:

- Network Security
- Connected Devices, IoT, and Control Systems
- Data Protection, Encryption, and Privacy
- Security Operations and Orchestration
- Anti-fraud, Authentication, and IAM Orchestration
- Applications and Website Security
- Governance, Risk Management, and Compliance (GRC) and Vulnerability Management

- Cloud and Infrastructure Security
- Endpoint Security
- Mobile Security
- AI-Driven Security

The Australian government could allocate resources towards supporting infrastructure that aids start-ups in their growth journey. This may include the establishment of accelerator programs and entrepreneurship initiatives tailored specifically to the cyber security domain.

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

The Australian Government's strategy must take into account the understanding of current and emerging cyber threats. The approach needs to implement proven methods that demonstrate successful factors in preventing attacks or reducing the impact of cyber-attacks.

Organisations should be required to adhere to strict guidelines, frameworks, and industry best practices to ensure foundational cybersecurity principles are implemented. This must be non-negotiable, and we should consider enforcing this through mandatory frameworks.

While we cannot predict the specific threats that will emerge in years to come, it is safe to assume that the future threat landscape will be more sophisticated, will increase in volume, will involve new actors, and be driven by AI.

Preventing attacks in the first place, before they have a chance to cause harm, will be crucial. The ability to share threat intelligence in near real-time across all attack surfaces, and the use of AI-driven prevention, detection, and remediation security controls will be key. Fostering a culture of security innovation must be a top priority.

In order to educate the younger generation about the risks posed by cyber-attacks, cyber awareness must be incorporated into the primary school curriculum. This will ensure that future generations are well-informed about potential threats and prepared to navigate the digital landscape safely and responsibly.

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?

Procurement can be used as a tool to enforce mandatory cybersecurity laws. Thus, products and services that support Critical Infrastructure need to meet the same level of security across the board; if not, there is a risk to the Critical Infrastructure security. To make it non-onerous and maintain consistency, adopting international standards and certifications would help. This would also assist companies that provide support to Critical Infrastructure sector to step up their cybersecurity and, in turn, contribute towards an improved ecosystem.

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

The Strategy should evolve to address the cybersecurity of emerging technologies and promote security by design in new technologies by focusing on data privacy and protection, transparency, accountability, responsibility, ethical considerations, and education and awareness. The proliferation of data-collecting devices and AI technologies presents significant risks, such as individual autonomy infringement and the misuse of personal data.

Liability must be considered, with policymakers establishing clear policies that define responsibility in the event of AI-generated errors or harm. The increasing use of AI technology to create deepfake content and spread misinformation highlights the need for proactive measures to counteract these threats.

Collaboration among policymakers, technology companies, cybersecurity vendors, universities, government agencies, and other organisations is essential for developing and implementing educational programs in both the public and private sectors. Ensuring society is well-informed about AI-related risks, data protection, and accountability is crucial.

As cyber-attacks become more sophisticated, organisations must continually evaluate and deploy effective AI-driven security controls to address emerging threats. Automation, consolidation, and comprehensive AI-driven cybersecurity controls must be integral components of the Strategy.

Policymakers must act swiftly to establish accountability and liability plans for AI misuse, particularly regarding rogue nations. By implementing robust policies and increasing public awareness, we can work together to mitigate AI technology risks and harness its potential for good.

The Center for Humane Technology provide some great policy principles designed to guide the internal development of legislative, regulatory, and other policy, and provide a means by which to evaluate any legislative, regulatory, or other policy proposals.

(1) Put people first.

(2) Avoid “atomizing” solutions.

(3) Confront power.

(4) Address root causes.

(5) Presume harm.

(6) Compel caution.

(7) Embrace complexity.

(8) Seek sustainability.

Reference: https://www.humanetech.com/policymakers

The most pressing need for safeguarding Australians lies in robust policies that address the ever-evolving AI threat landscape, ensuring our nation's security and resilience.

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

- Reduction in average time taken to identify a breach for all Australian organisations.
- Reduction in the average time taken to contain breaches for all Australian organisations.
- Reduction in average downtime of essential services such as critical infrastructure due to cyber-attacks.
- Reduction in number of successful cyber-attacks.
- Increase in number of organisations completing and report breach simulation exercise.
- The Australian Government could create and host online cyber safety and risk awareness training and measure the participation level from public.

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

The Australian government must earn the trust of the public and businesses by consistently sharing lessons learned while striving to become the world's most cyber-secure nation by 2030.

The government could regularly showcase achievements that demonstrate progress in national cyber maturity.

Consider hosting town hall sessions, inviting feedback from industry professionals on the Strategy's progress and where improvements could be made.

Analyse the number of successful cyber-attacks (breaches) quarter by quarter to understand trends and evaluate the government's cyber strategy effectiveness.

Compare the recovery time for Australian organisations following successful cyber-attacks.

Demonstrate accountability by financially penalising CEOs and boards for simple security oversights, reinforcing their responsibility for maintaining robust cybersecurity.