Submission to the Inquiry: The Review of the Cyber Security Legislative Package 2024

Submission by: Greg Peak

Date: 24 October 2024

[redacted]

Introduction

Thank you for the opportunity to provide a submission to the inquiry into the Review of the Cyber Security Legislative Package 2024. Cybersecurity is vital for protecting national infrastructure, safeguarding personal data, and ensuring the economic stability of Australia. This submission addresses key concerns and proposes recommendations for enhancing the legislation to meet emerging challenges in the cybersecurity landscape.

1. Enhancing Protection for Critical Infrastructure

The legislative package places considerable emphasis on protecting critical infrastructure. However, there is a need to further bolster security requirements to defend against sophisticated cyber threats.

- **Stronger Security Requirements:** Mandate more stringent security standards for all operators of critical infrastructure, including regular security testing and audits.
- **Supply Chain Security:** Ensure that third-party suppliers and service providers adhere to cybersecurity protocols, as they often present vulnerabilities in systems.

Recommendation: Introduce compulsory security audits for critical infrastructure and extend security obligations to include all entities within the supply chain.

2. Data Privacy and Consumer Protection

Data breaches have become more frequent, affecting millions of Australians. The legislative package's current provisions on data privacy and breach notifications need improvement to protect individuals more effectively.

- **Breach Notification Timeframes:** The legislation should require organisations to notify affected individuals of data breaches within a shorter timeframe (e.g., 48 hours instead of 72).
- **Increased Accountability:** Penalties for mishandling personal data or failing to comply with breach notification requirements should be significantly increased.

Recommendation: Reduce the breach notification window to 48 hours and impose stricter penalties for non-compliance to enhance consumer protection.

3. Addressing the Cybersecurity Skills Gap

Australia faces a shortage of cybersecurity professionals, which presents a major challenge in building a resilient cyber defence. The legislation should address this gap through workforce development programs.

- **Educational Incentives:** Encourage the creation of cybersecurity programs at both the university and vocational levels, providing scholarships and grants to attract talent.

- **Private Sector Collaboration:** Partner with private organisations to develop training programs and certifications that target the specific skills needed in today's cybersecurity landscape.

Recommendation: Provide government-funded incentives to promote cybersecurity education and create pathways for upskilling professionals in related fields.

4. Improving Cyber Incident Response

The current legislation outlines the importance of coordinated incident response but lacks clear, comprehensive guidelines for large-scale incidents.

- **National Cyber Response Team:** Establish a well-coordinated national cyber response team capable of rapid deployment in the event of a major attack.
- **Sector-Specific Guidelines:** Tailor incident response plans to meet the unique needs of different sectors, ensuring swift and effective actions are taken.

Recommendation: Centralise incident response with a national task force and implement sector-specific guidelines to streamline the response process.

5. Public Awareness and Cyber Literacy

A large portion of cyber vulnerabilities arises from human error and lack of awareness. Public education is crucial in reducing the risk of cyberattacks on individuals and businesses.

- **Cybersecurity Awareness Campaigns:** Implement national awareness campaigns that focus on common cyber threats and simple steps individuals and businesses can take to protect themselves.
- **Targeted Education Programs:** Develop cybersecurity education tailored to vulnerable groups, including small business owners and seniors.

Recommendation: Increase investment in public education initiatives aimed at improving cybersecurity literacy and awareness across all sectors of society.

Conclusion

The Cyber Security Legislative Package 2024 lays a strong foundation for Australia's cyber resilience, but further enhancements are necessary. By addressing critical areas such as infrastructure security, data privacy, the cybersecurity skills gap, incident response, and public awareness, Australia can remain vigilant and prepared in the face of evolving cyber threats. I hope this submission provides valuable insights into strengthening the legislative framework.

Thank you for considering my submission.

Greg Peak
[redacted]
