Submission to Horizon 2 of the 2023-2030 Australian Cyber Security Strategy

By [redacted]

(Cyber Security Consultant with over 25 Years experience)

Executive Summary

This submission challenges two key assumptions underpinning the Strategy: the existence of a widespread cybersecurity skills shortage and the proposed approach to professionalisation.

Based on over 25 years of experience in cybersecurity, I argue that current market conditions reflect misaligned expectations rather than genuine skills gaps, and that the proposed professionalisation pathway presents significant implementation challenges that require careful consideration.

The Cybersecurity "Skills Shortage" Myth

Market Reality vs Perception

The Strategy continues to perpetuate the narrative of a critical cybersecurity skills shortage. However, this does not align with current market conditions experienced by many seasoned professionals. During a recent two-month period of unemployment, I applied for over 100 roles and received only five interviews, despite having over 25 years of industry experience. This experience is shared by numerous peers across the sector.

The Entry-Level Paradox

A significant challenge facing the industry is the lack of genuine entry-level positions. Whilst there is an influx of graduates and junior professionals seeking their first roles, organisations increasingly expect senior-level experience for positions advertised as "junior" or demand highly specialised skills at entry-level salaries. This creates a pipeline problem where new professionals cannot gain the experience necessary to develop into the senior experts we will need in future.

Impact of Artificial Intelligence

The adoption of AI tools has begun to erode traditional entry-level functions. Tasks that once provided valuable learning opportunities for junior staff, such as basic policy writing, vulnerability assessments, and compliance documentation, can now be automated or significantly accelerated through AI assistance. Whilst this increases efficiency, it reduces the pathways for developing foundational skills and institutional knowledge.

Misleading Vacancy Statistics

The perceived volume of open roles is often inflated by advertising practices where single positions are posted across multiple platforms and frequently re-advertised. This creates an illusion of numerous unfilled positions when the actual number of unique opportunities is considerably lower.

Stakeholder Incentives

The skills shortage narrative benefits certain stakeholders who have commercial interests in maintaining this perception, including training providers offering cybersecurity bootcamps and certification programmes, and professional bodies that profit from membership growth and migration pathways.

Recommendations for Workforce Development

Rather than focusing solely on increasing supply through training programmes, the Government should:

1. Work with industry to create genuine entry-level positions that provide meaningful learning opportunities
2. Develop apprenticeship and internship programmes that bridge the gap between education and employment
3. Address salary and expectation misalignments in the job market
4. Critically evaluate the actual shortage areas rather than assuming a blanket skills deficit

Professionalisation Challenges

Community Division

The cybersecurity community remains significantly divided on the need for professionalisation. Whilst some form of professional structure may be inevitable, the current approach presents several concerning issues that require resolution before implementation.

The ACS Involvement Problem

The involvement of the Australian Computer Society (ACS) in any professionalisation scheme presents fundamental conflicts of interest and practical challenges:

- The ACS has commercial interests in migration and membership growth that may conflict with professional standards

- Their current membership base of 50,000 includes many who would likely be excluded from a rigorous cybersecurity professional scheme
- Their mandate to represent ICT professionals broadly conflicts with the specific requirements of cybersecurity professionalisation

Legal and Practical Implications

A critical question remains unaddressed: what legal implications will exist for "non-professionals" continuing to offer cybersecurity advice? The analogy with financial services regulation is instructive, just as non-AFSL holders cannot provide financial product advice, a cybersecurity professionalisation scheme might similarly restrict who can provide cybersecurity advice.

This raises several problems:

- Where does IT advice end and cybersecurity advice begin?
- How would such restrictions be enforced without being overly broad?
- Would the majority of current practitioners be excluded from providing services?
- How would this affect the broader IT industry where cybersecurity considerations are increasingly integrated into all technology decisions?

Alternative Professionalisation Approach

If professionalisation proceeds, it should:

1. Establish clear boundaries around what constitutes professional cybersecurity practice
2. Create granular specialisation categories rather than blanket coverage
3. Ensure the governing body has appropriate independence and expertise
4. Provide clear pathways for existing practitioners to demonstrate competency
5. Address the enforcement and scope challenges transparently

Conclusion

The Horizon 2 Strategy would benefit from a more nuanced understanding of current cybersecurity workforce dynamics and a more carefully considered approach to professionalisation. Addressing these foundational assumptions will lead to more effective policy interventions and better outcomes for Australia's cybersecurity posture.

The Government should prioritise fixing market dysfunction over expanding training supply and ensure that any professionalisation scheme is practical, fair, and actually serves to improve cybersecurity outcomes rather than creating barriers to practice or benefiting incumbent organisations.