CYBERCY

Beyond the Firewall: Elevating the Human Layer of Australia's Cyber Strategy

Submission in Response to "Charting New Horizons – Horizon 2"
From Cybercy Pty Ltd – August 2025

Cybercy welcomes the opportunity to contribute to the Charting New Horizons – Horizon 2 process. As a specialist consultancy in cyber literacy and behavioural change—with proven delivery across government, industry, the community sector, and internationally, including pilots with the Department of Defence and the Department of Home Affairs—we share the vision of building a secure, resilient, and prosperous digital Australia.

However, this aspiration will remain elusive unless we confront a central truth: cybersecurity is not solely a technical or regulatory problem—it is, at its core, a human one.

The very technologies driving Australia's innovation, productivity, economic growth, climate solutions, and health advances also create new levers of asymmetric power. Those who understand the digital environment—its architecture, incentives, and vulnerabilities—can exploit it to the disadvantage of those who do not. This imbalance is the defining feature of today's cyber threat landscape.

The Scale of the Problem

The global cybercrime market is now USD $13.8 trillion, growing at 15% annually. By contrast, global spending on cybersecurity products and services—USD $432 billion—is growing at 12.5% annually[1].

This gap tells a clear story: despite unprecedented investment in technology, the economics of cybercrime still favour the attacker. The missing link is not more tools, but a population-wide uplift in informed cyber contextual awareness and behaviour.

Research by Professor Erica Chenowyth shows that sustained change occurs when just 3.5% of a population adopts a new behaviour—creating a tipping point for systemic transformation[2]. In Australia, that means fewer than one million people could catalyse a national shift in cyber culture.

Where Horizon 2 Can Go Further

While Horizon 2 recognises the importance of digital literacy, it currently treats it as supplementary. In reality, behavioural capability must be central to every Shield.

Technology, regulation, and threat intelligence are only as effective as the people applying them and the contexts in which they operate. The primary vulnerability remains the behaviour and awareness of every digital user—each action, whether deliberate or

[1] sources: Gartner, Cybersecurity Ventures, Information Age, Tech Target, Precedence Research

[2] https://www.hks.harvard.edu/centers/carr/publications/35-rule-how-small-minority-can-change-world

inadvertent, can be exploited. Unless Australia embeds informed, proactive, and accountable digital behaviours at scale, the nation will remain reactive in the face of an increasingly complex and dynamic threat environment.

Key Points

1. Redefine "Cyber Capability" to Include Behavioural Intelligence

Cyber literacy must be treated as a baseline civic and organisational capability. Australians should have the skills to:

- understand the incentives to gather data and monetise it,
- recognise manipulation and deception,
- manage digital identity,
- assess personal and organisational risk,
- make informed decisions in a blended physical–digital reality.

2. Make Behavioural Change a Central Strategy, not a Footnote

Cybercy's programs, based on the IEEE Digital Literacy Standards, go beyond compliance—they create cognitive and cultural shifts. Participants don't just "know the rules"; they own their role in cyber safety.

Using Chenowyth's 3.5% tipping point model, targeted pilots can create rapid, self-reinforcing change across the nation.

3. Measure What Matters – The Cybercy Discovery Tool

The Cybercy Discovery Tool is a validated assessment instrument that measures an individual's or organisation's cyber awareness and behaviours at a point in time and tracks measurable change over an awareness program.

Built on evidence-based behavioural science, it:

- provides a reliable baseline by assessing knowledge, attitudes, and everyday digital habits through scenario-driven questions,
- identifies specific behavioural and awareness gaps,
- enables repeated measurement at defined intervals to quantify improvement,
- validates the effectiveness of training and policy interventions.

This data-driven approach ensures cyber awareness initiatives are not only delivered, but demonstrably improving resilience over time—directly answering Horizon 2's call for new ways to monitor and evaluate outcomes (Q4).

4. End the Diffusion of Responsibility

Cyber responsibility is currently “someone else’s problem.” Executives defer to IT teams; IT teams point to boards; employees assume it is managed elsewhere. This fragmentation mirrors the pre-reform state of workplace health and safety. Most think there is a manageable divide between professional/organisational digital experience and private/personal experience and they can behave differently in one environment without that behaviour bleeding into the other.

As OH&S became everyone’s responsibility, so must cybersecurity. This requires policy, leadership, and accountability frameworks that embed shared responsibility into daily practice.

.

5. Treat Digital Identity and Trust as Civic Infrastructure

Loss of control over digital identity undermines trust in institutions and democracy. Digital self-awareness, ethical decision-making, and identity literacy should be treated as core civic competencies—not optional skills.

Recommendations

1. Position cyber literacy as a national priority—equal to literacy and numeracy.
2. Fund targeted pilots to reach the 3.5% tipping point, then scale nationally.
3. Embed shared cyber responsibility across sectors, modelled on OH&S reform.
4. Integrate digital identity, ethics, and awareness into education, public campaigns, and civic programs.
5. Enable innovation pathways for SMEs like Cybercy to pilot, validate, and scale behavioural solutions.
6. Adopt a national program evaluation—providing government and industry with a consistent, evidence-based measure of human cyber capability uplift.

Conclusion

We cannot firewall or legislate our way out of this challenge. Australia’s cyber resilience will depend on developing behavioural intelligence at scale—measured, tracked, and improved over time.

Cybercy offers a tested, scalable approach that not only educates but proves its impact, aligning directly with Horizon 2’s aims and providing the government with the tools to monitor, evaluate, and accelerate progress.

Contact: