CYBER LEADERSHIP INSTITUTE
KNOW YOU'RE READY

Dear Australian Government,

In response to the question in the discussion paper - "*Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?*

As a co-founder of the Cyber Leadership Institute, an Australian based business, I would like to bring to your attention a crucial topic that is missing from your current strategic approach towards cyber security. While investing in foundational cyber skills at the grass roots level is essential (STEM - *science, technology, engineering, and mathematics*), it is equally important to invest in executive leadership skills for those more senior cyber security professionals

Australia's cyber security industry is rapidly growing, it is essential to equip our cyber security professionals with the necessary skills to handle the challenges and complexities of this industry. Foundational cyber skills, such as coding, hacking and technology, are necessary but not sufficient to deliver cyber resilience for the Australian economy. Cyber security is also about a broader skills framework for self, teams, organisation and domain, covering areas such as; Strategy, Transformation, Resilience, Influence, Knowledge and EQ (STRIKE).

At the Cyber Leadership Institute, we have identified a significant gap in executive leadership skills at the highest levels of the cyber security industry. Typically, the most senior cyber security professional in an organization is the Chief Information Security Officer (CISO), who often reports to the Chief Information Officer (CIO). However, like their bosses, CISOs are primarily expected to foster operational efficiency, and they rarely receive praise for their efforts. Instead, they only hear from leadership when things go wrong. CISOs with little or no senior leadership experience often spend more time saying "no" rather than finding ways to help drive innovation and a competitive advantage for the business. As a result, they become unpopular with their colleagues and often feel unappreciated. It's no surprise that a 2022 BlackFog survey reported that nearly one-third (32%) of U.S. and U.K. CISOs are considering leaving their current organizations.

Security experts that have advanced in their careers without possessing the necessary leadership abilities, could lead to serious repercussions, including financial losses, harm to reputation, decline in consumer confidence and regulatory fines. However, we can take steps to alleviate the burden on CISOs and other senior cyber leaders. Equipping them with the skills to speak the language of the business and the board, simplifying the cyber resilience narrative to galvanize support top-down to benefit the business and industry as a whole. We have seen the impact of effective communication and leadership skills first-hand and believe that investing in tailored education and training programs can drive positive societal change.

The Cyber Leadership Institute recommends education programs using the STRIKE framework, on a scalable digital platform. Training can be delivered for mid-level technical and security managers, emerging chief information security officers (CISO), and CISO's new in post (first 100 days). These programs should cover topics such as strategic thinking, transformation, communications,

stakeholder management, risk management, decision-making, crisis management, and cyber security culture. Training and skill development must be practical in nature, based on real-world scenarios and experience - equip them with the necessary skills to handle the challenges and complexities of this field as they rise through the ranks. Moreover, consumers expect securely designed products, manufactured by a workforce with world-leading cyber skills. To meet this demand and achieve Australia's goal of becoming a leading brand for cyber goods and services by 2030, it is essential to invest in executive leadership skills, as it will be skilled cyber leaders who will ensure software developers and infrastructure builders apply advanced cyber security built-in by design, a shift-left mindset.

In conclusion, we urge the Australian government to invest in executive leadership skills in the cyber security industry. It is essential for the growth and success of the broader Australian economy, both home and aboard. Cyber Leadership Institute, is ready and committed to supporting the government in this endeavour and willing to partner via our platform, leveraging our expertise and resources to ensure that this goal is achieved in a scalable and sustainable way. By doing so, together we can create a more resilient and secure digital ecosystem that benefits not only businesses but society as a whole.

Thank you for your attention to this matter.

Sincerely,

Darren Argyle,
Director and Co-Founder

Cyber Leadership Institute

www.cyberleadershipinstitute.com

Level 33 Australia Square
264 George Street Sydney, NSW 2000
contact@cyberleadershipinstitute.com
Australia +61 2 7908 0751