

**CYBERCOSMOUS**

Together We Secure

Cybercosmous Australia Pty. Ltd.

ABN: 58663524945

Website: [www.cybercosmous.com](http://www.cybercosmous.com)

# **2023 – 2030 AUSTRALIAN CYBER SECURITY STRATEGY**

SUBMISSION BY CYBERCOSMOUS

15-APR-2023

15-Apr-2023

Hon. Claire O'Neil MP & the Expert Advisory Board

Department of Home Affairs

Via Online form

Re: 2023-2030 Australian Cyber Security Strategy Discussion Paper

Dear Sir/Madam,

Cybercosmous Australia welcomes the initiative to make this submission on behalf of the business community to achieve Australia's vision of being the world's most cyber-secure country by 2030. This vision resonates with Cybercosmous's Mission to make the digital world more secure for every citizen of the globe. Our submission covers the following.

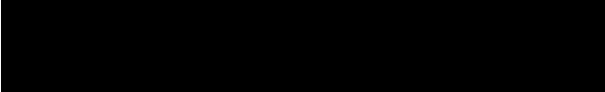
1. Australia's vision & current challenges in achieving this vision.
2. Recommendations to address the current and future challenges.
3. How can Cybercosmous help Australia in attaining these goals.

The Cybercosmous team wholeheartedly thank the Department of Home Affairs for providing this forum. Cybercosmous will appreciate the opportunity to partner with the Australian government to build a secure nation and further engage in this submission.

Yours Sincerely,

**Amritha Shenoy**

Co-Founder & CEO Australia



**Chetaan N T**

Founder & Global CEO



## **1. Australia's Vision - To become world's most cyber-secure country by 2030**

Australia's vision "to become the world's Most Secure Cyber Nation by 2030" is in alignment with Cybercosmious Mission to make digital world secure for every citizen of the globe. This vision can be achieved by setting a year-wise goal (for the next seven years) to make the country more secure and by sharing our success story; Australia's cyber security strategy model can be replicated worldwide in all countries.

## **2. Challenges in achieving this goal –**

### **a. People**

A shortage of skilled people in cyber security is the biggest challenge Australia is currently facing when it comes to Cyber Security. Huge surges in cybercrime, including ransomware, fraud and data theft, will leave Australia 30,000 cyber professionals short over the next four years of what is required to cover the country's security needs (Source: AFR - <https://www.afr.com/technology/cyber-skills-shortage-to-hit-30-000-in-four-years-20220912-p5bhde#:~:text=%E2%80%9Ccover%20the%20next%20four%20years%2C%20the%20shortfall%20in,previously%2C%E2%80%9D%20Mr%20Paitaridis%20told%20The%20Australian%20Financial%20Review.>).

Mr Nigel Phair, Director, Enterprise and former Cyber Director, UNSW Canberra, shares in his book, Cybercrime in Australia: 20 years of inaction some key statistics, which are quoted below

- i. Only one-fifth of the actual amount of online crime gets reported. Between July 2021 to July 2022, the Australian Cyber Crime Centre (ACSC) received over 76,000 cybercrime reports, an increase of 13% from the previous financial year. This means there are about 300,000 cybercrimes committed in Australia each year.
- ii. Mr Phair, also a former Australian Federal Police officer, estimates that there have been less than 300 completed investigations into cybercrime in the past 20 years, of which just 150 were prosecuted.

### **b. Policy**

- i. Absence of clear policies to encourage and leverage strengths of private business establishments to participate in the Nations Cyber Security Infrastructure - i.e. with Cyber Security Law enforcement departments.
- ii. Absence of policies in - making cyber security & data privacy integral part of regulatory compliance for businesses of all sizes.
- iii. Absence of Policy for leveraging crowdsourced cyber security models leading to increased cyber security breaches originating from the Internet (External Threat sources).

### **c. Focus on securing every Australian citizen**

When policies and visions are drafted - it is focused on government, governance, and businesses. These visions miss the main subjects who should get involved in the process - every common citizen living in the country. Only when the policy is focused on making every last man standing aware and ably equipped with the required

knowledge is when the objectives of the mission can be achieved. Hence the policy & mission should include making every citizen digitally secure in the cyber world by making them - educated, aware and equipped to deal with cyber security challenges.

### **3. Recommendation to Address these challenges-**

#### **a. People -**

##### i. Skill building

- Through College Curriculum - Encourage Universities to design and offer Cyber Security centric Undergraduate & Postgraduate programs. Announce scholarships for students pursuing these programs.
- Encourage National & International Private Training institutes / Businesses to provide Cyber Security Training & Certification by providing grants for setting up training centres / offering training in Australia. Link these grants to successful training and certifications completed by the students.
- Offer easy student loans through banks for students pursuing Certifications or formal education in Cyber Security subjects.

##### ii. Government Programs

- Create a Cyber Security program with a target to hire 25,000 skilled cyber security professionals & Cyber Lawyers in Law enforcement agencies in the next three years to ensure adequate staffing of skilled cyber police & cyber lawyers in the country.
- Create Special Lateral Entry programs with inclusiveness to hire cyber security investigators. These investigators do not need to fit the criteria of physical training / physical fitness like other sheriffs need to undergo. This is a job of brain and logical fitness and less of physical fitness. Hence it can also include physically challenged people qualifying for these roles, and this promotes inclusivity.

#### **b. Policy-**

##### i. Government Policies -

- Update the Criminal Code Act 1995 (Cth) ("the Code"), The Security of Critical Infrastructure Act 2018 (Cth) and The Telecommunications (Interception and Access) Act 1979 (Cth) to permit – the participation of private cybersecurity services providers in - Cyber Crime Investigation, Cyber Forensics, and Cyber Security Incident Management. This opportunity to collaborate and work together between government & private establishments can help in faster turnaround time in - cybercrime investigation, better cyber defense, and better cyber security incident management.
- Update the policy to cover businesses of all sizes to make cyber security & data privacy an integral part of business activity & compliance. While on a broader level - it can include –
  - ✓ for startups & small businesses - it can be a self-certification process
  - ✓ for mid-sized organisations - it should be a mix of self-certification + certifications through registered bodies,
  - ✓ whereas for enterprises, it has to be a mandatory program.

- ii. Business Policy -
  - Create an Australia Cyber Security - Business Policy to include -
    - ✓ Vision to create 10 Unicorns in Cyber Security (5 in Professional Services in cyber security & 5 in Products and Technologies in cyber security) based in Australia.
    - ✓ Create a grant & easy access to credits policy on promising startups in cyber security that can create a large number of Cyber Security Jobs in Australia.
    - ✓ International Collaboration & Immigration policy with grants and easy credit support for startups in Cyber Security from friendly countries (Ex: QUAD countries, India, Commonwealth countries)
    - ✓ To boost entry of high potential & high impact creating cyber security start-ups in Australia from overseas, lower the investment mandate for Permanent Residency Visa for promising start-up founders. Make business ideas & Proof of concept as major selection criteria instead of investment as a criterion for entry into the program.
    - ✓ Make Responsible Disclosure Programs mandatory for companies of all sizes as well as for all government institutions/departments – Responsible Disclosure programs help organizations secure themselves to a great extent from the threats originating from the internet. These programs can greatly help organizations that cannot afford to have a big team of security researchers working for them full-time. There is already existing advisory by the International standardisation organization through - ISO/IEC 29147:201811 and ISO/IEC 30111:201912. These describe in detail about vulnerability discovery, disclosure, and remediation. The government can leverage these guidelines or frame policies around them. This policy can also help address skills shortage issues in the cyber security domain and help leverage the crowdsourced model for building greater security for organizations in Australia.

#### 4. How Cybercosmous Can Help Australia in Realizing these goals?

**About Cybercosmous** - Cybercosmous is a Next Generation Crowdsourced Cyber Security Platform. At Cybercosmous, we harness the power of Crowdsourcing + Technology in Cyber Security to provide security at scale for our customers to secure their systems. Our 1400+ & Still growing team of security researchers community helps our customers to test their systems and applications for maximum possible scenarios for the vulnerabilities and helps in securing them in near real-time. To know more about us visit – [www.cybercosmous.com/about-us](http://www.cybercosmous.com/about-us)  
In Australia, we started operations in October 2022, and by 2027, we envision creating 30,000 freelancer security researcher jobs in Australia alone.

- a. On Skill Building – Cybercosmous has good experience in providing customised trainings for corporates as well as Law enforcement agencies in India. Our trainers have trained multiple law enforcement agencies in India on – Cyber Forensics, Cybercrime investigation, Cyber Threat Monitoring and Cyber Defence. We can help Australian Law Enforcement agencies with their Cyber-Security training requirements and also help design course content for Universities / Colleges if they plan to offer these courses.

- b. On Policy Updates –
  - i. The founders of Cybercosmious have been part of multiple advisory boards of think tanks and advisory boards that have steered lawmakers in framing policies on Cyber Security vision. Our founding team would be happy to be part of the advisory panel to do the best value add on the initiative.
  - ii. Cybercosmious team have also worked with some of the law enforcement agencies in India as Subject Matter Experts (SME) in assisting them on cyber-crime investigations when the law enforcement agency officers lacked expertise in handling some of the complex cases. This private & public partnership experience of us can be handy while advising on the collaboration policy framing and execution for Australia.
- c. On Start-up & Innovation – We at Cybercosmious strongly believe that cyber security must be an integral part of any organization’s business operation & Strategy from the day one. And to enable start-ups in this initiative, Cybercosmious through its offering named as “Vulhunt” offers “Vulhunt Start-up Program” where we offer 3 months of VDP (Vulnerability Disclosure Program) credits for free to secure their systems & applications. We intend to collaborate with Australian Government & Its start-up incubators to extend this program to all Start-ups based in Australia.
- d. On Awareness & Training of Common People -
  - i. Senior citizens are the most vulnerable population to cyber-attacks. Educating & sensitizing them on cyber security best practices is critical. Sessions at old age homes and retirement villages and partnering with religious institutions like temples, churches, mosques etc., to spread awareness can help to reach more senior citizens.
  - ii. Cybersecurity basics must be incorporated into the School Curriculum, especially for kids in years 5-7. Gamifying the cyber security programs will help grab kids’ attention as well as convey the importance of staying safe and vigilant while using the internet on digital devices. Setting up Cyber-tech labs in secondary schools will help budding engineers test new ways to combat ever-evolving cyber threats while using digital devices.
  - iii. Basic online cyber courses can be provided free of cost to all commoners, particularly seniors. For example, the course on Introduction to Cyber Security, provided free of cost from Dec 2022 -Feb 2023 by TAFE NSW Digital division, was a great initiative. However, to increase the reach & success rate, course completion can be incentivized with a gift voucher or an appreciation certificate / digital badge to post on social media.
- e. Responsible Disclosure – Cybercosmious offers Bug Bounty Managed Programs & Continuous Vulnerability Disclosure Programs (CVDP). The CVDP programs are suitable to organisations of all sizes and are affordable to even the smallest start-ups. Our Bug Bounty Programs help enterprises & MSMEs to reduce their Vulnerability assessment & Cyber Security Technical Audit costs in the range of 60-80%. To get started, we can explore helping Australian Government in implementing these programs to all government departments while we start offering these services to private enterprises and start-ups.