PISN
PRIVATE INFORMATION SHARING NETWORK

Australian Cyber Security Strategy - Discussion Paper

Mar 21, 2023

Who is PISN

The Australian Private Information Sharing Network (PISN) is a collection of cyber security practitioners, actively involved in the Australian cyber security industry. Our members are not limited by business or role. Members are a mixture of industry executives, cyber security specialists and rising cyber security talent. Building on the foundations of trust and collaboration, we share information freely with the collective aim of improving the security posture of the businesses we work amongst every day.

Introduction

The below comments represents the collective opinions from active member discussions on the questions proposed in the 2023-2030 Australian Cyber Security Strategy - Discussion Paper.

We approach these questions with the perspective that the majority of Small Businesses[1] in Australia are unlikely to be able to implement onerous controls, or a range of specific vendor-driven responses to niche cyber security threats[2]. We acknowledge that any formal recommendation that eventuated from the below responses would need to be practical, be able to be sustainably implemented, widely adopted and return measurable value to Australian Small Businesses.

We would like to thank the Government, and the Expert Advisory Board for the release of the discussion paper, and for the opportunity to submit our views. The PISN response is as follows.

[1] Parliament of Australia - Definitions and data sources for small business in Australia https://www.aph.gov.au/about_parliament/parliamentary_departments/parliamentary_library/pubs/rp/rp1516/quick_guides/data
[2] ACSC Small Business Survey Report - https://www.cyber.gov.au/sites/default/files/2020-07/ACSC%20Small%20Business%20Survey%20Report.pdf

PISN
PRIVATE INFORMATION SHARING NETWORK

Topic - Small Businesses

Discussion Paper Questions

- *What assistance do small businesses need from the government to manage their cyber security risks to keep their data and their customers' data safe?*
- *How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime?*

PISN Comments

With 97% of all businesses[3] being classified as small businesses in Australia, there is no surprise that this was a hot topic amongst PISN members. Members felt that business owners and leaders lack a clear understanding of their obligations with regards to safeguarding data.

Similar to the publication of the Australian Privacy Principles[4], Australian Businesses could benefit from the publication of clear descriptors for cyber security principles. This would help businesses design more proportionate and sustainable security programs. The publication of cyber security principles would enable businesses to align their privacy and security programs to common goals, saving small businesses time and money.

It was discussed and agreed amongst participants that Australian business could benefit from a similar certification program as the 'UK Cyber Essentials'[5] program. An Australian Cyber Essentials style program should reward businesses with a positive security credential, which businesses can use and showcase their ongoing commitment to minimum security standards in an evolving threat environment.
In an effort to promote clarity and transparency for small business, any endorsed certification process should clearly articulate relevant privacy and data security legislative commitments which would be addressed by the implementation of compliance certification.
As a key enabler of small businesses, state based small business agencies and industry associations should be incentivised to provide pathways to adopt recognised security frameworks[6].

[3] ASBFEO - Contribution to Australian Business Numbers 2022 - https://www.asbfeo.gov.au/sites/default/files/2022-08/Contribution%20to%20Australian%20Business%20Numbers_August%202022%20_4.pdf
[4] OAIC Australian Privacy Principles quick reference - https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-quick-reference
[5] UK Cyber Essentials Program - https://getreadyforcyberessentials.iasme.co.uk/questions/#gf_31
[6] NIST Small Business Cyber Security Corner https://www.nist.gov/itl/smallbusinesscyber/training

Topic - Skills / Training

PISN
PRIVATE INFORMATION SHARING NETWORK

Discussion Paper Questions

- Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?
- What more can Government do to support Australia's cyber security workforce through education, immigration, and accreditation?

PISN Comments

The PISN Member group consists of long-term cyber security professionals, business owners, board members, technology executives as well as students, entry level analysts and consultants. Feedback from the group who have actively participated in formal 'cyber security' training noted that there is a disconnect between the material and training taught, and the real-world job expectations.
It was noted and agreed that 'cyber security' roles in businesses have a heavy reliance on Information Technology. The PISN students who had recently graduated from secondary schools were vocal in their disappointment that while subjects like Maths and English were mandatory subjects in their final years, that Information Technology, which underpins their entry into working life is not. The positive effect of providing Information Technology skills to secondary school graduates, successfully shifts the focus in tertiary education from basic IT skills development to be able to use existing skills to tackle the more advanced data security, and data privacy topics that a graduate would be expected to know at the end of tertiary education.

Members noted that for most practicing cyber professionals, skills development is on-the-job. The Australian cyber security workforce could benefit from structured on-the-job training programs like cyber security apprenticeships. The Australian Vocational Education and Training (VET) program[7] could be easily expanded to include Cyber Security topics. This would provide a recognised and consistent set of qualifications for new cyber security professionals that align with recognised Australian cyber security principles and recognised international frameworks like ISO 27001.

[7] Australian VET program - https://www.studyaustralia.gov.au/english/study/vocational-education