# SUBMISSION TO THE DEPT HOME AFFAIRS RE CYBER SECURITY PLAN 2020


Prepared by:

**Paul Nielsen**

**CM&AA; CPBB; CCSRA; CMEA; LREA; FIIDM; FAIBB; MQJA; J.P (Qual)**

COSBOA COUNCIL OF SMALL BUSINESS ORGANISATIONS AUSTRALIA

Former Chair and

**Cyber Security Ambassador**

***Avantia Cyber Security (A Div. Of Avantia Corporate Services Pty Ltd)***

***Level 7, 320 Adelaide Street,BRISBANE QLD 4000***

***Ph:*** [redacted]

***www.avantiacybersecurity.com***

1a What is your view of the cyber threat environment?
*Bad, Getting worse and not going to get any better. the CS Industry is too large.*

1b What threats should Government be focusing on?
*Password Management; SME Resilience; State Sponsored Cyber Crime.*

2 Do you agree with our understanding of who is responsible for managing cyber risks in the economy?
*Yes*

3a Do you think the way these responsibilities are currently allocated is right?
Yes - Business & Citizens must see to their own protection other than for National Infrastructure and Government Operations

3b What changes should we consider?
Offer incentives for SME's to become Cyber Secure
Educational Institutions Councils etc must demonstrate Cyber Security to get Govt Funding.

4 What role should Government play in addressing the most serious threats to institutions and businesses located in Australia?
Regulate Banks to only let them Loan funding to Businesses that have demonstrated a level of Cyber Security commensurate with their operations.

5 How can Government maintain trust from the Australian community when using its cyber security capabilities?
In the same way it does with unilateral military action. Checks and Balances.

6 What customer protections should apply to the security of cyber goods and services? None - Buyers must take responsibility for their own actions & security

7 What role can Government and industry play in supporting the cyber security of consumers? Regulation of all Websites Selling online (Overseas websites pay a premium GST)

8 How can Government and industry sensibly increase the security, quality and effectiveness of cyber security and digital offerings? More Training and awareness

9 Are there functions the Government currently performs that could be safely devolved to the private sector?
See 11. Govt's could outsource to Private Sector subsidised Training and Certification

What would the effect(s) be?
More awareness, Higher level of Cyber Security overall, Lower Cyber Insurance, Higher SME Enterprise Values.

10 Is the regulatory environment for cyber security appropriate? Why or why not?
No. SME space is Self Regulating. "they don't know what they don't know" and they don't believe a breach will happen to them. Regulation is required.

11 What specific market incentives or regulatory changes should Government consider?
*Consider making a bi-annual Cyber Security Audit mandatory for all Companies/Trusts/NFP with T/O over $1mill PA - Cost of the Audit to be tax deductible.

*Consider offering SME's a program like CYBERSECURE CANADA 2019 allowing organisations to prove to the Certification bodies that they meet minimum standards.
*Initial Audit to be funded 50% by Gove & 50% by Companies.
*Certification entitles users to use promo material - should entitle them to cheaper CS Insurance and increase the Enterprise value of their business.
*COSBOA (Council Of Small Business Organisations Of Australia - 38 Industry Associations with a reach to around 600,000 SME's will work with Home Affairs to develop this program with its members as a 'pilot' with a view to rolling it out if successfully implemented and Project Managed by COSBOA.

12 What needs to be done so that cyber security is 'built in' to digital goods and services?
Unsure what this really means???

13 How could we approach instilling better trust in ICT supply chains? See 11 above. All links in the chain must be Certified.

14 How can Australian governments and private entities build a market of high quality cyber security professionals in Australia? Consider a basic Apprentice Type Training through TAFE with 50% Work & 50% Learning.

15 Are there any barriers currently preventing the growth of the cyber insurance market in Australia? If so, how can they be addressed? Unknown. People writing the 'risk' in insurance companies are not trained Cyber Security people.

16 How can high-volume, low-sophistication malicious activity targeting Australia be reduced? Offensive Cyber attacks on the perpetrators by Government Operatives.

17 What changes can Government make to create a hostile environment for malicious cyber actors? Criminal Code Jail-able Offense - Deportation (if dual Citizen),

18 How can governments and private entities better proactively identify and remediate cyber risks on essential private networks? Military Grade support to Enterprise.

19 What private networks should be considered critical systems that need stronger cyber defenses? Schools - Hospitals - Transportation -

20 What funding models should Government explore for any additional protections provided to the community? Tax Deductibility; Certification Incentive and Subsidy

21 What are the constraints to information sharing between Government and industry on cyber threats and vulnerabilities? There should be none except Military & Security apparatus.

22 To what extent do you agree that a lack of cyber awareness drives poor consumer choices and/or market offerings? Do not agree at all. Consumers are vaguely aware that there are risks but still buy.

23 How can an increased consumer focus on cyber security benefit Australian businesses who create cyber secure products? What Type of Products are you talking about?

24 What are examples of best practice behavior change campaigns or measures? How did they achieve scale and how were they evaluated? All BPB campaigns need to be evaluated on the basis of outcomes. If you cannot measure the outcomes the campaign is worthless. The CYBERSECURE CANADA Program for example can be measured in Businesses certified.

25 Would you like to see cyber security features prioritised in products and services? This question is too Vague.

26 Is there anything else that Government should consider in developing Australia's 2020 Cyber Security Strategy? Refer # 11