Australia 2020 Cyber Security Strategy response

1. (a) persistent and dangerous

(b) The threat from users/public

2. The Government has a crucial role to play in managing the cyber risks

3. Greater assistance for small business to improve their cyber standing/readiness

Govt. financial assistance to spend with certified cyber specialist to protect Australian business/Intellectual Property

4. Advice, timely information, monitoring and oversight

5. Use appropriate secure communication technologies that are difficult/near impossible to impersonate

6. Should work as advertised and should meet an agreed "Standard" or set of "Standards"

7. Electronic industry expected to "build-in" protections for consumers

8. Increased research and development, collaboration

9.

10.

11. Tighter standards in the consumer space

GDPR or something similar

12. Legislation / Standards / Accountability / Penalties

13. Use of blockchain technology

14. Support and build better pathways into Cyber Security – education / culture / collaboration

15. Qualified assessors / Easily understood policies

16. Education and awareness

Provide assistance to business – botnet blocklists, op sec intel

17. State red team – offensive cyber activity, wargames

18. Use of latest technology / hire good people / continual skill improvement

19. Government Depts, ASX, Telecommunication companies, Healthcare

20. Using proceeds of crime / state based financial recovery from cyber crime activities

Banks and Insurance companies

21. A secure platform / trust between entities / timely communications

22. A great extent – it adds costs to the manufacture of goods which then affects competitiveness. Consumers generally don't consider it or think it important

23. Promote trust and encourage ownership of made in Australia

24. KnowBe4.

25.Yes, must be through "Standards" to make it fair to all in the market place (bronze, silver, gold maybe?)