1. What is your view of the cyber threat environment? What threats should Government be focusing on?

We need to focus more on identity theft. In a world where we are trying to move to a federated identity management, public trust that the digital solutions offered by the government and private sector

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

Yes

3. Do you think the way these responsibilities are currently allocated is right? What changes should we consider?

Better industry and government co-operation and interaction. Proactive sharing of Intelligence and Information rather than reactive to Cyber Incidents

4. What role should Government play in addressing the most serious threats to institutions and businesses located in Australia?

Representatives of local governments and businesses should have regular interaction. Contacts and Services provided by ASD, ACSC should be more publicised

5. How can Government maintain trust from the Australian community when using its cyber security capabilities?

The community is unaware of the work that is being done already.

6. What customer protections should apply to the security of cyber goods and services?

Perhaps we should take a cue from the NCSC and provide guidance on commercial products and services that will help to protect the organisation and reassure customers that cyber security is taken seriously

7. What role can Government and industry play in supporting the cyber security of consumers?

Make sure that there is more public knowledge on the current threat environment that affects consumers, whether that is using targeted advertising on public transport or in the media the information needs to reach people even in remote areas.

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

9. Are there functions the Government currently performs that could be safely devolved to the private sector? What would the effect(s) be?

10. Is the regulatory environment for cyber security appropriate? Why or why not?

There needs to be better co-operation between various agencies nationally and internationally. Navigating the regulatory environment can be difficult for small businesses

11. What specific market incentives or regulatory changes should Government consider?

12. What needs to be done so that cyber security is ‘built in’ to digital goods and services?

Have a requirement for business self-certification that businesses need to meet as a minimum requirement for goods and services

13. How could we approach instilling better trust in ICT supply chains?

14. How can Australian governments and private entities build a market of high-quality cyber security professionals in Australia?

Make sure that new courses are introduced, and curriculum is updated to meet emerging trends and threats.

Start early, introduce Cyber Security in schools

15. Are there any barriers currently preventing the growth of the cyber insurance market in Australia? If so, how can they be addressed?

The lack of awareness around cyber insurance

16. How can high-volume, low-sophistication malicious activity targeting Australia be reduced?

    Sharing intelligence as and when available.
    Push notifications to organisations (available on subscription initially)
    Being able to take down malicious actors or websites quickly

17. What changes can Government make to create a hostile environment for malicious cyber actors?

    Better co-operation between state government agencies and Federal government.
    Responses to Cyber threats are often disjointed.

18. How can governments and private entities better proactively identify and remediate cyber risks on essential private networks?
    More focused Cyber threat hunting

    Create a better National Cyber Awareness System where threats, vulnerabilities and risks are highlighted (Similar to CISA in the US)

19. What private networks should be considered critical systems that need stronger cyber defences?
    Telecommunications
    Email

20. What funding models should Government explore for any additional protections provided to the community?
    Grants
    Industry – Government partnership

21. What are the constraints to information sharing between Government and industry on cyber threats and vulnerabilities?

A devolved model of threat intelligence, there needs to be a National intelligence sharing platform

22. To what extent do you agree that a lack of cyber awareness drives poor consumer choices and/or market offerings?
    Completely Agree. People get duped because of the lack of awareness. The awareness seems to be more concentrated in the larger cities than in the towns

23. How can an increased consumer focus on cyber security benefit Australian businesses who create cyber secure products?
    Link it with incentives to produce cyber secure products

24. What are examples of best practice behaviour change campaigns or measures? How did they achieve scale and how were they evaluated?
    Queensland Government campaign during Common Wealth Games. People became more aware of threats

25. Would you like to see cyber security features prioritised in products and services?

    Yes, this should be highlighted on the features

26. Is there anything else that Government should consider in developing Australia's 2020 Cyber Security Strategy?
    Build in better co-ordination with International Agencies