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

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

Yes, I think the understanding is correct. I also think the responsibilities are roughly correct – I'm not a fan of giving up personal responsibility in favour of big brother. Where I feel improvements can be made, is in setting good standards and exemplifying *why* these are good standards.

E.g., most of us have bank accounts and it is clear that fraud is rife. Dual/Multi-factor authentication is a relatively simple mechanism that makes stealing an account **much** more difficult – yet many bank accounts do not have the option to enable MFA, let alone it being a standard practice. MFA should probably not be mandated by legislation, but Gov could publish simple to follow guidelines to the public advocating MFA. Public pressure would soon lead financial institutions to implement solutions.

Alternatively, and perhaps better, get rid of passwords in favour of a public key

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

Expanding Gov powers to react without invitation sounds almost as frightening as the hack threat itself. Perhaps in addition to advice and best practice, enable essential services to subscribe to regular pent test and reviews

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

Stop saying stupid things. Enabling Gov to decrypt our data for criminal investigatory purposes, sounds a lot like weakening encryption as a whole. You already acknowledge that state actors are a concern – do you really think they wouldn't attack the central key store or whatever other mechanism is being dreamt up?

You need to align the message and decide which is more important. Protecting citizens and businesses from hacking, or, being able to more easily conduct criminal/terrorist activity tracking. It would seem they are mutually exclusive to me.

6) What customer protections should apply to the security of cybergoods and services?

I think it would help to have a recognised 'badge'. It would be opt-in, and would show customers that the service has been assessed for best practices. Not sure how it would roll out though – maybe via independent audit/pen test companies.

The cost of scheme would be the sticking point – if too expensive then it won't be adopted.

The bigger worry for me, is the increasing number of devices. IOT. Almost inevitably, a lot of these devices end up being insecure – common crypto keys or default passwords and so one. Is there a 'minimum standard' already established and is it enforced?

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

Education; many issues start with someone clicking a dodgy link or similar poor practice. I've seen many 'fake phish' emails at work, put together by the security team. Could this be rolled out more widely? E.g., could ISP's be encouraged to participate?

Can education be brought to schools? What about old peoples homes, and/or hospitals? Free community training maybe.

12) What needs to be done so that cyber security is 'built in' to digital goods and services?

We're more and more mobile phone driven – it's relatively easy to generate an asymmetric key pair, and have the public key 'saved' to the particular service in question *instead* of a password. Service then issues a challenge encrypted with public key, and user is prompted for PIN/fingerprint/face to unlock their private key so the challenge can be answered.

Ergo, encourage service providers to enable saving of public keys instead of passwords. Surely this would be MUCH more secure in the event of a breach?

22) To what extent do you agree that a lack of cyber awareness drives poor consumer choices and/or market offerings?

I think it's a combination of lack of awareness of the consequences, as well as lowest price.

In my circle, there are many who have no real idea about cyber security. Then there are those that acknowledge they have poor practice – and don't care. Those with poor practice but are happy to learn. And those who oscillate between paranoia and doing something relatively poor cyber-wise.

Those that 'don't care' tend to have the attitude that they're small fish, so no-one would bother coming after them.

There needs to be tangible consequences published – how does a stolen identity really work; from gathering the intel, to exploiting, to the fall out. Does publishing my birthday on Facebook **really** matter? To ensure it is widely viewed, make a Netflix movie!! 😊

To counter lowest price buying, there needs to be a value. I mentioned before the idea of a 'badge'. Perhaps there should be a 'security safety star rating' for digital services – or at least the essential digital services – something like ANCAP but for digital. A 5 star rating this year, might degrade to 3 stars next year as the latest threats and vulnerability responses are added to the measuring matrix.

A 5 star digital service doesn't imply it won't be hacked, anymore than a 5 star car won't crash. But the fallout should be less severe – like the car. Would we pay more for services that are deemed 'safer'? Possibly – certainly some would. At least it would be clearer that it is a choice.