Please note that this response is my personal opinion and not necessarily that of my employer, Dialog Information Technology.

You may wish to answer some or all of the following questions

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

> The Government should be focussing on threats to Government business as far as an end to end solution is concerned.
>
> For other threats, the Government focus should be on responsible governance; ensuring that legislation, regulations, standards and certifications are in place to deter threats and, if that fails, provide the framework to respond to threats.

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

> Responsibility for management of cyber risks should be the same as management of other security risks. The Government needs to provide a framework of legislation, etc to deter attack, protect the nation and prevent recurrence of successful attacks through effective legislation and border controls.
>
> Responsibility for providing the protection and recovery should be an owner responsibility. The Government needs to take ownership of the physical and logical protection of government assets while industry and individuals have responsibility for protection of their own assets.
>
> Compare cyber security with physical security; the principles and responsibilities should be similar if not the same. The government has responsibility to establish and enforce protection measures such as making it illegal to steal, damage or prevent the unrestricted use (data or physical property), it sets standards for security measures such as protection ratings for locks or encryption standards for data, it provides a framework for accrediting people to perform security activities (locksmith qualifications, crowd controller licencing, cyber security qualifications). It provides a response capability to identify and prevent recurrence of individuals or organisations in breach of the law (police and other law enforcement). It does not and should not provide recovery services for physical or data loss; that is an industry responsibility, potentially overlaid with an insurance option. It does not provide day to day monitoring or maintenance of security systems, that is an industry capability. As a component of its governance role, Government may conduct compliance checks to confirm that physical items, industry or processes that support the provision of security and recovery services continue to meet the standards and guidelines it has set.
>
> Due to the relatively new nature of cyber threats and rate of growth of malicious activity, there is a period of time where supply of cyber security support from industry lags behind demand so the Government could provide direct support in the interim and actions to address the shortfall until industry catches up with demand. Any such measures should only be temporary.

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

> We need a transition plan to move from Government direct involvement due to a shortfall in industry capability to industry providing those services.

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

> The scope of governance that Government has a national responsibility for incudes maintaining the law and protection of its citizens; that must be inclusive of the things that keep this country running, its institutions and businesses.
>
> Government can play a key role in identifying potential threats and being a central body that is able to collect information from all sources to support and conduct active threat assessment and reporting of those assessments. In doing so, it should consider approaches to minimising those threats, including any need to update legislation, regulations, standards and certifications, as well as consider support mechanisms to enable institutions and industry to respond to threats.
>
> Government can also provide education services through a wide range of means to increase threat awareness and damage avoidance.
>
> Where threats can be confirmed to originate from other nation states, Government can apply political leverage for that source to disincentivise their actions.
>
> Responses to threats directed at other than Government targets, regardless of the seriousness, should remain an industry responsibility.

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

> Do what is right, always, and be transparent about it to the maximum practical extent.

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

> There should be standards for levels of protection for goods and services and a regime for quality assurance of those standards clearly and consistently available to the consumer in the form of simple labels (think energy ratings on electrical products or protection ratings on physical security devices such as padlocks).
>
> Default settings on products should provide the maximum protection upon delivery. The consumer may change if they choose.
>
> Provide a capability to report issues with goods and services and adjust their ratings based on performance. Publish this information.
>
> Force (by legislation) service providers to protect consumers and their data, and mandate breach reporting and recovery support to the affected individuals and organisations.

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

> Support identity protection by providing a national ID register that can be used to verify a person’s identity supported by a two-factor authentication to access. People worried about privacy can opt-out however that will leave them with no assured protection.

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

> Set, monitor and update standards for hardware and applications and mandate packaging showing the product compliance to those standards.
>
> Do many of the things already stated above.

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

> Everything that the Government is currently directly doing that is not an act of governance could potentially be devolved to the private sector, as long as there is a viable business case for the private sector to undertake that work. That business case would need to support profitability, return on the training and establishment costs and a viable, ongoing marketplace.
>
> There are some areas where trust could be an issue so caution and due diligence would need to be applied to an assessment of market viability, particularly in the area of registers, logs and reporting of incidents or protection status. It could be seen that commercialising these would lead to potential commercialisation of the associated data and therefore reticence to supply/contribute.

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

> A critical feature of the regulatory environment for cyber security is agility to adapt and respond as the threats and activities change, ideally moving to a predictive rather than responsive model where possible. Government, and particularly Commonwealth, is notoriously slow to move and restricted through 'red tape' to take action.
>
> Government needs a fast track approach to regulatory change for cyber security to provide the agility needed to be effective. Traditional approaches will never lead to a regulatory framework at the leading edge of cyber security activity.

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

> Provide a regulatory framework that business can work towards from a skills and organisational capacity perspective. Make the broad population and wider industry aware of that framework and the threats that the services can address so that the market need can be established. Incentivise business to achieve capabilities based on the framework and publish success stories to give the wider population confidence that business can mitigate their cyber security risks and resolve their issues arising from malicious activity.
>
> Demonstrate Government agility to maintain the regulatory framework to build trust and awareness in the wider community.

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

> Establish and enforce standards for products and services, ideally as ISO standards, but at least as AS/NZ standards. Require publishing of those standards when offering goods and services (see 6 above).
>
> Provide, potentially through industry capability, ongoing quality assurance processes to confirm continued compliance to those standards.

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

Communicate evidence of effective protection measures, threat responses and malicious activity recovery, including industry preparations and responses, Government regulation validation and law enforcement effective actions.

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

Unfortunately, increase demand through cyber security threat volumes and complexity; we wouldn't have the need if there wasn't a problem. The problem at least continuing, and probably expanding, is what will create the demand and sustain it. Increasing the complexity of malicious activity will further grow the quality of response and preventative cyber security professionals as they rise to the challenge of the new threats.

It is a case where the ideal is no cyber security issues so no market for professionals in the sector. The positive is that there are many talented people in Australia who have patriotic values who rise to the challenge of the threats for both community benefit and personal gratification. We need to recognise and reward them for their commitment.

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

Two barriers; trust and cost.

The recent Banking Royal Commission highlighted the lack of trust of insurance companies generally in Australia, unfortunately for good reason. Any insurance offering, including cyber security, needs to be a win-win to build the trust in the community. A component of the trust building is recognising positive actions being taken by entities to protect themselves from cyber security threats and having that reflected in the terms and costs of any insurance offerings. In other words, increase the benefits and/or decrease the costs of insurance for those who have made other investment in cyber security protection. To add further to trust, as a part of the policy, offer assessments and advisory services. When a claim is required as a result of threat realisation, provide recovery services rather than the simple and easy payout option that doesn't solve the policyholder's problem.

Cost and risk balance is the primary driver for a decision to purchase insurance cover. It is difficult for anyone but a cyber security professional to conduct an effective risk assessment of their cyber security position so it is likely that cyber security insurance will always appear expensive. From the insurance provider aspect, the price needs to be realistic and reasonable, If it isn't, the product won't sell. The onus is on the provider to demonstrate value so that their product sells. To do this they need to provide tools to bridge the knowledge gap so consumers can make an informed decision. This comes back to trust; can the consumer trust the tools provided by the insurer? Perhaps there is scope for Government to provide the tools so that it is seen as an independent but informed authority, albeit needing to ensure that liability for the decision remains between the insurer and the customer. Despite all of this, the cost still needs to be seen by the consumer as a value proposition.

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

Require (and incentivise) telecommunications carriers to monitor network activity, report and act upon suspicious activity. The concept is to counter attack at the earliest opportunity so the source or the point of entry into Australia should be the point of action to address the threat. Only the carriers have that capability, so they also need the responsibility to protect their services and customers. They should be under a mandatory reporting regime to Government, and to their customers for both blocked threats and any successful attacks, including any preventative measures taken as consequence. The objective of reporting to customers should be to increase awareness of threats and instil confidence in the measures being taken by their service providers.

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

Implement and maintain an effective regulatory framework that is sufficiently agile to remain contemporary.

Set and ensure the application of standards for digital products and services to reduce cyber security threats.

Actively monitor and take immediate action on identified threats.

Publish prevention and recovery success stories.

Rapidly identify and prosecute offenders with appropriate punishments.

18 How can governments and private entities better proactively identify and remediate cyber risks on essential private networks?

Narrowing the focus of this question down to a specific environment does not alter any of the previous responses, nor demand anything specific for that environment. Every prior response continues to apply.

Paul Potter