CRYPTOPOCALYPSE NOW

MARK A. LANE

CRYPTOPOCALYPSE
A.B.N. 762 284 230 93
P.O. BOX 333
PYALONG. VICTORIA. 3521.

RE: Cyber Security Strategy Discussion Paper Questions

Dear Sir / Madam, et al

Cryptopocalypse's general view on the future strategy for Australia is rather specific, and relates to the adoption of a suitable '**Quantum Mitigation Policy**', ensuring a minimum Quantum Resistant algorithm bit strength and password length, via cryptography and/or steganography is created / enforced, to ensure that any blob of data, is protected in situ and in transit.

Ideally the blob of data, should be protected for 99+ years, as that is the normal lifespan of an individual, whom could be linked to any blob of data, without taking into consideration, National Security requirements.

The Quantum Mitigation conundrum, exists on a speculative timeline, where the actual Quantum Resistance of an algorithm, is unknown, due to the speculative impacts of Quantum and Quantum+ technologies, side channel attacks, etc over the next 99 years.

Therefore, the question that the Quantum Mitigation Policy, needs to enforce on the Australian Cyber Security Ecosystem is :

'if the protected blob of data, is harvested by an advisory today, will it still be protected, by a Quantum and/or Quantum+ technology solution, in 99 years time ?'

Recent cryptanalysis advancements, place grave doubts on whether or not, the current Advanced Encryption Standard (Rijndael) Algorithm, (AES-256), will survive the next 10 years on the timeline, let alone the 99 year litmus test.

Specific responses to the '**Cyber Security Strategy Discussion Paper Questions**' by Cryptopocalypse, et al, follow below, addendums may follow prior to COB, 15th of April, 2023.

–

Mark A. Lane
[redacted]
Founder, UNIX / Software Engineer, Cryptologist @ FooCrypt, A Tale Of Cynical Cyclical Encryption (Cryptography & Steganography)

Australia's Only Quantum+ Secure / Proof, Cryptography and Steganography Software Solution

Index

Definitions

Litmus Test

Something (such as an opinion about a political or moral issue) that is used to make a judgment about whether someone or something is acceptable

The Cryptopocalypse in reference to Quantum Computing

The "Cryptopocalypse" refers to the potential future where traditional cryptography used to secure data and communications is rendered obsolete by quantum computers. This is because quantum computers have the potential to break the most commonly used cryptographic algorithms that are currently considered secure.

Traditional cryptography relies on mathematical problems that are believed to be too hard for classical computers to solve, such as factoring large numbers. However, quantum computers have the potential to solve these problems much faster than classical computers by utilising quantum algorithms such as Shor's algorithm.

Once quantum computers become powerful enough, they could break the cryptographic algorithms that are currently used to protect sensitive data, such as bank transactions, government communications, and personal information.

To address this threat, researchers are developing quantum-resistant cryptography, also known as post-quantum cryptography. These cryptographic methods are designed to be secure against attacks from both classical and quantum computers.

In summary, the Cryptopocalypse refers to the potential future where traditional cryptography is no longer secure due to the development of powerful quantum computers, and the need for quantum-resistant cryptography to address this threat.

Quantum Mitigation

Quantum mitigation refers to the process of implementing measures to mitigate the potential impact of quantum computers on existing cryptographic systems.

Quantum computers, due to their ability to perform calculations at an exponentially faster rate than classical computers, could potentially break many of the cryptographic systems currently in use, rendering them insecure. This includes widely used encryption methods like RSA and elliptic curve cryptography.

Quantum mitigation strategies include developing and deploying post-quantum cryptography, which are cryptographic systems that are designed to be resistant to attacks by quantum computers. Additionally, some experts suggest that implementing quantum key distribution (QKD) could also provide a solution. QKD is a technique that uses quantum mechanics to securely distribute cryptographic keys between parties, ensuring that the keys cannot be intercepted or compromised.

In summary, quantum mitigation involves taking proactive steps to ensure that our cryptographic systems remain secure in the face of potential future attacks by quantum computers.

What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?

These ideas could contribute to making Australia the most cyber secure nation in the world by 2030:

1. Strengthening cybersecurity regulations: The Australian government should introduce and enforce strict cybersecurity regulations that cover both the public and private sectors. These regulations should include mandatory cybersecurity training, regular security audits, and breach reporting requirements.

2. Promoting cybersecurity education and awareness: The government should invest in cybersecurity education programs and awareness campaigns to raise awareness about cyber threats and encourage safe online behaviour. This could include initiatives targeted at children, young people, and vulnerable groups.

3. Encouraging collaboration and information-sharing: The government should promote collaboration and information-sharing between government agencies, businesses, and cybersecurity experts. This could involve the creation of a centralised cybersecurity information hub or the establishment of industry-specific cybersecurity working groups.

4. Investing in research and development: The government should invest in research and development to support the development of new cybersecurity technologies and techniques. This could include funding for universities and research institutions, as well as the establishment of innovation hubs focused on cybersecurity.

5. Developing a skilled cybersecurity workforce: The government should support the development of a skilled cybersecurity workforce by providing training and education opportunities, as well as encouraging businesses to invest in their employees' cybersecurity skills. This could include initiatives like tax incentives for businesses that invest in cybersecurity training for their employees.

6. Strengthening international partnerships: The government should strengthen its international partnerships to promote global cybersecurity cooperation and information-sharing. This could involve initiatives like joint cybersecurity exercises, bilateral agreements on cybercrime, and participation in international cybersecurity conferences and forums.

7. Investing in cybersecurity infrastructure: The government should invest in the development of robust cybersecurity infrastructure, including secure networks, encryption technologies, and advanced security software. This could involve public-private partnerships to build and maintain critical cybersecurity

infrastructure.

By implementing these ideas, Australia can work towards becoming the most cyber secure nation in the world by 2030.

What legislative or regulatory reforms should Government pursue to: enhance cyber resilience across the digital economy?

What is the appropriate mechanism for reforms to improve mandatory operational cyber security standards across the economy (e.g. legislation, regulation, or further regulatory guidance)?

To enhance cyber resilience across the digital economy, the government could consider introducing legislation or regulation to improve mandatory operational cyber security standards across all sectors. This could include requirements for regular risk assessments, employee training, incident response plans, and data breach reporting.

Is further reform to the Security of Critical Infrastructure Act required? Should this extend beyond the existing definitions of 'critical assets' so that customer data and 'systems' are included in this definition?

Further reform to the Security of Critical Infrastructure Act may be required to include customer data and systems within the definition of critical assets. This could help ensure that businesses take appropriate measures to protect sensitive information and systems from cyber threats.

Should the obligations of company directors specifically address cyber security risks and consequences?

Yes, the obligations of company directors should address cyber security risks and consequences. Directors have a duty to act in the best interests of their company and its stakeholders, and cyber security is increasingly recognised as a critical business risk that can have significant financial, legal, and repetitional consequences.

Should Australia consider a Cyber Security Act, and what should this include?

The government could consider a Cyber Security Act to provide a comprehensive framework for addressing cyber threats across all sectors. This could include requirements for regular risk assessments, incident response planning, data breach reporting, and penalties for non-compliance.

How should Government seek to monitor the regulatory burden on businesses as a result of legal obligations to Cyber Security, and are there opportunities to streamline existing regulatory frameworks?

To monitor the regulatory burden on businesses, the government could establish a review process to assess the effectiveness and efficiency of existing cyber security regulations. This could involve consulting with industry stakeholders and seeking feedback on the impact of regulations on businesses of different sizes and in different sectors.

Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by: victims of cybercrime; and/or insurers? If so, under what circumstances?

What impact would a strict prohibition of payment of ransoms and extortion demands by cyber criminals have on victims of cybercrime, companies and insurers?

The government could consider prohibiting the payment of ransoms and extortion demands by cyber criminals, as this can encourage further attacks and create a market for cybercrime. However, any such prohibition should be carefully considered to avoid unintended consequences and ensure that victims of cybercrime have access to appropriate support and resources.

Should Government clarify its position with respect to payment or non- payment of ransoms by companies, and the circumstances in which this may constitute a breach of Australian law?

The government should clarify its position with respect to payment or non-payment of ransoms by companies and the circumstances in which this may constitute a breach of Australian law. This could help ensure that businesses have clear guidance on how to respond to ransomware attacks and avoid legal or repetitional consequences.

How can Australia, working with our neighbours, build our regional cyber resilience and better respond to cyber incidents?

To build regional cyber resilience and better respond to cyber incidents, Australia could work with its neighbours in several ways:

1. Promoting information sharing: Australia could work with neighbouring countries to establish mechanisms for sharing threat intelligence and best practices on cyber security. This could include the establishment of regional cyber security centres or the sharing of cyber security incident response plans.

2. Building capacity: Australia could provide technical assistance and capacity-building support to its neighbours to help them build their own cyber security capabilities. This could include training programs for law enforcement, government officials, and private sector actors.

3. Developing regional norms and standards: Australia could work with its neighbours to develop regional norms and standards for cyber security. This could involve the establishment of a regional cyber security framework or the adoption of international standards and guidelines.

4. Strengthening law enforcement cooperation: Australia could work with neighbouring countries to strengthen law enforcement cooperation on cyber crime investigations and prosecutions. This could involve the sharing of information on cyber criminals and their activities, as well as joint law enforcement operations.

5. Supporting regional cyber incident response: Australia could work with its neighbours to establish a coordinated regional cyber incident response mechanism. This could involve the creation of a regional cyber security emergency response team, the sharing of incident response plans, and the provision of technical assistance and support during cyber incidents.

By working with its neighbours to build regional cyber resilience and better respond to cyber incidents, Australia can help create a more secure and stable regional cyber environment, which benefits everyone in the region.

What opportunities exist for Australia to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective?

There are several opportunities for Australia to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective:

1. Strengthening existing partnerships: Australia could deepen its relationships with key partners, such as the United States, United Kingdom, Canada, New Zealand, and Japan, to increase cooperation on cyber security issues. This could include sharing threat intelligence, conducting joint cyber security exercises, and developing joint policies and strategies.

2. Expanding partnerships: Australia could seek to expand its network of cyber security partners by engaging with other countries in the Asia-Pacific region, such as Singapore, South Korea, and India. This could help create a more cohesive and collaborative regional cyber security architecture.

3. Engaging with international organisations: Australia could engage with international organisations such as the United Nations, the International Telecommunication Union, and the Organisation for Economic Cooperation and Development to promote global cyber security norms and standards. This could involve participating in international negotiations on cyber security issues, contributing to the development of global cyber security policies, and providing technical assistance and support to developing countries.

4. Promoting public-private partnerships: Australia could promote public-private partnerships on cyber security issues, by bringing together government agencies, private sector actors, and civil society organisations to collaborate on cyber security initiatives. This could involve establishing public-private forums, promoting information sharing, and providing incentives for businesses to invest in cyber security.

5. Supporting capacity-building initiatives: Australia could support capacity-building initiatives in developing countries to help them build their own cyber security capabilities. This could involve providing technical assistance and training programs, sharing best practices and expertise, and promoting the adoption of international standards and guidelines.

By elevating its existing international partnerships from a cyber security perspective, Australia can help create a more secure and resilient global cyber environment, which benefits everyone in the international community.

How should Australia better contribute to international standards-setting processes in relation to cyber security, and shape laws, norms and standards that uphold responsible state behaviour in cyber space?

Australia can contribute to international standards-setting processes in relation to cyber security and shape laws, norms, and standards that uphold responsible state behaviour in cyberspace in several ways:

1. Participation in international organisations: Australia can participate in international organisations such as the United Nations, the International Telecommunication Union, and the Organisation for Economic Cooperation and Development to contribute to the development of global cyber security standards and guidelines. This could involve participating in negotiations, providing technical expertise, and supporting the adoption of international standards.

2. Collaboration with like-minded countries: Australia can collaborate with like-minded countries that share its values and interests to promote responsible state behaviour in cyberspace. This could involve the development of joint policies and strategies, sharing of best practices, and coordination on cyber security initiatives.

3. Engagement with the private sector: Australia can engage with the private sector to promote responsible state behaviour in cyberspace. This could involve promoting industry-led initiatives to develop cyber security standards, encouraging companies to adopt responsible practices, and working with industry groups to promote cyber security best practices.

4. Promoting international norms: Australia can promote international norms that uphold responsible state behaviour in cyberspace. This could involve advocating for the adoption of existing norms, such as the Tallinn Manual, and promoting the development of new norms that address emerging cyber security threats.

5. Capacity-building in developing countries: Australia can support capacity-building initiatives in developing countries to help them build their own cyber security capabilities and promote responsible state behaviour in cyberspace. This could involve providing technical assistance and training programs, sharing best practices and expertise, and promoting the adoption of international standards and guidelines.

By contributing to international standards-setting processes in relation to cyber security and promoting responsible state behaviour in cyberspace, Australia can help create a more secure and stable global cyber environment, which benefits everyone in the international community.

How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?

Commonwealth Government departments and agencies can better demonstrate and deliver cyber security best practices and serve as a model for other entities by taking the following actions:

1. Implementing robust cyber security measures: Departments and agencies should implement a comprehensive range of cyber security measures, including firewalls, antivirus software, encryption, and access controls. They should also conduct regular risk assessments and vulnerability scans to identify and address potential weaknesses.

2. Developing and implementing policies and procedures: Departments and agencies should develop and implement clear policies and procedures that outline how they will manage cyber security risks, respond to incidents, and protect sensitive information. These policies should be regularly reviewed and updated to ensure they remain effective.

3. Training and awareness: Departments and agencies should provide regular cyber security training and awareness programs for staff to ensure they are equipped to identify and respond to cyber security risks. This should include training on safe online behaviour, such as how to recognise phishing emails and how to use strong passwords.

4. Engaging in information sharing: Departments and agencies should engage in information sharing with other government entities and the private sector to improve their own cyber security capabilities and contribute to the overall cyber security of the country.

5. Compliance with standards and regulations: Departments and agencies should comply with relevant cyber security standards and regulations, such as the Australian Government Information Security Manual (ISM) and the Protective Security Policy Framework (PSPF).

6. Regular testing and auditing: Departments and agencies should regularly test and audit their cyber security measures to ensure they are effective and identify areas for improvement.

By demonstrating and delivering cyber security best practices, Commonwealth Government departments and agencies can set an example for other entities and promote a culture of cyber security across the public and private sectors.

What can government do to improve information sharing with industry on cyber threats?

The government can take several steps to improve information sharing with industry on cyber threats, including:

1. Establishing a trusted information sharing framework: The government can establish a trusted framework for information sharing with industry on cyber threats. This framework could involve the creation of a central information-sharing platform or portal that allows government agencies and industry partners to share information in a secure and confidential manner.

2. Developing clear guidelines and protocols: The government can develop clear guidelines and protocols for information sharing with industry on cyber threats. This could include guidelines on what information can be shared, how it should be shared, and under what circumstances.

3. Providing timely and actionable information: The government can provide timely and actionable information to industry partners on cyber threats. This could involve providing real-time updates on emerging threats and vulnerabilities, as well as detailed threat intelligence reports.

4. Engaging with industry partners: The government can engage with industry partners to understand their specific cyber security concerns and needs. This could involve holding regular meetings and workshops to share information and exchange ideas.

5. Encouraging collaboration and information exchange: The government can encourage collaboration and information exchange between industry partners. This could involve facilitating information sharing between companies in the same sector or industry, as well as promoting cross-sector collaboration.

6. Providing incentives for information sharing: The government can provide incentives for industry partners to share information on cyber threats. This could include offering financial incentives or recognition for companies that participate in information-sharing programs.

By improving information sharing with industry on cyber threats, the government can help to promote a more collaborative and effective approach to cyber security, which ultimately benefits the entire community.

During a cyber incident, would an explicit obligation of confidentiality upon the Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC) improve engagement with organisations that experience a cyber incident so as to allow information to be shared between the organisation and ASD/ACSC without the concern that this will be shared with regulators?

An explicit obligation of confidentiality upon the Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC) could potentially improve engagement with organisations that experience a cyber incident, as it would allow for greater trust and transparency in the information sharing process. If organisations are assured that the information they provide to ASD/ACSC will be kept confidential and not shared with regulators, they may be more willing to share sensitive information about the incident, including the scope and impact of the attack, as well as any remediation efforts.

However, it is important to note that any obligation of confidentiality would need to be carefully balanced against the government's regulatory responsibilities and the need to protect the public interest. In some cases, it may be necessary for regulators to have access to certain information in order to assess the impact of the incident on the wider community and take appropriate regulatory action.

In practice, the ASD/ACSC already has a range of measures in place to protect the confidentiality of information shared with them during a cyber incident. For example, they have a Trusted Information Sharing Network that allows for secure and confidential information sharing between government agencies and industry partners.

Overall, while an explicit obligation of confidentiality could potentially improve engagement with organisations during a cyber incident, any such obligation would need to be carefully considered in the context of the government's broader regulatory responsibilities and the need to protect the public interest.

Would expanding the existing regime for notification of cyber security incidents (e.g. to require mandatory reporting of ransomware or extortion demands) improve the public understanding of the nature and scale of ransomware and extortion as a cybercrime type?

Expanding the existing regime for notification of cyber security incidents, including the introduction of mandatory reporting of ransomware or extortion demands, could improve the public understanding of the nature and scale of ransomware and extortion as a cybercrime type. This is because it would provide greater visibility and transparency around the prevalence and impact of these types of cyberattacks, which could help to raise awareness and encourage greater vigilance among the general public and businesses.

Mandatory reporting requirements could also provide a more accurate picture of the scope and scale of ransomware and extortion attacks in Australia, which would be valuable for law enforcement agencies and other stakeholders seeking to combat cybercrime.

However, it is important to note that any expansion of the notification regime would need to be carefully balanced against the potential burden on businesses and organisations. Reporting requirements could be particularly onerous for small and medium-sized businesses with limited resources, and may result in a flood of reports that are difficult to triage and prioritise.

Therefore, any expansion of the notification regime should be accompanied by clear guidance and support for businesses, as well as a system for effective triage and response to reported incidents. Additionally, it may be useful to provide incentives for businesses to report incidents, such as protection from liability or reduced regulatory burden for companies that report incidents in a timely and transparent manner.

What best practice models are available for automated threat-blocking at scale?

There are several best practice models available for automated threat-blocking at scale. Here are some examples:

1. Machine learning and artificial intelligence (AI): Machine learning and AI can be used to analyse large datasets of threat intelligence and automatically identify patterns and anomalies that may indicate a cyber threat. This can help to automate threat-blocking at scale and reduce the workload on human analysts.

2. Network segmentation: By dividing a network into smaller segments and applying different security policies to each segment, organisations can better protect against threats and limit the potential impact of a breach. This can be achieved through the use of tools like firewalls and intrusion detection systems.

3. Zero trust security: The zero trust security model assumes that all users, devices, and applications are potential threats and requires constant verification of identity and access privileges. This approach can help to prevent unauthorised access and reduce the risk of data breaches.

4. DevSecOps: DevSecOps is a security-focused approach to software development that emphasises collaboration and automation between developers, security teams, and operations teams. This approach can help to integrate security into the software development lifecycle and reduce the risk of vulnerabilities and exploits.

5. Threat intelligence sharing: By sharing threat intelligence with other organisations and security providers, businesses can better understand emerging threats and quickly respond to incidents. This can help to automate threat-blocking at scale and reduce the time to detection and response.

Overall, automated threat-blocking at scale requires a combination of technology, processes, and people. By adopting best practices like those listed above, organisations can better protect themselves against cyber threats and improve their overall security posture.

Does Australia require a tailored approach to uplifting cyber skills beyond the Government’s broader STEM agenda?

Yes, Australia requires a tailored approach to uplifting cyber skills beyond the government's broader STEM agenda. While a strong foundation in science, technology, engineering, and mathematics (STEM) is important for developing cyber skills, the specific technical and non-technical skills required for cybersecurity require a more targeted approach. Cybersecurity is a rapidly evolving field, and the skills needed to address the latest threats and vulnerabilities are constantly changing. Therefore, a tailored approach is necessary to ensure that Australia's cybersecurity workforce has the necessary skills to keep pace with the evolving threat landscape.

Some potential elements of a tailored approach to uplifting cyber skills in Australia could include:

1. Establishing specialised cyber security training programs: These programs could be tailored to address specific skill gaps in the workforce and could provide both technical and non-technical training to help individuals develop the skills needed to work in the field.

2. Encouraging industry collaboration: Collaboration between government, academia, and industry can help to identify emerging skill requirements and develop training programs to address them.

3. Promoting cyber security as a career: Encouraging more individuals to consider cyber security as a career could help to build a pipeline of skilled professionals for the future.

4. Providing targeted incentives: Providing targeted incentives to individuals and organisations to invest in cyber security training and development can help to increase the number of skilled cyber security professionals in Australia.

Overall, a tailored approach to uplifting cyber skills in Australia is necessary to address the unique challenges of the cybersecurity field and ensure that the workforce has the skills needed to keep pace with the evolving threat landscape.

What more can Government do to support Australia’s cyber security workforce through education, immigration, and accreditation?

There are several steps the Australian Government can take to support the country's cyber security workforce through education, immigration, and accreditation:

1. Education: The government can work to promote cyber security education and training programs to help build a pipeline of skilled professionals for the future. This could include investing in cyber security programs at universities and supporting the development of vocational training programs for cyber security.

2. Immigration: The government can make it easier for skilled cyber security professionals to immigrate to Australia by streamlining the visa application process and providing targeted incentives to attract talent from overseas.

3. Accreditation: The government can support the development of industry-recognised accreditation programs for cyber security professionals. This could include working with industry associations to establish certification programs that align with international standards.

4. Workforce development: The government can work with industry partners to develop targeted workforce development programs that address specific skill gaps in the cyber security workforce. These programs could include on-the-job training, mentoring, and internships.

5. Public-private partnerships: The government can work with private sector partners to develop initiatives that support cyber security education, immigration, and accreditation. This could include public-private partnerships to fund cyber security research and development, as well as joint initiatives to promote cyber security as a career.

By taking these steps, the Australian Government can help to support the development of a strong and skilled cyber security workforce, which is critical to protecting the country's digital assets and ensuring the security and resilience of the national cyber ecosystem.

How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians? a. Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?

In responding to major cyber incidents, the government should consider a range of measures beyond existing law enforcement and operational responses. These could include:

1. Establishing a national incident response plan: The government could develop a comprehensive incident response plan that outlines the roles and responsibilities of key stakeholders in responding to major cyber incidents. This plan could include protocols for information sharing and collaboration between government agencies, industry partners, and international partners.

2. Providing support for affected organisations: The government could provide financial, technical, and other support to affected organisations to help them recover from a cyber incident. This could include funding for incident response teams, assistance with data recovery, and access to legal and other professional services.

3. Improving information sharing: The government could consider establishing a single reporting portal for all cyber incidents to harmonise existing requirements to report separately to multiple regulators. This would streamline the reporting process for organisations and enable more effective information sharing and collaboration between government agencies.

4. Strengthening regulatory frameworks: The government could review existing regulatory frameworks and consider whether additional measures are required to enhance cyber security across the economy. This could include mandatory reporting requirements, minimum cyber security standards, and penalties for non-

compliance.

5. Enhancing international cooperation: The government could work with international partners to improve cooperation and information sharing on cyber security issues. This could involve establishing formal agreements and partnerships with other countries to share threat intelligence, coordinate responses to major cyber incidents, and promote international norms and standards for responsible behaviour in cyberspace.

Overall, the government should take a proactive and coordinated approach to responding to major cyber incidents, with a focus on protecting Australians and strengthening the resilience of Australia's digital infrastructure.

What would an effective post-incident review and consequence management model with industry involve?

An effective post-incident review and consequence management model with industry would involve a collaborative and coordinated approach between government agencies and industry partners. The model could include the following elements:

1. Post-incident review: After a cyber incident, a formal post-incident review should be conducted to identify the cause of the incident, assess the impact, and identify any areas for improvement. This review should involve both government agencies and industry partners, and could include an independent assessment to provide an objective perspective.

2. Information sharing: During the post-incident review, information should be shared between government agencies and industry partners to ensure that all relevant information is taken into account. This information could include technical data, incident response logs, and any other relevant information that could help to inform the review.

3. Lessons learned: The post-incident review should identify lessons learned from the incident, including any gaps in policies, procedures, or technical controls that need to be addressed. These lessons should be shared with industry partners to help them improve their own cyber security posture and avoid similar incidents in the future.

4. Consequence management: In the event that the cyber incident has resulted in significant harm, consequence management measures may be required. This could include legal action against the perpetrators, compensation for affected individuals or organisations, or other measures to mitigate the impact of the incident.

5. Continuous improvement: The post-incident review and consequence management model should be reviewed and updated on an ongoing basis to ensure that it remains effective and relevant. This could include regular reviews of incident response plans, regular training and awareness programs for staff, and ongoing collaboration between government agencies and industry partners.

Overall, an effective post-incident review and consequence management model with industry should be based on collaboration, information sharing, and a continuous improvement approach, with a focus on improving cyber security resilience and preventing future incidents.

How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime? a. What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?

Small businesses often have limited resources and expertise to manage their cyber security risks effectively. Therefore, the government can provide several types of assistance to support small businesses in managing their cyber security risks and keeping their data and customers' data safe:

1. Cyber security education and training: The government can provide education and training programs tailored to small businesses to increase their awareness of cyber risks, best practices, and how to respond to cyber incidents.

2. Access to affordable cyber security tools and services: The government can work with industry partners to provide small businesses with access to affordable cyber security tools and services, such as anti-virus software, firewalls, and security assessments.

3. Financial assistance: The government can offer financial assistance to small businesses to invest in their cyber security infrastructure and improve their resilience to cyber threats.

4. Information sharing: The government can collaborate with industry partners to share information on emerging threats and best practices with small businesses, enabling them to be better prepared and protected against cyber threats.

5. Cyber insurance: The government can work with the insurance industry to develop affordable cyber insurance products that are tailored to small businesses.

Overall, the government can play a critical role in supporting small businesses in managing their cyber security risks, which in turn will help to protect their data and customers' data.

What opportunities are available for government to enhance Australia’s cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia?

There are several opportunities available for the government to enhance Australia's cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia:

1. Investment in research and development: The government can invest in research and development of new cyber security technologies, including emerging technologies such as artificial intelligence and machine learning.

2. Collaboration between industry and government: The government can collaborate with industry partners to foster innovation in the cyber security technologies ecosystem and to support the uptake of new technologies and services.

3. Government procurement: The government can leverage its purchasing power to support the growth of Australian cyber security companies by procuring cyber security products and services from local businesses.

4. Funding for start-ups: The government can provide funding and support for cyber security start-ups to help them develop and commercialise their products and services.

5. Export promotion: The government can promote Australian cyber security products and services in international markets, helping to create new opportunities for local businesses.

6. Supporting skills development: The government can support the development of skills and talent in the cyber security industry, through initiatives such as training programs and partnerships with universities.

Overall, by investing in research and development, fostering collaboration between industry and government, leveraging procurement power, funding start-ups, promoting exports, and supporting skills development, the government can enhance Australia's cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia.

How should we approach future proofing for cyber security technologies out to 2030?

Future-proofing for cyber security technologies out to 2030 requires a proactive and adaptive approach that considers both emerging threats and evolving technologies. Here are some key considerations:

1. Continuous monitoring and assessment of emerging technologies and trends: The cyber security landscape is constantly changing, and new technologies and trends can introduce new risks. Therefore, it is important to continuously monitor and assess emerging technologies and trends that may impact cyber security. This could be achieved through collaboration between industry, government, and academia.

2. Encouraging innovation and collaboration: Innovation and collaboration are key drivers of the cyber security industry. Government can support the growth of the cyber security ecosystem by creating a supportive environment for innovation and collaboration between industry, government, and academia. This could involve initiatives such as funding for research and development, creating incubators and accelerators for cyber security startups, and supporting collaborations between industry and academic institutions.

3. Promoting international collaboration: Cyber threats are global in nature, and it is important for Australia to collaborate with international partners to address these threats. Government can promote international collaboration by participating in international forums, sharing best practices and threat intelligence, and supporting joint initiatives to improve global cyber security.

4. Fostering a skilled workforce: The availability of a skilled workforce is crucial for the growth and sustainability of the cyber security industry. Government can support the development of a skilled workforce by promoting cyber security education and training programs, creating pathways for graduates to enter the industry, and supporting initiatives to attract and retain talent.

5. Adapting to new technologies: As new technologies emerge, it is important for cyber security technologies to adapt and evolve to address new threats. Government can support the adoption of new technologies by promoting standards and best practices, creating incentives for adoption, and supporting initiatives to build trust in new technologies.

Are there opportunities for government to better use procurement as a lever to support and encourage the Australian cyber security ecosystem and ensure that there is a viable path to market for Australian cyber security firms?

Yes, there are opportunities for the government to better use procurement as a lever to support and encourage the Australian cyber security ecosystem. One way to do this is by introducing procurement policies that prioritise the use of Australian cyber security products and services. This can include setting targets for government agencies to purchase a certain percentage of their cyber security products and services from Australian companies.

Another way to support the Australian cyber security ecosystem is by providing funding for research and development in the field of cyber security. The government can offer grants, loans or tax incentives to encourage the development of innovative cyber security technologies and solutions.

In addition, the government can promote collaboration between industry and academia by establishing partnerships with universities and research institutions to support the development of new cyber security technologies.

By taking these steps, the government can create a viable path to market for Australian cyber security firms, which can help to build a strong and sustainable cyber security ecosystem in Australia.

How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?

To address the cyber security of emerging technologies and promote security by design in new technologies, the Strategy should consider the following:

1. Collaboration and engagement with industry and academia: The government should collaborate closely with industry and academia to identify and address cyber security risks associated with emerging technologies. This could involve partnering with tech firms and research institutions to conduct risk assessments, develop best practices, and promote security-by-design principles.

2. Regulatory frameworks: The government should explore the development of regulatory frameworks that promote security-by-design principles and address cyber security risks associated with emerging technologies. This could involve establishing minimum security standards for emerging technologies, such as IoT devices or 5G networks, or requiring manufacturers to build security features into

their products from the outset.

3. Funding and support for research and development: The government should invest in research and development to support the creation of new cyber security technologies that can address the risks associated with emerging technologies. This could involve providing funding for startups and emerging technology companies that are developing innovative cyber security solutions, or providing support for research into new cyber security technologies that can be applied to emerging technologies.

4. Education and awareness: The government should work to educate the public and businesses about the cyber security risks associated with emerging technologies and promote best practices for securing these technologies. This could involve developing public awareness campaigns, providing training and education programs for businesses and individuals, or establishing certification programs for cyber security professionals working with emerging technologies.

5. International collaboration: The government should work closely with international partners to address global cyber security risks associated with emerging technologies. This could involve collaborating on the development of international standards or sharing information and best practices to address common threats.

Overall, the Strategy should take a proactive approach to addressing the cyber security risks associated with emerging technologies, promoting security-by-design principles, and supporting the development of new cyber security technologies that can address these risks.

How should government measure its impact in uplifting national cyber resilience?

Measuring the impact of government efforts in uplifting national cyber resilience can be challenging. However, here are some potential ways to measure impact:

1. Reduction in the number and severity of cyber incidents: The number and severity of cyber incidents could be used as a measure of the effectiveness of government efforts in enhancing cyber resilience. A decrease in the frequency and severity of cyber incidents could indicate that these efforts are having a positive impact.

2. Adoption of cybersecurity best practices: Increased adoption of cybersecurity best practices by organisations and individuals could be another indicator of success. This could include metrics such as the number of organisations implementing multi-factor authentication or regularly conducting security awareness training.

3. Cybersecurity workforce development: The development of a skilled cybersecurity workforce is critical to enhancing cyber resilience. Measuring the number of individuals completing cybersecurity-related training and certification programs or the number of cybersecurity job openings filled could help to assess the effectiveness of government efforts in this area.

4. International recognition: Australia's standing in international cybersecurity rankings and assessments, such as the Global Cybersecurity Index, could also be a measure of the effectiveness of government efforts in enhancing cyber resilience.

Overall, a combination of these measures could provide a comprehensive assessment of the effectiveness of government efforts in enhancing national cyber resilience.

What evaluation measures would support ongoing public transparency and input regarding the implementation of the Strategy?

To support ongoing public transparency and input regarding the implementation of the Strategy, the government could consider implementing the following evaluation measures:

1. Regular reporting: The government could regularly report on the progress made towards achieving the goals set out in the Strategy, as well as any challenges faced and the strategies employed to address them.

2. Independent review: The government could commission independent reviews of the Strategy's implementation to ensure that progress is being made and to identify areas for improvement.

3. Public consultations: The government could conduct public consultations to solicit feedback from stakeholders, including industry, academia, civil society, and the general public, on the implementation of the Strategy.

4. Performance metrics: The government could develop performance metrics to assess the effectiveness of the Strategy's implementation, such as the number of cyber incidents prevented, the time taken to respond to incidents, and the level of cyber awareness and resilience in the community.

5. Benchmarking: The government could benchmark Australia's progress against other countries' cybersecurity strategies to identify areas for improvement and share best practices.

By implementing these evaluation measures, the government can demonstrate its commitment to transparency and accountability and ensure that the Strategy's implementation remains responsive to the evolving cybersecurity landscape.