2023–2030 Australian Cyber Security Strategy

Engineers Australia's submission

21 April 2023

ENGINEERS
AUSTRALIA

2023–2030 Australian Cyber Security Strategy

Engineers Australia's submission

Author: Louis Field

Engineers Australia
11 National Circuit, Barton ACT 2600
+61 2 6270 6555
policy@engineersaustralia.org.au

engineersaustralia.org.au

Contents

Introduction

In a world ever more connected, cyber-crime has become legion. The cost of cyber-crime is predicted to hit $12 trillion in 2023 and grow to $15 trillion by 2025. Almost every company or governmental department and agency is connected and at risk from breach.[1]

Engineers Australia welcomes the initiative from the Department of Home Affairs to consult industry as it works on building the Strategy to protect and secure the nation from these constant cyber threats. Engineers are uniquely positioned to contribute to the development of the Strategy as their multi-discipline profession grants them a holistic view and systems approach to complex issues.

Securing Australian cyber space and building a robust and resilient cyber ecosystem will require the Strategy to be comprehensive, agile, and inclusive. The Government needs to commit to invest in the long-term on the development of Australia's sovereign cyber security capabilities. This will reduce our dependence on overseas technology, while fostering new partnerships with trusted allies within and outside Australia, helping us to learn and grow the tools needed to match the ever evolving and sophisticated cyber threats.

In this submission, Engineers Australia offers the view of its expert members on what the Government could do to achieve the goal of securing our nation's cyber ecosystem and shift the dial to move cyber security front of mind.

About Engineers Australia

With more than 115,000 individual members, Engineers Australia is the profession's peak body. We are the collective voice of the profession and exist to advance society through great engineering. We support engineers in the pivotal role they play in shaping the future of Australia: creating safe, successful, and sustainable communities.

Engineers Australia takes an evidence-based approach that harnesses the collective technical and professional skills of engineering leaders in contributing to important decisions and debates.

As Australia's signatory to the International Engineering Alliance, Engineers Australia maintains national professional standards, benchmarked against international norms. Under the Migration Regulations 1994, we are the designated assessing authority to perform the assessment of potential migrant engineering professionals' skills, qualifications, and/or work experience to ensure they meet the occupational standards needed for employment in Australia.

Engineers Australia can apply expertise in Cyber Security, Systems Engineering and Standards Development, offering the Government a unique view and advice to strengthen the security of our communities both offline and online.

Contact

Engineers Australia welcomes the opportunity to engage further with the Department of Home Affairs. These are complex and contextual issues. Engineers Australia has significant expertise in our Learned Society Colleges and Technical Societies that can assist in addressing them. Please do not hesitate to reach out if you would like to discuss this further. You can contact us at policy@engineersaustralia.org.au

[1] Forbes, *Cybersecurity Trends & Statistics For 2023; What You Need To Know*, https://www.forbes.com/sites/chuckbrooks/2023/03/05/cybersecurity-trends--statistics-for-2023-more-treachery-and-risk-ahead-as-attack-surface-and-hacker-capabilities-grow/?sh=5c29575b19db, March 5 2023

Response to the discussion paper questions

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

Cyber Security is a complex, ever evolving and often expensive concern all governments around the world are trying to tackle. Engineers Australia understands the challenges ahead of building a robust cyber security strategy for Australia, we recommend the following ideas be included in the Strategy to achieve the Government's goal of becoming the most cyber secure nation in the world by 2030:

1. **Focus on resilience and risk management**: as becoming the most cyber secure nation in the world will largely depend on our ability to ensure our infrastructure can cope with cyber-attacks, while avoiding full breakdowns, risk management plans and strategies need to be put in place.
2. **Cyber Security range**: build a cyber security range that all Critical Infrastructure operators can use in accordance with the Strategy
3. **Securing our Operation Technology (OT) systems**: Integrate OT cybersecurity concerns in all facets of cybersecurity (legislation, frameworks, etc…). Cybersecurity has historically focused solely on Information Technology (IT) systems, rendering OT systems, as a result, highly insecure. OT systems often don't work well with existing cybersecurity frameworks, standards, legislation etc… A focus on providing a balanced approach between IT and OT systems in the Strategy is vital to secure our nation.
4. **Workforce**: Building the right skilled workforce should be the key to the Strategy. More investments are needed in skills development and trusted accreditations for professionals across all industries. Taking for example the OT systems as referred to our previous point, cybersecurity professionals, their certifications, education and other training often don't experience or include skills development related to OT systems.

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

The Government has a unique opportunity to set a clear pathway for Australia to build a robust cyber security strategy to secure the nation. Before deciding on what legislative or regulatory reforms should be pursued, we recommend the Government to consider the following points:

1. **Consult and engage with industry**: i.e., the Security of Critical Infrastructure Act 2018 was perceived by many as having been presented as a *fait accompli* to the industry as opposed to having been built in collaboration with the industry.
2. **Avoid a "one size fits most" approach**: adopting a regulatory framework that allows a more nuanced approach like what is done in the UK. Here law supports a Cyber Assessment Framework (CAF) that is then assessed and customised when required for sectors by existing regulators. An agile framework would work best to secure and guide the whole industry.
3. **Consistency**: whether the nomination of a single branch of government to regulate the area or a full alignment of State and Commonwealth requirements, we need to simplify the current situation to ensure that Critical Infrastructure operators are no longer required to meet requirements from multiple regulators.
4. **Shift to measurable improvements**: change the focus away from reporting (compliance) to measurable improvements in security and resilience.

5. **Do not recreate the wheel**: adopt International Standards where possible and move those standards from behind paywalls.

a. 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)?

Mandatory operational cybersecurity standards across all sectors through either regulations or legislation, are needed and should be implemented. The example of the CAF implemented in the UK as mentioned above would provide a way to offer the industry more adapted regulatory guidance to ensure greater level of compliance from all.

Storage of sensitive data is the biggest concern at present. We recommend making it mandatory for companies that store sensitive data to implement a minimum standard of security. Should a company be unable to comply, they should be mandated to use a third-party data broker which is able to.

b. 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 (SOCI) Act is required. The compliance burden SOCI has brought has far out weighted the improvement in security performance produced. Our members are particularly concerned by the Risk Management Program Rules lack of alignment with accepted risk management practice. For OT systems used to control Critical Infrastructure, more security benefits would be gained if compliance with international standards like IEC 62443, IEC 61508, or IEC 61511 was mandated.

The introduction of SFAIRP (*so far as is reasonable practical*) has raised a lot of debates. In a safety context, SFAIRP is often interpreted as a requirement of extensive documentation of not only controls but also what controls where not select and why, raising concerns around the associated cost of any risk and assurance programme. While Engineers Australia is not against SFAIRP approach, we recommend a more in-depth review of the messaging to clarify the guidance.

The Security of Critical Infrastructure Act's definition of "critical assets" is already quite broad and not all included sectors can realistically be considered critical. However, in some instance, data security needs to go beyond 'critical' to 'essential'. Smaller entities managing services and data that enables the delivery of those 'essential' services increasingly rely on data to provide an essential service. This means that they are not getting the same kind of protection focus that the designated critical infrastructure is getting. Current studies are looking at the non-critical systems and assets to understand how they may potentially impact critical infrastructure systems instead of considering the real impact on local communities with respect to the services on which they rely. The data security for non-critical infrastructure is required but is not subject to current policy advice at a Commonwealth level.[2] A need for a more nuanced approach is clearly needed to influence and facilitate other entities also managing their data security risks.

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

Cyber security risks and the associated consequences have become a concern no company directors can ignore. The recent Medibank, Optus or Latitude breaches have shown the importance for all executive teams to be well prepared and informed on cyber security risks.

[2] Engineers Australia, *DHA National Data Security Action Plan*, June 2022, p19

Company directors are already responsible for the risk management, including cyber. Should obligations of company directors specifically address cyber security and consequences be implemented, this would only reinforce the existing monitoring and investment undertaken to protect companies' systems and data.

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

At present, the Privacy and SOCI Acts are covering in principle two main aspects, the protection of personal data and the protection of integrity of system operation, i.e., for Critical Infrastructure systems. The need for further reform of SOCI has already been made above, therefore if a Cyber Security Act is implemented, it should result in the repeal of the existing SOCI and State regulations.

A Cyber Security Act would be the opportunity to introduce a more coherent and consolidated approach to securing our nation while lessening the burden on companies and alleviating the existing confusions. An Act would need to require organisations to consider not only the consequences of stolen or manipulated data, but also the disruption of service provision. It should also include consideration of OT system protection and not IT systems only, in addition to all the recommendations previously listed above.

e. 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?

Regulatory burdens should always be subject to efficacy measurement. The current compliance state of play is showing some signs of unmeasured efficacy. Separating the cost of compliance from the cost of implementing beneficial controls is challenging. However, a Cyber Security Act could be an opportunity for Government to achieve some streamlining and lessen the regulatory burden on businesses while increasing the level of protection for all consumers.

The existing frameworks in place (Information Security Manual (ISM), Information Security Registered Assessors Program (IRAP), cloud certification framework to name a few) are relatively robust, yet are all geared toward classified IT systems, making it difficult to implement in commercial settings and on OT systems. Government should consider expanding the ISM to cover OT systems and modifying the ISM to apply to non-government organisations.

A Cyber Security Act would also offer a chance to harmonise all existing frameworks to ensure they all work together to streamline processes and reduce the regulatory burden on businesses while strengthening businesses' defences against cyber-attacks.

f. Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by:

(a) victims of cybercrime; and/or

(b) insurers? If so, under what circumstances?

I. WHAT IMPACT WOULD A STRICT PROHIBITION OF PAYMENT OF RANSOMS AND EXTORTION DEMANDS BY CYBER CRIMINALS HAVE ON VICTIMS OF CYBERCRIME, COMPANIES AND INSURERS?

Engineers Australia stands with the Government in prohibiting the payment of ransoms and extortion demands by cyber criminals. Allowing payments would be detrimental and only encourage cyber criminals in their ventures. We encourage the Government to implement greater penalties for cyber attackers in an effort to deter more from using this route of action.

However, it remains advisable to keep some room for a discretionary "national interest" plan carve out to allow Government to endorse potential payment in extreme cases, such as cyber-attacks rendering vital systems completely inoperable. This would inevitably increase the Australian Signals Directorate's (ASD) involvement as the incident coordinator but would lead to greater exchange of information with critical business operators to assist with the protection of their systems.

The impact of a strict prohibition of payment of ransoms and extortion demands by cyber criminals would most likely have a lesser impact on companies and insurers than on victims of cybercrimes. We have seen how businesses impacted by such scenarios in the past few years have systematically complied with Government recommendation to not pay, with minimised consequences on their line of business, excluding reputational damages.

g. 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?

Engineers Australia would recommend the Government to clarify its position to non-payment of ransoms by companies. The public needs to be clear on how no financial gain would come from attempting a cybercrime on Australian businesses.

However, we would advise against clarifying the circumstances in which this may constitute a breach of Australian law. Best to keep a simple and clear message and avoid potentially advertising the rare and exceptional circumstances where it would not constitute a breach of law, as explained above, to limit the promotion of cyber-attacks on critical services, which could be the only instance where payment could be advisable.

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

A multi-level collaboration with our regional neighbours would be highly recommended, not only between governmental agencies. Cooperation is essential on both standards and skills level. Building the necessary workforce to secure nations is a must for all countries and would be best done a in collaborative context. Skills development could be greatly encouraged using temporary working visas/permits to enable more employment in leading organisations as well as exchange programs of certified staff within APAC would bring faster development of these critical skills needed.

Therefore, a regional cyber defence/investigations treaty within APAC would lead the way to strengthening our regional cyber resilience and allow better, faster and pro-active response to cyber incidents within the region.

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

A major defence partnership like AUKUS seems to elevate an existing multilateral partnership from a cyber security perspective. Defence relies on exchange of information and skills development to build the necessary capabilities linked to the nuclear submarines deal, would offer a suitable platform to further enhance our cyber security capabilities too.

Any existing and future international bilateral and multilateral partnerships should be accompanied with the opportunity for Australia to strengthen its knowledge and skills development from a cyber security perspective. This should be mandated for all future partnerships and sought to the added to any existing ones systematically as it would reinforce cyber capabilities of all parties involved.

5. 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 needs to continue its presence and be active participants to all current and future forums. Involving peak bodies and industry representative would be a quick and easy way to strengthen its presence and better its contribution. Engineers Australia would welcome the opportunity to collaborate more closely with the Government to contribute to international standards-setting processes and advise the Government on how best to optimise international standards while minimising the regulatory burden on organisations. As the collective voice of the engineering profession, Engineers Australia can provide the technical expertise the Government needs in such settings.

Australia should also consider raising the following points:

1. **Provide free access to standards**: costs associated with accessing standards are significant, which can be a deterrent factor for business in their attempts to increase their cyber security protocols. These costs are also passed on to supplier organisations in other instances, creating significant additional financial burden and inefficiencies. Alleviating such costs would generate a greater level of collaboration within industry and help secure our nation.
2. **Including OT systems**: as mentioned previously, mandates should be made on compliance with standards like IEC 62443, IEC 61508 or IEC 61511 for all OT systems for Critical Infrastructure. Only IT systems are currently targeted, increasing the vulnerability of our OT systems.
3. **Creating a commercialised ISM version**: introducing an ISM framework compatible with a commercial setting could replace or be integrated into international standards. Cyber Security currently focusses predominantly on the victim end of the problem when ISM would allow a more perpetrator focused solution.

6. 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, particularly those holding large amounts of personal data, need to demonstrate their capability in protecting data and be held to a higher standard. The Australian Cyber Security Centre (ACSC) and the ASD have developed excellent guides, models and frameworks to help any departments and agency to implement robust cybersecurity strategies and protocols, like the Essential Eight Maturity to ISM mapping or Cyber Skills framework.

ISM framework implementation is mandatory for all Commonwealth departments and agencies yet to date, its implementation is haphazard. More transparency around which departments and agencies have implemented this, where they are in the process of implementing or have they yet to implement them, would provide not only an incentive for those which have not, but also assurance to the whole nation that they are leading by example and doing everything possible to secure and protect Australians' data.

More concerns are around departments and agencies handling large infrastructure contracts involving contractors/contracting organisations. Anecdotal reports have been made by Engineers Australia members on the lack of consistency seen in these cases and understanding by these contractors and contracting organisations of cyber security issues, often confusing standards with security. Similarly, frequent confusions have been observed around the application of information security management systems (ISMS) in contracts, which as a result has the tendency to misdirect efforts to address security.

Engineers Australia recommends the introduction of more transparent mechanism to assess and inform the public of the quality of cyber protections for all Commonwealth Government departments and agencies. We also recommend embedding a more consistent ISMS application for all contractors in all Commonwealth Government departments and agencies procurement policies.

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

Information sharing is the key to minimise cyber threats impact. The Cyber Threat Intelligence Sharing (CTIS) program introduced by the ACSC in late 2021 is an excellent platform to improve information sharing with industry and academia. More needs to be done by the Government to promote the program across industry to increase CTIS positive impact and information sharing.

The Government needs to also be mindful of the need for information sharing to occur at both non-technical and technical levels. We hear anecdotally from our members how some of the alerts provided by the ACSC can be challenging to understand due to an excessive use of jargon, making it harder for non-experts to make use of the information shared or deterring them from sharing theirs because of a lack of confidence in the relevance of their information. Shared information should need to have sufficient detail to be actionable but should refrain from using too many unreferenced acronyms.

The strategy should aim at supporting mechanism for making cyber threats and vulnerability management easy and transparent. Tracking the threat environment and managing system vulnerabilities requires the implementation and maintenance of complex technical controls which only a small part of the Australian workforce is capable of, adding up on cost and recruitment challenges.

One domain of focus for the Government should be on securing third-party software packages as it represents a widely common source of vulnerability for all. Operating systems (OS), browsers, MS Office and the like are usually insecure by configuration and present on all computers. Securing third-party packages is a challenging task for businesses and even more for households.

The Strategy should include the formation of a national service to define and secure third-party software configurations through greater level of information sharing and free optional configuration tools made publicly available, installable and maintainable as a secure option. The aim should be to provide to the wider community with an equivalent of the Essential Eight for everyone, helping the citizens and businesses with free solutions to secure their networks in an efficient and transparent manner without the financial burden.

8. 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?

Rapid exchange of fulsome information is vital. However, companies can be reluctant to share information in fear of any potential legal ramifications, impairing the flow of information shared significantly. An explicit obligation of confidentiality upon both ASD and ACSC would alleviate this too often seen stumbling block and significantly improve the amount of information shared.

Most of the recent breaches seen are not due to technology failure but are implementation failures. The perception of risking to be “punished for doing the right thing” by reporting to regulators is detrimental to improving the current safety parameters as vital information and incident report are not shared but kept secret in fear of potential prosecution, limiting the learning experience for all. Relieving the concern that these incident reports will be shared with regulators would encourage more organisations to share their real-world learnings with ASD and ACSC and in return allow further engagement and learnings from these cyber incidents.

9. 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 would improve the public understanding of the nature and scale of ransomware and extortion as a cybercrime type. However, we need to remain mindful of the relevance of that information and who it is shared with. The public is already being made aware of an always greater number of significant breaches by medias, incidents such as the Medibank Private, Optus or more recently Latitude. The need for more information on all cyber security incidents for the public would not necessarily be of the greatest relevance as it would result in greater level of mistrust in cyber security capabilities.

However, making a publicly accessible information platform and mandatory for all ransomware or extortion demands to be reported would be highly relevant for company directors, business leaders, policy makers and similar sub-groups. The key in this exercise would be to ensure the right audience is provided with this vital information to improve the current state of play, not inundate the wrong one and create fear and mistrust.

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

There are several best practice models for automated threat-blocking at scale. Some of these include:

- **Artificial intelligence and machine learning (AI/ML)**: This involves using algorithms and models to identify and block threats in real-time. AI/ML models can be trained on large datasets to improve accuracy and reduce false positives.
- **Behavioural analysis**: This involves analysing user behaviour to detect anomalies that may indicate a potential threat. Behavioural analysis can be used to detect insider threats, phishing attacks, and other types of attacks.
- **Cloud-based security**: This involves using security solutions that are hosted in the cloud, allowing for scalable threat detection and blocking. Cloud-based security solutions can be updated in real-time, providing protection against new and emerging threats.
- **Automated patching**: This involves using automation tools to apply security patches to systems and applications. Automated patching can reduce the risk of vulnerabilities being exploited by attackers.
- **Threat intelligence sharing**: This involves sharing threat intelligence information between organizations to help identify and block threats. By pooling resources and sharing information, organizations can improve their ability to detect and block threats.
- **Domain Name System (DNS) layer security**: Phones are a widely used channel for cyber criminals to perpetuate cybercrimes. SMS spams and caller ID spoofing are among the biggest source of cyber criminality. Using Domain Name System (DNS) layer security is one practice model available to stop malware earlier and prevent call-backs to attackers if any infected machines connect to a network. Secure DNS servers would block requests coming from these staging sites over any port or protocol, preventing both infiltration and exfiltration attempts.

Overall, Engineers Australia recommends the Government adopt a combination of these approaches in a comprehensive security strategy.

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

A rethink of the current cyber skills approach in Australia is needed. Focus should be put on developing a quality framework, reassessing the currently provided IT trainings and certification programs to ensure they are up to the current standards. An uplift in cyber skills is required across all sectors, may it be IT, engineers, technologists and users to help them better understand cyber risks.

Cybersecurity skills are in high demand, and the nature of the cybersecurity industry requires specialised skills and knowledge beyond the broader STEM fields. Promoting cybersecurity as a career path may require changes in the way that cybersecurity is perceived and presented to students and job seekers. This may involve promoting the diversity and inclusivity of the cybersecurity industry, highlighting the important role that cybersecurity plays in protecting businesses and individuals from harm, and showcasing the various career paths available within the field.

Engineers Australia recommend the Government champion cyber security apprenticeships as well as encouraging the greater adoption of OT cyber specific programs. More sufficient rigour needs to also be applied to the design, procurement and maintenance of digital systems at the same time to produce a significant uplifting of Australia's cyber security as a whole.

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

With the growth of the use of digital technologies across all sectors of the economy, engineering disciplines and practices that support cyber security is increasing in importance. Cyber security is now impacting all professions as all businesses, academia and governments are making use of software technologies. Therefore, it is of high importance to ensure that academia integrate more cyber security literacy for all professions. The Government needs to collaborate further with all academia and course providers to add cyber security literacy in all degrees.

Government should work with professional associations, such as Engineers Australia, to explore and articulate the relevant competencies and cyber engineering skills required for the cyber security profession so that 'fit for purpose' programs can be delivered. Cyber engineering skills are a key component within the cyber security industry. Engineers Australia is currently developing a new area of practice in cyber engineering for engineers to gain Chartered credential, to provide a framework for engineers to better understand, develop and gain the appropriate recognition for their skills in that emerging industry. An area of practice in cyber engineering would also allow for regulators to potentially introduce the registration of all cyber engineers. Engineers Australia would welcome the opportunity to collaborate further with the Government on the need and requirements for such scheme to be introduced.

Furthermore, domestic skills supply will not suffice to close the skill gap and immigration is key to helping reduce it. The Government needs to provide the necessary means to support these programs. This could also include fast-tracking visa applications for highly skilled workers, as well as offering incentives for cyber security professionals to relocate to Australia.

13. How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians?

The Government needs to respond to major cyber incidents beyond existing law enforcement and operational responses to protect Australians. Communication around major cyber incidents should be clear and consistent to avoid repercussions seen recently during the Optus breach and the replacement of driver licence in many states. However, Engineers Australia recommends that communication to be left to the Government's relevant departments and agencies rather than its cabinet to ensure clarity and consistency to build on public trust in Australia's public service therefore should be depoliticised.

a. Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?

A single reporting portal for all cyber incidents would be greatly beneficial to simplify and reduce the financial burden. However, any such portal would need to be designed with privacy and security considerations in mind to ensure that sensitive information is protected as well as fear of potential reporting legal ramification does not become a deterrent to reporting.

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

Engineers Australia recommends reporting to be scaled in detail based on the estimated impact the cyber incident has had to be effective, similarly to what is currently done in other industries for safety. Smaller impact cyber incidents that a majority of small and medium enterprises (SMEs) are the victim of should not require the same amount of details than larger impact cyber incidents targeting larger organisations would need. For small impact cyber incidents, a simple triage of basic details should suffice to satisfy learnings. For larger impact cyber incidents, more data should be mandated to be reported to better assess vulnerabilities and methods used to provide greater levels of understanding and opportunities to learn from them.

An effective post-incident review and consequence management model with industry in Australia should involve a collaborative effort between the government, industry stakeholders, and other relevant parties. The model should aim to identify the root cause of the incident, assess the impact of the incident, and develop appropriate mitigation measures to prevent future incidents.

The model should include a formal process for reporting incidents to the appropriate authorities, and for sharing information and expertise between the government and industry stakeholders. This would enable a more comprehensive understanding of the incident, including the techniques and tactics used by the attackers, and the vulnerabilities that were exploited.

The post-incident review process should also involve a comprehensive evaluation of the incident response plan, including an assessment of its effectiveness and identification of any gaps or weaknesses. The review should also consider the adequacy of the organization's cybersecurity policies and procedures, as well as any training or awareness programs.

Consequence management is an essential component of an effective post-incident review model. This involves taking appropriate action to mitigate the impact of the incident and prevent it from happening again. This could include implementing new cybersecurity measures, such as stronger access controls or increased monitoring, and taking disciplinary action against employees who failed to follow established security policies and procedures.

15. How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime?

Government and industry can work together to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime in several ways, including:

- **Public awareness campaigns**: to educate individuals and businesses about cyber threats and how to protect themselves.
- **Training and education**: to help individuals and businesses develop the skills and knowledge needed to protect against cyber threats.
- **Collaboration and information sharing**: to establish forums for collaboration and information sharing on cyber security issues with industry and academia.
- **Victim support**: to provide support and assistance to victims of cybercrime, including financial assistance, counselling, and other resources to help them recover from the attack.
- **Regulatory frameworks**: The Government can establish regulatory frameworks that require businesses to implement certain cyber security measures and report cyber incidents.
- **Cyber insurance**: to promote the use of cyber insurance to help businesses manage the financial risks associated with cyber incidents.

- **Research and development:** to invest in research and development of new technologies and strategies for combating cyber threats.

Improving cyber security best practice knowledge and behaviours and supporting victims of cybercrime will require a collaborative effort between the government and industry, as well as a long-term commitment to education, training, and research.

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 effectively manage their cyber security risks, making them more vulnerable targets for cyber-attacks than larger organisations. The Government can provide various forms of assistance to help small businesses manage their cyber security risks and protect their data, including:

- **Education and awareness**: to raise their understanding of cyber risks and how to mitigate them.
- **Funding and grants**: to support small businesses in implementing cyber security measures such as installing firewalls, encryption, and other security software.
- **Cyber security advice and guidance**: to provide small businesses with access to cyber security experts and guidance on best practices for managing cyber risks.
- **Cyber insurance**: to promote cyber insurance for small businesses to provide financial protection in the event of a cyber-attack.
- **Reporting and sharing information**: to establish a single reporting portal for all cyber incidents that harmonizes existing requirements to report separately to multiple regulators. This will allow small businesses to report cyber incidents to a central authority and receive support and guidance in response.
- **Regulation and compliance**: to ensure that small businesses are aware of their regulatory obligations regarding data protection and privacy while providing guidance on how to comply with regulations.
- **Collaboration and information sharing**: to encourage collaboration and information sharing between small businesses and government agencies and promote the sharing of information on cyber threats and best practices.

Engineers Australia would recommend the introduction of a data verification management system. Small businesses are the most vulnerable and sensitive data needs to be better secured. Under such system, once customer information has been verified, storage of such sensitive information would be replaced by a code, rendering any potential breach of no value and risk.

16. 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. In addition to the recommendations made in previous questions, some of these include:

- **Professional certifications**: to act as an enabler for the industry for the required upskilling. Leveraging from existing professional certifications (Chartered or engineering oversight practices in the Australian Defence Force) would allow greater focus on cyber engineering quality as essential part required in controls for cyber security.

- **Securing by design**: to prevent cyber threats at procurement level using existing methods such as Secure Development Lifecycle (SDL) and Software Bill of Materials (SBOM).
- **Providing incentives for businesses to adopt cyber security measures**: to provide incentives, such as tax breaks or grants, to businesses that adopt cyber security measures. SMEs are particularly vulnerable to cyber threats but have limited resources to implement cyber security solutions. Such incentive scheme would help early adoption and give SMEs the appropriate tools to secure their networks and data.

The Government has a vital role to play in enhancing Australia's cyber security technologies ecosystem and promote the uptake of cyber security services and technology. Long-term commitment to support and promote education, research and innovation are key to help create a robust and resilient cyber security ecosystem in the country.

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

Future proofing cyber security technologies is a challenging task as equipment lifecycles are short and technologies ever changing. However, the Government could take a few initiatives to help consumers to better understand the quality and resilience of cyber security technologies. These could include:

- **Create a cyber security star rating for internet of things (IoT) devices**: the simplest way to raise public awareness and future proof cyber security technologies. Star ratings are a commonly used methodology to educate and reassure users on the quality of devices/products used. Standards are adaptable and re-adjustable to new technologies being introduced, offering a simple, agile yet powerful way to future proof technology out to 2030 and beyond.
- **Establishing new standards and regulations**: supporting the cyber security star rating for IoT devices, the Government can ensure cyber security technologies meet specific requirements and are proven to protect effectively against cyber threats through testing, evaluation and other quality control measures.
- **Mandating secure wireless networks**: Internet service providers (ISP) could be mandated to configure their wireless access points to have a minimum of two virtual local area networks (VLAN), trusted and untrusted, to better isolate potential threats and have consumer IoT devices connected to the untrusted network. Vulnerabilities are often exploited from consumer IoT devices connecting onto trusted networks, opening the door to sensitive areas and potentially giving access to sensitive data.

A comprehensive and effective future proofing approach will require constant ongoing monitoring and evaluation to sustain the rapidly changing cyber security landscape.

18. 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?

Making use of the Government's purchasing power using procurement policies is the quickest way to implement change to support and encourage growth of the Australian cyber security ecosystem. Mandating a "Product and Application Security" requirement for all government tenders and making it a weighting for procurement decisions would automatically result in an uptake by the industry on cyber security importance.

To create a viable path to market for Australian cyber security firms, the Government ought to implement locally made procurement requirements. This would not only boost Australia's sovereign cyber security capabilities but also incentivise international cyber security firms to setup local capabilities, generating new jobs, boosting the economy and tax revenues.

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

Proactivity is key to establishing a robust and resilient safety measures to secure Australia from emerging technologies in an ever-changing cyber landscape. The desire to adopt emerging technologies early should never outweigh caution or the risk of technical debt and longer-term vulnerabilities will be increased. The Strategy needs to shift the thinking around security, too often considered as a "non-functional requirement", but rather set it at its heart as it underpins the sustainability of any technology longer-term.

The Strategy should focus on acting from the source as opposed to reacting at the end. In a similar way, ISPs could play a larger role in securing domestic homes and small business networks. The Strategy could also focus on the following:

- **Collaborate and engage with industry and academia**: to ensure the development of secure and resilient technologies from the outset. This could involve partnerships with universities, research organizations, and industry to establish best practices for security by design, such as incorporating cyber threat modelling and security testing early in the development process.
- **Agile and proactive**: to keep pace with emerging technologies and adapt the strategy proactively to adapt to new cyber threats. Continuous monitoring of emerging technologies and threats is required, as well as the incorporation of new approaches and solutions into the strategy when necessary. It also involves staying up to date with international standards and best practices to ensure that Australian businesses and organizations are competitive and secure.
- **Innovate**: through initiatives such as start-up accelerators, research and development grants, and tax incentives. This would help support the growth of Australian cyber security firms and create a thriving ecosystem of companies focused on developing innovative, secure technologies.
- **Protect**: to ensure emerging technologies are subject to appropriate regulatory oversight, to address cyber security risks and prevent malicious actors from exploiting vulnerabilities. This could involve developing new regulations and standards specific to emerging technologies, such as artificial intelligence, internet of things, and blockchain.
- **Ongoing education and training**: to raise awareness of emerging cyber security risks and best practices. This would include working with schools and universities to provide cyber security education, as well as developing training programs for businesses and organizations to help them stay abreast of emerging threats and technologies.

Using a holistic approach to address the cyber security of emerging technologies is key to success. Security by design should be a mandated requirement in all new technologies as essential to ensure the safety and sustainability of a robust and resilient Australian cyber security ecosystem.

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

Measuring the impact of efforts to uplift national cyber resilience is crucial to ensure that the strategies implemented are effective and efficient. The Government could measure its impact by:

- **Establish clear goals and objectives**: to enable effective measurement of success.
- **Conduct regular assessments**: of the state of the nation's cyber resilience, using metrics such as the number of cyber-attacks and their severity, the number of vulnerabilities identified and addressed, and the level of cyber awareness and education in the population.

- **Collaborate with industry**: to establish realistic benchmarking metrics for cyber resilience and share best practices for measuring and improving it.
- **Incorporate feedback**: from stakeholders, including businesses and individuals, to ensure that its efforts to uplift national cyber resilience are aligned with their needs and expectations.
- **Regular reporting**: on progress towards its cyber resilience goals and objectives, including the effectiveness of initiatives and any areas for improvement.
- **International collaboration**: to benchmark its efforts and learn from best practices in other regions.

A multi-faceted approach incorporating the above measures would help the Government in effectively measuring and improving its impact in uplifting national cyber resilience.

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

There are several evaluation measures that could support ongoing public transparency and input regarding the implementation of the Government's Strategy in cyber security:

- **Metrics and Key Performance Indicators (KPIs)**: to track the progress of the strategy's implementation. This could include measuring the number of cyber incidents reported and resolved, the number of organizations that have implemented recommended cybersecurity measures, the percentage of the population with cybersecurity awareness training, and the number of cybersecurity-related jobs created.
- **Stakeholder feedback**: to gather feedback on the effectiveness of the strategy and allow adjustments on a per need basis.
- **Independent reviews**: to provide an objective assessment of the Strategy effectiveness. These reviews should be conducted by third-party experts in cybersecurity, public policy, and related fields to ensure consistency and reliability.
- **Public reporting**: to report on the progress of the strategy's implementation. Made publicly available, this would allow the public to track the Government's progress and provide feedback on its effectiveness.
- **Transparency and accountability**: to ensure that its implementation of the Strategy is transparent and accountable to the public. This could include regular updates to the public on its progress, transparency in decision-making, and mechanisms for public input and feedback.

By adopting these evaluation measures, the Government could ensure ongoing public transparency and input regarding the implementation of its cybersecurity strategy.

ENGINEERS
AUSTRALIA