2023-2030 Australian Cyber Security Strategy Discussion Paper Submission

By Michael Plis - Cyberkite - Updated 14/04/2023 at 8:38 PM (version 2)

Government discussion paper related to this submission:

- **Title:** 2023-2030 Australian Cyber Security Strategy Discussion Paper
- **Link:** https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/2023-2030-australian-cyber-security-strategy-discussion-paper

The Government is developing cyber security policy and initiatives under four key areas:

- A **secure economy** and thriving **cyber ecosystem**
- A secure and resilient **critical infrastructure** and **government sector**
- A sovereign and assured **capability to counter cyber threats**
- **Australia** as a trusted and influential **global cyber leader**, working in partnership with our neighbours to lift cyber security and build a cyber resilient region

Contents

About Michael

- **Michael Plis** is an IT Professional based in Australia. With over 18 years of experience in the fields of Information Technology and Cybersecurity for small businesses. He has also worked in IT service delivery in automotive and non profit sector at medium scale business. Although most of his experience is in small business cyber security, the principles that he has gained and the experience he has gained translate "in principle" into medium and large size businesses and government organisations.

- Michael is also the founder of Cyberkite, a small Cybersecurity and Information Technology services business in Australia.

- Michael shares unique insights into the benefits and potential risks of technology from a neurodiverse perspective.

- This submission is not exhaustive so the combined Cybersecurity knowledge and ideas from Australians will be needed to protect Australia. This submission provides ideas outside the square to help enhance Australia's Cybersecurity.

- **Visit, learn more and follow Michael if you like, via his LinkedIn profile here: linkedin.com/in/michaelplis**

Disclaimers

- Due to his neurodiversity Michaels comments and answers on this submission may be a bit over verbose or under verbose or may not make sense to some readers.
- Michael has also used the assistance of ChatGPT generative Ai service to help him improve the grammar, spelling & meaning of his submission.
- He has also spoken with other business people to refine those ideas.
- He's also using voice typing because keyboard input is more difficult so there may be some grammar or spelling mistakes in the submission.
- With his neurodiverse mind on the topic of information technology and cybersecurity he has a high functioning mind. But on subjects such as interaction or interpretation or communication or human subjects, he has difficulty so he hopes the submission will be understandable enough to be useful in forming the Australian cyber security strategy.
- He is also at times using technical speech in this submission so it may be difficult to understand by non-technical people. He tries to be very general wherever possible.
- Please also note that the opinions expressed by Michael in this submission are his own and may not necessarily reflect the views of Cyberkite. He shares his opinions based on his extensive experience in the IT and Cybersecurity industry, learning from the world's top subject matter experts and passing on this knowledge to his audience in the hopes of benefiting them.
- The information in this submission is for information purposes only. Miuchael Plis and Cyberkite is not liable for any damages as a result of following the advice or information in the submission.

Introductory comments

My name is **Michael Plis**, I have been in the IT industry in Australia for over 18 years in the fields of information technology and cyber security for small businesses. I have also worked in service delivery in the automotive and non-profit sector at medium scale business.

The lessons and principles I've learned during that time lend themselves to provide useful feedback on developing a national strategy for cybersecurity. There are many points of view and some of the points of view that I have built up over time are reflected in my submission but may have other angles that I have not covered or thought of.

There also may be some ideas and feedback that some cybersecurity professionals or business professionals or others may not agree or be happy with, so to those, I'll only say one thing: This is a strategy ideas gathering document. It's all about brainstorming. My ideas will be worthless and some ideas will be useful. Other professionals may have better ideas and approaches. But that's what it’s all about, consulting with many subject matter experts and strategists to find the best ideas to protect Australia. In the Bible in Proverbs 11:14 it sums up the principle of the benefit of more counsellors or subject matter experts well: “**Where no counsel is, the people fall: but in the multitude of counsellors there is safety**.” (*King James version*)

Cybersecurity, previously referred to as Information Technology, remains a part of IT, but has evolved into a distinct sub-branch. It is closely related to physical security and the overall security & defence industry, but focuses specifically on safeguarding data, systems, and individuals in cyberspace. While security measures can never be perfect and completely prevent cyber attacks, a holistic approach to cybersecurity can significantly enhance protection for the Australian nation.

I will provide some introductory comments below on a number of areas and then go into the submission discussion points in Attachment A. Then I will provide concluding comments. The submission is not exhaustive so I haven't covered every angle and every side of the issues discussed including the whole of cybersecurity in Australia. I think it's humanly impossible to cover everything by one person so all the submissions that are submitted for the 2023-2030 Australian cybersecurity strategy discussion will be required and careful planning by cybersecurity scientists, engineers, professionals, government and policy developers, hand feedback from the public and businesses concerned as well as feedback from all government departments.

In this submission I will try to go into the fabric of Australian life and propose some out-of-the-box and sometimes perhaps strange and outlandish ideas that may most likely help enhance the cyber security of the whole Australian nation.

In my opinion, all of Australia needs to be consulted together with the best options so there's full public support for changes in the coming 7 years. Government also needs to listen to feedback because we do not want to create an authoritarian state in the digital space, so it's good to listen and implement the feedback that is practical and sound in increasing the Cybersecurity of the nation.

Why has cybersecurity become so important in the last 15 years and what will the future hold?

Information technology systems have become increasingly powerful and accessible to everyday people. This enables people to use technology for good or bad, making cybersecurity essential given the increasing power of the desktop computer and mobile devices and access to cloud computing.

What was considered secure in the past? For example, an 8-character password is no longer considered long enough. Nowadays, a minimum of 12 to 14 characters is recommended. Why? An 8-character password can be cracked within minutes with the current power of computers, particularly in a server farm or cloud environment. With many systems working together, an 8-character password can be easily hacked, which was almost impossible 20 years ago. Even as early as 2013, an 8-character password was no longer enough to protect an account.

The rapid development of artificial intelligence, quantum computing and other technology advancements will mean the following in the coming 7 years till 2030:

- **Development of AI-powered malicious security hackers that are not human,** but programmed by people and replicated multiple times to work together as solo agents, hidden within systems, or distributed server farms. These hackers will be able to intelligently attack and alter code themselves on the fly and they get stronger as they learn. In the past they were called self-altering computer viruses. Ai-powered malicious programs will use a higher form of learning as if they are a malicious security hacker programmed to search & destroy or search and steal or some other purpose. Governments and cybersecurity software providers need to develop equivalent systems to match the capabilities of these hackers. While government-sponsored human offensive teams are still the primary means of cyber defence and cyber offensive actions, there is also a need to design AI-based self-learning and self-controlled cyber attack automated systems that are automated and self-learning but will be overseen by human offensive teams in the government cyber security department: ACSC.

- **The development of quantum computers is accelerating,** and it could be considered a quantum computer arms race. Why? Because quantum computing has the potential to decrypt any standard decryption method known today. Whoever achieves quantum computing usability first will have the opportunity to design quantum encryption to create much stronger encryption in the future, which will protect customers or citizens. Alternatively, they could develop decryption tools to decrypt traditional encryption, which could be used maliciously by security hackers or nations intending to launch cyber attacks on the poor businesses or citizens of other nations.

- **Computing power will continue to increase,** and new technologies, such as light computing, where the entire computer or parts of it are built to run similarly to fibre optic cabling or circuitry, will be developed. This will significantly increase the computing power available on every computer or server. Even smart devices will have light-based circuitry, as it is less prone to interference and more efficient in terms of power usage. This will mean further enhancement of the capabilities that malicious security hackers will have at their fingertips.

- **Network speeds will continue to increase,** and the entire nation will convert to fibre optic, 5G, and high-speed satellite services. From a cybersecurity standpoint, this means that malicious security hackers will be able to copy large amounts of data in a very short period of time. Attacks on services and computers will also happen more quickly due to the speed of the network. The faster the network speed, the faster the attack will take place. There will be a need for AI-based defences and quantum computing to protect and defend IT systems, especially in critical infrastructure assets.

- **According to analysts, the world will continue to become more and more politically and ideologically divided.** This will further increase the risks in the cybersecurity space, both in terms of their severity and quantity.

- **Unemployment resulting from the development of generative AI and self-learning general-purpose robots will lead to more people losing their jobs** and experiencing financial difficulties. This, in turn, increases the risk of them resorting to malicious security hacking to make ends meet or earn extra income by joining hacker communities. Laws to protect human jobs and define AI laws are important to manage cybersecurity in the long run. Otherwise, the situation will further destabilise the world and Australia. The discussion in all countries should revolve around basic human income when a person goes out of a job and is unable to find one due to the volume of unemployment caused by AI.

- **Natural disasters** will keep increasing due to the scientifically accepted data about climate change thus destabilising businesses and governments infrastructure running the risk of vulnerabilities.

- **Conflicts** will further increase and destabilise the cybersecurity of governments and businesses.

Bragging or accusatory tone & cybersecurity in government

This is unbiased feedback not specifically pointing fingers at any party or politician. It simply shows examples of what to do and not what to do.

On the subject of making accusatory statements on calling war against hackers or "bragging rights" of un-hackability statements there are a number of precautions and suggestions. I personally think this rule should be considered cyber security communication: *No government official, politician or government worker should engage in accusatory or bragging rights statements publicly.*

Why Is bragging rights and accusatory public comments not a good idea?

a) The example is the 2016 census run by the Australian Bureau of Statistics (ABS) where the then Australian federal minister for small business Michael McCormack advised the public quoting "***Whilst there has been breaches ... there's never been a breach of the actual Census data,***" McCormack told reporters at the time. He went on to say "***Never been a breach, the ABS assures us that this won't happen into the future with this Census, and governments of all persuasion take that information and assurances on board***." And he further advised "***The ABS has never had a privacy breach with Census data showing, and they have assured me as the minister responsible, they've assured the government, that they have every protocol in***

place, every process in place to ensure that there isn't a breach this time." (**reference** ZDNet Article on 3 Aug 2016 by Chris Dickett: https://www.zdnet.com/article/abs-tells-australian-governament-there-will-be-no-census-data-breaches-in-future/). In 2016 not long after those statements were made, the Australian Bureau of Statistics (ABS) was hacked approx on Tuesday 3 April 2016 through a denial of service attack and inconsistencies in its IT infrastructure. IBM and Census decided to disable access to the census to address the cyber attack. No data appears to have been stolen.

b) We can draw lessons out of this that malicious hacking is **not just a seeking of theft of money or valuable data, but it can also be a bragging rights thing for malicious hackers**: "Hey, they just claimed that their systems are unhackable, hey, let's hack it just to prove it isn't". Or "they just accused all hackers of being scum, let's teach them a lesson". Ultimately, everyone involved on the bad side of hacking and the good protection side against hacking are human beings. Human beings have feelings. Antagonising or making false statements of un-hackability is simply inviting unnecessary attention and focus for a possible attack. It is similar in the physical battlefield, you respect the enemy and you do not antagonise them.

c) **It's not a judgement against anyone or previous politicians statements, but simply the fact of the matter of the human condition.** Humans do not like to be accused, and humans do not like others bragging. It is very difficult for politicians to resist the bragging rights or emotionally charged accusatory statements to resonate with the voters. Saying things like "we've got the unhackable systems' ' or "we going to destroy you scum" simply aggravates the situation and creates increased possibility of cyber attacks against Australia and its systems both in government and private sector and everyday citizens. So my recommendation is no government official or politician should brag on things like "our systems are unhackable" or accuse like "we will destroy you hacker scum". Defence starts with respect to all. Demoralising the enemy through action rather than words is better and then reporting on the results in a non-confrontational but authoritative manner. Examples of that is how military generals in the United States Army speak. They dare not antagonise the enemy unless they have the weapons to make it happen or the defences to defend. And they use it sparingly.

d) **I would suggest always avoiding such statements publicly as it'll increase the threats to Australia.** For example, many of the cyber hacking groups may consist of people that were forced into servitude without their consent. That's been documented cases of that so they don't even want to be there and they're being forced under threat of their lives. And then a government accuses them of being scum or a government claims that their systems are unhackable. What will the malicious hackers do?

e) **The other matter is the fact that no IT system is completely unhackable**. And some will take it as a challenge to prove that point. The best thing everyone can do is improve protections and work on producing the chances of attacks.

f) **Also very important to use correct language when referring to hackers. Which ones?** There are valid hackers in the research community and in commercial companies in testing the defences of their clients. They provide a vital service to test the products and services that defend us and for scientific research in discovering new scientific discoveries. For example, biohacking a biological system to understand it. So when referring publicly to hackers that have hacked an IT system maliciously they should be called "malicious security hackers". Security hackers are not necessarily the bad guys, It could be genuine white hat hackers who are providing a service to companies, clients and the community to help protect them. But "malicious security hackers" are the ones that can cause damage or loss to the user(s). Also there are a number of colours of "hats" of the roles that security hackers take on, some good and some bad eg. white hat hackers help defend and black hat hackers have malicious intent. (Reference: Security hacker page on Wikipedia: https://en.m.wikipedia.org/wiki/Security_hacker)

g) **Managing media commentary is also important** to maintain the right information in the right quantity. Transparency but also cautious language should be used before event based government activities such as the ABS or new system being launched. Also, following an attack, the right language needs to be used and if the popular media uses incorrect details that should be corrected by the government in public statements. In ACSC 2016 Cyber Threat Report on page 5 under "**Scope of malicious cyber activity – a high level overview**" the report states "***If a nation says it has been subjected to an 'attack', this is weighted with tremendous significance. As such, the Australian Government's definition of cyber attack can be at odds with what the information security community, the public and the media envisage cyber attacks to be. A recent example is the disruption to the Australian Bureau of Statistics (ABS) 2016 online Census. On 9 August 2016, as a precaution to ensure the security of census data already submitted, the ABS and its service provider IBM temporarily disabled access to the Census website after experiencing multiple DDoS incidents. However, this incident was initially described in some media reporting as being the result of a "foreign cyber attack" – a description that led to a heightened sense of threat and risk, increased concerns from the public about the security of their personal information, and triggered media speculation about nation state motivations, tradecraft, and the possibility of further 'attacks'***." In my commentary about this commentary from the 2016 report, I would say it's best to be transparent with the people of Australia following a cyber attack so that citizens can take proper actions as quickly as possible to secure their data to the level they see fit. Some citizens may feel like their personal privacy has been severely breached and need to take greater actions than others and that must be respected. The comments above try to water down that public perception in my opinion. Although personal data was not stolen in the census, the perception that was created that this system was unhackable beforehand and then it was breached and went down, it created the perception among the public that it wasn't secure and the data was not secure. So it's all about controlling what information you say and what statements are claimed as to its hackability or not at least in part. In my opinion, this cyber security report was influenced by politicians to some degree to water down the severity of that 2016 ABS attack. That is also not a good idea in my opinion. Let's cyber security professionals make an assessment without any influence to water down the report by political parties or politicians or government officials. Attack reports and thread reports should be unbiased and bring out all sides of the issues rather than playing things down. Public perception is as important as the defences themselves in Cybersecurity especially for governments because in the end they serve the people. Malicious security hackers love public perception of negativity towards the government or system and they may act on it so transparency and honesty from the government is the best in a controlled manner to enhance security government systems. Before an attack, no statements of un-hackability or negative statements towards malicious hackers should be made. Following an attack accurate and limited but necessary information should be provided to those affected directly through the communication channels such as an email address, letter poor phone call or if it's a public thing then the public should be informed republic channels such as television or website and support should be provided even if It appears as if it's not necessary. Levels of severity are viewed by the public differently depending on how they feel about privacy And that should be respected.

In no way do I mean to disrespect anyone in positions of government or politicians or malicious hackers in my submission. I keep a neutral and technical point of view on all of this. I'm just purely providing technical feedback and examples on what to avoid in terms of what type of communication should be done before and after an event to improve security in Australia. Of course this will not completely remove the need for protections, but it helps to address one little aspect that is important: government communication before and after events or releases of systems.

Appropriate training and instruction should be provided to all departments and politicians on that aspect of cyber protection which is communication before and after an attack to minimise its severity. Playing down a cyber attack in public after it has happened is not a good idea because some citizens have a more sensitive point of view about the privacy of data than others and that must be respected.

Involving the government IT & Cybersecurity technical teams to work with communication teams in government to help formulate responses will be good to ensure as best cyber security is possible and as best as possible response to an attack.

Modern 7 cyber protection layer model

I believe a modern set of Cybersecurity defences or areas of consideration to protect any size organisation or business should be a combination of 7 cyber protection layers model that I have identified to cover most aspects of IT security.

I propose and use such a 7 layer model in my cybersecurity work. It’s in a way similar to the need for the 7-layer OSI model of computer networking which helps structure networking. Further work by Cybersecurity engineers and scientists is needed to create a simple Cybersecurity model for cyber security across all IT systems.

I believe to help all Australian citizens and companies and the wider world be aware of all the areas of this 7 layer model and more a standard universal model similar to the OSI model for IT networking is needed in Cybersecurity.

Here is my cyber protection planning and review model for small business, but in extension all size organisations below. It’s been useful in keeping at the back of my mind the possible deficiencies and areas of cyber security protections that need to be considered in modern IT protections for any organisation but to an appropriate degree.

Here is my 7 layer cyber protection model for planning:

1 **Human**	2 **Governance**	3 **Detection & Triage**	4 **Updating**	5 **Hardening**	6 **Recovery**	7 **Insure & Document**
Staff training & policies	Manage users, devices & data	Stop or catch the threats	Keep everything up to date	Strengthen defences	Restore after an attack	Last line of defence
Cyber security awareness training IT/Cyber security policies and procedures Others	Company user & devices accounts Password management User & device access control MDM/MAM Solutions Access control to data Other access control systems including physical security Others	Secure Firewalls (application and hardware) Antivirus/ Malware software EDR solutions Intrusion Detection Systems Honey pots Other	Latest software updates for applications and Operating Systems Latest hardware firmware updates on routers, switches etc. Other updating	Strategic configuration of software Site filtering (whitelist/black list sites) Improve firewalls Analyse all device, software and user account settings in detail to improve security Others	Backup recovery plans & procedures Full and incremental regular backups Multiple backup locations including different cloud backups Physical and cloud backups Third party backup (cloud or endpoint) Others	Cyber Liability Insurance Business liability and indemnity insurance Thorough risk & IT recovery documentation Others
***Comments**: The weakest link in Cybersecurity protections is usually humans and on rare occasion animals. This layer puts humans at the number one spot as part of cybersecurity protection of an organisation.*	***Comments**: This layer is all about managing users, devices and data. This layer helps to establish a set of gatekeeping measures to protect the most valuable parts of the organisation.*	***Comments**: This layer is all about stopping threats from getting into your organisation or if these threats or malicious entities enter your organisation that they are detected and eliminated.*	***Comments**: This is an important layer as well but it concerns itself with updating all applications, operating systems, hardware and other aspects to ensure all identified vulnerabilities are patched regularly.*	***Comments**: Review all settings in devices, software and network to strengthen defences of the organisation.*	***Comments**: This layer concerns itself with the recovery facilities and procedures after a cyber attack including having backups of all sorts to recover data and settings.*	***Comments**: This layer of protection is the last line of defence when all else fails. Insurance to help recover the business and the documentation to rebuild everything that can be rebuilt.*

Attachment A: Cyber Security Strategy Discussion Paper Questions

This attachment consolidates the questions for consultation in the 2023-2030 Australian Cyber Security Strategy Discussion Paper and includes further specific detail. I'm making a submission regarding the entire discussion paper (introductory and concluding comments) and full list of questions in Attachment A as per the discussion paper.

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?

I'm going to provide a number of points as ideas to include in the strategy below:

- **Cybersecurity communication coming from government departments and officials and politicians** should be subdued and specific and never make bragging statements or war on every hacker or cybercriminal. Communication strategy should be formulated so that the public isn't unnecessarily frightened if they don't need to be and also properly informed with full transparency. Careful and well orchestrated and timed communication and training advice to the public should be given not by politicians but primarily by subject matter experts working for the government eg: National Cybersecurity Coordinator role that is being planned. This will carry more weight similar to how an AFP Chief or a Police Chief or a Military General conducts a press conference. Politicians can speak and have their share and say things but the National Cybersecurity Coordinator should have the "main" mic time. Why? Because politicians will always be biassed and try to insert comments about how bad the previous government was etc etc. This simply switches off half the population in not wanting to listen to "political" bias messages. Politicians can speak as second speakers but same as in Covid-19 lockdowns the Chief Medical Officer was the main speaker same thing with National Cybersecurity Coordinator - they should not be aligned to any party and publically stay neutral. Also, the ACSC chief should have something to say, and under some circumstances if there's Cybersecurity offensive action needed, then the ASD chief should speak publicly as well. This will build trust in the cyber security, Australian department and ACSC and ASD.

    - **Additionally, I propose that a new Government department before and called National Cybersecurity Department**, under its oversight there should be the ACSC and the ASD. The department should work closely along with the AFP and state police departments as well as the military. The Home Affairs minister can also double as Cybersecurity Minister. This will create a better structure all the way to the top of government.

    - **Due to the fact that each state has its own jurisdictions, it might be advisable for each state to form their own cybersecurity centre similar to the ACSC** and the chiefs of those states centres should meet regularly with the national ACSC and the National Cybersecurity Department sub agencies. This approach of state and national equivalent bodies for work together on state, council and federal level.

    - **I also strongly think that the appointment of the National Cyber Security Coordinator should be someone, whatever gender, who has the best industry experience in cyber security for many year**s so that they can make good decisions and think on the fly as needed with proper and seasoned experience in cybersecurity craft. Favouritism in selecting someone in that position or simply making cyber security in Australia ineffective, cyber security decisions are always based on experience and knowledge and cyber security wisdom.

- **Cyber security education providers such as tafes and universities should have their curriculum reviewed by a panel in the education department and the ACSC to ensure that the right education is being provided to upcoming cyber security professionals** to ensure the best quality of graduates. They should review what is being taught and whether it is up to date with the current cyber security industry standards.

- **Surveillance or Mercenary or Commercial spyware is increasingly becoming a problem where state sponsored or commercial companies create spyware that uses new zero day vulnerabilities** and exploits them covertly in order to spy on targets. It needs to be very tightly controlled and regulated by western nations including Australia. So any companies developing this legally to sell to customers need to be controlled and have export controls in place to make sure it's only sold and used within the legal frameworks and not outside of that. There may be legitimate reasons why this type of spyware is used. But sometimes leaking of such tools can mean that it gets used by malicious security hackers to take advantage of its spreadability and potency. Laws and regulations around the creation of these types of spyware are needed. In some ways such zero day vulnerability exploitation tools can create mass vulnerabilities and infections very quickly. And it is hard to know whose phones have these spyware installed by surveillance and spy agencies from governments and malicious entities.

    - **Due to the potency and serious nature and spreadability of such type of spyware commercial companies that create such software need to be regulated and monitored and if they do not want to be regulated then they need to be banned from operating in Australia or at the very least, watched carefully.** If such a spyware tool falls into the wrong hands, it can be severely misused on a wider scale. And Apple products are not immune to this spyware because regularly zero day vulnerabilities are being discovered not just on Windows and Android devices but also on Apple devices now on a regular basis.

    - **What is mercenary or surveillance or Commercial spyware?**
        - Example is Pegasus developed by an Israeli firm: https://en.m.wikipedia.org/wiki/Pegasus_(spyware) -
        - Apple has taken on a serious stand against this type of software: https://www.apple.com/au/newsroom/2022/07/apple-expands-commitment-to-protect-users-from-mercenary-spyware/
        - EuroNews article describes it this way: "***Once installed in a device, spyware allows the invader to conduct real-time surveillance, find passwords and sensitive files, track locations and plant fabricated evidence. It is usually installed through a malicious app or website link and leaves very few traces for its detection.***" (Reference article: https://www.euronews.com/my-europe/2022/11/08/eu-democracy-is-under-attack-by-mercenary-spyware-claims-new-report)

    - Citizen Labs identifies details on the QuaDream's surveillance spyware "ENDOFDAYS" out in the wild (Reference article: https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/)

- **Foreign nationals of enemy nations that are at odds with the Australian way of living should be denied access to cyber security courses and training in tafes and universities and other education providers in the interest of national security**. In the end you don't want hackers that will fight against you in the future. I think every nation has that in place or should have that in place to protect its interests, whatever they are.

- **Every business, nonprofit and government organisation should be required to have an IT security policy in place and procedures along with it.** That's on top of a general IT policy that's already in place in most businesses and government departments. Especially medium to large businesses. These policies should be updated to ensure that they have relevant industry standard information. For example, many IT security policies require a minimum of eight character password, which is no longer sufficient to protect a user account. It's more like 12 to 14 characters now. Funding should be provided to provide legal writing assistance to small businesses, IT security policy template and IT policy template so that they can provide that to their staff.

- **Medium to large businesses and government departments should be required by law to have a cyber security awareness system in place such as from KnowB4, Webroot and many other cyber security providers**. These systems don't cost much and have the ability to make all staff aware of cyber security threats and attacks through email, phone, text and other means. Awareness training is one of the best cyber protection tools in any organisation.

- **Australian citizens should be given the option to sign up to a government service called "Australian Cyber Awareness Training" (ACAT) service funded and provided by the government for the citizen, and run under the myGov login system.** When a citizen signs up to this service that will get regular cyber awareness, training emails and text messages as well as phishing simulations. It will be an opt-in service. They will need to be made very clearly aware that they will receive fishing simulations without notice occasionally each month to help them become more cyber aware. Just like commercial cyber awareness training systems provide that to clients. The side by awareness training aspect should be provided in many common languages and English and it should be clearly worded with accompanying video explanations of the concepts. There are many people not part of companies that are affected such as the elderly and young people who are maybe not as aware of the cyber attacks as business people are part of companies with cyber awareness training software. These groups would greatly benefit from such a government service and it would be very easy to implement with off-the-shelf Cybersecurity awareness training apps but a solution that is selected that can be used at scale across the whole of Australia. That measure and service provided to the citizens would help increase the cyber awareness and cyber security experience of every citizen thus increasing their individual cyber security.

- **All government provided public WiFi services, wireless charging pads and USB charging ports need to be checked regularly for tampering and addition of additional malicious devices** designed to inject spyware or malware. This is an increasing problem in public areas. Also monitoring for rogue imitation WiFi services that may be turned on by malicious security hackers near genuine Public WiFi services. Once a device connects to a rogue WiFi network it can be an easier target for cyber attack.

- **Phone / Internet exchange buildings and NBN wiring boxes near each street need greater security and anti tamper protection as they could be places of cyberattack or manipulation**. This could be done by a malicious security hacker or a genuine NBN maintenance contractor That might have been compromised through a bribe by a malicious hacker to inject or install or plug in some software, etc. In phone or internet exchange buildings full CCDV 24/7 surveillance should be installed across Australia and anyone that accesses these buildings should trigger an alert in a centralised monitoring centre run by the ACSC or state based equivalent cybersecurity centre. It sounds over the top but if someone gains access to these buildings or the NBN exchange boxes, they can install plug-in all sorts of devices to start intercepting data and causing havoc. In principle, mobile transmission towers and their buildings next to them should also be secured in the same way. In cyberspace, the mobile towers should also be monitored from the cybersecurity end to make sure there's no rogue activity or any interception activity being conducted. Perhaps there are some devices that can monitor for raw signals or rogue activities and alert the ACSC or state based equivalent cybersecurity centre.

- **Kindergartens, primary schools and secondary colleges, types in universities in general should have a cyber security training module every 6 months to cover aspects of cyber security relevant to the audience and age group** to protect their privacy and cyber security. You want every level of the nation being aware and the education industry needs all students to have cyber security as part of the curriculum.

- **The elderly should receive every 6 months a 30 to 60 minute cyber security & cyber awareness training session at the home or residence**. Keep him up today in cyber security protections or they can be invited to a free service security awareness training session if they don't sign up to a cyber awareness training service by the government as mentioned in the previous bullet point. I assist a number of older ones to help them with securing their IT systems on their tablets and phones and computers. I also assist them in making them aware of what to click and what not to click on text messages when phone calls come in and through emails. Would those basic cyber hygiene aspects? All the ones can feel safer and more informed about the dangers. This should be made available to aged pensioners that cannot afford it themselves and are on the aged pension.

- **In cooperation with the CSIRO and the public sector, the Australian government could set up a Cyber Security Research Center nationally** to research new ways of protecting the nation such as artificial intelligence-based defence and offensive systems, enhanced cybersecurity technologies, which can then be sold to the public sector and new Australian cyber security companies can be formed that will provide those new tools to the world and to Australian public. That would also research enhancements to existing products, software and services across the public sector as well as the private sector organisations. They could also take on the job of offering bounty programs to enhance the protections of products and services from companies that do not have bounty programs whereby those companies would sign up for a fee to a joint Government funded bounty program pool that includes their products and services in that offering. Medium to large businesses and government departments should have a bounty program. If they cannot afford one then a nationally provided bounty program should be in place, perhaps through this research centre. Tiers of membership fees should be implemented so that this program is self-funded for the long term.

- **Cyber security stress testing (aka. Cyber war games)** should be implemented, conducted and mandatory on every medium and large businesses and nonprofit and all government departments annually or every 6 months across the physical security and cyber security. Because physical security also plays a part in cyber security. This would involve an ACSC stress testing team to be formed to go out in person or remotely and attempt to gain access and still government or company data then report back through official channels to those companies. old government departments and public sector companies medium to large would need to sign up to this program to be allowed to be stress tested and then receive a report and recommendations. This would go a long way in convincing some of the staunch opponents of cyber security on the benefits addressing cyber security concerns and dangers of not doing anything. Last year's ACSC threat report mentioned something like 50% of organisations don't think cyber security is important.

- **The ACSC should have a feedback team where they can receive feedback and ideas** from the public and from the cyber security community and white hat hackers on what things should be improved in different levels of government and departments as well as the public sector. The ACSC could then practically relay that information where it deems valid to the relevant private sector company or organisation or public sector government department. Proactivity and shed intelligence gathering across the community will be very good to increase cyber security in Australia. This should include cyber security anonymous whistleblower service to report cyber security vulnerabilities without the recourse of penalties or internal chastisement. There are some situations where when such reports are provided, there are consequences to the person reporting. Full cybersecurity whistleblower protections should be in place and if the feedback is serious enough about you should be provided to the whistle blower to incentivize reporting.

- **The traditional telephone system in Australia needs to be upgraded**. Add spam protection protocols to reduce spam colours through a verified system or enhancement of the caller ID system across the world. Currently, the caller ID can be spoofed or faked by spam colours from foreign countries and locally local phone numbers can be obtained very easily and faked. Knowing who's calling and being able to verify who's calling will be essential in the future to enhance the protections around telephone calls. ACMA, The telecommunication industry and governments need to come together to upgrade the telephone system. Call ID system and the whole phone system to have verifiable phone numbers. And Ben foreign use of local numbers even in marketing which is the common place where caller ID is spoofed where subsidiary or subcontractors provide sales and marketing services which are then abused by some to provide impersonation and spam calling..

- **Similar to the telephone system, the SMS system needs to be upgraded to RCS or something even better to enhance the protections around text messages** that are faked and spoofed and sent as if they are on behalf of the official governments or banks. Apple needs to be encouraged to join the consortium for RCS to be implemented so that SMS can be phased out and RCS implemented across the world. RCS has greater reporting and verification mechanisms, but further research into this space needs to be conducted.

- **The email service needs by law to be at a higher level of anti-spam protection in Australia**. Some companies neglect this or are unaware of the stronger protections. They can be turned on and the email systems are more vulnerable to misuse and attack. Many of the commercial email systems such as Google mail or Microsoft mail services already have anti-spam protection settings and protocols such as DMARC, SPF and DKIM. These three protocols should be mandatory on all Australian email servers for the general public and for companies and for government accounts to enhance the anti-spam protections and verifications in Australia. The general public email services provided by such companies as Apple, Microsoft and Google should by default have DMARC, SPF and DKIM - additionally, all other Australian based email service providers for the general public should also have those established. Any email services from foreign countries that have not established these three protocols should be sent straight to spam which will enhance the protections to Australian citizens from emails coming from foreign or local malicious sources. ACMA, government and IT industry needs to research further ways of enhancing email services to reduce spam and cyber attacks such as proactive antivirus, scanning within all email servers to prevent impersonation attacks. On that note, there are many domain name registrars offering webmail services and internet service providers such as Optus we're there with mail that is highly insecure and does not have some of these aspects in place. These services must be mandated to be shut down, be phased out or be replaced with webmail services that have DKIM, DMARC and SPF settings in place.

- **All social media platforms that provide services to the Australian public should be mandated not to reveal private information in public profiles unless the customer has expressly been able to review those details and allow them** to be visible. Those details are used in open source information gathering by malicious security hackers.

- **When government departments create publicly accessible databases about citizens or companies in Australia, they should first get permission from those companies or citizens before they post that data publically**. For example, recently the Start Up Victoria government department set up a startup database (https://launchvic.org/startup-database/) and made it publicly accessible to the world. Some of the data was scraped through publicly accessible but not easily visible information and it was added to the database. It also exposes the startup without the permission to unnecessary sales contact from foreign and local business development and other companies. That is okay and good if the owner of the startup once did that but they didn't seek permission for that and reveal that database with publicly scraped information which they confirmed to me. My company was publicly scraped, my contact and business data was combined and put into that startup database including an email address which I never revealed publicly, but I used internally to communicate with Startup Victoria. The ethical considerations of exposing some startups information without their permission, such as email addresses that aren't supposed to be revealed to the public Must be considered before starting any kind of databases with citizen or company information by going departments all by private companies wanting to offer a service. This particular example has possibly resulted in increased spam emails to startup businesses that those startups have to deal with now because of all that publicly scraped information combined together. These are consequences of not following due diligence in reviewing privacy and cyber security common sense measures. Government departments should know better and so do businesses.

- **Data scraping without the authorization permission of the person or organisation involved should be made illegal in Australia**. Open source information is becoming a big industry and a lot of companies are scraping for data for commercial purposes but also malicious security hackers are using open source information to scrape the internet for any data they can combine. Currently that practice is not illegal currently but it has potential dangers when data is combined. And even if it's gathered for benign purposes, what if the data is sensitive and becomes exposed one day? Another example of data combining after that is scraping is publicly accessible stolen databases from companies. When combined, bring more and more pieces of information about a company or a private citizen and can be used to hone in on additional systems that the entity is using. This includes for research purposes or for personal use or to threaten someone. For example, data scraping should be made legal only with the permission of the person that the data scraped about. That's the example of generative AI service called Stable Diffusion, they apparently scraped the data of a lot of places on the internet to extract photos and artist paintings to train them AI models. What if some of this data was exposed but was private? They then add it to their learning algorithms, then those learning algorithms then create results for the Stable Diffusion end user. Is there a chance of that data being sensitive from other people and becoming revealed through those results? Also the generative AI chat and text services that are coming out such as ChatGPT, where did they scrape the data from? And is the data private or exposed but private? Did they seek the permission of the people or sites where they sourced the data from? In the past in the research community that other has been permitted as fair use. But as recently seen the ChatGPT service became vulnerable and personal chat history was accessed. So the question needs to be raised is data scraping across the board - does it need to have laws set in place to make data scraping illegal unless it's been given express permission by the person or company about which the data has been scraped in case there is some sensitive data that is scraped that is exposed but it shouldn't be. For example, a while back, Google used vans to drive around the community and search for unprotected Wi-Fi networks and then downloaded large amounts of data on those networks that they didn't get permission from for the purposes of research. Then they were able to design Google Home Wi-Fi home routers. The question arises is scraping without permission for research is good or bad? I think it should be with permission because some of the data may be sensitive and the user may not be aware that it is exposed and then gets combined and becomes more potent. And then what if the research company gets hacked and that data is exposed to hackers? This can have serious consequences. So data scraping without permission should be made illegal even for research purposes. Transparency & permission from participants in research is the best policy. It may slow down research but maybe that's a good thing because then there's sufficient time for everyone to be okay with it and the person from which the data is scraped is fully aware that it is happening.

- **A new service type should be formed by commercial companies with government support to create data vaults or banks**. These data volts can offer highly secure data storage for sensitive information such as product designs, cryptocurrency keys, and other private information stored digitally in cyberspace. This should be low cost and accessible to everyone in Australia. The definition of a data vault or bank would also include any digital ID system that stores sensitive information about a person and then can be connected to other systems to provide verification.

- **Personal information such as driver's licence, passport, Medicare card, bank card, bank statements and other highly sensitive personal information should never be submitted to companies or governments**. Instead, this data/documents should be submitted into a digital ID verification system such as MyGov ID or a commercially supported system run by the commercial world in conjunction and regulated by the government, which requires a citizen to submit that sort of information and verify a 100 point ID check. MyGovID is run by the government but it should be a cooperation between businesses and government and it should be an independent organisation that's funded by companies and government to provide an ID system that is not influenced by or necessarily accessible by government or companies. It should also be stored in a distributed manner so that if one database is stolen it would contain encrypted information and you would need to combine that with several other locations to make sense of it and even then it would be encrypted. That sort of information should be submitted (For example, during a new client application process) into a secure digital ID system, it should then be able to be connected to verify any client application in any business and government department in Australia (For example, applying for unemployment or wanting to sign up for a bank account). This way no personal information of that nature would not be stored in any company or government department, but it's distributed insecure digital ID system at the highest security level just like a bank. This would reduce the likelihood of very sensitive government IDs being stored in company servers that are not sufficiently secure to hold such data and are often misconfigured. Basically outlaw the use of physical government ID copies to be stored in government department systems or companies. Instead have a referensible verified ID number connected to that physical driver's licence that can be verified and stored without keeping the actual copy as visual scans as a PDF which can then be copied and reused elsewhere. such data also should be started in multiple locations in a government ID system across distributed locations so if data is stolen from one database it is garbled and requires several locations that are combined to make any sense.

- **Additionally, the aspect of physical ID being stolen is a problem**. For example Driver's licences across each state should be digitised and kept in an app that's secure instead of carrying physical driver's licences that can be lost or stolen. It should be linked to that government digital ID system and can be shown in an app to someone. The physical driver's licences or passports should have digital aspects to it to be verifiable in the real world. When you go into a department or company, I need to verify that ID. This way the elderly and those not wanting to use digital IDs can use physical IDs more securely. Basically make the physical copy of a government ID so it's hard to plagiarise just like Australian banknotes. Currently, government IDs such as passports and Medicaid cards can be easily replicated and falsified. In other words, make physical government ID cards very hard to falsify and link them to the digital versions of them so that they can be kept securely in an app under strong security so that the citizen does not have to carry the physical copies which can be lost easier. If the coming ID is stored inside a secure app on the phone pin and additional fingerprint security. If the phone is lost it can't be easily accessed. But if you lose a physical driver's licence, for example, it can be used easily.

- **Cyber security insurance industry needs to be reviewed and regulated**. Government needs to ensure that cyber security insurance is available for companies and individuals. Cyber security insurance for companies is the last line of defence after an attack happens. Such insurance should be affordable and accessible to everyday citizens as well as small businesses. All the way to large business and government departments should all be cyber security insured. Why? Because of the possible reputational damage that can occur and the cost associated with rebuilding and repairing systems after a cyber attack or data theft. Government should work with cyber security insurance companies and regulate them so that the cover is reasonable and it does not escalate in price to be unaffordable. It should also regulate the industry so that cyber security insurance products are valid and genuine and are not fake. The insurance industry has been through a royal inquiry so this should be fairly easy to implement. Cyber security insurance should also be encouraged and perhaps even mandated or legislated as required to run a business.

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

My Answer:

- **New data scraping laws should be formulated** to outlaw doctor scraping without express permission in research, for commercial purposes, for personal use or to threaten someone? Any law enforcement.

- **Digital ID systems standards laws should be formulated** to define what a digital ID system needs in terms of its security and technical requirements in order to protect the sensitive information related to someone's digital ID. The whole framework of digital ID needs to be refined so that digital ID providers such as the government's MyGovID and other digital ID providers from the commercial sector or a development of this to a joint government and commercial sector solution would require a legal and regulatory framework and ensure the system maintains strong security and also provides a really great service of verifying a real person in cyberspace.

- **The receival, use, share and destruction of personal or sensitive documents -** That's also part of the privacy act laws regulating the taking off sensitive documents and information and starting that and then disseminating that should be defined. Enhanced cybersecurity legislation and regulation regarding storage, use, sharing and destruction of personal information and sensitive documents or any documents whatsoever in business and in personal life.

- **All government department levels of government including in council, state and federal need to follow privacy and cyber security regulations** not just by face value but actually implement and regularly review those laws and enforce them within their departments. Example is Launch Victoria startup organisation had privacy statement on their website but they data scraped supposedly legally data of startups such as email address, another details about the business without their permission (which I was a victim of as well without my permission) added them to a database that they didn't give consent to aka The Startup database - https://launchvic.org/startup-database/ That's privacy law versus the implantation of privacy law problem. These implementations have consequences in the physical world with people and companies and government departments. Proper responsibility needs to be allocated within departments for the protection of citizen data. Bending the rules to accomplish a purpose is not the right way.

- **Social media platforms that provide services to Australians should be required by law to ensure that private information such as birthday or address or location or any other property information is not automatically revealed** through complicated settings such as how Facebook social media application has done for many years. They are now improving that, but this needs to be set in law to make sure that no personal information is revealed to a public audience or even to friends without the person's permission and the option to switch that off first before publishing.

- **Regulations that need to be created around email servers hosted in Australia should be established to require all of them to have settings around SPF, DKIM and DMARC related protocols, at least for all businesses and email services provided by companies to**

citizens. And ban all webmail services that do not have those basic protections in place to reduce spam and verify the validity of an email address. This will address the insecure webmail services such as the ones provided by Optus and other service providers and domain registrars. It will either force them to upgrade those webmail services to include those settings or commission them and force them to offer more secure email services from the major providers such as Microsoft, Google and Apple.

- **Ban foreign students from foreign nations at odds with Australian way of life from learning anything related to cyber security and information technology including programming** so that they don't then go back to the country and become hackers for the nation state that is at odds with Australia, whoever they are. Being naive about this and allowing enemy states to learn these subjects in our schools will simply pass them the cybersecurity craft that students learn here to defend Australia. I might sound cruel or selective, but the better approach to preventing unnecessary knowledge transfer to the enemies. Also, all information technology and cybersecurity students should be police checked with a national police check or an international police check to make sure that they are not malicious security hackers learning more about malicious hacking.

- **Require the education departments in states and federal and the ACSC to regularly review the curriculums of tapes, universities, and other education institutions that teach cyber security** to ensure that they teach up to date information to ensure the cyber security workforce is probably educated for the current scenarios and requirements. Include legislation to fund this verification process on an annual basis.

- **We need laws to require all software, hardware, database and website service providers to set some basic security in place** such as two factor authentication and longer password length as a requirement to setting up a user account.

- **Bug bounty programs laws might be needed:**
  - Perhaps require all large companies and government departments and non-profits to have bug bounty programs so that vulnerabilities can be located easier by the cyber security community.
  - Perhaps also require medium sized businesses, medium and small sized government departments and medium sized non-profits to either provide a bug bounty program or be able to sign up to a government provided bug bounty program under a subscription based on the companies or organisations funding or profit level.

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)?
Regulatory guidance without enforceable legislation and regulation has no teeth so it should only be to advise. Legislation and regulation should be enforceable with criminal or legal consequences. Especially board of directors on medium to large size businesses who often cut costs in cyber security and IT systems to save on funds. Define the levels of cyber security that needs to be in place around client and company data in medium to large businesses and make it impossible so that board of directors are criminally liable for making decisions that are not based on industry practice at the time. The level of cyber security in medium to large organisations needs to be defined by an industry and government joint panel that is impartial and follows industry practice.

- Additionally, legislation needs to be tabled to outlaw overpricing of cyber security products in order to ensure that they are accessible to small, medium and large size organisations so that everyone can equally access the protections that they need.

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?
Yes, I really think so from my professional experience there's a set of industries that are not included in the "Security of Critical Infrastructure Act" that need to be added as part of the critical assets:

- Information technology managed service providers that provide party services to companies and act as their IT department and cyber security department. Often some MSPs have lax measures internally to protect client data and client access. There are recent examples of that.

- The software providers that provide software to IT managed service providers (MSPs) that provide remote management software and remote assistance software. They need to be part of the critical assets. There's examples of black cyber security in those companies. Therefore they had vulnerabilities and cyber attacks that affected many other businesses.

- The NBN and other internet technologies from internet service providers that provide internet services to citizens and to businesses, including when services and managed network services. Just like Optus and Telstra purely internet service providers, often sell phone services but also data services such as NBN services. Some service providers also provide non nbn related internet services such as wireless internet and satellite internet such as the low earth orbit Starlink. They also hold a little sensitive information and provide sensitive services to businesses that could be intercepted.

- The above are critical assets because they provide the infrastructure and all the IT systems in Australia.

- Additionally to that, any customer data stored by any organisation, company and government department becomes a critical asset to sectors of society and should also be covered in that regulation if practicable affordable to those smaller organisations.

- Critical assets are also for example large scale systems that offer valuable services to the everyday citizen and company such as Apple, Google and Microsoft services and apps including the two main office suites that are used by a lot of companies and individuals in Australia: Microsoft 365 and Google Workspace. Those need to be included as critical assets and must meet strict guidelines and be regularly reviewed.

- Also IT managed service providers and their contractors and the subcontractors of IT managed service providers, cyber security managed service providers and contractors of the cyber security companies all need to come under that Act. Because they deal with Australia's information technology infrastructure which is required to run the whole country. Australia cannot function without information systems so if they are not treated as critical assets of the nation then they will be more vulnerable to attack.

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

Yes wholeheartedly yes. Company directors cannot ignore the topic of cyber security risks and consequences. I need to and should be required to set minimum measures in place and protections in place in their companies to protect client data and company data and systems from attack and from infection. These decisions should be made with the consultation of that information technology departments and if affordable can be also done with an additional independent cyber security auditor to provide a second opinion in line with the Security Of Critical Infrastructure Act. Often internal departments for example accounting, communications, management and information technology departments can be adults with each other and conflict and nothing is done. Often management listens to the communications department or accounting department to make IT and cyber security decisions that are misinformed and exclude information technology departments from those decisions at their detriment. Company directors should be required to consult information technology departments in their companies and if the company is big enough, they should be required to also get an independent cyber security company risk assessment report annually or every 6 months.

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

Yes, Australia should consider a cyber security act. It should encompass every area of Australian life for maximum protection of the Australian citizen, Australian companies, Australian organisations including non-profits and Australian, state and council government departments. They should come by enforcement and protection regulations across all walks of life to enhance the security of the nation long term. General public consultation from Australian citizens, from Australian business communities, from cyber security information technology industry, and all industries affected and involved should be consulted on such an Act. In effect such an act would form the Australian IT security policy. Much the same as a local business would have an IT security policy in place.

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?

Cyber security regulatory requirements and legal obligations should be simplified and a legal advice service to businesses to help them create IT security and IT policies that are up to date with the current industry trends should be provided to smaller businesses that cannot afford to do it themselves such as organisations that are so traders and small businesses up to a certain size. Also, the price of such compliance should be affordable working with industry partners. Open government paperwork is confusing on regulations or no sufficient communication is provided in industries and to businesses, for example, the recent add-on insurance product laws enacted by ASIC. Industry took another year to understand what's going on because no sufficient communication was enacted across the business sector. It wasn't ASICs fault necessarily but perhaps a lack of funding in implementing those laws meant that ASIC didn't have enough funds to conduct proper communication strategy in implementation of these new laws. Same problem will be experienced if new wide-ranging privacy and cyber security laws are enacted without proper communication, planning and industry and business consultation.

Also on the subject of simplifying the regulatory framework, If there are possibilities to streamline such regulatory aspects into a single regulatory reporting requirement, then it should be enacted through our independent review panel or organisation to advise the government on where things need to be streamlined and simplified. Businesses should have a means of submitting feedback about the regulatory process so that it can be considered by this panel to improve the process and simplify it. But in the end some regulation is regulation and it's going to be painful and hard for some businesses that don't recognize cyber security is important or want to consider implementing the requirements. So in that case it will be difficult for them and there's nothing that can be done but to enforce it. It will mean that some businesses will go out of business, but if they are unable to establish the required protection and reporting regulations then perhaps they may not be adequately funded to provide products and services to their clients and the current cyber dangerous world.

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?

My answer says this: both should be prohibited, see below why:

- The best way to prevent ransomware or deal with stolen data and then extortion is to protect data better and it's to have good backups. Having good backups will allow a company to erase all the systems to clear them from ransomware and restore the data that was encrypted. Also stolen data cannot be recovered and it should be viewed that way.

- Companies and government departments who are victims of ransomware attacks should be required by law to not pay ransoms punishable by fines. This will discourage ransomware attacks.

- In my opinion, insurance companies should never pay ransom demands or extortion demands by cyber criminals. They should also be outlawed in doing that because it aggravates the problem across the industry further. In the end, there's no guarantee they will unlock the system or send back the stolen information and not sell that information behind their back later. There's no proof that they can pr want to. In a way malicious security hackers function as pirates with a pirate code They sent themselves and you don't know what that pirate code is. Some may say they will destroy the data after a ransom was paid or extortion is carried out but around the other end they may still sell it on the dark web. In my opinion, there's no point in paying the ransom.

- Everyday Citizens in Australia may choose to pay ransomware extortion demands or payment of ransoms if they want to because they are private citizens and can do what they like. Government communication should discourage private citizens from paying ransom work. Extortion demands for data because in the end there's no guarantee that the data is returned or the system is unlocked as mentioned above.

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?

- If a company or insurer pays a ransom or extortion demand payment and they are discovered by law enforcement or by government or reported, They should be fined so it sets the real cost of paying ransoms and discourages the use of that form cyber attack to extort money.

- If it's "victims of cyber crime" as in a company that company should never pay ransom or extortion demand payment enforceable by government regulation. And a regular education campaign for businesses to never pay ransom demands or extortion demand payments. Why? Because it proliferates that type of attack further and further without improving it across the industry. And a business owner may be scared and want to address it by paying the ransomware extortion demand payment, but in the end there's no guarantee that information will not be still sold on the dark web or their systems unlocked. In regards to the moral or ethical code by malicious security hackers: some malicious security hackers might have a moral code and some may not. We don't know.

- If we are talking about the "victims of cyber crime" as an individual's/ Australian citizens then they should not be liable if they choose to pay a ransom or an extortion demand. Citizens can only be educated that it's not worth it; a regular public campaign about it to inform the public would be advisable.

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?
Yes, clear laws about that aspect should be defined. Also, the government should assist companies that experience a breach or ransomware attack and they choose not to pay ransoms or extortion demand payments by assisting them in restoring their systems. and make it clear to those businesses that if they pay a ransom the government will not assist and the business will be fined. It seems harsh but it won't encourage the best approach to ransomware and extortion demand payments. Which is not paying and restoring all the systems.

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

Australia can do this in the following ways:

- Regular Australia wide and region wide Cyber security stress testing of government and large company systems and any critical infrastructure assets as defined by the Security Of Critical Infrastructure Act. How would that occur? Just like military drills conduct military operations with regional partners. The same can be done in cyber defence through simulated and need to know only by high level management cyber security stress testing drills to refine the systems and cut over systems when there's a cyber attack so that basic services are maintained and cut over properly, which is often the problem. For example, there was no workable cut over for the Australian bureau of statistics census in 2016.

- Work with other nations to establish a regional Cyber security centre with regional Partners around Australia.

- Invite cyber security centre staff from regional nations to work at each other's centres. Eg: ACSC staff invited to work with Japanese cyber security centre government department professionals to learn from each other. This will build up the experience of both teams.

- Set up regional cyber security trade craft knowledge bases that combine and enhance the knowledge gathered by every single cyber security professional within each government cyber security department from the regional nations. Combining knowledge bases across countries by the cyber security departments will further enhance the tradecraft of those teams. Obviously streak security to access those knowledge. Databases of Cybersecurity trade craft should be established to ensure only the authorised personnel are regularly monitored and strictest access to the systems where knowledge bases are kept should be established.

- Established setups and measures in place to create a joint cyber security team across many regional nations that work as one organism to conduct coordinated, cyber, offensive and defensive actions in each other's countries. This would enhance the capability of smaller nations and combine them with larger nations in the region to have a larger cyber defence against larger, malicious security hacker groups and nation states that run malicious security hacker groups.

- Each government cyber security centre in each regional country locally should meet together on an annual or every 6 month basis to exchange tradecraft and intelligence to enhance the protection of their nation.

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

- Be more cautious about making public statements of attacking malicious security hackers. Words must be used carefully. Like military generals do in battlefield statements.

- Work more often on joint cyber security, offensive and defensive operations That includes law enforcement and the cyber security centres of each country like the Australian ACSC.

- Work with regional and international governments that are aligned with their own values to align each other's cyber security and privacy regulations so that they are more uniform with us making business. More sure of being able to trade in Australia and in international partners So define standardised cyber security and privacy Acts that align with leading nations and promote that along with them to other nations and assist more disadvantaged or developing nations to establish those protections as well.

- Improve and strengthen cooperation between law enforcement and sub-security departments of every nation so that they work as one against malicious security hackers, groups and individuals. Thus improving the deterrents of this activity as not worth the effort and too expensive to undertake.

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?

- Investigate within boundaries and legal parameters of Australian law and international law to name and shame and expose the relationships between malicious security hackers that are secretly funded by nation states that promote malicious security hacking as a means of acquiring sensitive data for financial gain or to disrupt or damage other nations.

- Australia should be more coordinated in communicating cyber attacks and responses to cyber attacks that affect other like-minded nations as Australia. Once the Australian cyber security is at a better level, promote the cyber security of Australia to businesses to come and do business here to have more assurance.

- As discussed previously, be cautious about public communication before a new service or IT system that the government has created is launched or after a data breach happens to companies or government departments. It is important that comments are subdued and all emotion is removed out of those statements. So for example, government officials and politicians should never brag about the un-hackability of a government system e.g. ABS Census 2016.; Also, government officials and politicians should never declare war on malicious security hackers for any reason. They should always focus on the actual incident and finding the perpetrators without declaring an all-out war against all hackers in the entire world because that just invites further hacks by other organisations that when even discussed or covered.

- Hold nation states that have been discovered as funding or supporting or establishing malicious security hacker teams to attack other nations and their citizens - to submit joint submissions with evidence to the international criminal courts or set up a new international cyber security crime court nation states come before the tribunal and the evidence is laid out and formal charges are laid on those nation states that conduct such malicious activities. Also, independent Malaysia security hacker groups that undertake criminal operations should be tried in an international court because often they affect many nations and no single governments can try them.

- Encourage nations that have lost that unnecessarily. Protect malicious security hackers to adjust the laws to not protect such individuals and have extradition laws improved when it relates to cyber security attacks and hacking.

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

Every department in the Commonwealth government needs to have regular cyber awareness training and simulations on a monthly basis. All staff in every government department in government departments should be fully informed and aware of the cyber security policies and standards so they need to be understandable to them just like every other person in every other company. Managements of each government department that decide on a lack of cyber security standards and cut corners should be penalised or removed from their position to ensure accountability and liability for bad decisions that affect possible loss of client data in those departments.

Also, staff in government departments in the federal government should also be made aware at times that there are going to be cyber stress testing incidents on a regular basis but not be told when it happens. So they need to be trained on how to act and what their responsibilities are in the event of a cyber security attack or breach.

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

I think the government department ACSC need to open up the information sharing portal to all businesses and cyber security professionals that service other clients so they can log in and see all the past alerts and for them to be able to submit additional vulnerabilities and incidents and manage those so that historical data on alerts and reporting can be accessed.

- Also, a secure mobile app provided by the ACSC needs to be created for the general public as well as access to all the alerts and to submit incidents via an Android and Apple app. This app should have an alert mechanism that allows cyber security professionals and information technology professionals and business owners to be alerted based on the severity colour of a cyber security vulnerability or threat. 60% of digital access is now conducted on a mobile device rather than a computer but the ACSC website is very verbose and hard to access on mobile phones. So I think that in itself would enhance the governance ability for ACSC to share information on cyber threats to the very sectors of society. When the app is installed it should ask the person first what they are: individual, business, cyber security professional, IT professional, government department. This would then set up settings in place on the app that would be relevant to them and the alerts that they need to see. Also, if the person changes the status, they can change that profile in settings. If they, for example , suddenly become a cyber security professional, but they were an individual (public citizen).

- The ACSC also needs to start educating and not scaring the public with scary videos and scary commentary which is okay too. But they also need to temper that with education videos on YouTube and their website.

- Also, the ACSC website is over verbose and difficult to read for people with neurodiverse backgrounds who struggle to read it and make sense out of it because it's incoherent and all the verbose. The website needs to be readable even to a child if it's the public sections that discuss public cybersecurity advice. Probably primary school level education readability level should be added.

- Also, the ACSC website has to have a section for children and teenagers to get some cybersecurity advice on social media and their IT devices.

8. During a cyber incident, would an explicit obligation of confidentiality upon the Australian Signals Directorate (ASD) and 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?

Yes, that's correct. It would encourage companies to engage with ASD and ACSC if they knew that strict confidentiality is observed and the details and data that these governments access would not be passed on to any other department or become liable for it. Regulators should never be allowed to access activities that the ASD or the ACSC undertake to assist businesses in trouble. I think that's the most logical and very clear direction and the question kind of answers itself.

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?
Yes, I think so, all companies should be required to report ransomware and extortion demand incidents throughout the reporting platform under the penalty of a fine. But only businesses over 3 million should be publicly advised to the public that this has happened. The businesses under 3 million reporting data should be anonymized to protect those businesses from collapsing through bad reputation. I don't think the public needs to know whether a company paid the ransom or not. Such enforcement or fines should not be a "name and shame" activity but an internal fine by the government to that organisation if they did the wrong thing. If the public gets to know that a business paid the ransom, the government should make a statement that the company will be fine for paying your answer. So it encourages companies to do the right thing and not pay ransom or extortion demand payment.

10. What best practice models are available for automated threat-blocking at scale?
I am not aware of best practice models in automated thread blocking because that is something the antimalware and EDR systems developers have defined and keep strictly confidential. I think there would be best places to provide that guidance for the Australian government in automated thread blocking at scale.

I will provide some best practice points to consider when implementing and creating an automated thread blocking at scale system. If Australian government is planning to create an automated thread blocking system at scale It will need to include the following:

- **Intrusion detection system** in every government department and required of all companies that are part of the "security of the critical infrastructure Act". Such an intrusion detection system needs to be running 24/7 and monitored for all government departments for signs of malicious activity or attempts of it. Both at the firewalls and internally. When these automated systems detect malicious activity, it should block it straight away.

- **Honey pots -** these are fake networks and fake systems that can be implemented in every government department that pretend to be part of the department and when a hacker accesses those systems, they get attacked back or caught red-handed.

- Some government departments should never have Wi-Fi services because that service can be prone to easier access by unauthorised people.

- An automated thread blocking system at scale should include self-learning AI that's monitored by a team that undertakes proactive detection and protection where it needs to tighten or loosen in order to catch and to prevent attacks, breaches or theft of data. A lot of off-the-shelf systems already have that, but stronger forms of that should be developed in conjunction with service providers and government departments for the highest level of protection, automated and instantly responding. Government should undertake joint research with cyber security software service providers to improve such automated thread blocking systems.

- Government should also design in conjunction with the ACSC's cyber offensive team an automated cyber offensive system that can be replicated many times and used at will to undertake mass cyber offensive operations against malicious security hacker groups and Also used to detect nation states that get involved or caught up in the use of malicious security hacker groups. With the ability to create an instance of an offensive automated AI security, white hat hacker system, it will be possible to replicate it many times to use a whole team of automated "drone" programs that will work with human cyber offensive professionals.

- Automated thread blocking at scale systems is useless if access to those systems is physically not highly secure.

- Research the application of the generative AI approach to cyber defence and offensive cyber security in an automated thread blocking system at scale. Use as much as possible off the shelf industry, standard products that are already available or can be developed or enhanced at lower cost.

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

- Yes. There are many information technology professionals either retired or currently working in IT that just need a little bit of extra schooling to add the capability of being cyber security professionals within their companies or to retrain to find a role in cyber security. For a very long time has not provided funding for professionals within companies to be able to retrain in their own time to become cyber security professionals to move to cyber security jobs, since they have the foundation of information technology roles. They could easily transition to a cyber security role with a small amount of training that's focused and short. But opening the barrier for them is the cost of such retraining. Governments should provide retraining funding for professionals to upscale to cyber security.

- In terms of the cyber security research side of things in STEM, government should set up a national cyber security research centre and national institute of cyber security where top of the range students can be identified in Australian schools and trained with the best teachers and the best tools to become the best sub-security professionals and white hat hackers to then be deployed in developing cyber security software and tools as well as providing defences around that.

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

- Cyber security immigration: Cyber security professionals from other countries that are aligned with the Australian values should be allowed to come to Australia and be given full citizenship status and incentives to work here in Australia in the cyber security industry. Their qualifications must be verified because some can fake those on off the street fake certifications. So a cyber security exam should be required for those people to enter the country and become Australian citizens.

- **Cyber security Retraining** funding for IT professionals to enter cyber security in the street should be provided for short very focused retraining courses that can be done online and in person by IT professionals wanting to retrain to become cyber security professionals. Australian IT professionals already have a big foundation in information security through information technology. They just need extra schooling which they often cannot afford to complete that transition.

- **Cyber security accreditation:** Whole cyber security professionals should be required to be accredited just like the physical security industry with CCTV systems and security guards. It's no different in cyberspace. Cyber security professionals. I like digital security guards so they need to be licensed and monitored and regulated and that's fine because that then increases the value in a business or organisation. Because they are responsible for very sensitive access to systems, they need to be properly recognized and valued in the community. Same goes for information technology professionals. They should be accredited and licensed because they often deal with cyber security aspects in the job. After all, cyber security is a subsection of the information technology industry.

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

They should hunt down those responsible in an offensive manner when legally okay to do so. And I should work with other cyber offensive teams in other governments that are aligned to Australian values to work together to help each other similar to what NATO does to protect the countries part of NATO. So I propose that Western nations create a Cyber Security Treaty Organization (CSTO) where each member state contributes a part of the cyber security department as an offensive team to join a global team of cyber offensive professionals with international headquarters. Much the same as NATO works inside the fence and offensive activities against security malicious hackers. The combined computing power and expertise would be a great offensive and defensive deterrent to any malicious security hacker groups that might want to do harm on a large scale or even a small scale. The principle of you hurt one member. You heard everyone in CSTO. This small coordinated approach to what already is being done would help in creating a greater deterrent to the nation, states and Malaysia. Security individuals are groups that intend cyber harm to companies and citizens of other nations.

a. Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?
Yes, that would be easier for the companies that need to report incidents to several departments in the government if they could have a single combined reporting portal that's multipurpose. It's pointless to use resources if you have multiple reporting portals for cyber incidents. They could report nationally in one portal which is accessed using MyGov with proper ID verification and authorization.

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

- Industry meetings would need to be conducted to review the security practices in that industry.

- If an industry says that they are okay and under control, this should be taken with a grain of salt because it's always vested interest. Cyber security professionals need to be consulted along with that industry being reviewed after the post incident so that the practice recommendations can be implemented based on what has happened in that industry to improve the whole industry's cyber security. If an industry is trusted at face value to do their own policing or their own implementation without any regulation, it ends up like the telecommunication industry. Promise that they were all secure and all got hacked in one time or another in a very serious way eg Optus.

- Appropriate new penalties need to be established as law in industries that undertake certain bad practices in cyber security if that has not already been in place.

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

IDCare is an example of government and private funded organisation that helps victims of cyber crime to deal with the lots of government ID to monitor for its breach and use.
Similar organisations need to be formed funded by private and public and government to provide cyber security advice sessions for each citizen, and hold information sessions, and also assist with subsidised anti malware protections apps. Perhaps that not for profit organisation could also be the organisation that provides and runs the proposed citizen cyber awareness system that I proposed earlier to provide to each Australian citizen. The ability to sign up to a cyber training and fishing simulation service (cyber security awareness training) that each month trains them and simulates an attack to train them that they could register to. I still think that medium to large companies would have to still provide their own several awareness training systems and report on its proper use. Because some of these awareness systems are purchased but never used. That is on top of a government provided cyber awareness training and simulation system to citizens that I'm proposing.

a. What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?

- The Australian government should provide a free cyber stress testing service for a business to sign up to be booked in for a cyber attack simulation that is booked by the owner of the business to see what vulnerabilities they have this could include impersonation attack, cyber fishing, simulation and stress test of the defences such as firewalls and antivirus mechanisms on a business's computers and mobile devices. This Service should be provided once a year for each business that is under $3 million turnover. Businesses earning over $3 million should be required to do a cyber security stress test out of their own pocket.

- That service of cyber security stress testing should be done on the government oversight and records kept for that in the cyber reporting portal that is run by the government that was mentioned in the earlier questions. When a small business books the government provided cyber stress testing, it must be done randomly without the staff's knowledge. Only the business owner should know so that it has weight and validity. This would increase cyber security awareness among business owners and move them to invest in cyber security.

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?

- As I suggested earlier, the Australian federal government should set up a cyber security national institute department in CSIRO that researches cyber security improvements and new technologies and from that research, it should encourage the formation of new companies that are Australian based that are leaders in cyber security services and software.

- Also, Australia needs to regulate the cost of cyber security software. So it is affordable to any size business. For example, EDR systems are very expensive and inaccessible to small businesses. Also, the additional cost of cyber security awareness systems adds to further cost. Pricing should be monitored and regulated. Also a website page that outlines the top best price. Best technology offerings for cyber awareness, training and EDR and antimalware software providers should be provided by the ACSC. So that people can make an informed decision as to what they spend on cyber security services and products actually matters. Watch the same way as NBN retailers being reviewed for internet speed performance and displayed on the ACCC website page on internet speeds from NBN retailers (Reference: https://www.accc.gov.au/consumers/telecommunications-and-internet/broadband-performance-data). Review metrics on cyber security software, both for companies and domestic individuals should be listed on this Cybersecurity apps monitoring website. This will encourage the industry to provide better prices and better featured applications and software in cyber security. Despite the paid cyber security apps and services recommendations also include a list of free cybersecurity software and services like IDCare for enhancing one's cyber security in business and in domestic individual space and business space. This will help people inform who are the best leaders in cyber security apps and services in Australia and help make those services more accessible.
- Also, a list of cybersecurity businesses and providers would be great for people to refer to as a list to choose from. But being very much transparent in advising about free tools that free tools can only provide basic protection. Paid tools provide a lot more. Sometimes cyber security application providers provide software to defend devices and systems promise a lot of things but aren't always that secure. So a review process to increase and enhance the effectiveness of these tools will be good.

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

- Set up preventative measures in government departments.

- Fully fund cyber protection in government departments to 2030

- Keep increasing the ACSC and ASD departments' funding to watch the needs that grow because of a growing population by reviewing its requirements each year and the increasing intensity and volume of cyber attacks in Australia.

- Conduct round tables each year with all federal department heads on use of cyber security technology and how it can be used and improved in government departments.

- Conduct cyber security round tables by inviting business and all industry sector leaders or associations to improve and enhance the use of cyber security technology.

- Research and innovation in cyber security through universities and research institutes and government research departments such as the CSIRO should be implemented and fully funded till 2030 because through innovation and research better cyber security can be implemented in Australia and Australian organisations and the everyday citizen.

**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?

- That's a simple one. All government departments should be mandated to purchase Australian made or Australian company owned cyber security technology and solutions. And to hire local cyber security firms to conduct their stress testing and cyber enhancement. Where those companies don't have good enough technologies of software then any international provider should be engaged. But local providers should be always looked at first and if they don't have the level of features and tools then international sellers need to be engaged.

- Just like the space race industry has competitions on achieving a certain thing by creating a competitive bidding process for a solution. In a similar way, ACSC government department could create competitions that awards prize money to only 100% Australian owned companies and/or Australian made cyber security software and hardware Solutions that have innovation and things like artificial intelligence, quantum computing and generative AI technologies and other innovations. This will push businesses that offer cyber security applications, services and hardware that is Australian made to reach new heights in service delivery. Imagine world leading cyber security companies originating in Australia offering services to the world.

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

- Cyber security principles and best practices and behaviours should be enshrined in the strategy. Principle-based approach cyber security of emerging technologies and the promotion of security by design and your technologies should be undertaken.

- A cyber security stress testing and certification process should be required on all new emerging technologies and products as well as any new cyber security services and software and hardware. Just like safety testing or security testing is conducted in other sectors. For example, if a new antivirus app is introduced to the Australian market, it should be stress tested and reviewed before being approved in the Australian market. This will ensure fake or watered down protections aren't in place to defend Australian individuals or business.

    - And this aspect includes of course country of origin and state connections. Verifications of cyber security software used in Australia, for example Kaspersky used to be based in Moscow, Russia. In my opinion Kaspersky claims it hasn't got any state connections in Russia, but it has had a lot of connections for many decades to the intelligence agencies in Russia. It had a head office in Russia and it started the company in Russia. That is fine if you live in Russia, but if you are a citizen or company-based in western nations. This may be a conflict of interest. So cybersecurity software needs to be verified that has no enemy state connections of any kind. Eg: TikTok. It is of course all my subjective opinion and may not be accurate but the principle of verification of cybersecurity products is important.

- It should also undertake yearly awards for technology that has security by design to promote and highlight security by design as the best practice in product design, both physical products and software products.

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

- Regular cyber security stress testing of national assets and critical assets should be conducted and the results of those tests should be published on the national cyber resilience website page where those results are tabled like scorecards highlighting which industries need to improve and which government departments need to improve. Without naming specific departments or names of companies in industries.

- Also statistics on cyber incidents by industry and government departments and statistics on cyber compliance activities should all be collated together for score cards based on industries and government departments, and also in summary on the general public.

- Government can then review its laws, regulations and legislation in those particular industries to improve or address issues that arise or aspects that are not properly implemented by that industry or watered down based on perhaps something like a National Cyber Resilience Index (NCRI). This NCRI metric could define the cyber resilience of Australia on a monthly or quarterly basis. This would then govern improvements over time where it's needed.

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

- Perhaps the national cyber resilience index could include a transparency aspect of implementation of the strategy.

- That should also be a public feedback and ideas submission portal about the Australian cyber security of both businesses and government departments. And they should be an anonymous whistleblower portal where an everyday citizen or a staff member in a company can anonymously report a company in neglecting cyber security just like they do with corruption in government departments or in companies.

Concluding comments

In conclusion, I believe that a proactive approach to cybersecurity is the best policy for formulating Australia's strategy to protect against cyber threats. This is because the adage "**prevention is better than a cure**" holds true.

Improving cybersecurity in Australia will have immense benefits for the economy and encourage the use of digital services by everyday people, thus increasing the digitization of the economy. As most businesses rely on technology, enhancing cybersecurity will improve performance and reduce downtime through collaboration between the government and the private sector. This can be achieved through regulatory assistance and partnerships and practical solutions across all levels of the Australian nation.

It is important to recognize that **all digital systems have flaws in their design**, making them vulnerable to attack. Human nature and imperfection also contribute to weakening cybersecurity defences. However, regular preventative maintenance, setting up preventative measures, and conducting regular stress testing of cyber defences (cyber war games) can greatly enhance the security of Australian citizens and organisations, reducing the severity of cyber attacks. **While no digital system is completely unhackable**, cyber hygiene and preventative measures can make it more difficult to hack, serving as a deterrent to some degree.

It is likely that cyber attacks will increase in severity and frequency due to Australia's growing population and increasing reliance on technology. Over the next seven years, older generations will increasingly use technology, and in 20 years, millennials will be in their 60s and fully utilising technology. However, through concerted efforts to educate all segments of the population, we can create a **cyber-smart nation** that is more difficult to hack and steal data from.

In my opinion, **privacy and cybersecurity are inextricably linked**, and increased privacy protections should correspond with increased cybersecurity protections. Australians are very privacy-conscious, so it stands to reason that they will also want to be more cyber-security conscious. Achieving this goal requires joint efforts across the public and private sectors.

So to reinforce the point, based on my experience in cybersecurity, "**prevention is better than a cure**," and a proactive approach to cybersecurity is the best policy for protecting against cyber threats in Australia. The triage approach and responding to incidents after they happen is the most expensive way to manage Australia's cybersecurity. Prevention and proactive approaches, including cybersecurity maintenance and cyber hygiene, will reduce costs and reduce the severity and chances of cyber infection or attack. From history, we can learn that this approach has been effective, and I highly recommend its improvement in Australia in the coming seven years.

Regards,

Michael Plis
Founder of Cyberkite & IT Professional
linkedin.com/in/michaelplis
Cyberkite
Melbourne, Australia
14/04/2023 8:38 PM