We are responding to:

question 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?

The world is becoming increasingly digital, and this has led to an exponential increase in cyber threats. As more organizations digitize their operations, cyber threats have become a significant challenge that must be addressed. Therefore, cybersecurity has become a critical skill that is essential for the success of any modern society. To achieve this,

we propose that cybersecurity should be made the third pillar of education alongside literacy and numeracy.

We propose a comprehensive strategy for making cybersecurity a third pillar of education, ensuring that we become the leading nation in 2030 in combating the challenges of continuous cyber threats.

Reasons:

1. The need for cybersecurity skills has become increasingly important over the past decade. As more businesses and government agencies rely on digital systems to manage their operations, the risks of cyber threats have become more apparent. Cyberattacks have become more sophisticated, and the cost of cybercrime has risen dramatically. A report by Cybersecurity Ventures estimates that the cost of cybercrime will reach $10.5 trillion annually by 2025, making cybersecurity one of the biggest challenges facing modern society.

   While literacy and numeracy have always been considered essential pillars of education, cybersecurity has not received the same level of attention. However, with the increasing importance of digital technologies, cybersecurity has become a critical skill that must be taught to future generations. Cybersecurity education is essential in ensuring that our society is safe and secure in the digital age.

2. Humans are often the weakest link in cybersecurity, and studies have shown that up to 90% of cyberattacks are due to human error. This highlights the need for cybersecurity education to be incorporated into our education system at a young age, so that children can develop good cyber hygiene habits from an early age.

   It is often harder to change the habits of adults, who have already developed a set of behaviours and attitudes towards technology. Children, on the other hand, are still in the process of developing their behaviours and attitudes and are more receptive to learning new skills and adapting to new ways of thinking. By incorporating cybersecurity education as a third pillar alongside literacy and numeracy, we can ensure that children develop good cyber hygiene habits from an early age, making them less susceptible to cyber threats in the future.

By teaching children about the importance of cybersecurity, we can raise a generation that is more aware of the risks of cybercrime and has the skills to protect themselves and others. In addition, children who develop good cyber hygiene habits at a young age are more likely to carry these habits into adulthood, making them less likely to fall victim to cybercrime in the future. Therefore, it is crucial that we make cybersecurity education a third pillar of education alongside literacy and numeracy, so that we can build a safer and more secure digital society for generations to come.

3. Educating kids about the basics of cybersecurity can have a significant positive impact on families, especially as many families are not cyber aware and are vulnerable to cyber threats. Children who learn about cybersecurity in schools can become a valuable resource for their families, as they can share their knowledge and skills to help protect their families' devices and online activities.

   This is particularly important given the growing threat of cybercrime against families, which often involves targeting vulnerable family members such as grandparents and parents. By educating children in schools about cybersecurity, we can create a **junior cyber force** that can help defend their home networks and protect their families from cyber threats. This can include teaching children about topics such as password security, phishing, and malware, as well as strategies for staying safe while using social media and other online platforms.

4. In addition, educating children about cybersecurity can also help to bridge the digital divide between generations. As technology continues to play an increasingly important role in our lives, many older individuals may feel left behind or overwhelmed by the rapidly changing digital landscape. By empowering children with cybersecurity knowledge and skills, we can create a new generation of cyber-savvy individuals who can help to educate and support their older family members, bridging the gap between generations and creating a more digitally inclusive society.
5. In addition to raising a generation of individuals with good cyber hygiene habits, incorporating cybersecurity education as a third pillar of education will also create a **strong pipeline of future cybersecurity professionals**. By introducing cybersecurity education at a young age, children will have the opportunity to develop a passion and interest in this field, which can be nurtured and developed as they progress through their education.
6. Moreover, by integrating cybersecurity education into the education system, we can create a proper pathway for individuals who wish to pursue a career in cybersecurity. This pathway can include courses and certifications that provide specialized cybersecurity training, as well as internships and apprenticeships that provide practical experience in the field. By creating a clear pathway for individuals interested in cybersecurity, we can help to address the growing shortage of skilled cybersecurity professionals, which is a significant concern in the industry today.
7. Ultimately, by making cybersecurity education a third pillar of education alongside literacy and numeracy, we can not only create a safer and more secure digital society,

but also build a strong and sustainable cybersecurity workforce for the future. This is critical if we want to achieve and maintain our position as a leading player in the digital economy by 2030 and ensure that we are well-equipped to address the evolving cybersecurity challenges of the future.

Strategy:

To make cybersecurity a third pillar of education, the following strategies should be implemented:

Curriculum development: To make cybersecurity a third pillar of education, it is essential to develop a comprehensive curriculum that covers all aspects of cybersecurity. This curriculum should be developed in collaboration with cybersecurity experts and industry leaders to ensure that it is up to date with the latest threats and best practices.

Teacher training: To teach cybersecurity effectively, teachers need to be adequately trained in cybersecurity. Teachers should receive regular training on the latest cybersecurity threats and how to teach cybersecurity effectively. This training should be provided by cybersecurity experts and industry leaders.

Digital literacy and numeracy: Cybersecurity education should be integrated with digital literacy and numeracy. This will ensure that students have a strong foundation in digital technologies and understand the importance of cybersecurity in the digital age.

Partnerships: To ensure the success of cybersecurity education, partnerships with industry leaders and cybersecurity experts should be established. These partnerships can provide resources, expertise, and mentorship to students and teachers.

Certification: To ensure that students have a solid foundation in cybersecurity, a certification program should be developed. This certification should be recognized by industry leaders and should be a requirement for students who want to pursue a career in cybersecurity.

Conclusion:

by making cybersecurity a third pillar of education alongside literacy and numeracy, we can create a generation of cyber-aware individuals who can help to defend their families and communities against cyber threats, while also fostering greater digital inclusion and connectivity across generations.

In conclusion, cybersecurity has become a critical skill that must be taught to future generations. To achieve this, cybersecurity should be made the third pillar of education alongside literacy and numeracy. This will ensure that our society is safe and secure in the digital age. The implementation of a comprehensive curriculum, teacher training, digital literacy and numeracy, partnerships, and certification programs can help achieve this goal. By making cybersecurity a third pillar of education, we can become the leading nation in

2030 in combating the challenges of cybersecurity, privacy and safety, hygiene and cyber wellbeing.