1. To make Australia the most cyber secure nation in the world by 2030, the following ideas could be included in the Strategy:
    - Establish a national cyber security framework that sets minimum standards and best practices for all sectors of the economy.
    - Invest in research and development of new technologies and tools to enhance cyber security.
    - Increase public awareness of cyber threats and the importance of cyber security through education and awareness campaigns.
    - Strengthen partnerships and collaboration between government, industry, and academia to share information, expertise, and best practices.
    - Develop a national incident response plan that outlines roles and responsibilities, and procedures for responding to cyber incidents.
    - Enhance international cooperation and information-sharing on cyber security issues.
    - Develop a comprehensive regulatory regime that establishes clear obligations and penalties for cyber security breaches.
    - Implement mandatory reporting requirements for certain types of cyber incidents to improve visibility and understanding of cyber threats.
2. The following legislative or regulatory reforms could be pursued by the government to enhance cyber resilience across the digital economy:

    a. Legislation is an appropriate mechanism for reforms to improve mandatory operational cyber security standards across the economy. Regulations and further regulatory guidance could also be useful.

    b. Further reform to the Security of Critical Infrastructure Act may be required to extend beyond the existing definitions of 'critical assets' to include customer data and 'systems.'

    c. Company directors should have specific obligations to address cyber security risks and consequences.

    d. Australia could consider a Cyber Security Act, which would establish clear obligations and penalties for cyber security breaches.

    e. The government could monitor the regulatory burden on businesses resulting from legal obligations to cyber security, and streamline existing regulatory frameworks where possible.

    f. The government should prohibit the payment of ransoms and extortion demands by cyber criminals by victims of cybercrime and insurers, except in limited circumstances. Strict prohibition could have some impact on victims of cybercrime, companies, and insurers.

    g. The government should clarify its position with respect to payment or non-payment of ransoms by companies, and the circumstances in which this may constitute a breach of Australian law.

3. Australia can build its regional cyber resilience and better respond to cyber incidents by:
    - Developing stronger partnerships and information-sharing mechanisms with neighboring countries.
    - Providing technical assistance and capacity-building to other countries in the region.
    - Promoting the adoption of international best practices and standards across the region.
    - Participating in regional cybersecurity initiatives and organisations.
4. Australia can elevate its existing international bilateral and multilateral partnerships from a cyber security perspective by:
    - Strengthening existing partnerships and developing new ones with countries that share common interests in cyber security.
    - Participating in international forums and organisations focused on cyber security.
    - Contributing to the development of international standards and norms related to cyber security.

5. Australia can better contribute to international standards-setting processes in relation to cyber security and shape laws, norms, and standards that uphold responsible state behavior in cyberspace by:
    - Participating in international forums and organisations focused on cyber security.
    - Contributing to the development of international standards and norms related to cyber security.
    - Advocating for the adoption of international best practices and standards across the world.
6. Commonwealth Government departments and agencies can demonstrate and deliver cyber security best practice and serve as a model for other entities by:
    - Implementing robust cyber security policies and practices within their own organisations.
    - Sharing their expertise and best practices with other government agencies, industry, and academia.
    - Participating in cyber security exercises and simulations to test their own readiness and identify areas for improvement.
7. The government can improve information sharing with industry on cyber threats by:
    - Developing mechanisms for sharing threat intelligence in real-time with industry.
    - Establishing public-private partnerships to enhance collaboration on cyber security issues.
    - Providing incentives for industry to share information on cyber threats.

8. An explicit obligation of confidentiality upon the Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC) may improve engagement with organisations that experience a cyber incident. If organisations are assured that their information will be kept confidential and not shared with regulators, they may be more willing to share information with ASD/ACSC, which in turn can help in the investigation and resolution of the incident.

9. Expanding the existing regime for notification of cyber security incidents could improve the public understanding of the nature and scale of ransomware and extortion as a cybercrime type. Requiring mandatory reporting of ransomware or extortion demands could increase awareness of the prevalence of these types of cyber attacks and help organisations prepare better to defend against them.

10. Several best practice models are available for automated threat-blocking at scale. These models use machine learning and artificial intelligence to identify and block threats in real-time, and can be customized to fit the specific needs of an organisation. Examples of these models include the MITRE ATT&CK framework, the Cyber Kill Chain model, and the Diamond Model of Intrusion Analysis.

11. Australia may require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda. While STEM education can provide a foundation for developing cyber skills, additional specialized training and certification may be necessary to address the specific needs of the cyber security industry.

12. The government can support Australia's cyber security workforce through education, immigration, and accreditation. This can involve funding cyber security education programs, creating immigration policies that attract cyber security talent to Australia, and developing accreditation programs that recognize and certify cyber security professionals.

13. The government can respond to major cyber incidents by implementing a range of measures beyond existing law enforcement and operational responses. This can involve creating a single reporting portal for all cyber incidents, harmonizing existing requirements to report separately to multiple regulators, and developing a comprehensive incident response plan that involves all relevant stakeholders.

14. An effective post-incident review and consequence management model with industry would involve close collaboration between government and industry. This can involve conducting a thorough review of the incident, identifying the root causes and vulnerabilities that led to the incident, and implementing measures to prevent similar incidents from occurring in the future.

15. Government and industry can work together to improve cyber security best practice knowledge and behaviors, and support victims of cybercrime. Small businesses may require assistance from government to manage their cyber security risks and keep their data and their customers' data safe. This can involve providing education and training programs, access to affordable cyber security tools, and financial assistance to help implement cyber security measures.

16. The government can enhance Australia's cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia by investing in research and development programs, providing funding for start-ups and small businesses, and creating policies that promote innovation and collaboration between government and industry.