2023-2030 Australian Cyber Security Strategy Discussion Paper:

https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/2023-2030-australian-cyber-security-strategy-discussion-paper

Global Cyber Alliance: response to specific questions within Attachment A:

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

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

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

It could potentially prevent organisations and individuals seeking help if they think they will have been deemed to have broken the law. A heavier burden may be placed on Law Enforcement to provide specialist support to assist with negotiation/restoration.

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

To the extent that the law is unclear, it should be clarified. Ransomware situations create significant pressure and compressed decision-making for targeted organisations. Greater clarity in the law on points such as these can assist organisations in managing these incidents more effectively.

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

While improving government-to-government approaches are an important aspect of building regional cyber resilience and better response to cyber incidents, it is equally important to develop multi stakeholder approaches that include industry (e.g., Internet infrastructure operators, cybersecurity tools and solutions providers, as well as other industry verticals) and civil society organisations (e.g., NGOs focused on cybersecurity standards, skills building, tools and solutions). Most of the cyber risks faced by Australia and its neighbors cannot be addressed and resolved by one organisation or stakeholder group. Collaboration and sharing of data should be both regional and global and include public, private and law enforcement actors. Global Cyber Alliance has developed projects related to domain abuse and IoT threats that are community-driven and aim to create cybersecurity risk reduction at scale. GCA would be happy to share its experience working with multi stakeholder groups to develop cybersecurity tools and solutions for deployment across the Internet and for implementation by end user communities (e.g., small businesses, mission-based organisations, journalists, elections officials, individual Internet users)

11. Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?
Cybersecurity is very often viewed as jargon filled and highly technical, yet an approach that is flexible and meets everyone "where they are" in their digital skills journey is also needed. Incorporating cyber in STEM educational curriculum is essential for students' formative years. It must also be noted that university level degree/diploma-based programs are still in relatively early stages of development and need to become more robust to address the cyber skills gap and cybersecurity jobs market needs. There are a number of cybersecurity skills certification programs available that do not require a university degree and that can open the door to entry level cybersecurity jobs. Creative thinking must be applied to providing training resources for those who do not have access to a university-based degree or specialized certification training to ensure they can develop essential cyber hygiene skills to protect themselves and, perhaps, to be enabled to address current cyber skills gaps.

12. What more can Government do to support Australia's cyber security workforce through education, immigration, and accreditation?
See response to #11.

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

a. Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?
Yes, consideration should also be given to how this is addressed by other governments with a potential view of harmonisation/standardisation which could allow efficient cross-border collaboration between law enforcement/relevant agencies.

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

a. What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?
Clear, precise messaging and access to the tools and resources required to implement best practices, in particular 'essential cyber hygiene.'

Please provide responses to auscyberstrategy@ homeaffairs.gov.au by COB 15 April 2023.