Ransomware – Australian Policy and Obligations

Our reading of the situation is that the Australian Government maintains a firm stance against paying ransoms in response to cyber extortion, including ransomware attacks. While perhaps not outright illegal, such payments are strongly discouraged due to the risks they pose to national security and the potential for violating sanctions laws.

AU Government Policy on Ransomware Payments

- **Zero Tolerance Approach**. The government does not condone ransom payments, asserting that paying ransoms fuels the ransomware business model and endangers other Australians. homeaffairs.gov.au
- **Sanctions Compliance**. Making or facilitating a ransomware payment to a person or entity subject to Australian cyber sanctions is a criminal offence, punishable by up to 10 years' imprisonment or significant fines. guidance-note-cyber-sanctions.pdf

---

Mandatory Reporting Requirements

As of 30 May 2025, under the Cyber Security Act 2024, certain entities must report ransomware payments to the Australian Signals Directorate (ASD) within 72 hours. factsheet-ransomware-payment-reporting

Who Must Report.

Directors should take advice on reporting. These are two examples of reporting requirements:

- Businesses operating in Australia with an annual turnover exceeding AUD 3 million.
- Entities responsible for critical infrastructure assets.

Reporting Details.

Directors should assemble as many relevant details as possible, having taken advice first on reporting requirements.

- Information about the cyber security incident, including the nature and impact.

- Details of the ransom demand and payment, including method and amount.
- Communications with the extorting entity.

Penalties for Non-Compliance

- Failure to report within the prescribed timeframe may result in civil penalties. NB criminal penalties that may be applied re sanctions compliance.

Legal and Operational Risks

- **No Guarantee of Data Recovery**. Paying a ransom does not guarantee access to locked systems or sensitive data and may lead to repeat attacks. There is no guarantee either that your data will not be on sold or made available to third parties. You should operate with the mindset that you are dealing with criminals. Ransomware Action Plan
- **Potential Legal Consequences**: Payments to sanctioned entities can result in severe criminal penalties, including imprisonment and substantial fines. dfat.gov.au

---

Government Support and Resources

- **Ransomware Playbook**: The government has released a "Ransomware Playbook" to guide Australians and businesses in managing ransomware attacks, from confronting demands to recovering lost data.
- **Cyber Security Hotline**: For assistance, contact the Australian Cyber Security Centre's 24/7 Hotline at 1300 CYBER1 (1300 292 371).

In summary, while paying ransoms is not explicitly prohibited, the Australian Government's policy strongly discourages such actions due to the associated risks and potential legal implications. Entities are encouraged to report incidents promptly and seek assistance through official channels.