Article Information

Author: Craig Subocz
Service: Cyber Security, Intellectual Property & Technology, Privacy & Data Protection
Sector: IT & Telecommunications

Mandatory reporting of ransomware payments may soon be law. What you need to know

On 9 October 2024, in accordance with its 2023-2030 Cyber Security Strategy, the Government introduced into Parliament legislation to create a standalone Cyber Security Act, which would mandate an obligation to report ransomware payments.

As we wrote in our December 2023 Insight (which you can read here), the Commonwealth Government outlined a new Cyber Security Strategy, the centrepiece of which was a standalone Cyber Security Act as one of the "shields" to make Australia a "world leader in cyber security by 2030". Ten months later, the Government has introduced into Parliament legislation to establish the Cyber Security Act.

According to the current Cyber Security Minister, the Hon. Tony Burke MP, the "creation of a Cyber Security Act is a long-overdue step for our country and reflects the government's deep concern and focus on these threats. The legislation ensures we keep pace with emerging threats, positioning individuals and businesses better to respond to, and bounce back from cyber security threats".

The Cyber Security Act would establish the following:

- A reporting obligation for ransomware payments by all businesses with an annual turnover exceeding $3 million;
- Mandated minimum security standards for entities involved in the supply chain of internet-connected devices;
- The ability of entities to voluntarily provide information concerning a significant cyber security incident to the National Cyber Security Coordinator, who has the role of leading a whole of Government response; and
- A Cyber Incident Review Board, with responsibility for initiating reviews into certain cyber security incidents and making recommendations to Government and industry about improving cyber resilience.

Mandatory reporting of ransomware payments

Although the Strategy flagged an obligation to report all ransomware attacks, the proposed Cyber Security Act would only require businesses with an annual turnover exceeding $3 million, as well as government entities, to report ransomware payments to Government. A failure to make a report could attract a fine of up to $15,000.

The Bill proposes that a business which makes a payment would be obliged to report to the Government information concerning:

- the cyber security incident;
- the demand made by the extorting entity;
- the amount paid or benefit provided; and
- communications between the business (or a party on its behalf) and the extorting entity.

The business would be required to submit the report within 72 hours of making the payment and the Government intends that such reports would be made to the Department of Home Affairs.

The Bill makes it clear that a business that reports the ransomware payment would not be liable to an action or other proceeding for damages in complying with the reporting obligations. According to the Government, this provision is intended to protect reporting entities from incurring liabilities, such as breach of confidentiality, other contractual requirements or for other civil proceedings that may exist when complying with the reporting obligation. The Government

views this as necessary to exempting businesses from having to choose between complying with a mandatory requirement and complying with contractual or other obligations that could result in proceedings for damages.

Mandated minimum security standards

Under the Cyber Security Strategy, the Government set out an intention to adopt international security standards for consumer-grade smart devices by working with industry to co-design a mandatory standard.

The proposed Cyber Security Act would allow the adoption of security standards for specified classes of relevant "connectable products" that would be acquired in Australia in specified circumstances. Where a set of security standards have been adopted for a "connectable product", then the manufacturers of those products must comply with the standard in the manufacture of the product. Through the extraterritorial provisions under the proposed Act, this would extend to international manufacturers of connectable products that are imported into Australia for sale.

The Act would prohibit the supply in Australia of a product that was not manufactured in compliance with the relevant standard. The Act would also require manufacturers and suppliers to provide, for the supply of the product in Australia, a statement of compliance with the relevant security standard.

The Act would confer on the Government the right to issue notices to require the relevant entity to comply with the obligation to manufacture and supply devices that meet the minimum standards. If the entity continues to fail to comply wit the security standards despite receiving the notices, the Government would then have a right to publish information concerning the non-compliant entity and the relevant products.

Protection of information submitted to the Government

The Bill would set out the framework for the permitted recording, use and disclosure of the information in the ransomware payment report. In particular, there would be five permitted purposes for which the information could be recorded, used or disclosed, including:

- Assisting the business making the report (and other entities acting on the business' behalf) to respond to, mitigate or resolve the incident;
- Exercise powers or perform functions conferred on the Government by the Act;
- Performing functions of a Commonwealth and/or State body relating to responding to, mitigating or resolving a cyber security incident;
- Performing functions of the National Cyber Security Coordinator relating to the cyber security incident; and
- Informing and advising the relevant Minister (and other Commonwealth Ministers) about the cyber security incident.

The Government intends to legislate limited use provisions to govern how the information disclosed to the Government would be managed, in order to protect sensitive or commercial-in-confidence information from businesses. In particular, under the Bill, the recipient of the report cannot make a record of, use or disclose the information for the purposes of investigating or enforcing, or assisting in the investigation or enforcement, of any contravention by the reporting entity of a law other than a contravention of the Cyber Security Act or a law that imposes a penalty or sanction for a criminal offence.

The coordination of significant cyber incidents

The Bill would allow an entity that is impacted by a "significant cyber incident" to voluntarily provide information to the National Cyber Security Coordinator (**Coordinator**) to enable the Coordinator to lead across the whole of Government the coordination and triaging of action in response to the incident. The Cyber Security Act would permit the Coordinator to record, use and disclose information received from the impacted entity for limited purposes.

A cyber incident will be significant for the purposes of the Cyber Security Act if there is a material risk that the incident has seriously prejudiced, is seriously prejudicing or could reasonably be expected to prejudice the social or economic stability of Australia or its people, the defence of Australia, or national security. The incident will also be significant if the incident is, or could reasonably be expected to be, of serious concern to the Australian people.

If an entity is suffering a significant cyber security incident, or it could reasonably be expected that the incident is significant, then the entity may submit information about the incident to the Coordinator (who also has the power to request information from the affected entity).

Where it is unclear as to whether the incident is significant or not, then the entity would be entitled to disclose information to the Coordinator, and the Coordinator would be entitled to collect and use the information for the purpose of determining

whether the incident is significant or not.

The Bill would recognise that the role of the Coordinator would be to lead the Government's response to the significant cyber security incident and to keep the Minister informed in relation to the Government's response. The Bill would restrict the Coordinator's ability to use or disclose the information for other purposes.

Crucially, the Bill would provide that the provision of information to the Coordinator would not affect a claim of legal professional privilege made in relation to that information in any legal proceedings (except in limited circumstances).

The Cyber Incident Review Board

The new Cyber Security Act would establish a Cyber Incident Review Board to oversee no-fault assessments of cyber security failures, in order to better understand the reasons why the incident occurred and what steps other businesses can take to mitigate the risk of similar incidents occurring in the future. The structure and operation of the Board would be based on similar function within the US Government, and the Board would have the power to mandate reviews and collect information concerning the incident.

A review would be initiated where one of the following three criteria are met:

- The incident (or a series of incidents) have seriously prejudiced or could reasonably be expected to seriously prejudice the social or economic stability of Australia or its people, the defence of Australia, or national security;
- The incident (or a series of incidents) involved novel or complex methods or technologies and, by undertaking the review, the understanding and recommendations made would result in being able to significantly improve Australia's cyber resilience; or
- The incident (or a series of incidents) are, or could reasonably be expected to be, of serious concern to the Australian people.

Under the proposed legislation, the relevant Minister, the Coordinator, the impacted entity or a member of the Board can refer an incident to the Board for review in accordance with the Act.

According to the Government, the intention of a review conducted by the Board is to not apportion blame or provide a means for determining liability of an entity in relation to a cyber security incident. Reports would not include personal information, information that is confidential or commercially sensitive , or information that could cause damage to the security, defence or to Australia's international relations.

Conclusion

The introduction into Parliament of legislation establishing the Cyber Security Act is a key plank of the 2023-2030 Cyber Security Strategy. Businesses with a minimum annual turnover in excess of $3 million should take note of the mandatory obligation proposed in the legislation to report ransomware payments to the Government, while those entities involved in the supply chain of smart devices and internet-connected devices should be aware of and plan for the introduction of the mandatory minimum security standards that will apply to those devices.

Key Takeaways

- The Government has taken steps to implement its 2023-2030 Cyber Security Strategy by introducing into Parliament legislation to establish a standalone Cyber Security Act.
- If passed, the Cyber Security Act will mandate minimum security standards for smart devices and internet connected devices.
- The Cyber Security Act will also establish a mandatory ransomware payment obligation on Australian entities with annual turnover exceeding $3 million.
- Additionally, the Cyber Security Act will establish a National Cyber Security Coordinator with responsibility for coordinating and managing a whole of Government response to significant cyber incidents, and will also establish a Cyber Incident Review Board to review and make recommendations on incidents referred to the Board for review.