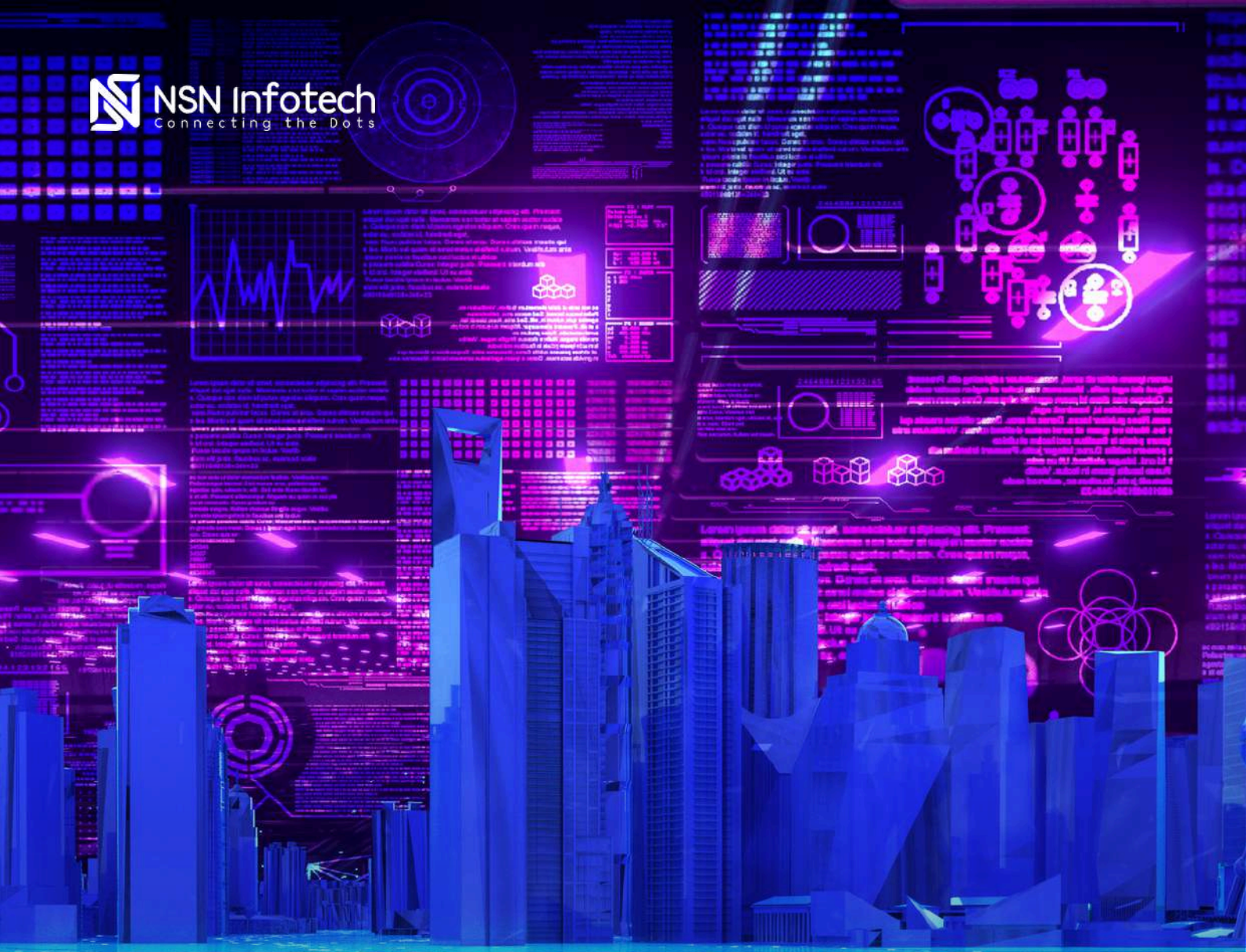


Australian Mandatory ransomware payment reporting

Factsheet

March 2025

Mandatory ransomware payment reporting

What is mandatory ransomware and cyber extortion payment reporting?

Part 3 of the Cyber Security Act 2024 establishes a ransomware and cyber extortion payment reporting obligation on reporting business entities.

By mandating ransomware reporting for these entities, the Australian Government will be able to build a more informed picture of the threat landscape and provide tailored advice and support to industry to help disrupt the ransomware business model. As outlined under section 2 of the Act, the ransomware reporting obligation under Part 3 will commence by Proclamation 6 months following Royal Assent.

How do I know if I am a reporting business entity?

An entity will be a reporting business entity if it:

- is carrying on business in Australia with an annual turnover that exceeds the turnover threshold specified in the Rules; and
- is not a Commonwealth body or a State body.

The Minister for Cyber Security can prescribe Rules to specify the relevant annual turnover threshold. The development of the Rules are subject to a minimum 28-day consultation period. The Government has indicated during the development of the legislation its intention to consult on setting the turnover threshold at AU$3 million.

This reflects feedback from industry stakeholders on a range of thresholds that would seek to best balance the need to get a clear whole-of-economy picture of the threat landscape, and to avoid imposing regulatory burden on small businesses. A responsible entity for a critical infrastructure asset to which Part 2B of the Security of Critical Infrastructure Act 2018 applies will also be a reporting business entity.

When do I have to report?

A reporting business entity must make a report within 72 hours of making the ransomware payment (or becoming aware that the ransomware payment has been made). The following questions can assist you to determine when a report is required:

1. Has a cyber security incident occurred, is it occurring or is it imminent?

Where the incident is not a cyber security incident, such as a physical threat, this obligation does not apply. Note that this is not restricted to only ransomware incidents in the technical sense. It may also extend to other types of cyber extortion, such as data exfiltration accompanied by a demand and subsequent payment.

2. Has the incident had, is the incident having or could the incident reasonably be expected to have a direct or indirect impact on a reporting business entity?

The incident must impact a reporting business entity. That means, the incident must impact an entity that meets the criteria above.

3. Has an entity (the extorting entity) made a demand of the reporting business entity or any other entity in order to benefit from the incident or the impact on the reporting business entity?

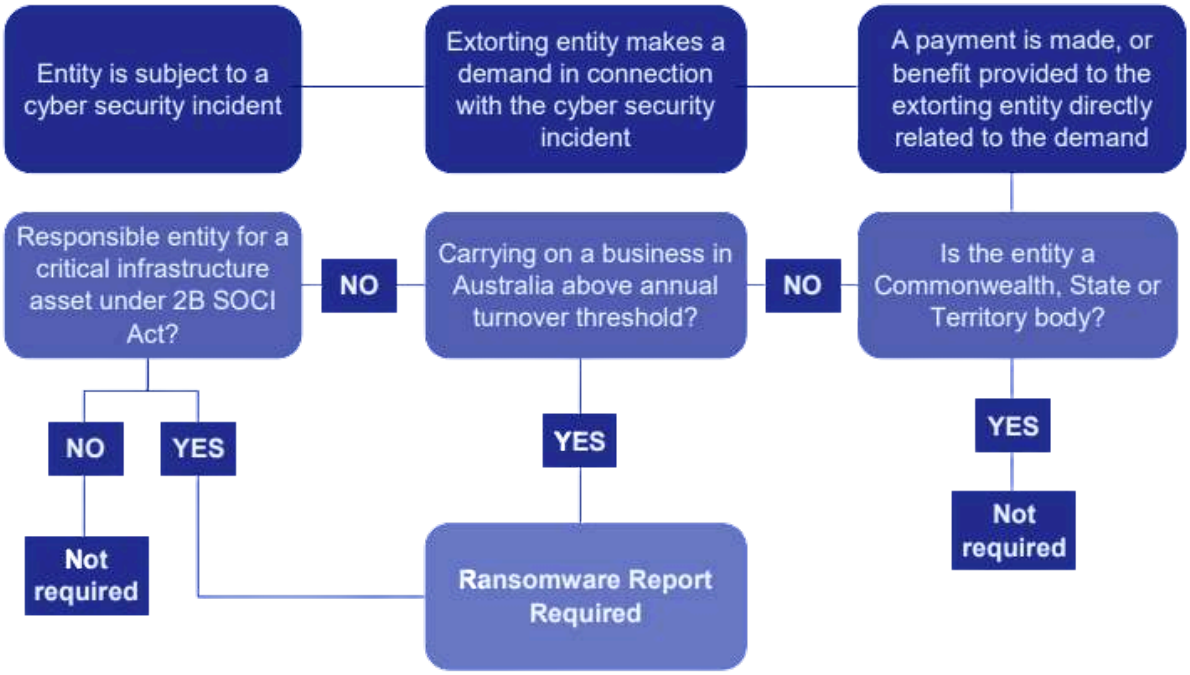
This is the extortion element. An extorting entity must have made a demand of the reporting business entity for a payment or benefit in connection with the incident.

The extorting entity does not necessarily have to be the same entity that is responsible for the cyber security incident. Often the identity of the entity responsible for the cyber security incident is not known. Similarly, the identity of the extorting entity may not be verifiable. The important element to be satisfied here is that a demand has been made in order for the extorting entity to benefit from the incident or the impact on the reporting business entity.

Benefit is defined in section 8 to include any advantage, so may not be limited to just money (as the entity may demand cryptocurrency, a service or information).

4. Has the reporting business provided, or is the reporting business entity aware that another entity has provided on their behalf, a payment or benefit to the extorting entity that is directly related to the demand?

This encompasses circumstances where an entity pays the ransom, or provides the benefit, or engages a third party service provider to negotiate and provide a payment or benefit to the extorting entity on its behalf



What happens if I don't report within 72 hours?

The Act provides that a civil penalty of 60 penalty units can apply where a reporting business entity does not make a mandatory ransomware payment report when they are obligated to do so.

However to support entities in complying with this new obligation, the Department is committed to an education first approach to regulation. The Department will prioritise warnings, meetings and engagements, before pursuing civil penalties, especially in respect of small and medium enterprises.

How do I report?

Reports must be made on a portal which will be developed on the Australian Signals Directorate's cyber.gov.au website.

The Department will continue to work closely with industry as this portal is developed to ensure businesses are able to acquit their reporting obligations. Entities making the report are only required to report information that it knows, or is able, by reasonable search or enquiry, to find out, relating to:

- the contact and business details of the entity that made the payment;
- the cyber security incident, including its impact on the reporting business entity;
- the demand made by the extorting entity;
- the ransomware payment; and
- communications with the extorting entity relating to the incident, demand and the payment. Entities may also include other information relating to the cyber security incident in the ransomware payment report.

Need help with your Disaster Recovery Strategy?

Schedule a consultation with our experts!

For more information, please contact marjorie.valera@nsninfotech.com