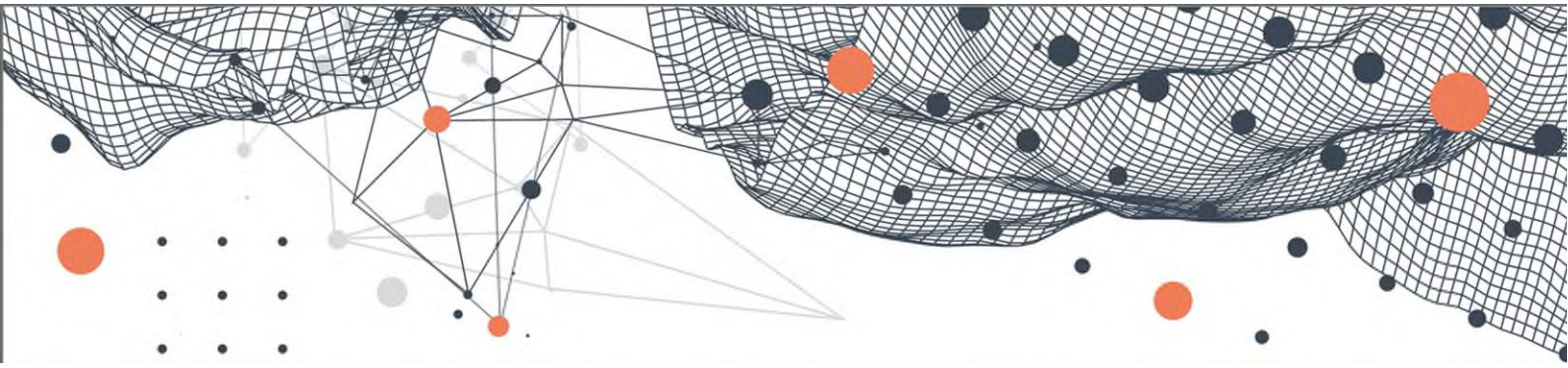


FREQUENTLY ASKED QUESTIONS

Mandatory ransomware and cyber extortion payment reporting is active from 30 May 2025

When are entities obligated to make a ransomware and cyber extortion payment report?

The key criteria that need to be met in order for the mandatory ransomware payment and cyber extortion obligation to apply are:

1. An entity needs to be a **reporting business entity** as defined under section 26(2) of the *Cyber Security Act 2024*;
2. The reporting business entity needs to be impacted by a cyber security incident (either directly, or indirectly);
3. The reporting business entity must have provided, or is aware another entity has provided on their behalf, a ransomware payment to an extorting entity, that is seeking to benefit from the impact or the cyber security incident.

Broadly, reporting business entities are entities that are carrying on a business in Australia and have an annual turnover of $3 million or are the responsible entity for a critical infrastructure asset required to report under Part 2B of the *Security of Critical Infrastructure Act 2018*.

There is no mandatory reporting obligation where there is no ransomware or cyber extortion payment. For example, if there is only a demand, but a reporting business entity elects *to not* make payment, then there is no obligation to report.

Do Australian entities need to make a report for cyber security incidents that have occurred overseas – especially where the impact on the Australian entity is minor or peripheral?

A reporting business entity by definition carries on business within Australia and is only obligated to make a report **if the above criteria are met.** Whether a cyber security incident originated overseas or impacts overseas entities does not change the reporting obligation. Where a reporting business entity is impacted (directly or indirectly) by an incident, receives a demand, and then elects to make a payment, they are required to make a report in accordance with section 27 of the *Cyber Security Act 2024*.

Use this key to reference in the following scenarios:

Company A – Carries on a business in Australia and meets the annual turnover threshold as defined in the Rules, so is a ***reporting business entity***.

Company B – Is a Software-as-a-Service (SaaS) provider that does not carry on a business in Australia, providing an essential service for Company A.

Company C – Is a cybersecurity firm that does not carry on a business in Australia.

Below are different scenarios outlining instances where a reporting business entity is and is not required to make a ransomware or cyber extortion payment report:

Scenario 1: Entity outside of Australia experiences a cyber security incident, there is a direct impact on the Australian subsidiary

Company B experiences a cyber security incident from an advanced cyber-criminal syndicate. This threat actor accesses Company B's systems, which operate all around the world, and locks out *all* analysts from the main network, including from **Company A** (direct impact). The threat actor leaks commercially sensitive and confidential data held by both **Company A** and **Company B** on the dark web.

The threat actor (the extorting entity) makes a demand of **Company A** and all other companies around the world that **Company B** provides essential services to for an encrypted bitcoin payment (the demand). Without the transfer, the threat actor would periodically release all of the illicitly obtained commercially sensitive and confidential data on an illegal online marketplace.

Company A then hires **Company C** to negotiate with the extorting entity and a deposit, albeit of a lesser amount, into the bitcoin wallet occurs (the payment). The extorting entity still releases all the information it scrubbed from **Company B's** networks on the dark web.

In this scenario, **Company A** is captured by the legislation and must make a ransomware and cyber extortion payment report to the Australian Government within 72 hours.

Scenario 2: Entity outside of Australia experiences a cyber security incident, there is no direct impact on the Australian subsidiary

Company B experiences a cyber security incident from a known threat actor operating out of Europe. Through an unpatched vulnerability, the threat actor obtains a backdoor into **Company B's** systems and deploys various types of malicious malware, including ransomware. Tech analysts within **Company B** notice that files are beginning to encrypt themselves.

Fortunately, the tech analysts in **Company B** were able to act quickly, isolating and containing the code, preventing widespread damage. However, the files encrypted are still essential to **Company B's** business operations, and the threat actors begin demanding USD $250 for every file encrypted (20 in total). **Company B** decides that USD $5,000 is a small price to pay for having the files unencrypted and released, and elects to make a ransomware payment to the threat actor using a bitcoin wallet. **Company B** then decides to let all subsidiaries operating overseas know of the ransomware event and subsequent demand and payment.

Because **Company A** does not experience any direct or indirect impact on their own systems and was not aware that **Company B** elected to make a ransomware payment, they are not captured by the legislation and are not obligated to report to the Australian Government.

Sometimes the impacted entity is not the entity that ends up making a ransomware or cyber extortion payment. Who is responsible for reporting in this case?

The Department understands that there may be circumstances where a third-party or another entity within the reporting business entity's own business structure makes a ransomware or cyber extortion payment on behalf of a reporting business entity. In such cases, the reporting business entity is still required to make a mandatory ransomware or cyber extortion report.

If a payment is made without the knowledge or not on behalf of a reporting business entity, then the reporting business entity is not required to make a report until such a time that the reporting business entity becomes aware that the payment was made on their behalf.

Section 3 of the *Cyber Security Act 2024* specifies that the Act applies both inside and outside of Australia. This means the Act applies for cyber security incidents that may have initiated outside of Australia and considers that entities operating in Australia, may still procure services or share information with other entities (including parent companies) that operate outside of Australia.

Where there are multi-jurisdictional components to consider for captured entities, it may be difficult for an entity to determine **who is responsible** for providing a ransomware or cyber extortion payment report to the Government. If you are uncertain about whether or not you are obligated to make a report, please refer to the three key criteria outlined above.

How is the information I provide in a ransomware payment report protected?

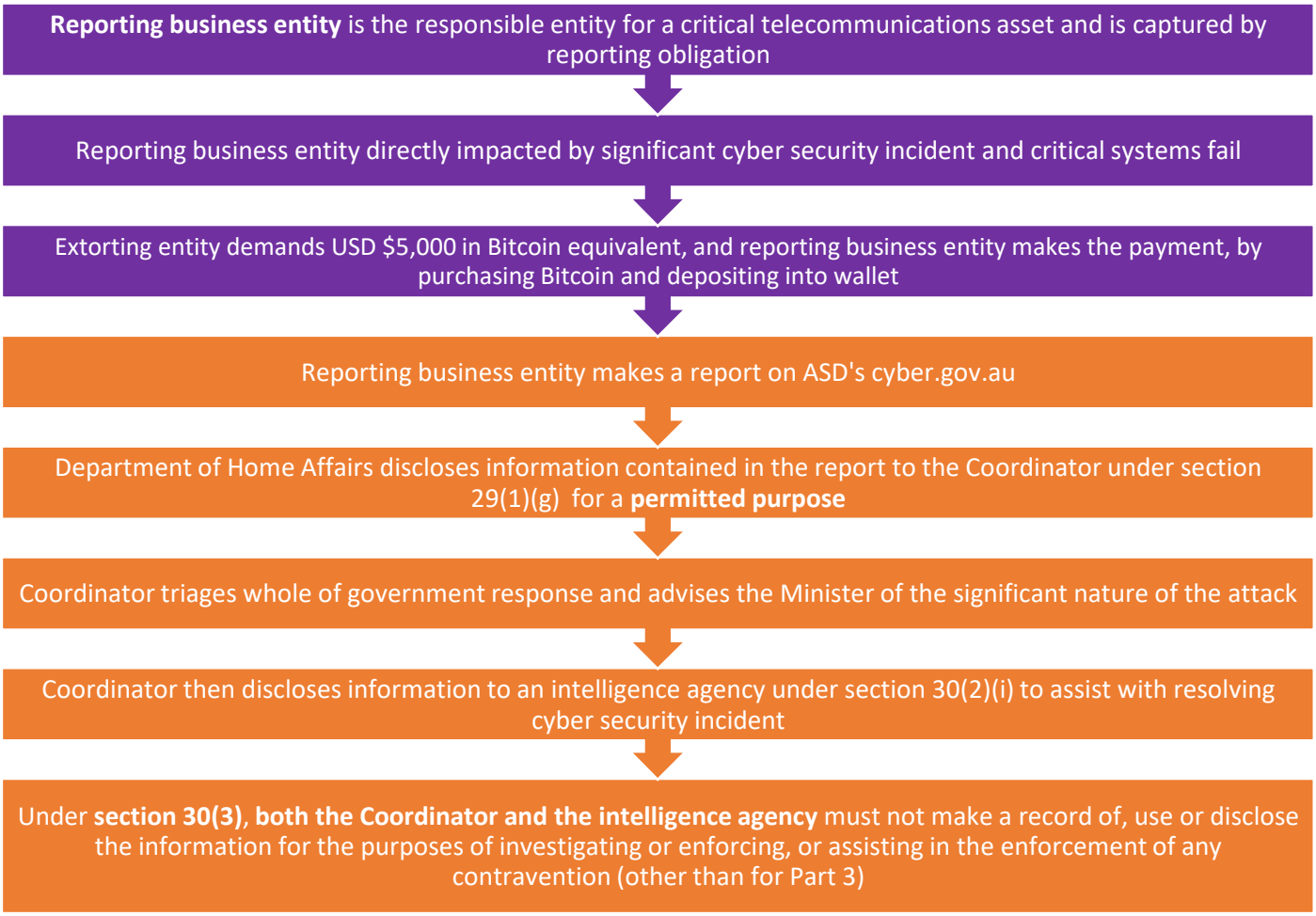
The ransomware and cyber extortion payment reporting obligation only applies if **three criteria** listed above have been met (an entity is a reporting business entity, the reporting business entity is impacted by a cyber security incident directly or indirectly, the reporting business entity provides a ransomware payment to an extorting entity, in response to a demand, that is seeking to gain from the impact of the cyber security incident).

Information that is provided to the Department of Home Affairs from the reporting form on ASD's cyber.gov.au following a ransomware or cyber extortion payment can only be used in accordance with Part 3 of the *Cyber Security Act 2024*. Section 29 details the permitted use and disclosure of the information contained in a ransomware payment report, for example, assisting the reporting business entity in responding to, mitigating or resolving the cyber security incident or for the performance of the functions of an intelligence agency.

Section 30 details the limitations on the secondary use and disclosure of information contained in ransomware payment reports, that is, information that has been provided by a reporting business entity and obtained and held by another entity.

This process map below details the three criteria that have been met (in purple) for the ransomware payment reporting obligation to apply. The process map then shows the Department of Home Affairs disclosing information contained in the report to the National Cyber Security Coordinator (the Coordinator), which then discloses the information to an intelligence agency for **permitted purposes**. Both the Coordinator and the intelligence agency **must not** make a record of, use or disclose the information for the purposes of investigating, or enforcing, or assisting in the enforcement of any contravention (other than those outlined in Part 3 of the Act).

Process Map showing hypothetical flow of information – disclosed twice for permitted purposes



How does the ransomware and cyber extortion payment reporting obligation interact with 'limited use' outlined in Part 4 of the *Cyber Security Act 2024*?

Additional information relating to the cyber security incident, or the ransomware or cyber extortion demand and payment can be voluntarily provided to the National Cyber Security Coordinator, in accordance with section 35 or

section 36 of the *Cyber Security Act 2024*. Where information is voluntarily provided to the Coordinator, Part 4, Division 3 of the *Cyber Security Act 2024* applies to the handling of that information.

Voluntary disclosure of information to the Coordinator **does not satisfy the s27 ransomware and cyber extortion payment reporting obligation**. If your entity is a reporting business entity and captured by the mandatory reporting obligation, you must make a report to the Government through the form on ASD's website if a ransomware or cyber extortion payment is made. If there is no payment made, **you do not need to make a report**.

Both information provided for ransomware reporting, and cyber security incident information voluntarily provided to the Coordinator have similar protections applied. For example, claims of legal professional privilege are not affected, and information is inadmissible in civil and criminal proceedings, with exceptions for a Royal Commission or a coronial inquiry.