Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Annual Cyber Threat Report 2024–25 fact sheet

For businesses and organisations

Cybercriminals commonly target Australian businesses and organisations for financial gain. This can be through scams or the on-selling of personally identifiable information, usernames or passwords.

State-sponsored cyber actors continue to target Australian businesses and organisations to support political, economic and military objectives. Many Australian businesses and organisations hold large amounts of sensitive and valuable data. State-sponsored cyber actors may use this data to support the targeting of government and critical infrastructure organisations, as well as their supply chains.

Cyber threat facts for 2024–25

The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) responded to over 1,200 cyber security incidents – an 11% increase from last year.

In FY2024–25, ASD's ACSC received over 84,700 cybercrime reports – an average of one report every 6 minutes.

For businesses, the average self-reported cost of cybercrime per report was up 50% overall ($80,850).

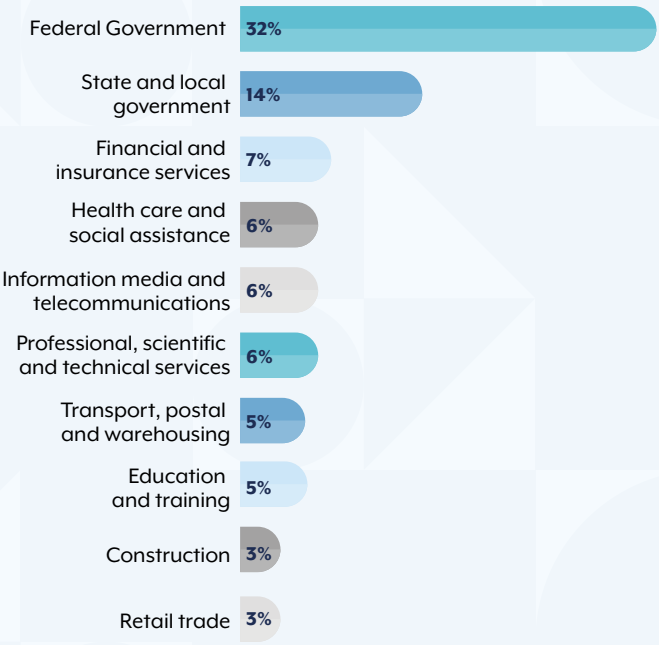
The average self-reported cost per report and business size was:

- small business – **$56,600** (up 14%)
- medium business – **$97,200** (up 55%)
- large business – **$202,700** (up 219%).

The top **cybercrimes** reported by **businesses** were:

- email compromise resulting in no financial loss **(19%)**
- business email compromise fraud resulting in financial loss **(15%)**
- identity fraud **(11%)**.

Top 10 reporting sectors from incidents reported to ASD's ACSC



Annual Cyber Threat Report 2024–25 fact sheet

For businesses and organisations

Take action to protect your networks and digital infrastructure

Businesses and organisations must operate with a mind-set of 'assume compromise' and consider which assets or 'crown jewels' need the most protection.

There are 4 key actions that ASD's ACSC considers critical for organisations to improve their cyber security:

1. Ensure you have best-practice event logging in place.
2. Replace legacy technology or put appropriate mitigations in place.
3. Choose products and services that are secure by design.
4. Adopt post-quantum cryptography to safeguard your digital infrastructure.

The years ahead will bring challenges for organisations in emerging technology, such as post-quantum cryptography. Effective transition plans for a post-quantum computing world will be critical to operating in 2030 and beyond – this planning must start now.

More Information

If your organisation services or supports critical infrastructure, read the ***Annual Cyber Threat Report 2024–25 fact sheet for critical infrastructure*** to stay up-to-date with the threats and trends to CI. Read the full report and find the latest cyber security advice and a range of practical how-to guides for business on cyber.gov.au.

ASD encourages every business and organisation that detects suspicious activity, incidents and vulnerabilities to report them to ReportCyber at cyber.gov.au/report or by calling the Australian Cyber Security Hotline 1300 CYBER1 (1300 292 371).

ASD's ACSC provides free technical incident response advice and assistance, 24 hours a day, 7 days a week.