



Annual Cyber Threat Report 2025-26

Factsheet for critical infrastructure

The threat landscape

Critical infrastructure (CI) underpins Australia's economy, security and way of life, making it an attractive target for cyber actors seeking financial gain, espionage opportunities or strategic advantage. [Artificial intelligence \(AI\)](#) is reshaping the threat landscape by lowering barriers for cyber actors and increasing the scale, speed and sophistication of malicious activity. At the same time, the growing interconnectedness of systems, operational technology and supply chains is increasing the threat surface and potential impact of cyber incidents.

Key facts and statistics



Received over
82,000
cybercrime reports



1,500+
cyber security
incident responses



4,400+
notifications issued
to organisations



One report
was made every
6 minutes



\$148,100
average self-reported
cost of a cybercrime
incident
(Large Business)



150+
cyber security incidents
responded to involving
critical infrastructure
entities



**Top sectors
for CI Incidents**
Financial & Insurance Services (**30%**),
Public Admin & Safety (**21%**),
Electricity, Water & Utilities (**17%**)††

Factsheet for critical infrastructure

Advice for critical infrastructure

CI entities should operate with an 'assumed breach' mindset, build resilience and prepare for disruption. There are several key actions that ASD's ACSC considers critical for CI organisations to improve their cyber security:

- Replace [legacy technologies](#) where possible, otherwise apply strong compensating controls.
- Implement best practice [event logging](#) to mitigate abnormal or malicious activity.
- Manage [supply-chain](#) and third-party risk and choose [secure by design](#) products and services.
- Prepare for [post quantum cryptography](#).
- Prepare for [AI-enabled cyber threats](#).
- Prepare for the capability to isolate and operate critical systems and networks for 3 months.
- Maintain visibility of vital assets and enabling systems, and prove the ability to rapidly restore them while sustaining critical services.

Reporting and assistance

- Reporting cybercrime, cyber security incidents or vulnerabilities helps ASD identify threats and protect other Australians from becoming victims. It is critical that CI organisations report malicious or suspicious activity to ASD's ACSC.
- **Online:** cyber.gov.au/report
- **Call:** 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. Stay engaged through our [Cyber Security Partnership Program](#) and help build the nation's collective cyber resilience.

Further information

- Read the full [Annual Cyber Threat Report 2025–26](#) for the latest insights into Australia's cyber threat environment.
- You can also access [ASD Essentials](#) and [CI Fortify: Guidance for Australian Critical Infrastructure Service Continuity and Resilience](#), which provides practical advice to help critical infrastructure entities strengthen resilience and maintain essential services during disruptions. Both publications are available at cyber.gov.au