Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Annual Cyber Threat Report 2024–25 fact sheet

For critical infrastructure

Critical infrastructure (CI) continues to be a target for state-sponsored cyber actors, cybercriminals and hacktivists. This is due to the sensitive data CI organisations hold and its role in providing services that support Australia's national resilience, sovereignty and prosperity.

State-sponsored cyber actors continue to use built-in network tools to carry out their objectives and evade detection by blending in with normal system and network activities. This is called living off the land and these cyber actors are enabled to strategically steal information or cause harm to an organisation's network at a time of their choosing.

Access to a CI network can provide a malicious cyber actor with control over Australia's CI systems, which could lead to a degradation in system confidence, major disruptions to availability, or even destructive effects.

Cyber threat facts for 2024–25

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. CI made up 13% of all incidents (up 2% from last year).

The average self-reported cost of cybercrime per report for businesses is up 50% overall ($80,850) and up 219% for large business ($202,700).

ASD's ACSC responded to more than 200 incidents involving DoS or DDoS attacks (up more than 280% from last year). DoS and DDoS were present almost twice as often (31%) in incidents against CI entities when compared with all incidents that ASD's ACSC responded to (16%).

Top 3 **ANZSIC Divisions for CI incidents:**

- financial and insurance services **(32%)**
- transport, postal and warehousing **(26%)**
- information media and telecommunications **(16%)**.

The 3 most common **activity types** leading to CI-related incidents were:

- scanning or reconnaissance **(41%)**
- Denial of Service (DoS) / and Distributed DoS **(31%)**
- phishing **(20%)**.

Annual Cyber Threat Report 2024–25 fact sheet

For critical infrastructure

Take action to protect your networks and digital infrastructure

There are 4 key actions that ASD's ACSC considers critical for CI 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.

CI Fortify

To address the threat of state-sponsored cyber actors targeting CI, CI Fortify is the first in a series of guidance designed to prepare CI operators for periods of crisis, conflict or heighted cyber threat.

The guidance outlines two key preparatory steps for CI operators:

- **Maintain a current inventory** of operational technology (OT) assets and their enabling systems.
- **Identify the isolation point(s)** to isolate vital OT assets and enabling systems to ensure ongoing functionality.

In the event of crisis, conflict or heightened cyber threat, CI operators should develop the capability to:

- **Isolate vital OT and enabling systems** for 3 months.
- **Fully rebuild vital OT and enabling systems** to minimise the impact of potential service disruptions to critical services.

More Information

If your organisation engages third-party suppliers or service, read our ***Annual Cyber Threat Report 2024–25 fact sheet for businesses and organisations*** to stay up-to-date with the threats and trends to Australian businesses. Read the full report and find the latest cyber security advice and a range of practical how-to guides for CI on cyber.gov.au.

ASD encourages every CI 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.

Stay engaged with cyber security. Join ASD's Cyber Security Partnership Program and help build the nation's collective cyber resilience.