2023–2024 Cyber threat trends
For critical infrastructure

- Answered over 36,700 calls to the Australian Cyber Security Hotline, an average of 100 calls per day and an increase of 12% from FY2022-23.
- The most frequently reported critical infrastructure sectors were electricity, gas, water and waste services (30%), education and training (17%) and transport, postal and warehousing (15%).
- The top 3 cyber incidents types affecting Australian critical infrastructure were:
  - compromised accounts or credentials
  - malware infection (other than ransomware)
  - compromised asset, network or infrastructure.
- Responded to 128 incidents reported by organisations who self-identified as critical infrastructure.
- ASD responded to over 1,100 cyber security incidents. 11% of all incidents responded to included ransomware, a 3% increase from last year.
- Notified critical infrastructure organisations over 90 times of potential malicious cyber activity.

Australian critical infrastructure networks were persistently targeted by malicious cyber actors in the 2023–24 financial year because they provide critical services, hold sensitive data, and are often connected to other critical infrastructure organisations.

Nation-states and their proxies, transnational criminal organisations and cybercriminals use sophisticated and malicious tactics to target critical infrastructure, steal intellectual and innovation, and engage in espionage.

This is not just an issue for Australia. Critical infrastructure networks worldwide continue to be targeted by malicious cyber actors, including in conflict, where cyberspace is now an established domain of warfare and cyberattacks are used for strategic, political, economic and national security objectives.

Operational technology (OT) and connected systems, including corporate networks, are of interest to malicious cyber actors and can be targeted to access a corporate network and vice versa, potentially allowing malicious cyber actors to move laterally through systems to reach their target. Designing robust information security measures is vital to protect the confidentiality, integrity and availability of systems.

What should Australian critical infrastructure organisations do?

Adversaries evolve and so does cyber security. Good cyber security is not set and forget. To mitigate cyber security threats, critical infrastructure organisations should:

- treat a cyber incident as a 'when' not an 'if' – have a cyber security incident response plan and test it regularly to ensure an effective response and fast recovery.
- follow best practice cyber security, such as ASD's Essential Eight, which is evolving to address new threats and mitigations.
- undertake due diligence on a supplier's products and cyber security practices before and while engaging them, and look for best-practice cyber security products that are secure-by-design and secure-by-default.
- thoroughly understand your networks, map them and maintain an asset registry to help manage devices and all networks, including operational technology (OT).
- implement an event logging system.
- scrutinise your ICT supply chain vulnerabilities and risks.
- educate your supply chains on cyber security vulnerabilities.
- develop and maintain a culture of cyber security awareness, particularly in regard to phishing.
- limit the use of Remote Desktop Protocols (RDP) and other services.
- only connect OT and IT systems when necessary.

For more cyber security advice, visit the Resources for Critical Infrastructure on cyber.gov.au.

Report cyber security incidents, including suspicious activity, incidents and vulnerabilities, early 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 the ASD's ACSC Cyber Security Partnership Program and help build the nation's collective cyber resilience. ASD has a number of programs and services for critical infrastructure organisations, including the Critical Infrastructure Uplift Program (CI-UP), the Cyber Threat Intelligence Sharing (CTIS) Platform, and a range of engagement activities aimed at assisting in hardening the cyber defenses of our essential services.