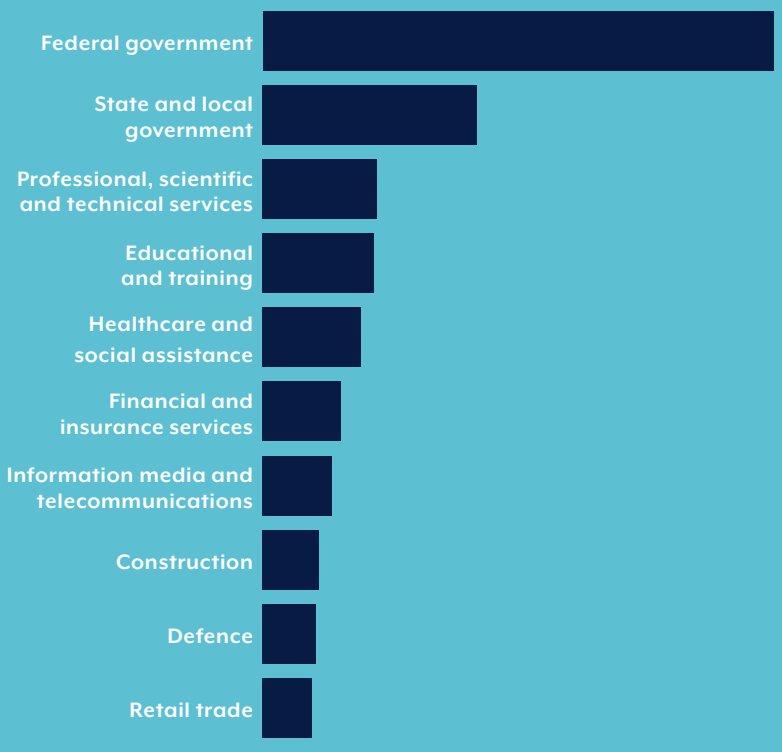
Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

2022–2023 CYBER THREAT TRENDS FOR CRITICAL INFRASTRUCTURE

Answered over **33,000** calls to the **Australian Cyber Security Hotline** an average of **90 calls** a day, an **increase of 32 per cent** from the previous financial year.

Top 10 reporting sectors with confirmed cyber incidents were:



2022–2023 CYBER THREAT TRENDS

FOR CRITICAL INFRASTRUCTURE

Top 3 cyber incidents reported by **critical infrastructure** were:

1. compromised accounts or credentials
2. compromised assets, networks and infrastructure
3. denial-of-service attacks.

ASD **responded** to **over 1,100** cyber security incidents. **Ransomware** comprised over **10 per cent** of all incidents similar to the previous financial year.

2022–2023 CYBER THREAT TRENDS FOR CRITICAL INFRASTRUCTURE

Australian critical infrastructure networks regularly experienced targeted and opportunistic malicious cyber activity in the 2022–23 financial year. Activity against these networks is likely to increase as they grow in size and complexity.

This is not just an issue for Australia. Critical infrastructure networks worldwide continue to be targeted by malicious cyber actors, and Russia's war on Ukraine has demonstrated that critical infrastructure is viewed as a target for disruptive and destructive cyber activity during times of conflict.

Malicious cyber actors can steal or encrypt data, or gain insider knowledge for profit or competitive advantage, and some actors may attempt to degrade or disrupt services.

Operational technology (OT) and connected systems, including corporate networks, will likely be of enduring interest to malicious cyber actors. OT 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 critical infrastructure do?

- Follow best practice cyber security, such as ASD's Essential Eight Mitigation Strategies, or an equivalent framework as required for a critical infrastructure risk management program.
- Prioritise secure-by-design or secure-by-default products.
- Thoroughly understand networks, map them and maintain an asset registry to help manage devices and all networks, including OT.
- Scrutinise the organisation's ICT supply chain vulnerabilities and risks.
- Develop and test robust business continuity and disaster recovery plans to ensure your organisation can quickly respond in the event of a cyber incident.
- Report cyber security incidents early to ReportCyber at cyber.gov.au/report.
- Join the ASD Cyber Security Partnership Program and help build the nation's collective cyber resilience. ASD has a number of programs and services for critical infrastructure entities, 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.