# CI Fortify

## Guidance for Australian critical infrastructure service continuity and resilience

CI Fortify provides high-level cyber security recommendations for Australian critical infrastructure (CI) operators to strengthen their security posture and resilience in preparation for instances of crisis or service disruption.

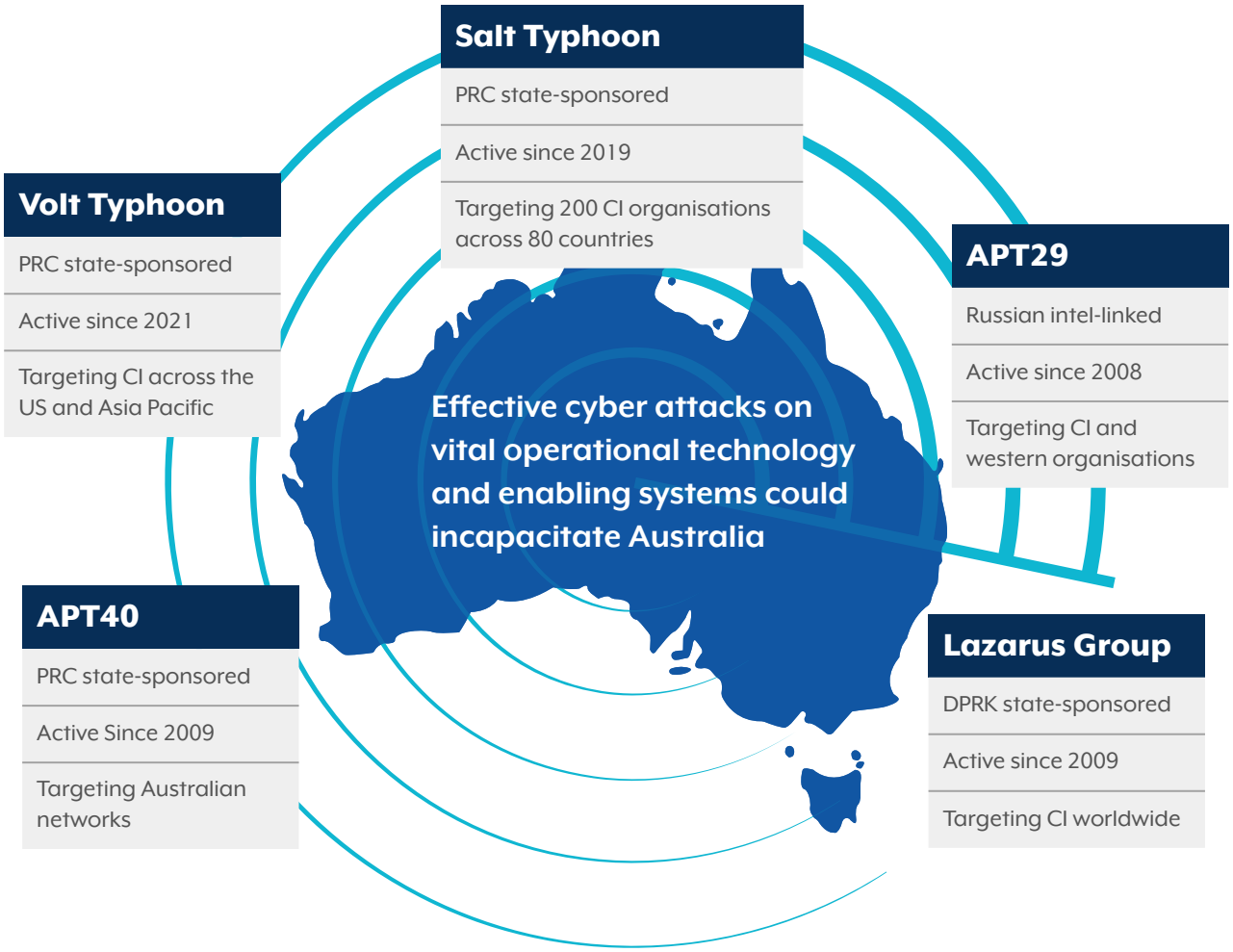
The cyber threat landscape for operational technology (OT) environments maintained by CI operators continues to evolve. Prioritising the security, reliability and recovery of these essential systems must be a strategic priority for CI operators nationwide.

State-sponsored cyber actors routinely target Australia's CI networks, possibly to conduct espionage or to pre-position for disruptive and destructive cyber effects in the event of crisis or conflict. In crisis or conflict, 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 the confidence of systems, major disruptions to availability, or even destructive effects.

Cybercriminals continue to opportunistically target CI operators. The sensitivity of the data stored by these entities, and the importance of their services, makes them attractive for cybercriminals seeking to extort victims via data exfiltration or conducting ransomware attacks for disruptive or destructive purposes.

CI often relies on complex information technology (IT) and OT networks with complex supply chains. While these networks allow CI providers to deliver services to the Australian people, they also present an ever-growing attack surface, which includes both the provider themselves and those within their supply chain. Supply chain dependencies should be considered when reviewing the advice within this publication.

## State-sponsored actors are targeting Australia




Australian CI is, and will continue to be, an attractive target for state-sponsored cyber actors. Australia has joined multi-country advisories warning of the threat of state-sponsored actors targeting CI as highlighted in the recent Salt Typhoon advisory *Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System*.

The Australian Security Intelligence Organisation's (ASIO) Annual Threat Assessment 2025 has assessed espionage and foreign interference are already at extreme levels and are anticipated to intensify[1].

ASIO also assessed that authoritarian regimes are demonstrating a growing willingness to disrupt or destroy CI to impede decision-making, damage war fighting capabilities and sow social discord.

**Australian CI operators must take action now to strengthen cyber resilience.**

1 For more, refer to the *Director-General's Annual Threat Assessment 2025* at asio.gov.au

## Operational technology systems are at risk

Operational technology (OT) and enabling systems are now prime targets for malicious actors. Despite their critical role, many were not engineered to endure cyber security incidents. An increase in both the targeting of OT systems and the sophistication of threat actors has been observed over the past 15 years.

**2010**

**Stuxnet**

- First malware to target OT systems
- Caused damage to Iranian nuclear centrifuges

**2016**

**Industroyer**

- Targeted Ukrainian power grid, depriving Kyiv of energy
- Malware had progressed to becoming modular and extensible

**2017**

**Triton (HatMan)**

- Targeted Saudi Arabian petrochemical plant
- Target shifted to systems that protect human life
- Shows escalation of threat to include physical harm

**2021**

**Colonial Pipeline**

- Targeted largest refined-fuel pipeline in the US, forcing an 8,850km shutdown
- IT breach triggered a proactive OT shutdown showing IT-OT interdependency
- Caused fuel shortages across the US East Coast for one week

**2022**

**Industroyer 2**

- Used exact values specific to its Ukrainian substation target
- Demonstrated deep-seated system knowledge
- Showed willingness of state-sponsored actors to spend time learning the target environment to create unique and precise attacks

OT environments often have legacy devices, outdated protocols and slow replacement cycles. Many CI operators remain tied to long-standing engineering contracts that were not designed with cyber security in mind. The result is a widespread, persistent cyber risk to Australia's most vital services.

**The risk is already being realised, mitigating it must be a priority now.**

# Definitions

For the purpose of this guidance, ASD uses the following terms and definitions:

### Critical services

Services  required to sustain the survival of Australians, or that support national security and economic stability.

### Vital OT and enabling systems

Systems  essential to the continuity of a critical service provided by a CI operator.

# Preparing to adopt CI Fortify

Before implementing the actions of CI Fortify, CI operators should complete three important preparatory steps to ensure these actions are effective.

## Maintain an up-to-date inventory of OT assets and enabling systems

An accurate inventory is the foundation of any OT cyber security strategy. CI operators should identify and record all OT asset types, roles, locations and dependencies. This inventory should use a clear classification structure to show function and criticality of OT assets and enabling systems. Inventories should be kept current throughout the asset lifecycle to support risk assessments, prioritise protection efforts and enable effective isolation or rebuild strategies. For more guidance around OT inventories refer to *Foundations for OT cybersecurity: Asset inventory guidance for owners and operators* at cyber.gov.au

## Identify vital OT and enabling systems

CI operators should define the organisation's critical services. Once defined, operators should determine which vital OT and enabling systems must remain in a functional state to maintain delivery of those services.

When identifying vital OT and enabling systems, consider perspectives across the total provision of a critical service – from the business impact in degraded availability or health, to the technical dependencies of the critical services in operations. Not all OT systems may be vital to this critical service provision and CI operators should make this distinction for each service. Understanding this distinction will inform decision-makers where to focus isolation measures or rebuild planning.

## Identify the isolation points

With all vital OT and enabling systems identified, the CI operator can determine at which locations to enact isolation.

# Planned actions

This guidance includes two planned actions that CI operators are encouraged to achieve. These are the ability to:

- isolate vital OT and enabling systems from the internet, other networks and systems for 3 months while maintaining critical services.
- rapidly rebuild vital OT and enabling systems completely to minimise disruptions to critical services.

## Isolate vital OT and enabling systems

### Temporary isolation

The ability to temporarily isolate vital OT and enabling systems for a period of **3 months** while maintaining critical services.

Malicious actors can persistently target a CI operator. To protect against persistent threats, CI operators should develop the capability to isolate vital OT and enabling systems from other networks and systems, including corporate and third-party systems for 3 months. This will enable CI operators to sustain critical services and protect against catastrophic effects – both to their core functions and their businesses.

CI operators should have a graduated plan to enact isolation measures. This plan should:

- define the vital OT and enabling systems required to deliver their critical services (refer to *Principles of operational technology cyber security at* cyber.gov.au )
- prioritise protection efforts across vital OT and enabling systems to assure critical service continuity
- set thresholds to assess the risks and impact of isolating systems on business operations and continuity of critical services.

A graduated plan allows CI operators to assess the risk to their operations in response to a heightened threat environment. This plan also proactively reduces their attack surface in anticipation of a potential cyber security incident.

Isolating vital OT systems will break businesses processes. Any automated processes that cross from the isolated network to adjacent networks will most likely need to be completed manually during the period of isolation. Organisations should have a plan to do this in instances of crisis or service disruption.

## Prove the ability to rebuild vital OT and enabling systems

### Rapidly rebuild

The ability to rebuild isolated vital OT and enabling systems completely and continue provision of critical services

Being able to rebuild isolated OT and enabling systems completely is crucial for restoring services safely and quickly – especially when:

- malicious actions occur before or trigger after isolation occurs
- isolation measures are not fully effective
- there is low confidence in the ability to evict malicious actors from an environment
- normal business-as-usual backups are unavailable or are no longer trustworthy due to malicious activity.

CI operators should assess the minimum requirements to rebuild a critical function to determine which backup components are prioritised, what spare equipment needs to be readily available and where these spares should be pre-positioned for rapid access.

Maintain offline known-good and tested backups of firmware, configuration and processes for all vital OT and enabling systems.

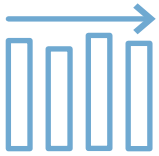
This minimum operating state may differ significantly from business-as-usual and could involve manual processes.

# Parallel benefits

Implementing guidance in CI Fortify has compounding benefits for CI operators regardless of any impending cyber security incidents.

### Proactive resilience for OT systems

CI Fortify supports a proactive approach to OT cyber security. Instead of reacting to cyber security incidents with a unique solution for each, CI Fortify aims to protect against cyber threats through isolation.



### Long-term stability

Teams and systems that are ready for high-risk scenarios will maintain operations and critical services in a range of contingency scenarios, including weather and safety events.

### Minimising the cost of disruption

Maintaining currency of tested isolation and rebuilding plans drastically reduces recovery time and financial loss in the event of a cyber security incident.

## Key takeaways

CI operators may initially struggle to achieve complete isolation of vital OT and enabling systems. This is dependent on how their networks are architected and implemented, their business processes and staffing levels. It is important to understand these dependencies to create a plan to maintain continuity of critical services.

It is important for CI operators to prioritise the continuation of their critical services even if this affects the delivery of non-critical services in the short term.

For assistance with planning and additional insights on how CI operators might protect the critical service(s) they provide, visit cyber.gov.au/ci-fortify.

**Disclaimer**

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.



**For more information, or to report a cyber security incident, contact us:**
cyber.gov.au | 1300 CYBER1 (1300 292 371)

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre