Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Preparing for and Responding to Cyber Security Incidents

JUNE 2020

Introduction

The Australian Cyber Security Centre (ACSC) is responsible for monitoring and responding to cyber threats targeting Australian interests. Cyber threats can result in the denial of access to, the theft of, or the destruction of information and systems. In addition to the damage done to Australia's economic wellbeing as a result of such cyber security incidents, they can undermine public confidence in organisations and consume significant resources to respond to.

The ACSC can help organisations respond to cyber security incidents. Reporting cyber security incidents ensures that the ACSC can provide timely assistance. This may be in the form of investigations, analysis and/or remediation advice.

How prepared are you to respond?

Organisations should ask themselves the following questions to determine how prepared they are to respond to cyber security incidents:

- Have we identified systems and information critical to our business operations?
- Do we have business continuity and disaster recovery plans?
- Do we have an up-to-date and regularly tested incident response plan?
- Do our agreements with service providers include cyber security incident reporting and response activities?
- Do we have the ability to detect when cyber security incidents may have occurred?
- How easily and quickly can we access appropriate resources to respond to cyber security incidents?
- What are our legislative obligations in regards to reporting cyber security incidents?
- Who has the primary responsibility for cyber security incident reporting, and do we have standard operating procedures in place?

When should I report a cyber security incident?

A cyber security incident is a single or series of unwanted or unexpected events that have a significant probability of compromising an organisation's business operations. Cyber security incidents can impact the confidentiality, integrity or availability of a system and the information that it stores, processes or communicates.

The types of cyber security incidents that should be reported to the ACSC include:

- suspicious system and network activities

- compromise of sensitive information
- unauthorised access or attempts to access a system
- emails with suspicious attachments or links
- denial-of-service attacks
- suspected tampering of electronic devices.

The following are examples of suspicious system and network activities:

- domain administrator accounts being locked out due to failed authentication attempts
- unusual authentication events on remote access systems such as users being logged in from local workstations and a VPN simultaneously or a number of log-in attempts from geographically disparate or overseas locations within a short timeframe
- service accounts communicating with internet-based infrastructure.

How do I report a cyber security incident?

Organisations are encouraged to report cyber security incidents to the ACSC. Once a cyber security incident is reported to the ACSC, it is recorded and triaged. At this time the priority and extent of assistance that is necessary to respond to the cyber security incident is determined.

Further information

The ***Australian Government Information Security Manual*** (ISM) assists in the protection of information that is processed, stored or communicated by organisations' systems. It can be found at https://www.cyber.gov.au/acsc/view-all-content/ism.

The ***Strategies to Mitigate Cyber Security Incidents*** complements the advice in the ISM. The complete list of strategies can be found at https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents.

Further information on reporting cyber security incidents can be found at https://www.cyber.gov.au/acsc/report.

Contact details

If you have any questions regarding this guidance you can contact us via 1300 CYBER1 (1300 292 371) or https://www.cyber.gov.au/acsc/contact.