Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Cyber Security Incident Response Planning: Executive Guidance

First published: September 2012
Last updated: April 2024

Introduction

The Australian Signals Directorate (ASD) 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 systems and data. 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. Reporting cyber security incidents to ASD ensures that timely assistance can be provided, if required. This may be in the form of investigations or remediation advice.

Preparing to respond to cyber security incidents

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

- Have we identified systems and data critical to our business operations?
- Do we have business continuity and disaster recovery plans?
- Do we have an up-to-date and regularly tested cyber security 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?
- Do we have a public communications plan in case of cyber security incidents?

Reporting cyber security incidents

A cyber security incident is a single or series of unwanted or unexpected cyber security 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 data that it stores, processes or communicates.

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

- suspicious privileged account lockouts
- suspicious remote access authentication events
- service accounts suspiciously communicating with internet-based infrastructure
- compromise of sensitive or classified data
- unauthorised access or attempts to access a system
- emails with suspicious attachments or links
- denial-of-service attacks
- ransomware attacks
- suspected tampering of electronic devices.

Organisations should report cyber security incidents to ASD. Once a cyber security incident is reported to ASD, 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.

Communicating cyber security incidents to customers and clients

Cyber security incidents can attract public and media interest, particularly if they compromise customer or client data, or disrupt supply of goods and services. As such, organisations should prepare for communicating publicly about cyber security incidents, including cyber security incident response activities, and plan for how they will keep customers and clients, stakeholders, and the broader public informed.

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

- Who has responsibility for producing information about the cyber security incident?
- Who has responsibility for approving the release of information about the cyber security incident?
- Who has the responsibility for communicating information about the cyber security incident?
- Do we have clear and consistent communications channels to communicate information about the cyber security incident?
- Do we have ways for the media, customers and clients, stakeholders, and the broader public to make enquiries regarding the cyber security incident (e.g. via email, telephone hotlines or social media)?

Further information

The *Information Security Manual* is a cyber security framework that organisations can apply to protect their systems and data from cyber threats. The advice in the *Strategies to Mitigate Cyber Security Incidents*, along with its Essential Eight, complements this framework.

Contact details

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).

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)

Australian Government

Australian Signals Directorate