Australian Government
Australian Signals Directorate

Australian Cyber Security Centre

Information Security Manual

Published: 02 March 2023

Guidelines for Cyber Security Incidents

Managing cyber security incidents

Cyber security events

A cyber security event is an occurrence of a system, service or network state indicating a possible breach of security policy, failure of safeguards or a previously unknown situation that may be relevant to security.

Cyber security incidents

A cyber security incident is an unwanted or unexpected cyber security event, or a series of such events, that has either compromised business operations or has a significant probability of compromising business operations.

Cyber resilience

Cyber resilience is the ability to adapt to disruptions caused by cyber security incidents while maintaining continuous business operations. This includes the ability to detect, manage and recover from cyber security incidents.

Detecting cyber security incidents

One of the core elements of detecting and investigating cyber security incidents is the availability of appropriate data sources, such as event logs. The following event logs can be used by an organisation to assist with detecting and investigating cyber security incidents:

- **Cross Domain Solutions:** May assist in identifying anomalous or malicious network traffic indicating an exploitation attempt or successful compromise.
- **Databases:** May assist in identifying anomalous or malicious application or user behaviour indicating an exploitation attempt or successful compromise.
- **Domain Name System services:** May assist in identifying attempts to resolve malicious domain names or Internet Protocol addresses indicating an exploitation attempt or successful compromise.
- **Email servers:** May assist in identifying users targeted with phishing emails thereby helping to identify the initial vector of a compromise.
- **Gateways:** May assist in identifying anomalous or malicious network traffic indicating an exploitation attempt or successful compromise.

- **Operating systems:** May assist in identifying anomalous or malicious activity indicating an exploitation attempt or successful compromise.
- **Remote access services:** May assist in identifying unusual locations of access or times of access indicating an exploitation attempt or successful compromise.
- **Security services:** May assist in identifying anomalous or malicious application or network traffic indicating an exploitation attempt or successful compromise.
- **Server applications:** May assist in identifying anomalous or malicious application behaviour indicating an exploitation attempt or successful compromise.
- **System access:** May assist in identifying anomalous or malicious user behaviour indicating an exploitation attempt or successful compromise.
- **User applications:** May assist in identifying anomalous or malicious application or user behaviour indicating an exploitation attempt or successful compromise.
- **Web applications:** May assist in identifying anomalous or malicious application or user behaviour indicating an exploitation attempt or successful compromise.
- **Web proxies:** May assist in identifying anomalous or malicious network traffic indicating an exploitation attempt or successful compromise.

Incident management policy

Establishing an incident management policy can increase the likelihood of successfully planning for, detecting and responding to malicious activity on networks and hosts, such as cyber security events and cyber security incidents. In doing so, an incident management policy will likely cover the following:

- responsibilities for planning for, detecting and responding to cyber security incidents
- resources assigned to cyber security incident planning, detection and response activities
- guidelines for triaging and responding to cyber security events and cyber security incidents.

Furthermore, as part of maintaining the incident management policy, it is important that it is, along with its associated incident response plan, exercised at least annually to ensure it remains fit for purpose.

Control: ISM-0576; Revision: 9; Updated: Dec-22; Applicability: All; Essential Eight: N/A
An incident management policy, and associated incident response plan, is developed, implemented and maintained.

Control: ISM-1784; Revision: 0; Updated: Sep-22; Applicability: All; Essential Eight: N/A
The incident management policy, including the associated incident response plan, is exercised at least annually.

Cyber security incident register

Developing, implementing and maintaining a cyber security incident register can assist with ensuring that appropriate remediation activities are undertaken in response to cyber security incidents. In addition, the types and frequency of cyber security incidents, along with the costs of any remediation activities, can be used as an input to future risk assessment activities.

Control: ISM-0125; Revision: 6; Updated: Dec-22; Applicability: All; Essential Eight: N/A
A cyber security incident register is developed, implemented and maintained.

Control: ISM-1803; Revision: 0; Updated: Dec-22; Applicability: All; Essential Eight: N/A
A cyber security incident register contains the following for each cyber security incident:

- *the date the cyber security incident occurred*

- *the date the cyber security incident was discovered*
- *a description of the cyber security incident*
- *any actions taken in response to the cyber security incident*
- *to whom the cyber security incident was reported.*

Trusted insider program

As a trusted insider's system access and knowledge of business processes often makes them harder to detect, establishing and maintaining a trusted insider program can assist an organisation to detect and respond to trusted insider threats before they occur, or limit damage if they do occur. In doing so, an organisation will likely obtain the most benefit by logging and analysing the following user activities:

- excessive copying or modification of files
- unauthorised or excessive use of removable media
- connecting devices capable of data storage to systems
- unusual system usage outside of normal business hours
- excessive data access or printing compared to their peers
- data transfers to unauthorised cloud services or webmail
- use of unauthorised Virtual Private Networks, file transfer applications or anonymity networks.

Control: ISM-1625; Revision: 1; Updated: Dec-22; Applicability: All; Essential Eight: N/A
A trusted insider program is developed, implemented and maintained.

Control: ISM-1626; Revision: 0; Updated: Nov-20; Applicability: All; Essential Eight: N/A
Legal advice is sought regarding the development and implementation of a trusted insider program.

Access to sufficient data sources and tools

Successful detection of cyber security incidents requires trained cyber security personnel with access to sufficient data sources, such as event logs, that are complemented by tools that support both manual and automated analysis. As such, it is important that during system design and development activities, functionality is added to systems to ensure that sufficient data sources can be captured and provided to cyber security personnel.

Control: ISM-0120; Revision: 5; Updated: May-20; Applicability: All; Essential Eight: N/A
Cyber security personnel have access to sufficient data sources and tools to ensure that systems can be monitored for key indicators of compromise.

Reporting cyber security incidents

Reporting cyber security incidents to an organisation's Chief Information Security Officer, or one of their delegates, as soon as possible after they occur or are discovered provides senior management with the opportunity to assess the impact to their organisation and to oversee any incident response activities. Note, an organisation should also be cognisant of any legislative obligations in regards to reporting cyber security incidents to authorities, customers or the public.

Control: ISM-0123; Revision: 3; Updated: Sep-18; Applicability: All; Essential Eight: ML3
Cyber security incidents are reported to an organisation's Chief Information Security Officer, or one of their delegates, as soon as possible after they occur or are discovered.

Reporting cyber security incidents to the ACSC

The Australian Cyber Security Centre (ACSC) uses the cyber security incident reports it receives as the basis for providing assistance to organisations. Cyber security incident reports are also used by the ACSC to identify trends and maintain an accurate threat environment picture. The ACSC utilises this understanding to assist in the development of new and updated cyber security advice, capabilities, and techniques to better prevent and respond to evolving cyber threats. An organisation is recommended to internally coordinate their reporting of cyber security incidents to the ACSC.

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

- suspicious activities, such as privileged account lockouts and unusual remote access activities
- 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 ICT equipment.

Control: ISM-0140; Revision: 6; Updated: May-19; Applicability: All; Essential Eight: ML3
Cyber security incidents are reported to the ACSC.

Further information

Further information on event logging can be found in the event logging and monitoring section of the *Guidelines for System Monitoring*.

Further information on incident response plans can be found in the system-specific security documentation section of the *Guidelines for Security Documentation*.

Further information on establishing and operating a trusted insider program can be found in the Carnegie Mellon University's Software Engineering Institute's *Common Sense Guide to Mitigating Insider Threats* publication.

Further information on reporting of cyber security incidents by service providers can be found in the managed services and cloud services section of the *Guidelines for Procurement and Outsourcing*.

Further information on reporting cybercrime incidents and reporting cyber security incidents is available from the ACSC.

Responding to cyber security incidents

Enacting incident response plans

Following a cyber security incident being identified, an organisation's incident response plan should be enacted.

Control: ISM-1819; Revision: 0; Updated: Mar-23; Applicability: All; Essential Eight: ML3
Following the identification of a cyber security incident, an organisation's incident response plan is enacted.

Handling and containing data spills

When a data spill occurs, an organisation should inform data owners and restrict access to the data. In doing so, affected systems can be powered off, have their network connectivity removed or have additional access controls applied to the data. It should be noted though that powering off systems could destroy data that would be useful for forensic investigations. Furthermore, users should be made aware of appropriate actions to take in the event of a data spill, such as not deleting, copying, printing or emailing the data.

Control: ISM-0133; Revision: 2; Updated: Jun-21; Applicability: All; Essential Eight: N/A
When a data spill occurs, data owners are advised and access to the data is restricted.

Handling and containing malicious code infections

Taking immediate remediation steps after the discovery of malicious code can minimise the time and cost spent eradicating and recovering from the infection. As a priority, all infected systems and media should be isolated to prevent the infection from spreading. Once isolated, infected systems and media can be scanned by antivirus software to potentially remove the infection or recover data. It is important to note though, a complete system restoration from a known good backup or rebuild may be the only reliable way to ensure that malicious code can be truly eradicated or data recovered.

Control: ISM-0917; Revision: 7; Updated: Oct-19; Applicability: All; Essential Eight: N/A
When malicious code is detected, the following steps are taken to handle the infection:

- *the infected systems are isolated*
- *all previously connected media used in the period leading up to the infection are scanned for signs of infection and isolated if necessary*
- *antivirus software is used to remove the infection from infected systems and media*
- *if the infection cannot be reliably removed, systems are restored from a known good backup or rebuilt.*

Handling and containing intrusions

When an intrusion is detected on a system, an organisation may wish to allow the intrusion to continue for a short period of time in order to fully understand the extent of the compromise and to assist with planning intrusion remediation activities. However, an organisation allowing an intrusion to continue in order to collect data or evidence should first establish with their legal advisors whether such activities would be breaching the *Telecommunications (Interception and Access) Act 1979*.

To increase the likelihood of intrusion remediation activities successfully removing an adversary from their system, an organisation can take preventative measures to ensure the adversary has limited forewarning and awareness of planned intrusion remediation activities. Specifically, using an alternative system to plan and coordinate intrusion remediation activities will prevent alerting the adversary if they have already compromised email, messaging or collaboration services. In addition, conducting intrusion remediation activities in a coordinated manner during the same planned outage will prevent forewarning the adversary, thereby depriving them of sufficient time to establish alternative access points or persistence methods on the system.

Following intrusion remediation activities, an organisation should determine whether the adversary has been successfully removed from the system, including whether or not they have since reacquired access. This can be achieved, in part, by capturing and analysing network traffic for at least seven days following remediation activities.

Control: ISM-0137; Revision: 4; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Legal advice is sought before allowing intrusion activity to continue on a system for the purpose of collecting further data or evidence.

Control: ISM-1609; Revision: 2; Updated: Dec-21; Applicability: All; Essential Eight: N/A
System owners are consulted before allowing intrusion activity to continue on a system for the purpose of collecting further data or evidence.

Control: ISM-1731; Revision: 0; Updated: Dec-21; Applicability: All; Essential Eight: N/A

Planning and coordination of intrusion remediation activities are conducted on a separate system to that which has been compromised.

Control: ISM-1732; Revision: 0; Updated: Dec-21; Applicability: All; Essential Eight: N/A
To the extent possible, all intrusion remediation activities are conducted in a coordinated manner during the same planned outage.

Control: ISM-1213; Revision: 2; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Following intrusion remediation activities, full network traffic is captured for at least seven days and analysed to determine whether the adversary has been successfully removed from the system.

Maintaining the integrity of evidence

When gathering evidence following a cyber security incident, it is important that it is gathered in an appropriate manner and that its integrity is maintained. In addition, if the ACSC is requested to assist with investigations, no actions which could affect the integrity of evidence should be carried out before the ACSC becomes involved.

Control: ISM-0138; Revision: 5; Updated: Mar-23; Applicability: All; Essential Eight: N/A
The integrity of evidence gathered during an investigation is maintained by investigators:

- *recording all of their actions*
- *maintaining a proper chain of custody*
- *following all instructions provided by relevant law enforcement agencies.*

Further information

Further information on incident response plans can be found in the system-specific security documentation section of the *Guidelines for Security Documentation*.

Further information on handling malicious code infections can be found in National Institute of Standards and Technology Special Publication 800-61 Rev. 2, *Computer Security Incident Handling Guide*.