



Information Security Manual

DECEMBER 2021

Guidelines for Cyber Security Incidents

Detecting 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 have 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. Fortunately, many data sources can be extracted from existing systems without requiring specialised capabilities.

The following table describes some of the data sources that organisations can use for detecting and investigating cyber security incidents.

Data Source	Description
Domain Name System logs	Can assist in identifying attempts to resolve malicious domains or Internet Protocol addresses which can indicate an exploitation attempt or successful compromise.
Email server logs	Can assist in identifying users targeted with spear-phishing emails. Can also assist in identifying the initial vector of a compromise.

Operating system event logs	Can assist in tracking process execution, file/registry/network activity, authentication events, operating system created security alerts and other activity.
Security product logs	Can assist in the identification of anomalous or malicious activity which can indicate an exploitation attempt or successful compromise.
Virtual Private Network and remote access logs	Can assist in identifying unusual source addresses, times of access and logon/logoff times associated with malicious activity.
Web proxy logs	Can assist in identifying Hypertext Transfer Protocol-based vectors and malware communication traffic.

Intrusion detection and prevention policy

Establishing an intrusion detection and prevention policy can increase the likelihood of detecting, and subsequently preventing, malicious activity on networks and hosts. In doing so, an intrusion detection and prevention policy will likely cover the following:

- methods of network-based intrusion detection and prevention used
- methods of host-based intrusion detection and prevention used
- guidelines for reporting and responding to detected intrusions
- resources assigned to intrusion detection and prevention activities.

Security Control: 0576; Revision: 7; Updated: Aug-19; Applicability: All

An intrusion detection and prevention policy is developed and implemented.

Trusted insider program

As a trusted insider's system access and knowledge of business processes often makes them harder to detect, establishing a trusted insider program can assist organisations to detect and respond to trusted insider threats before they occur, or limit damage if they do occur. In doing so, organisations 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 (e.g. mobile devices and digital cameras)
- 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.

Security Control: 1625; Revision: 0; Updated: Nov-20; Applicability: All

A trusted insider program is developed and implemented.

Security Control: 1626; Revision: 0; Updated: Nov-20; Applicability: All

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 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.

Security Control: 0120; Revision: 5; Updated: May-20; Applicability: All

Cyber security personnel have access to sufficient data sources and tools to ensure that systems can be monitored for key indicators of compromise.

Further information

Further information on detecting cyber security incidents can be found in the event logging and auditing section of the [Guidelines for System Monitoring](#).

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.

Managing cyber security incidents

Cyber security incident register

Recording cyber security incidents in a register can assist with ensuring that appropriate remediation activities are undertaken. In addition, information such as 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.

Security Control: 0125; Revision: 5; Updated: Jun-21; Applicability: All

A cyber security incident register is maintained that covers the following:

- *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.*

Handling and containing data spills

When a data spill occurs, organisations 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.

Security Control: 0133; Revision: 2; Updated: Jun-21; Applicability: All

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.

Security Control: 0917; Revision: 7; Updated: Oct-19; Applicability: All

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, organisations 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. Organisations allowing an intrusion to continue should first establish with their legal advisors whether any actions, such as collecting further data or evidence, 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, organisations 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, 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.

Security Control: 0137; Revision: 4; Updated: Dec-21; Applicability: All

Legal advice is sought before allowing intrusion activity to continue on a system for the purpose of collecting further data or evidence.

Security Control: 1609; Revision: 2; Updated: Dec-21; Applicability: All

System owners are consulted before allowing intrusion activity to continue on a system for the purpose of collecting further data or evidence.

Security Control: 1731; Revision: 0; Updated: Dec-21; Applicability: All

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

Security Control: 1732; Revision: 0; Updated: Dec-21; Applicability: All

To the extent possible, all intrusion remediation activities are conducted in a coordinated manner during the same planned outage.

Security Control: 1213; Revision: 2; Updated: Dec-21; Applicability: All

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.

Integrity of evidence

When gathering evidence following a cyber security incident, it is important that its integrity is maintained. Even though an investigation may not directly lead to a prosecution, it is important that the integrity of evidence, such as manual logs, automatic audit trails and intrusion detection tool outputs, be protected.

If the Australian Cyber Security Centre (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.

Security Control: 0138; Revision: 4; Updated: Aug-20; Applicability: All

The integrity of evidence gathered during an investigation is maintained by investigators:

- *recording all of their actions*
- *creating checksums for all evidence*
- *copying evidence onto media for archiving*
- *maintaining a proper chain of custody.*

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 event logging, including retention periods, can be found in the event logging and auditing section of the [Guidelines for System Monitoring](#).

Further information on handling and managing data spills can be found in the ACSC's [Data Spill Management Guide](#) publication.

Reporting cyber security incidents

Reporting cyber security incidents

Reporting cyber security incidents, including unplanned outages, to an organisation's Chief Information Security Officer (CISO), 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 take remediation actions if necessary. In doing so, organisations should be cognisant of any legislative obligations in regards to reporting cyber security incidents to authorities, customers or the public.

Security Control: 0123; Revision: 3; Updated: Sep-18; Applicability: All

Cyber security incidents are reported to an organisation's CISO, or one of their delegates, as soon as possible after they occur or are discovered.

Security Control: 0141; Revision: 5; Updated: Dec-21; Applicability: All

Service providers report cyber security incidents to their customer's CISO, or one of their delegates, as soon as possible after they occur or are discovered.

Security Control: 1433; Revision: 3; Updated: Dec-21; Applicability: All

Service providers and their customers maintain 24/7 contact details for each other, including additional out-of-band contact details for when normal communication channels fail, in order to report cyber security incidents.

Reporting cyber security incidents to the ACSC

The 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. Organisations are 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 (e.g. domain administrator 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 or mobile devices.

*Security Control: 0140; Revision: 6; Updated: May-19; Applicability: All
Cyber security incidents are reported to the ACSC.*

Further information

Further information on [reporting cyber security incidents](#) is available from the ACSC.