Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre

# How the ACSC can help during a cyber security incident

cyber.gov.au

# Table of contents

# Supporting Australian organisations

The Australian Signal's Directorate's (ASD) Australian Cyber Security Centre's (ACSC) incident management capabilities provide technical incident response advice and assistance to Australian organisations that have been impacted, or may be impacted by a cyber security incident.

This publication is intended for those individuals who may lead an organisation's incident response, and provides guidance on:

- Reporting a cyber security incident to the ACSC
  - What types of cyber security incidents should you report to the ACSC?
  - What happens when you report?
  - What further involvement you can expect from ACSC?
  - What if you are contacted by the ACSC?
  - How does reporting your incident helps others?
- The ACSC's role in whole of government cyber security incident response
- Becoming an ACSC Partner

# Reporting a cyber security incident to the ACSC

## What types of cyber security incidents should you report to the ACSC?

Cyber security incidents[1] can be reported to the ACSC via ReportCyber at www.cyber.gov.au/report, or the Australian Cyber Security Centre Hotline on 1300 CYBER1 (1300 292 371).

Types of incidents you should report include, but are not limited to:

- Denial of service (DoS)
- Scanning and reconnaissance
- Intentional or malicious unauthorised access to network or device
- Data exposure, theft or leak
- Malicious code/malware
- Ransomware

[1] A cyber security incident is a single or series of unwanted or unexpected event(s) that impact the confidentiality, integrity or availability of a network or system or the information that it stores, processes or communicates.

- Phishing/spear-phishing (e.g. successful instances, those that may be part of a campaign, or originated from a compromised legitimate business email)
- Any other irregular cyber activity that causes concern.

Timeliness is an important factor when managing a cyber security incident, so the earlier you report the better. The ACSC recommends that you report a potential incident as soon as it's detected even if you suspect it to be a false alarm.

## What happens when you report?

When you report, the ACSC will seek to establish the nature of the malicious cyber activity that has impacted your organisation. If you request support from the ACSC, we will provide you with immediate advice and assistance which may include:

- information on how to contain and remediate the incident
- intelligence and advisory products to assist you with your incident response
- linking you to Australian Government entities that may further support your response.

### What the ACSC may need from you when you report

The ACSC is here to help your organisation respond to the technical aspects of the incident. To do so, the ACSC may request that you share, where available, evidence of malicious activity. This can include:

- Logs
- Memory dumps
- Disk images
- Network traffic captures
- Network diagrams/documentation
- Indicators of compromise
- Samples of malware
- Other analysis or reporting products.

The ACSC can also discuss possible tools to assist with provision of these artefacts, along with a secure means to transfer them to the ACSC.

While these requests can seem resource intensive, the more information you can pass to the ACSC in a timely manner, the more effective our support to you will be. Remember that your reporting is crucial in helping protect others from cyber threats, and reports from other organisations can in turn help protect you.

## Other questions the ACSC may ask

- Has there been an impact on business activities, provision of services, impact on clients, potential loss of data?
- Do you have a Cyber Incident Response Plan? Has this been implemented? And can this be shared?
- Who has primary responsibility for incident response in your organisation? What are their contact details?
- Do you have an up-to-date after-hours contact list for key personnel and external stakeholders?
- Are procedures in place to provide information and reporting to relevant parties during an incident?
- Do you have technical resources (including an incident response provider) readily available to investigate and mitigate an incident? Can you provide their contact details?
- What actions have been taken so far, why and how have you recorded this? What steps have been taken to contain the threat? Is the threat actor still on your systems?
- Do you have the ability to identify and isolate an affected workstation or system?
- What are your next steps for investigating and mediating this incident?

## What further involvement can you expect from the ACSC?

Following the immediate incident response advice and assistance provided by the ACSC, we can also provide more hands-on assistance including: The ACSC may:

- triage the incident to determine if there are more detailed actions to be undertaken. This could involve further communication with your organisation, understanding impact to the organisation, facilitating cyber threat intelligence and and analysing indicators of compromise.
- If it assesses the incident is likely to cause significant impact to Australia or involves a sophisticated malicious actor, offer a more detailed approach that could include:
  - An incident response resource to support your investigation
  - A team of digital forensics specialists to support a comprehensive technical investigation
  - Guidance on approaching public communications.
- work alongside you to liaise and coordinate technical briefings with other government agencies or industry partners to support your response. This could include the federal/state/territory government chief information security officers, federal law enforcement and international cyber partners. Although the ACSC coordinates these briefings, it does not equal ACSC endorsement of system hygiene or assurance.
- Once the incident investigation is complete, depending on the responses provided, the ACSC may provide your organisation with information and reports to help you finalise your investigation.
- introduce you to different areas within the ACSC for additional support such as cyber resilience uplift activities, and if requested, assist you on how to contact the Department of Home Affairs or Australian Federal Police.

## Working with your commercial incident response provider

Where an organisation has engaged the services of an incident response provider, the ACSC will work collaboratively with them to establish the full nature and extent of your incident. This collective approach to sharing technical expertise, threat intelligence and capabilities strengthens and provides a more comprehensive investigation into the activity on your organisation's network.

The success of this collaboration however, relies on your organisation's authorisation to share information between the ACSC and your incident response provider.

## What if you are contacted by the ACSC?

In some cases, the ACSC may notify you of a vulnerability, potential compromise or a confirmed compromise. Where possible we will provide you with this information, which is obtained through numerous trusted sources, or as a result of our own monitoring of the cyber threat environment. Our information may include:

- indicators of compromise
- compromised credentials
- ransomware precursor activity (i.e. from detection of malware or spear phishing activity)
- interactions between malicious infrastructure and Australian networks or devices

If you are an ACSC Partner, ensure your contact details are up to date and you've registered "out of hours" contact details so we can contact you quickly.

## Not sure if you're talking to a genuine ACSC representative?

If you're contacted by the ACSC, we will provide you with an incident/reference number. If you are concerned about the legitimacy of a call from the ACSC, you can verify that you are speaking to a genuine ACSC representative by calling the Australian Cyber Security Hotline (1300CYBER1) and quoting your incident/reference number.

## How does reporting your incident help others?

One of the ACSC's key strengths is our ability to aggregate and analyse information to produce a national cyber threat picture. We draw upon information gathered through ASD intelligence sources and crucially, the information provided by organisations and entities impacted by cyber incidents in Australia.

We use this understanding to assist with developing new and updated cyber security advice, capabilities, and techniques to better prevent and respond to evolving cyber threats. For example, anonymised information from your incident may be used to produce public communication products to help build whole of economy cyber resilience.

Products could include:

- Advisories published on the ACSC Partner Portal
- Alerts published on cyber.gov.au
- Quarterly Trends and Insights reports
- The ASD Annual Cyber Threat Report

Some anonymised technical details, such as indicators of compromise can also be shared via our Cyber Threat Intelligence Shared (CTIS) platform.

### How the ACSC protects your privacy

The ACSC is subject to rules to protect the privacy of Australians under the *Intelligence Services Act 2001*. The ACSC's staff are also trained to manage sensitive data, and adhere to principles of confidentiality and data protection.

# The ACSC's role in whole of government cyber security incident response

The ACSC is the Commonwealth lead for technical cyber incident response and advice for cyber security incidents. We also work closely with other partners including the National Cyber Security Coordinator and the Cyber Security Response Coordination Unit (CSRCU) within the Department of Home Affairs.

## Data on the Dark web

As a result of a cyber security incident, if data has been exfiltrated from your system or your data has been released, who will support you?

- The ACSC will support you in containing the initial compromise.
- The Australian Federal Police (AFP) will support you through a criminal investigation into the perpetrator of the cybercrime.
- The Department of Home Affairs, through the CSRCU can support you to manage the consequences[2] to other Australian organisations as a result of the leaked data.
- The National Cyber Security Coordinator leads the coordination of responses to major cyber security incidents, including bringing together expertise and resources from across government and security agencies.

Remember, the ACSC is not a regulator. We will only use the information you provide for cyber security purposes.

Providing information to us may not in itself meet the regulatory obligations that you may have with the Australian Government, except for your mandatory obligation to report cyber security incidents in accordance with s30BC and/or s30BD of the *Security of Critical Infrastructure Act 2018*. More information on reporting and compliance, including Mandatory Cyber Incident Reporting, can be found on the Cyber and Infrastructure Security Centre's website: https://www.cisc.gov.au/compliance-and-reporting/overview.

Similarly, while the ACSC is not a law enforcement agency, we work closely with the AFP Cyber Command under the standing joint counter cybercrime Operation Aquila. If you refer your incident to the AFP for criminal investigation, we can work collaboratively with the AFP to support your investigation. ACSC can also assist you in engaging AFP Cyber Command support.

[2] Consequence management relates to the second and subsequent order effects from cyber security incidents. It requires government and industry to work together to identify and mitigate the secondary harms that may result from a cyber incident.

# Becoming an ACSC Partner

As an ACSC Network Partner you may be provided access to:

- threat intelligence, news and advice to enhance situational awareness
- collaboration opportunities
- resilience-building activities (e.g. exercises, discussions, workshops)
- the ACSC State and Territory network.

Review and apply the ACSC advice alerts, advisories, Partner Portal products at cyber.gov.au.

Sign up for the ACSC's free cyber security services to reduce your exposure to threats–connect with ACSC through a click of a link on the Partner Portal at cyber.gov.au.