Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Data Spill Management Guide

First published: August 2012
Last updated: October 2021

Introduction

A data spill is the accidental or deliberate exposure of data into an uncontrolled or unauthorised environment, or to persons without a need-to-know. A data spill is sometimes referred to as data breach or a data leak.

Data spills usually fall into one of two categories:

- The transfer of data to a system which is not authorised to handle the data. Such a transfer may be performed via email or digital media.
- The unauthorised disclosure of data on the internet, including via web forums, social media and other types of cloud-based storage.

Data spills are considered cyber security incidents and should be reported to the Australian Cyber Security Centre (ACSC).

Data spill management overview

Educating users of system and web usage policies, as well as how to appropriately identify and handle data, can greatly assist in preventing data spills. However, in the event of a data spill, organisations should use the following five step process:

- **Identify:** Recognise that a data spill has taken place.
- **Contain:** Determine the breadth of the data spill.
- **Assess:** Decide on the most appropriate course of action to address the data spill.
- **Remediate:** Remediate the data spill based on the course of action chosen.
- **Prevent:** Implement prevention measures to stop similar incidents from occurring in the future.

Step 1: Identify

Data spills are usually identified by users. Organisations should include in standard procedures for all users that they notify an appropriate security contact of any suspected data spill or access to data that they are not authorised to access.

Data spills can also be identified through monitoring, auditing and logging. For example:

- Preventing non-protectively marked emails from being sent or received by an organisation's email server or email client.

- Using data loss prevention tools that can warn users and alert administrators of possible security violations.

An immediate assessment should be performed to:

- Track data flow, movement and storage locations of the spilled data to assist in determining what devices and systems are affected.
- Identify affected system users, including any external to the organisation.
- Determine the length of time between the data spill and the identification of the data spill.

Step 2: Contain

Containment may involve physically isolating or logically separating affected systems from a network. Logical separation can be achieved by temporarily removing software functionality or applying access controls to systems to prevent further exposure.

For example, the containment process taken for a data spill involving an internal email may include:

- Identifying the sender and recipients of the email, contacting them and directing them not to forward or access the email.
- Determining if it is necessary to retain a copy of the email so that the sensitivity of the data can be verified by the data owners for a damage assessment.
- Determining if it is necessary to delete the email from affected users' inboxes as quickly as possible to prevent further dissemination of the email.
- Proceeding to the assessment phase to determine what further actions are required, including potential sanitisation of the email server and workstations.

Step 3: Assess

After containment, to prevent further access and exposure of spilled data, a thorough assessment should be performed. This includes:

- Identifying affected system users, systems and devices. While the identification process highlights the systems and users that are initially affected, a more thorough assessment should be performed after the containment process. This should include devices such as workstations, backup storage, printers, print servers, network shares, email inbox and servers, content filtering appliances, webmail and external systems. Organisations should involve their system and network administrators in this process.
- Contacting the data owners and relevant authorities. The data owners should be contacted and notified of the data spill. The data owners should be able to provide guidance on any specific handling requirements for the data, if applicable, to minimise its exposure.
- Performing a damage assessment. Organisations should perform a damage assessment to determine what harm was caused by the data spill. Organisations should assume that the spilled data is compromised and base remediation procedures or risk management on a worst-case scenario.

Step 4: Remediate

Organisations should work in collaboration with data owners to determine a satisfactory remediation of any data spill noting remediation is usually achieved through a balance of technical controls and risk management activities.

For each system identified during the assessment stage, a remediation strategy should be developed that covers:

- access controls to the data and the systems that hold the data
- utilisation rate of memory storage (i.e. ability for the system to naturally overwrite free space through data attrition and growth)
- criticality of the system to the business (e.g. mission critical Storage Area Network or a user workstation)
- the exposure duration of data (i.e. is it a recent exposure or has the data been exposed for a long period of time)
- sanitisation options available for the media (e.g. raw disk overwrite, file overwrite or physical destruction)
- disposal consideration of the asset at end of life (i.e. will the asset be resold or physically destroyed)
- balancing the risk of drawing attention to the data versus accepting the damage
- resources, impacts and financial costs to replace or sanitise affected systems.

All remediation actions, including their outcomes, should be appropriately documented.

Step 5: Prevent

Actions that cause data spills should be reviewed to determine why they occurred (e.g. non-adherence of policy, gaps in existing procedures or absence of a technical control).

The review should result in the implementation of preventative measures to reduce the likelihood of future data spills occurring. This may include additional user training or improved technical controls.

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).