STEPS TO ADDRESS DATA SPILLAGE IN THE CLOUD

SEPTEMBER 2019 **ITSAP.50.112**

This document outlines the steps that your organization should follow if data spillage occurs when using cloud services.

Data spillage occurs when sensitive information is placed on information systems that are not authorized to process or store the information or when data is made available to an unauthorized individual. For example, a spill occurs if secret data is transferred or made available on an unclassified network.

STEP ONE: IDENTIFY

A data spill can be identified by the originator of the spill, the recipient of the information, a monitoring system, or other personnel. When using cloud services, your organization retains legal responsibility for your data. Cloud service providers (CSPs) do not manage customer data unless contracted to do so. Additionally, CSPs do not determine data sensitivity. Therefore, your organization is better suited to analyze the impact of the spill.

To triage the resulting damage, the identifier of the spill needs to do an initial assessment.

- What information was compromised?
- Who was the information sent to?
- Where did the information come from?
- Where was the information moved to?
- When did the spill occur?
- How was the information moved (e.g. USB, email)?

STEP TWO: CONTAIN

Use available platform functions to contain the spill as soon as it is identified. For example, delete the affected files and any known copies off of your system. For spilled information that is in an email, recall the message if possible. For all forms of data, including email, contact the recipients and direct them not to forward or access the data. Ask all recipients to delete the spilled information from their environments and empty their recycle bins.

Containing data spillages on cloud services can be challenging for two reasons:

1. You may not be able to verify that all traces of the spilled data have been removed after the clean-up.
2. You cannot verify whether the data has actually been compromised or not once it has been spilled.

STEP THREE: ALERT

Contact your IT service desk to report a spill. If assigned as the remediation authority, the IT service desk can triage the incident following your organization's security incident management process. If the IT service desk is not the remediation authority, the IT service desk will assign the incident to the remediation authority to manage. Provide all information from steps one and two and ensure you understand your responsibilities for correcting the incident. If your organization does not have an IT service desk, ask your management chain to help you determine the appropriate authority.

Use only a secure communication method to contact a CSP. If included in the service agreement, ensure that cleared CSP personnel have found and deleted all possible copies of the data. Unless you have both a secure communications method and cleared CSP personnel in place, speak to your manager to determine whether the CSP should be contacted for assistance (benefits verses risks).

ADDITIONAL CONTACT INFORMATION

Regardless of the type of breach, your management chain must be made aware of the incident and its progress so that they can support and direct the remediation effort and respond to questions as required.

Government of Canada (GC) departments: Report serious breaches to the Canadian Centre for Cyber Security at 1-833-CYBER-88 (1-833-292-3788). When reporting a breach, follow your organization's incident response procedures and the GC Cyber Security Event Management Plan (GC CSEMP).

Critical infrastructure sectors: Report breaches to the Canadian Centre for Cyber Security at 1-833-CYBER-88 (1-833-292-3788). Refer to Public Safety's *Fundamentals of Cyber Security for Canada's CI community* for more information.

Privacy: If a data spill impacts, or potentially impacts, the privacy of Canadians, report the spill to the Office of the Privacy Commissioner (OPC) at priv.gc.ca.

STEP FOUR: REMEDIATE

Your organization should identify a remediation authority who investigates and corrects the spill. Corrective measures vary, depending on the data classification, the extent of the breach, the impacted hardware, and the use of cloud services.

The remediation authority also coordinates corrective measures with all stakeholders, including the CSP and any external organizations that are involved. These external organizations may have their own procedures and priorities for addressing data spills. The remediation authority is responsible for ensuring that stakeholders are informed on the progress of all corrective measures.

To remediate a spill in the cloud, the remediation authority should do as many of the following actions as applicable:

- Work with the CSP to contain the spill.
  - You need a service agreement and a secure communication method in place first.
- Use platform functions to clean up the spill (e.g. remove tags or pointers, crypto-shred).
  - You might not need to contact the CSP if the available platform functions are sufficient. Notifying the CSP may also alert unauthorized individuals who can access the data.
  - You cannot always guarantee the complete removal of data because it may be replicated across multiple vendor sites.
  - You may use automated corrective procedures to purge the leftover data from the system.
- Recall, destroy, and replace any affected mobile devices, servers, or a portion of the cloud tenant space that contain spilled data by using crypto-shredding, if necessary.

NOTE: Ensure senior management accepts the risks associated with the selected remediation plan.

You organization's information management policies and procedures are critical in preventing data spillage. These policies and procedures include marking all documents with the correct security classifications and other protection markings, using cross-domain tools to transfer data securely, and for moving data within systems and across domains according to established procedures.

LEARN MORE

The guidance in this document adheres to *ITSP.40.006 V2 IT Media Sanitization,* which provides advice on properly disposing of IT media. Proper disposal reduces the risk of threat actors exploiting residual data that is left on IT equipment with electronic memory or data storage media. This advice is applicable when considering data spillages using cloud services.

Need help or have questions? Want to stay up to date and find out more on all things cyber security? Come visit us at Canadian Centre for Cyber Security (CCCS) at **cyber.gc.ca**