Data Breach Playbook

CyberAlberta

March 13, 2024

Contact Information:
Cybersecurity Division
Technology and Innovation
5th floor, Terrace Building
9515 – 107 ST NW
Edmonton, AB T5K 2C1

Published by:
Technology and Innovation, Cybersecurity Division

CYBER ALBERTA

Preface

This document is a generic playbook based on the Government of Alberta's data breach standard operating procedure. You can use this document to construct your own organization's data breach playbook or process. References to internal teams or policy instruments have been encapsulated in brackets ("< >"). These should be replaced with information specific to your organization. For more information, please contact the CyberAlberta general mailbox:

CyberAlberta Support
cyberalberta@gov.ab.ca

Anyone who observes a breach of data should immediately report it to <your help desk or IT service desk>, per the <your organization's Security Incident Response Process>, where the incident will be tracked and managed.

Note: This page can be excluded or re-written to be a preface tailored to your organization.

Effective Date

This publication takes effect on March 16, 2024.

Approved by: Martin Dinel	**Owner:** CyberAlberta (Martin Dinel, ADM)	
Approval date: 16-02-2024	**Reviewed date:** 16-03-2024	**Next review date:** 16-03-2025
Contact: Martin Dinel, ADM for the Cybersecurity Division Email: martin.dinel@gov.ab.ca	**Policy Instrument type:** Playbook	

Table of Contents

Overview

A **data breach** is a security violation, in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen, altered or used by an individual unauthorized to do so. Other terms are unintentional information disclosure, data leak, information leakage and data spill. Incidents range from concerted attacks by individuals who hack for personal gain or malice (black hats), organized crime, political activists or national governments, to poorly configured system security or careless disposal of used computer equipment or data storage media. Leaked information can range from matters compromising national security, to information on actions which a government or official considers embarrassing and wants to conceal. A deliberate data breach by a person privy to the information, typically for political purposes, is more often described as a "leak".

Data breach differs from **data loss** in that a data breach involves a loss of confidentially of sensitive data to unauthorized persons, whereas a data loss simply means that data has been destroyed without authorization.

Data breaches may involve financial information such as credit card and debit card details, bank details, personal health information (PHI), personally identifiable information (PII), trade secrets of corporations or intellectual property. Data breaches may involve overexposed and vulnerable unstructured data – files, documents, and sensitive information.

Data breaches can be quite costly to organizations with direct costs (remediation, investigation, etc.) and indirect costs (reputational damages, providing cyber security to victims of compromised data, etc.).

A Data Breach Playbook serves as a comprehensive guide to effectively respond to potential data loss incidents within our organization. This playbook can be used as a template which outlines the steps and procedures that the incident response team must follow to detect, assess, contain, and mitigate data loss events promptly and minimize their impact on sensitive information.

The primary objective of this playbook is to safeguard the organization's sensitive data, including intellectual property, customer information, and confidential documents, from unauthorized access, exfiltration, or accidental exposure. By having a well-structured data loss incident response process, we aim to minimize financial losses, maintain the trust of our stakeholders, and comply with applicable data protection regulations.

This document outlines the steps to take when affected by a data breach incident. It is broken down into three phases:

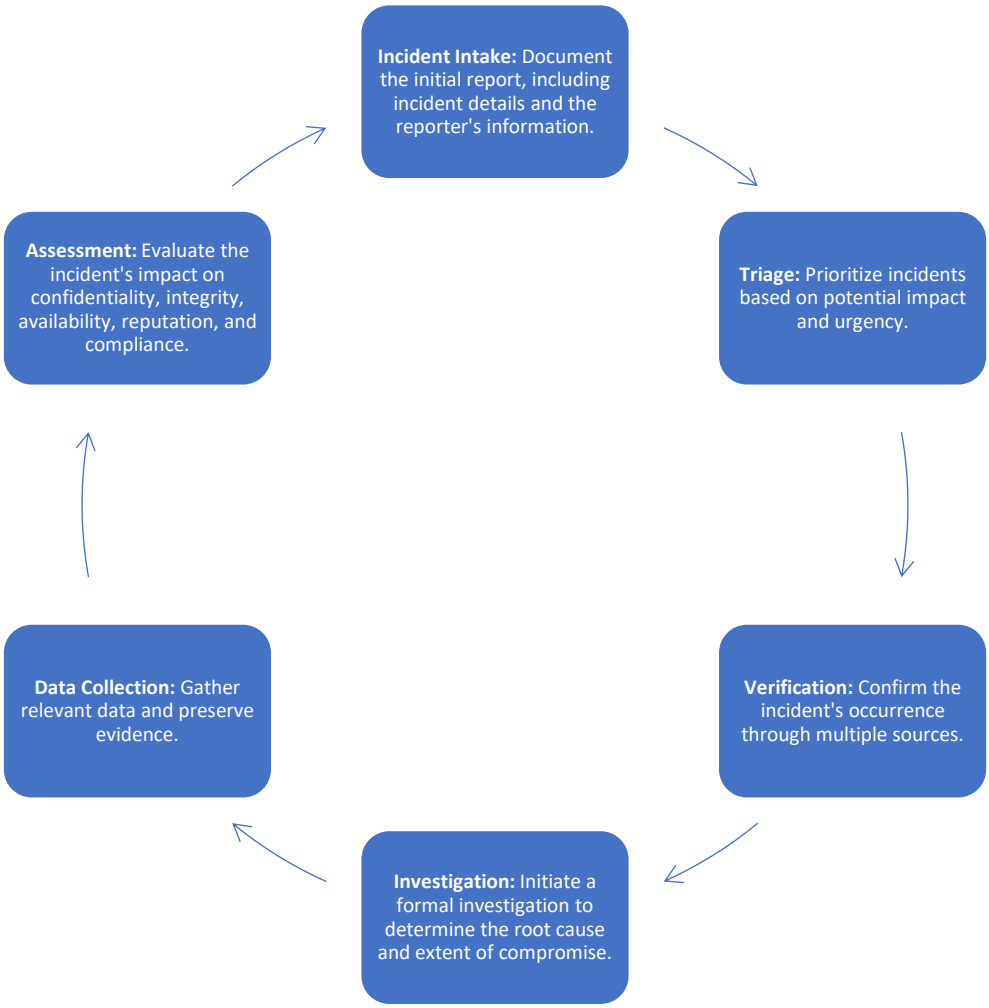
1. Assessment
2. Response
3. Post-Incident

If you have experienced a data loss incident and need advice and guidance on how to recover jump to the Assessment Phase and report the data loss incident to <your Service Desk> at <phone number or contact information>.

For more information on data loss incidents or other cybersecurity-related topics please email <your cybersecurity department mailbox>

Assessment

Verifying reported incidents and assessing their potential impact on the organization is a critical part of the incident response process. It involves a systematic approach to gather information, analyze data, and make informed decisions about the nature and severity of the reported incident. Below is a guide on accomplishing this.



Once a data breach incident has been reported, it enters the assessment phase. Key activities that occur during the assessment phase include, but are not limited, to the following:

Activity	Actions
1	☐ Determine the legitimacy of the data breach (e.g., is it genuine? Is confidentially breached, where was it located)
2	☐ Notify leadership within your organization accordingly based on severity
3	☐ Mobilize cybersecurity incident response team to determine the scope of the data loss. This initial investigation will include the following steps: ○ determine whether data loss or data breach has occurred; ○ determine the preliminary business impact;

Activity	Actions
	○ determine how the cyber incident was reported; ○ determine the initial number of affected assets across the organization; ○ identify the attack email or ingress point; ○ identify indicators of compromise; ○ examine additional reporting relating to affected assets, including AV logs, system event logs, and network monitoring logs; ○ research threat Intelligence sources to gain further intelligence and support mitigation by others; & ○ note any current action(s) being undertaken.

Essential communications during the assessment phase of a data loss incident can include:

Timing	From	To	General Message
After initial investigation and confirmation of data loss incident	Cybersecurity	Senior Management Corporate Communication Canadian Centre for Cybersecurity (CCCS) Local Law Enforcement CyberAlberta (Recommended)	Confirmation of incident and extent of incident, as well as high level plan to resolve the incident. It is important to also notify CCCS so that they are aware of the issue. They may provide assistance depending on the severity of the incident and will ensure that other Canadian organizations are alerted to potential related attacks. Intentional destruction of data is a crime and just as any other crimes, the information should also be reported to law enforcement. Consider identifying a contact for your Corporate Communications team who can facilitate reviews and approvals. CyberAlberta may be able to provide assistance, as well as reach out to COI members to warn of potential attacks.
If a privacy breach is suspected	Cybersecurity	Office of the Information Privacy Commissioner (OIPC)	Communicate incident details and evidences suggesting that this may result in a privacy incident. Provide details as to the records and individuals whose data might be compromised.
In response to multiple public concerns or media inquiries	Communications	Public	High-level messaging noting that service impacts are being investigated and thanking clients for their understanding. At this stage, public communications should remain reactive. Avoid sharing undetermined information, including details about the potential attack and restoration timelines. Messaging should be approved by appropriate members of cybersecurity and leadership. Responding to public comments can help control the narrative and reduce speculation.

Response

There are several key activities to the response phase when dealing with a data loss incident, with the main goal being to recover from the incident in the least amount of time possible.

Key activities of responding to a data breach incident include:

Activity	Actions
1	☐ If your organization has a forensics team, the internal forensic team should be contacted immediately upon detecting a data breach incident within the organization
2	☐ Isolate all affected systems or accounts from the infrastructure through removal from the network or application of strict access controls, to prevent further data exfiltration. ☐ Implement rules to block detected suspicious traffic leaving the network.
3	☐ Review the impact of the data breach based on the sensitivity of the data.
4	☐ Identify any data impacted by the data breach incident, including data-in-transit. Data owners and the business should be engaged to understand the business impact of the compromised data
5	☐ Initiate contacting administration of any external platform that is now hosting copies of the breached data ☐ Remotely erase any lost or stolen assets where possible.
6	☐ Provide an interim incident report to the service owners of the affected system(s).
7	☐ Preserve any compromised assets or copies, if possible, for future analysis including forensic investigation.
8	☐ Incorporate technical and business analysis in developing a prioritized remediation plan which includes a communication strategy.
9	☐ If malicious, suspend confirmed and suspected compromised accounts.
10	☐ If malicious, reduce any further malicious activity by quarantining affected systems (either using manual or automatic means) and removing them from the network, where possible, or applying access controls to isolate them from production networks. Business data owner(s) and stakeholders should be kept abreast of the progress of containment activities. ☐ The scope of containment can be defined by searching for the: ○ SHA-1 process name; ○ executable file name; & ○ URL or IP address of similar connections on the network. ☐ Protection measures derived from the results of malicious code analysis to protect infrastructure from the malicious code and other malware that may attempt to infect using the same mechanism should also be developed at this time.
11	☐ Conduct a restoration of any compromised systems from a trusted and tested backup. The priority of recovery of these systems will be based on business impact analysis and business criticality.
12	☐ The systems/ devices that have been affected should be re-imaged. This includes, at a minimum the following: ○ Re-install any standalone systems from a clean Operating System (OS) backup before updating with trusted data back-ups.

Activity	Actions
	○ Reset the credentials of all compromised system(s) and users' account details if applicable. ☐ Coordinate the implementation of any necessary patches or vulnerability remediation activities.
13	☐ Once the data or system(s) have been restored and re-imaged the restoration of service can begin. Activities involved in this step include, but are not limited to: ○ Complete malware scanning of environment systems, if applicable. ○ Reintegrate previously compromised systems. ○ Restore any corrupted or destroyed data. ○ Restore any suspended services. ○ Continue to monitor for signatures and other indicators of compromise to prevent the malware attack from re-emerging. ○ Confirm policy compliance across the organization.

Essential stakeholder communications during the response phase of a data breach incident include:

Timing	From	To	General Message
After initial assessment is completed and initial communication occurred	Cybersecurity	Forensics Team IT Support Teams Leadership	Notify Forensics team to preserve any evidence as required for root cause analysis. IT support teams (namely, server, storage and/or back-up teams) to resolve encrypted files. Leadership should be provided a high-level resolution plan.
Routinely according to the impact and urgency to restore the data	Cybersecurity	Leadership	Leadership should retrieve routine status updates.
After the initial impact has been assessed	Cybersecurity	Communications Team	If your organization has a communications team, they may be able to support stakeholder, internal, and public communications. Ensure communications is aware of high-level updates, as they may impact messaging. Public communications materials and approach should be approved by appropriate members of cybersecurity and leadership.
After privacy impacts have been discovered	Cybersecurity	Privacy Team	The Privacy team will need to be notified to initiate their own processes for response to privacy beaches.
After the initial impact has been assessed and there are any suspected acts, regulation, or policy violations	Cybersecurity	Legal Team	The legal team should be notified of the nature of the impact, including the type of data, and whom the stakeholders are for this data. They may need to look at the legal implications the loss could present.

Depending on the severity of the incident, essential public communications during the response phase of a data breach incident can include:

Timing	From	Tactic	General Message
Upon notification	Communications	Communications plan Key messages	Outline the overall communications approach for stakeholders, staff, and the public. Develop key messages that share the most important pieces of information with the audience to help keep messaging consistent. Consider timing and messaging. Be transparent without sharing sensitive information. The plan and messaging should be approved by appropriate members of cybersecurity and leadership.
In response to public inquiries	Communications	Social media	Provide high-level updates to keep clients informed on the situation. Responding to public comments can help control the narrative and reduce speculation. Individuals will often go to social media when experiencing a technical issue. Avoid sharing sensitive or undetermined information, including restoration timelines. Depending on the level of public impact, consider whether a reactive or proactive approach is most appropriate. Reactive may be more suitable when public impacts are minimal, whereas proactive may be more suitable for larger incidents.
In response to media inquiries	Communications	Media statement or response Web content Direct stakeholder communications	Provide information about the incident. If a breach results in significant public impacts, inform stakeholders of the incident and steps being taken to resolve the situation. Use existing channels and, if required, provide multiple updates. This will help reduce speculation and assure clients they are being considered during response. Be transparent without sharing sensitive information. Avoid undetermined information, including restoration timelines. It should be approved by appropriate members of cybersecurity and leadership.

Post Incident

A comprehensive post-mortem analysis should be conducted after resolving a data loss incident or any significant cybersecurity event. It involves a detailed examination of the incident response process to identify strengths, weaknesses, and lessons learned. The analysis should be carried out by the incident response team and key stakeholders, using incident data, logs, and documentation to gain insights into the incident's root causes, response effectiveness, and opportunities for improvement. The findings from the post-mortem analysis serve as valuable input to update the data loss playbook, enhance incident response procedures, and fortify the organization's security posture against future incidents.

If the organization does experience a data loss incident, conducting lessons learned exercises post-recovery is an excellent method to implement further mitigation measures and corrective actions and strategies that did not go as planned. Revising the incident response plan based on these lessons learned will ensure that the organization has the most robust response and recovery plans possible. These lessons learned may also be shared through secure channels with other organizations, such as the CyberAlberta Community of Interest, as sharing these lessons can benefit other organizations and the cybersecurity community, ensuring greater all-around protection for Albertans.

Key activities of the post-incident phase include, but are not limited to:

Activity	Actions
1	☐ Complete root cause analysis, possibly in conjunction with the forensic team, to determine how the data loss occurred.
2	☐ Draft a post-incident report that includes the following details as a minimum: ○ details of the cause, impact, and actions taken (successful or otherwise) to mitigate the cyber incident; ○ timings, type, and location of the incident; ○ any effects on users and/or clients caused by the attack or during the remediation; ○ activities undertaken by relevant operations groups, service providers, and business stakeholders that enabled normal business operations to resume; ○ recommendations of any aspects of people, processes, or technology that could be improved across the organization to help prevent a similar cyber incident from reoccurring; & ○ a review of staff welfare (e.g., working hours, overtime, time off in lieu and expenses).
3	☐ Complete the formal lessons identified process to feedback into future preparation activities. Document the lessons learned from the incident response. This includes best practices, new insights, and strategies to enhance the data loss playbook and incident response procedures
4	☐ Publish internal communications to inform and educate employees on data loss incidents and security awareness.
5	☐ Publish external communications, if appropriate, inline with the communications strategy to provide advice to customers, engage with the market, and inform the press of the cyber incident. ☐ These communications should provide key information about the cyber incident without leaving the organization vulnerable or inciting further data attacks.
6	☐ Reverse-engineer any malware used in a secure environment to understand its mechanisms and the functionality it implemented ○ The reverse-engineering may be helped by executing the malware in a secure environment or sandbox, segregated from the business network, to determine its behaviour on a test system, including created files, launched services, modified registry keys, and network communications ☐ Classify the malware by submitting it to AV vendors and determining the family it belongs to.
7	☐ Use the findings from the post-mortem analysis to update the data loss playbook. Incorporate improvements, refine response procedures, and integrate new knowledge gained from the incident.
8	☐ Complete root cause analysis, possibly in conjunction with the forensic team, to determine how the data loss occurred.

Essential communications during the post incident phase of a data breach incident attack include:

Timing	From	To	General Message
After the incident has been resolved	Cybersecurity	Leadership	Post incident report, including: • Root cause analysis • High level information about what happened, when, how it was resolved, and any potential repercussions or related advice to stakeholders • Lessons Learned • Planned preventative measures
After post-incident report has been communicated to leadership	Cybersecurity and leadership or Communication team	Clients/ stakeholders/ or the public if it makes sense for the organization	High level information about what happened, when, how it was resolved, and any potential repercussions or related advice to stakeholders. Consider alignment with previously shared messaging.