PRIVACY BREACH
NOTIFICATION PROCEDURE

DEFINITIONS

A privacy breach occurs when there is unauthorized access to or collection, use, disclosure or disposal of personal information.

A breach may be the result of:

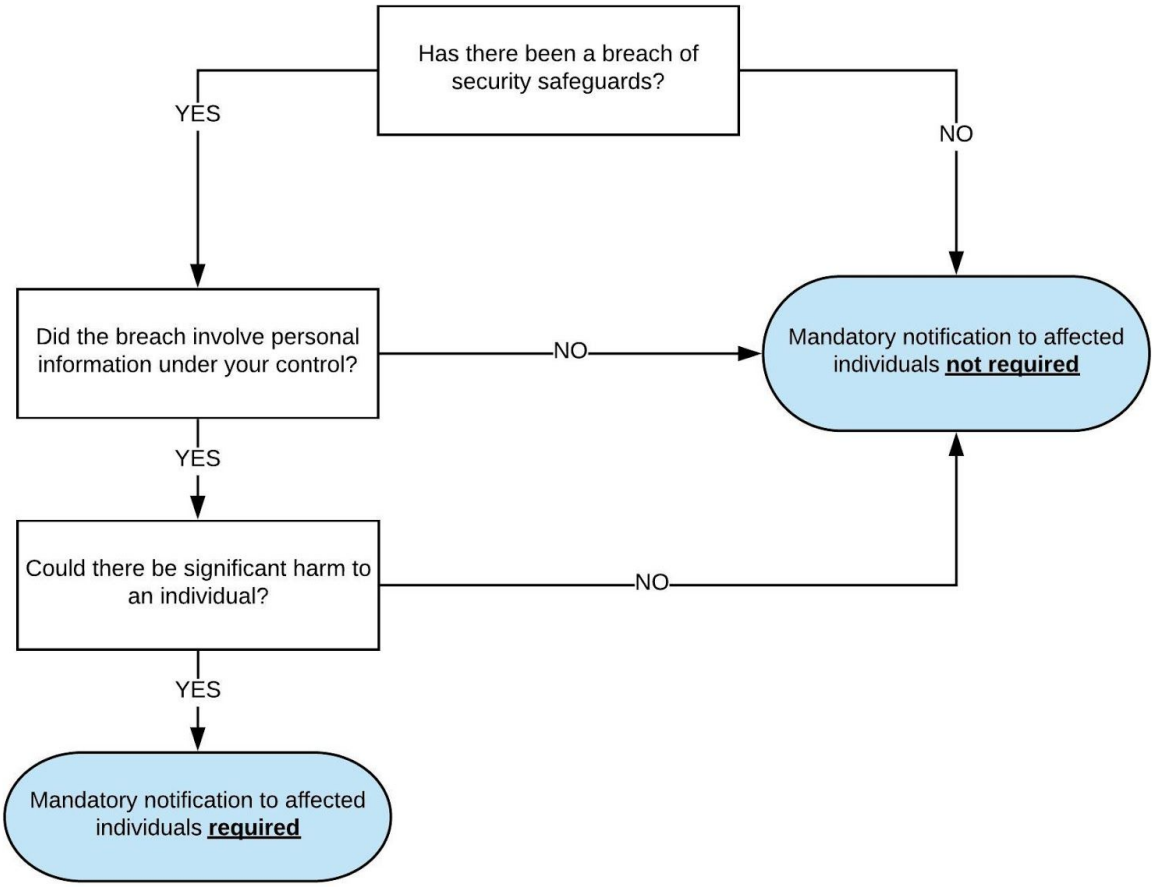
- Internal error
    - Email, mail and faxes sent to the wrong individual(s)
    - Emailing unauthorized information
    - Faxes sent to an unsecure fax
    - Mail or couriers sent to the wrong person
    - Documents lost or gone missing on public transport
    - Documents disposed of in the trash, or intended for shredding and disposed of improperly
    - Loss of files or devices, including laptops, phones, and hard drives
    - Verbal disclosure
- Theft
    - Information taken by a current/former employee
    - Office and car break-ins resulting in the loss of files and devices, including laptops, phones, and hard drives
- System Compromise
    - Targeted attacks by external actors

Examples of a data breach would be the publishing of or loss of any of the following information:

- Names, email addresses, telephone numbers, passwords of Cybera members or cloud users
- Names, addresses, telephone numbers, passwords, salary information of Cybera employees

PROCEDURE

In the event that a Cybera employee becomes aware of a potential breach, the following procedure is triggered, with reference to the Personal Information Protection Act Breach Reporting Guide.



Source: Adapted from PrivaTech for IAPP Canada Conference 2017

Date Updated: January 24, 2018

Immediately upon recognizing breach

The employee must immediately inform their manager and Cybera's Privacy Officer of the date, location, and circumstances of the breach.

Within 72 hours of recognizing breach

Under the leadership of Cybera's Privacy Officer, staff will perform an analysis and determine:

a. The type of personally identifiable information affected by the breach.
b. The type of harm that could occur as the result of the breach.
c. An assessment of whether the harm is significant or not, and why.
d. An assessment of the likelihood that harm could result.
e. Estimated number of individuals to whom there is a real risk of significant harm as a result of the incident.
f. Steps Cybera has taken to reduce the risk of harm to individuals, including actions planned that have not yet been implemented.
g. The CEO, in consultation with the Privacy Officer will inform the Board of Directors.
h. The CEO, in consultation with the Privacy Officer and the Board of Directors will determine whether to activate the Crisis Communications Plan.

Within 48 hours of completing the breach analysis

If a real risk of harm to individuals is identified, staff will provide notice to the Office of the Information and Privacy Commissioner of Alberta without unreasonable delay. The Office of the Privacy Commissioner provides a breach report form on its website. Fill out the most up to date breach report form document. Notice to the OIPC will contain the following:

i. a description of the circumstances of the loss or unauthorized access or disclosure;
j. the date on which or time period during which the loss or unauthorized access or
disclosure occurred;
k. a description of the personal information involved in the loss or unauthorized access or disclosure;
l. an assessment of the risk of harm to individuals as a result of the loss or unauthorized access or disclosure;
m. an estimate of the number of individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure;
n. a description of any steps the organization has taken to reduce the risk of harm to individuals;

o. a description of any steps the organization has taken to notify individuals of the loss or unauthorized access or disclosure;
p. the name of and contact information for a person who can answer, on behalf of the organization, the Commissioner's questions about the loss or unauthorized access or disclosure.

If a real risk of harm to individuals is identified, staff will notify the affected individuals of the breach and their compromised personal information by email or mailed letter. The notice will include the circumstances, date of the breach (or at least an estimate), a description of the personal information, steps taken to control the harm, measures those affected can take, and the contact information of Cybera's Privacy Officer.