Commissariat à la protection de la vie privée du Canada
Office of the Privacy Commissioner of Canada

Lignes directrices | Guidelines

Key Steps for Organizations in Responding to Privacy Breaches

Purpose

The purpose of this document is to provide guidance to private sector organizations, both small and large, when a privacy breach occurs. Organizations should take preventative steps prior to a breach occurring by having reasonable policies and procedural safeguards in place, and conducting necessary training. This guideline is intended to help organizations take the appropriate steps in the event of a privacy breach and to provide guidance in assessing whether notification to affected individuals is required. Not all steps may be necessary, or some steps may be combined.

What is a privacy breach?

A privacy breach occurs when there is unauthorized access to or collection, use, or disclosure of personal information. Such activity is "unauthorized" if it occurs in contravention of applicable privacy legislation, such as PIPEDA, or similar provincial privacy legislation. Some of the most common privacy breaches happen when personal information of customers, patients, clients or employees is stolen, lost or mistakenly disclosed (e.g., a computer containing personal information is stolen or personal information is mistakenly emailed to the wrong people). A privacy breach may also be a consequence of faulty business procedure or operational break-down.

Four key steps in responding to a privacy breach

There are four key steps to consider when responding to a breach or suspected breach: 1) breach containment and preliminary assessment; 2) evaluation of the risks associated with the breach; 3) notification; and 4) prevention. Be sure to take each situation seriously and move immediately to investigate the potential breach. You should undertake steps 1, 2 and 3 either simultaneously or in quick succession. Step 4 provides recommendations for longer-term solutions and prevention strategies. The decision on how to respond should be made on a case-by-case basis.

Associated with this guideline is a checklist that organizations can use to help ensure they have made the appropriate considerations in dealing with a possible privacy breach.

30, rue Victoria | 30 Victoria Street
Gatineau (Québec) K1A 1H3
Sans frais/Toll free 1-800-282-1376 Tél./Tel: 819-994-5444 Téléc./Fax: 819-994-5424 www.priv.gc.ca

Step 1: Breach Containment and Preliminary Assessment

You should take immediate common sense steps to limit the breach:

- Immediately contain the breach (e.g., stop the unauthorized practice, recover the records, shut down the system that was breached, revoke or change computer access codes or correct weaknesses in physical or electronic security).
- Designate an appropriate individual to lead the initial investigation. This individual should have appropriate scope within the organization to conduct the initial investigation and make initial recommendations. If necessary, a more detailed investigation may subsequently be required.
- Determine the need to assemble a team which could include representatives from appropriate parts of the business.
- Determine who needs to be made aware of the incident internally, and potentially externally, at this preliminary stage. Escalate internally as appropriate, including informing the person within your organization responsible for privacy compliance.
- If the breach appears to involve theft or other criminal activity, notify the police.
- Do not compromise the ability to investigate the breach. Be careful not to destroy evidence that may be valuable in determining the cause or allow you to take appropriate corrective action.

Step 2: Evaluate the Risks Associated with the Breach

To determine what other steps are immediately necessary, you should assess the risks associated with the breach. Consider the following factors in assessing the risks:

(i) Personal Information Involved

- What data elements have been breached?
- How sensitive is the information? Generally, the more sensitive the information, the higher the risk of harm to individuals. Some personal information is more sensitive than others (e.g., health information, government-issued pieces of identification such as social insurance numbers, driver's licence and health care numbers, and financial account numbers such as credit or debit card numbers that could be used in combination for identity theft). A combination of personal information is typically more sensitive than a single piece of personal information. However, sensitivity alone is not the only criteria in assessing the risk, as foreseeable harm to the individual is also important.
- What is the context of the personal information involved? For example, a list of customers on a newspaper carrier's route may not be sensitive. However, the same information about customers who have requested service interruption while on vacation may be more sensitive. Similarly, publicly available information such as that found in a public telephone directory may be less sensitive.

- Is the personal information adequately encrypted, anonymized or otherwise not easily accessible?
- How can the personal information be used? Can the information be used for fraudulent or otherwise harmful purposes? The combination of certain types of sensitive personal information along with name, address and date of birth suggest a higher risk due to the potential for identity theft.

An assessment of the type of personal information involved will help you determine how to respond to the breach, who should be informed, including the appropriate privacy commissioner(s), and what form of notification to the individuals affected, if any, is appropriate. For example, if a laptop containing adequately encrypted information is stolen, subsequently recovered and investigations show that the information was not tampered with, notification to individuals may not be necessary.

(ii) Cause and Extent of the Breach

- To the extent possible, determine the cause of the breach.
- Is there a risk of ongoing breaches or further exposure of the information?
- What was the extent of the unauthorized access to or collection, use or disclosure of personal information, including the number and nature of likely recipients and the risk of further access, use or disclosure, including via mass media or online?
- Was the information lost or was it stolen? If it was stolen, can it be determined whether the information was the target of the theft or not?
- Has the personal information been recovered?
- What steps have already been taken to mitigate the harm?
- Is this a systemic problem or an isolated incident?

(iii) Individuals Affected by the Breach

- How many individuals' personal information is affected by the breach?
- Who is affected by the breach: employees, contractors, public, clients, service providers, other organizations?

(iv) Foreseeable Harm from the Breach

- In assessing the possibility of foreseeable harm from the breach, have you considered the reasonable expectations of the individuals? For example, many people would consider a list of magazine subscribers to a niche publication to be potentially more harmful than a list of subscribers to a national newspaper.
- Who is the recipient of the information? Is there any relationship between the unauthorized recipients and the data subject? For example, was the disclosure to an unknown party or to a party suspected of being involved in criminal activity where there is a potential risk of misuse? Or was the recipient a trusted, known entity or person that would reasonably be expected to return the information without disclosing or using it?

- What harm to the individuals could result from the breach? Examples include:
    - security risk (e.g., physical safety);
    - identity theft;
    - financial loss;
    - loss of business or employment opportunities; or
    - humiliation, damage to reputation or relationships.
- What harm to the organization could result from the breach? Examples include:
    - loss of trust in the organization;
    - loss of assets;
    - financial exposure; or
    - legal proceedings (i.e., class action suits).
- What harm could come to the public as a result of notification of the breach? Harm that could result includes:
    - risk to public health; or
    - risk to public safety.

Step 3: Notification

Notification can be an important mitigation strategy that has the potential to benefit both the organization and the individuals affected by a breach. If a privacy breach creates a risk of harm to the individual, those affected should be notified. Prompt notification to individuals in these cases can help them mitigate the damage by taking steps to protect themselves. The challenge is to determine when notices should be required. Each incident needs to be considered on a case-by-case basis to determine whether privacy breach notification is required. Organizations are also encouraged to inform the appropriate privacy commissioner(s) of material privacy breaches so they are aware of the breach.

The key consideration in deciding whether to notify affected individuals should be whether notification is necessary in order to avoid or mitigate harm to an individual whose personal information has been inappropriately accessed, collected, used or disclosed. Organizations should also take into account the ability of the individual to take specific steps to mitigate any such harm.

(i) Notifying Affected Individuals

Organizations should consider the following factors when deciding whether to notify:

- What are the legal and contractual obligations?
- What is the risk of harm to the individual?
- Is there a reasonable risk of identity theft or fraud (usually because of the type of information lost, such as an individual's name and address together with government-issued identification numbers or date of birth)?
- Is there a risk of physical harm (if the loss puts an individual at risk of physical harm, stalking or harassment)?

- Is there a risk of humiliation or damage to the individual's reputation (e.g., when the information lost includes mental health, medical or disciplinary records)?
- What is the ability of the individual to avoid or mitigate possible harm?

(ii) When to Notify, How to Notify and Who Should Notify

At this stage, you should have as complete a set of facts as possible and have completed your risk assessment in order to determine whether to notify individuals.

When to notify: Notification of individuals affected by the breach should occur as soon as reasonably possible following assessment and evaluation of the breach. However, if law enforcement authorities are involved, check with those authorities whether notification should be delayed to ensure that the investigation is not compromised.

How to notify: The preferred method of notification is direct – by phone, letter, email or in person – to affected individuals. Indirect notification – website information, posted notices, media – should generally only occur where direct notification could cause further harm, is prohibitive in cost or the contact information for affected individuals is not known. Using multiple methods of notification in certain cases may be appropriate. You should also consider whether the method of notification might increase the risk of harm (e.g., by alerting the person who stole the laptop of the value of the information on the computer).

Who should notify: Typically, the organization that has a direct relationship with the customer, client or employee should notify the affected individuals, including when the breach occurs at a third party service provider that has been contracted to maintain or process the personal information. However, there may be circumstances where notification by a third party is more appropriate. For example, in the event of a breach by a retail merchant of credit card information, the credit card issuer may be involved in providing the notice since the merchant may not have the necessary contact information.

(iii) What should be Included in the Notification?

The content of notifications will vary depending on the particular breach and the method of notification chosen. Notifications should include, as appropriate:

- Information about the incident and its timing in general terms;
- A description of the personal information involved in the breach;
- A general account of what the organization has done to control or reduce the harm;
- What the organization will do to assist individuals and what steps the individual can take to avoid or reduce the risk of harm or to further protect themselves. Possible actions include arranging for credit monitoring or other fraud prevention tools, providing information on how to change a social insurance number (SIN), personal health card or driver's licence number. For example, to obtain a new SIN see http://www1.servicecanada.gc.ca/en/cs/sin/0200/0200_010.shtml;
- Sources of information designed to assist individuals in protecting against identity theft (e.g., online guidance on the Office of the Privacy Commissioner's website http://www.priv.gc.ca/resource/ii_4_01_e.cfm and Industry Canada website at http://strategis.ic.gc.ca/epic/site/oca-bc.nsf/en/h_ca02226e.html;

- Providing contact information of a department or individual within your organization who can answer questions or provide further information;
- If applicable, indicate whether the organization has notified a privacy commissioner's office and that they are aware of the situation;
- Additional contact information for the individual to address any privacy concerns to the organization; and
- The contact information for the appropriate privacy commissioner(s).

Be careful not to include unnecessary personal information in the notice to avoid possible further unauthorized disclosure.

(iv) Others to Contact

- **Privacy Commissioners:** organizations are encouraged to report material privacy breaches to the appropriate privacy commissioner(s) as this will help them respond to inquiries made by the public and any complaints they may receive. They may also be able to provide advice or guidance to your organization that may be helpful in responding to the breach. Notifying them may enhance the public's understanding of the incident and confidence in your organization. The following factors should be considered in deciding whether to report a breach to privacy commissioners' offices:
    - any applicable legislation that may require notification;
    - whether the personal information is subject to privacy legislation;
    - the type of the personal information, including:
        - whether the disclosed information could be used to commit identity theft;
        - whether there is a reasonable chance of harm from the disclosure including non-monetary losses;
    - the number of people affected by the breach;
    - whether the individuals affected have been notified; and
    - if there is a reasonable expectation that the privacy commissioner's office may receive complaints or inquiries about the breach.

Regardless of what you determine your obligations to be with respect to notifying individuals, you should consider whether the following authorities or organizations should also be informed of the breach, as long as such notifications would be in compliance with PIPEDA or similar provincial privacy legislation:

- **Police:** if theft or other crime is suspected.
- **Insurers or others:** if required by contractual obligations.
- **Professional or other regulatory bodies:** if professional or regulatory standards require notification of these bodies.
- **Credit card companies, financial institutions or credit reporting agencies:** if their assistance is necessary for contacting individuals or assisting with mitigating harm.
- **Other internal or external parties not already notified:**
    - third party contractors or other parties who may be impacted;
    - internal business units not previously advised of the privacy breach, e.g., government relations, communications and media relations, senior management, etc.; or
    - union or other employee bargaining units.

Organizations should consider the potential impact that the breach and notification to individuals may have on third parties and take actions accordingly. For example, third parties may be affected if individuals cancel their credit cards or if financial institutions issue new cards.

Step 4: Prevention of Future Breaches

Once the immediate steps are taken to mitigate the risks associated with the breach, organizations need to take the time to investigate the cause of the breach and consider whether to develop a prevention plan. The level of effort should reflect the significance of the breach and whether it was a systemic breach or an isolated instance. This plan may include the following:

- a security audit of both physical and technical security;
- a review of policies and procedures and any changes to reflect the lessons learned from the investigation and regularly after that (e.g., security policies, record retention and collection policies, etc.);
- a review of employee training practices; and
- a review of service delivery partners (e.g., dealers, retailers, etc.).

The resulting plan may include a requirement for an audit at the end of the process to ensure that the prevention plan has been fully implemented.