How to Diagnose, Stem and Repair a Privacy Bleed

September 20, 2007

Catherine Tully

Office of the Information and Privacy Commissioner

Case Study

- A complainant alleges inappropriate access to her personal information contained in the organization's customer data base.
- Her ex-husband told the complainant's daughter that he has access to the organization's customer data base and that he will use it to access her home address.
- The complainant fears for her safety.

Tasks

- Task 1: Diagnose
- Task 2: Stem
- Task 3: Repair
  - Assess risks
  - Notify
  - Develop Prevention Strategies

Timing is Everything

- Diagnose, contain & notify within days, if not hours of the breach
- Prevention strategies are more long term and may take weeks or months to complete

Task 1: Diagnose

i. Get organized
ii. Get the facts
iii. Determine whether the event is a privacy breach
iv. Determine the cause of the breach

(i) Get Organized

- Follow your breach management policy
- If no breach management policy
  - Designate a lead investigator
  - Assemble a breach response team
  - Determine who within the organization needs to be notified
  - Determine if the police need to be notified

(ii) Get the Facts

- Conduct a preliminary examination of the data base
- Determine if complainant's personal information was accessed and by whom
- Consider email audit for emails to the complainant's ex-husband
- Consider immediate notification

(iii) Determine if a privacy breach occurred

- Review audit results – if complainant's information was accessed was it by an authorized individual for a legitimate purpose?
  - Review job description
  - Discuss with supervisor
  - Consider use patterns for other improper uses

(iv) Determine the Cause of the Breach

- Informs steps necessary to stem and repair
- In case study cause was employee misconduct

Task 2: Stem

- Take common sense steps to stop the breach from continuing or to reduce the potential for further harm:
  - Revoke the employee's access rights to the data base
  - Seize her computer for a more thorough audit of data base access and email use

Task 3: Repair

(i) Risk Assessment

- Nature and sensitivity of the personal information – home address of an individual at risk
- Prospect of criminal activity or other intentional wrongdoing
- Foreseeable harm – risk of physical harm to complainant

(ii) Notify

- Immediately notify affected individual
  - Harm mitigation strategy
  - Follow OIPC guidelines regarding content
- Notify others
  - Privacy Commissioner
  - Insurers
  - Professional organizations
  - Other contracted organizations

(iii) Prevention Strategies

- Privacy & security training for employees
- Policies – clear and well publicized policies regarding inappropriate use
- Discipline?
- Technical security enhancements – appropriate user access permissions & 'real time audit' capacity to flag this type of authorized but inappropriate use

OIPC Order F07-01

- For a full evaluation of this fact situation and the response, see OIPC Order F07-01 at:

http://www.oipc.bc.ca/orders/investigationreports/IR-F07-01.pdf

Best Practices

- Develop a Privacy Breach Management Policy in advance of any privacy breach
  - Assign roles and responsibilities
  - Set timelines for response
- Develop privacy breach reporting form
- Develop template breach notification letters