Privacy First Aid for the Private Sector

How to Diagnose, Stem and Repair a Privacy Bleed
September 20, 2007

Presented by: Catherine Tully

Introduction:
Timing is extremely important when it comes to managing a privacy breach. The problem should be diagnosed and containment & notification steps taken within days, if not hours of the breach. Preparation is also important. A well prepared organization reduces its chances of experiencing a privacy breach and can effectively minimize the consequences of the breach.

Task 1: Diagnose

(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 policy need to be notified

(ii) Get the facts
- Require business area staff to complete a breach reporting form
- Preserve evidence
- Collect witness names

(iii) Determine whether the event is a privacy breach
- "Privacy breach" according to BC OIPC is any unauthorized access to or collection, use, disclosure or disposal of personal information. Such activity is "unauthorized" if it occurs in contravention of the *Personal Information Protection Act* or part 3 of the *Freedom of Information and Protection of Privacy Act*.

(iv) Determine the cause of the breach
- Conduct a site visit, interview witnesses
- Enlist assistance from IT security specialists
- Hire physical security specialists and/or private investigators if necessary
- Consult with the police

Task 2: Stem

Take common sense steps to stop the breach from continuing and/or to reduce the potential for further harm:

- Retrieve the information
- Address weaknesses in physical security
- Address weaknesses in technical security
- Address employee misconduct

Task 3: Repair

(i) Evaluate the risks

- Consider the nature and sensitivity of the personal information
- Consider the number of individuals affected
- Consider the foreseeable harm to individuals, to the organization's reputation and to the public
- Consider the causes of the breach – technical, physical or personnel?

(ii) Notify

- Notify affected individuals
  - Notification is a harm mitigation strategy
  - Follow OIPC guidelines regarding content[1]
- Notify others
  - Privacy commissioner[2]
  - Insurers
  - Professional organizations
  - Other contracted organizations

(iii) Prevention Strategies

Develop and implement a prevention strategy:

- Improve physical security
- Enhanced security architecture
- Policies including security standards policy & breach management policy
- Training
- Contractor supervision including regular audit and set policy standards
- Audit schedules

---

[1] See the Breach Notification Assessment Tool at:
http://www.oipc.bc.ca/pdfs/Policy/ipc_bc_ont_breach.pdf

[2] The BC OIPC document "Key Steps in Responding to Privacy Breaches" provides a list of considerations when deciding whether or not to report to a privacy commissioner. The Commissioner noted in Investigation Report F07-01, *"Prompt notification to the OIPC aids the OIPC in assisting public bodies and affected individuals, in the case of public bodies by helping them develop effective strategies to mitigate the harms arising from the breach."* The Key Steps document recommends that you consider the sensitivity of the information, the risk of identity theft, the likelihood of non pecuniary losses, the number of people affected and whether the information has been fully recovered when deciding whether or not to report the breach to the OIPC.