Office of the Information and Privacy Commissioner of Alberta

Privacy Breach Response and Reporting

AFNIGC - Privacy Education Series

October 18, 2017

Chris Stinner
Senior Information and Privacy Manager
Office of the Information and Privacy Commissioner of Alberta

Agenda

- Overview
- Before a Breach
- Responding to a Breach

What is a privacy breach?

- Occurs when there is unauthorized:
  - access to, or
  - collection, use, disclosure, or
  - disposal or loss of

  personal or health information.

- "unauthorized" if it is in contravention of FOIP, HIA or PIPA

Causes of Privacy Breaches

- Lack of privacy and security training
- Human Error – misdirect correspondence
- Security Incidents
  - Social engineering such as phishing
  - Hacks leading to unauthorized access to information
- Lack of adequate & appropriate privacy and security controls
  - Weak or no privacy & security policies
  - Poor IT change management
  - Legacy systems

Breach Reporting Requirements

- FOIP – Voluntary Breach Reporting
  - Most public bodies report serious incidents

- HIA – Voluntary Breach Reporting
  - Serious breaches reported to us
  - May become mandatory in future

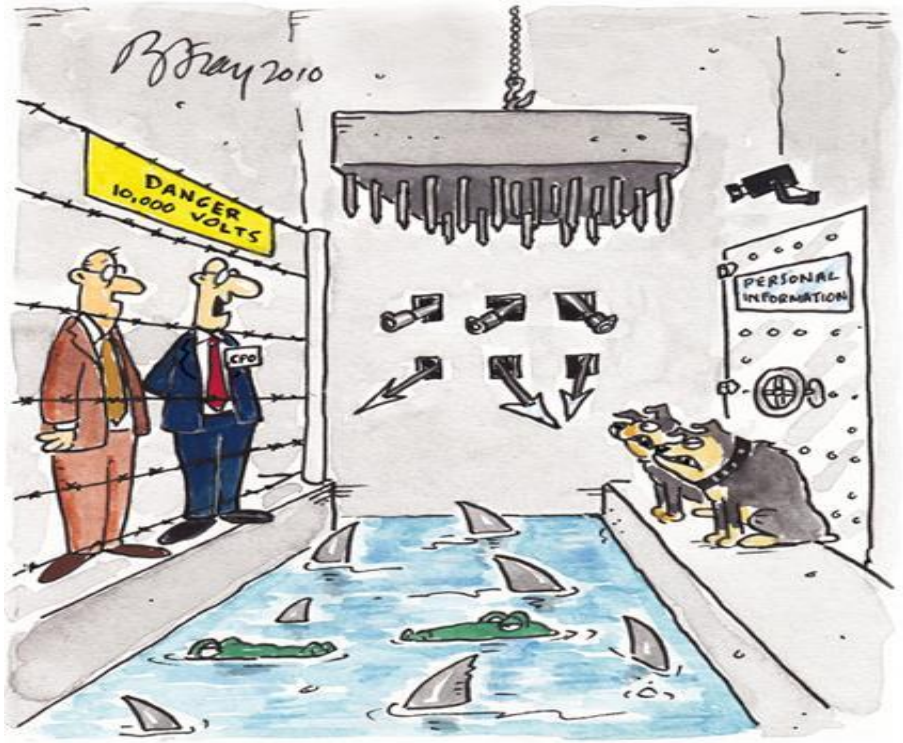
- PIPA – Mandatory Breach Reporting
  - Breaches with RROSH **must** be reported
  - And individuals affected notified

Does a breach mean you failed the duty to protect?

- Yes and no…
- Does not necessarily mean a failure to meet the duty to protect under FOIP, PIPA or HIA.
- May experience privacy breach despite reasonable safeguards.
- However, may reveal gaps in your security arrangements that should be addressed.

What does “Reasonable Steps” Mean?

- NOT a standard of perfection
- “Fit and appropriate to the end in view”
- Depends on circumstances



BEFORE A BREACH

- Work to avoid them
- Addressing privacy risks
- Be in the know
- Mitigate their impact

How to avoid breaches (as much as possible)

- Review organization practices
- Conduct privacy impact assessments for new systems, processes
- Security review/audits, penetration tests
- Policy & procedures reviews
- Training and awareness

Mitigating privacy risks

- Mitigation plans should address each of these risks.
  - Unauthorized c/u/d by internal or authorized parties.
  - Unauthorized c/u/d by external parties.
  - Loss of integrity.
  - Loss, destruction, or loss of use.
  - Unauthorized c/u/d by contractor or business partner

Be in the know

- Stay abreast of developments in your sector
- Review OIPC Breach Notification Decisions, Investigation Reports
- Involve your stakeholders
- Encourage reporting of near-misses

Mitigating the Impact of Breaches

- Assume you will have a privacy breach, despite your efforts
- Identify a breach response team ahead of time
- Establish a policy and plan regarding breaches
- Practice makes perfect – test your plan and make sure staff is aware

Summary of Tips to Prevent Breaches

- Put someone in charge
- Implement Policies and Procedures
- Train Staff
- Review OIPC online reports
- Communicate regularly with staff

BREACH RESPONSE

- Step 1. Contain the Breach
- Step 2. Evaluate the Risks
- Step 3. Notification
- Step 4. Prevention

Step 1 – Contain the breach

- Take immediate steps to stop the breach
- Take remedial action
- Investigate what happened
- Gather information and start the risk assessment

Step 2 – Evaluate the Risks

- What information is involved?
- What was the cause and extent of the breach?
- Who are the affected individuals?
- What is the foreseeable harm?

Step 3 – Notification

- Who
  - Internally
  - Externally
- Why
  - Legislation
  - Contract
  - Policy
- When

Step 3 – Notification continued

- No need to wait for us!
- Be open and honest
- Explain what happened
- Explain what you are doing
- Offer support
- Be prepared to answer questions or develop FAQs

Step 3 – Reporting

- Deciding whether to report
- Reporting to Authorities or organizations
- Reporting to OIPC or counterparts

Step 4 – Prevention

- Take time to thoroughly investigate the cause of the breach.
- Develop or improve long term safeguards against further breaches.
- Review and update policies and training based on lessons learned.
- Audit to ensure the prevention plan has been implemented.

Breach Response Pitfalls

1. No written breach response and report plan
2. No backup person when decision makers are away
3. Scrambling to secure external agencies such as forensic audit company, law firm, etc...
4. Waiting for "perfect" information
5. Improper risk assessment of the harm to individuals
6. Contact person for affected individuals difficult to reach
7. No internal communication and/or action plan
8. Vague notification to affected individuals
9. Not reporting a privacy breach at all

Wrapping things up

- Manage your privacy function
- Prepare for contingencies
  - Breach response plan
  - BCP / DRP
- Know when / how to notify
- Keep yourself / your staff up-to-date
- Periodically assess

Questions?

Office of the Information and
Privacy Commissioner of Alberta

Resources

- OIPC Breach reporting resources
  https://www.oipc.ab.ca/action-items/how-to-report-a-privacy-breach.aspx
- OIPC AB Breach Notification decisions
  https://www.oipc.ab.ca/decisions/breach-notification-decisions.aspx
- OPC Federal Privacy Commissioner key steps in responding to a breach
  - https://www.priv.gc.ca/information/guide/2007/gl_070801_02_e.asp
- Alberta Health Legislation page - Guidelines and Practices Manual
  - http://www.health.alberta.ca/documents/HIA-Guidelines-Practices-Manual.pdf
- Service Alberta PIPA
  - http://www.servicealberta.ca/pipa-overview.cfm
- Service Alberta FOIP
  - http://www.servicealberta.ca/foip/