OH *@#%! WE HAVE A PRIVACY BREACH!

Brian Hamilton
Cara-Lynn Stelmack
Office of the Information and Privacy Commissioner, Alberta

Privacy and Access 20/20 – Workshop October 9, 2013

Agenda

- What is a privacy breach?
- Breaches we investigate
- How to prepare for a breach
- What to do when (not if) it happens
- Reporting a breach to the Commissioner
  - RROSH test in Alberta and how to assess risk generally
- How to avoid a breach in the first place
- How to learn from your (and others') mistakes
- Case studies (group work)

We are in the Breach Business

- FOIP
- 2012 21
- 2013 41

- HIA
- 2012 59
- 2013 57

- PIPA
- 2012 94
- 2013 84

What is a privacy breach?

- Not defined in Alberta's health or public sector legislation
- Alberta PIPA s.34.1 defines a reportable incident as:
  - any incident involving the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result.
  - BC PIPA s. and part 3 of BC FOIP.
- Generally, a privacy breach occurs when
  - Someone collects, uses or discloses personal information in contravention of a privacy law, deliberately or accidentally
  - An public body/organization/custodian/trustee loses control of personal information
  - Confidentiality of personal information is compromised

How do we learn about breaches?

- Mandatory breach reports under s. 34.1 Alberta PIPA
- No mandatory breach reporting under Alberta's Health Information Act or Freedom of Information and Protection of Privacy Act
  - High level of self-reported breaches from health professionals
  - Breach reports from health care providers subject to Personal Information Protection Act
- People become suspicious when someone 'knows too much,' gather evidence and report to us
- Individuals are notified of a breach by organization and then notify us
- Lost records are found, delivered to us (or delivered to the media)
- Information found on hard drives, servers, lost USB and reported to us
- Media reports

How do we respond to breaches?

- RROSH Decision (PIPA)
- Investigate and mediate a resolution (HIA and FOIP)
  - Has the breach been stopped?
  - Reasonable measures been taken to prevent recurrence?
  - Sanctions administered?
  - Affected individuals informed?
- Public Investigation Report
  - Purpose is to educate
- Hearing, leading to an Order
- Offence prosecution

Challenges to investigations

- In electronic records, root cause hard to find
  - Is it the viewer, the feeder system, the network?
  - Lack of audit trails to confirm what has been accessed or disclosed.
- System boundaries hard to define
  - Many interrelationships, informal ties
- If policies and training are not in place, or not enforced, difficult to sanction or prosecute those who break the rules
- Lack of audit trail
- Tendency to minimize the breach
- Difficulty in identifying personal information

BREACHES WE INVESTIGATE

Breaches we investigate

- Shredding, disposal mishaps
- Lost, stolen, unencrypted data
- Misdirected communications
- Malware infestation
- Unauthorized access by insiders
- Deliberate intrusions

Shredding and disposal

- Common scenario:
  - Records found in garbage or dumpster
  - Records blowin’ in the wind
  - Records forwarded to media, then to us
  - Shredded health records “gone to the dogs”

- Causes
  - Lack of awareness, carelessness
  - Cleaners pick up the wrong box and dump it

Lost and stolen documents

- Unsecured/informal filing areas
  - “we store admission forms in a pile by the nursing station until we have time to file them”
- Taking work home, papers stolen from car, theft from office premises
- P2012-ND-12 – laptop & files stolen in January 2012 – hard copy documents turn up in dumpster later
- Files left on the bus, train, etc.

Misdirected communications

- Wrong fax number
- Human error
- Machine errors that affect mass mail-outs or result in printing errors
- Wrong email
- Email with reply to all
- Data errors – wrong report sent to wrong provider
- Use secure channel where available
- Data errors often caused by poor change controls

Unencrypted data

- Lost and stolen mobile devices
- Passwords are not enough
- Common mistakes:
  - Policy requires staff to encrypt, but no tools or training provided
  - No policy enforcement
  - Decision made to give someone mobile device without considering necessity or risk
  - Storing data on device when tools are available to allow secure, remote access

Malware
i.e. How to get pwned

- Unpatched systems
- Unnecessary administrator privileges
- Out-of-date anti virus
- Poor understanding of infrastructure (whose network is this anyway?)

Insider abuse or unauthorized access to employee information

- Looking up friends, family, enemies in health or other information systems
- Sensitive personnel information saved or accessible in error on intranet or internal drives
- Increasing number of reports discovered through:
  - Internal audit
  - Individuals reviewing own audit logs
- Issues
  - Training and user agreements won't stop rogue staff, but may make it harder for them if colleagues are more privacy-aware
  - Lack of training and user agreements hinders discipline, sanctions
  - User account sharing makes it difficult to investigate reports of abuse

BE PREPARED

Getting ready for a breach

- Assume you will have a privacy breach
- Identify breach-response team ahead of time
  - Privacy officer, legal counsel, security, contractors/service providers, records management, communications, senior executive
- Establish a policy and plan regarding breaches:
  - Who will you inform? OIPC, Police, clients, business partners?
  - How do you decide whether to tell (risk of harm, legal obligations under contract or law, professional ethics)?
  - Determine jurisdiction (If you are a service provider (e.g. EMR), you may be in the private sector, but your customer is subject to other laws), what law applies
  - Communications are key
- Refer to accountability principles when crafting policy or a responsive plan. **"*Getting Accountability Right with a Privacy Management Program*"**

  at: www.oipc.ab.ca or www.oipc.bc.ca
- Practice makes perfect – test your plan and make sure staff is aware

UH OH!

When it happens

- Take immediate steps to stop the breach
- Assemble your team
- Take remedial action
    - Fix the problem
    - Attempt to retrieve records
    - Staff education, discipline
- Investigate what happened
- Preserve and gather evidence of extent of breach
- Analyse risk to affected individuals
- Consider notification to regulators (that’s us folks!), police, affected individuals
- Establish communications plan
- Make decisions on notification
- Communicate internally and externally

When to report to the Commissioner

- AB PIPA is currently the only law that has mandatory breach reporting requirements. It is self-reporting under AB and BC FOIP and PIPA, AB HIA and PIPEDA.
- AB PIPA section 34.1 requires an organization having control of PI must, without unreasonable delay, notify the Commissioner of any “incident involving the loss of or unauthorized access to or disclosure” of PI where a reasonable person would consider that there exists a real risk of significant harm (RROSH) to an individual.
- It is an offence in AB not to notify the Commissioner of a breach – s. 59.1 (e.1) offence & fine up to $100,000.

Assess the possible harm to individuals

- Is there harm – some damage or detriment or injury?
- Is the harm “significant”? It must be important, meaningful, and with non-trivial consequences or effects.
- Is there a “real risk” the significant harm will occur? - does not require that harm will certainly result from the incident, but the likelihood that it will result must be more than mere speculation or conjecture. There must be a cause and effect relationship between the incident and the possible harm.
- This is the RROSH test under AB PIPA, but is a good general guideline.

Factors to consider

- Case by case analysis
- Factors considered include:
  - The PI involved and the degree of sensitivity
  - Harm (financial, identity theft, reputation, physical)
  - Circumstances of breach
    - Likelihood of unauthorized access/accessibility
    - Number of affected individuals
    - Cause of incident – nefarious, accidental
    - Length of time of exposure
    - Audit trail of exposure
    - PI recovered ?– undertaking re: copying, use, destruction
    - Vulnerable group

What to report

- S.19 of the AB PIPA Regulation – required in AB, a good guideline to follow:
  - Circumstances of incident
  - Date or time period of incident
  - Personal information involved
  - Assessment of risk of harm
  - Estimate of number of affected individuals
  - Steps taken to reduce harm
  - Organization contact person to answer questions

  - Also include steps taken to avoid re-occurrence of similar incident – i.e.. Change in security or storage or retention protocols, training, audit or testing of systems.
  - If the organization has notified affected individuals, the date, form and a copy of the content of the notification.

What we are seeing in reports

- Organizations are having some challenges
- Inadequate information reported to conduct a proper investigation
- Failure to report all the circumstances associated with the breach
- Failure to report all personal information breached
- Risk not being assessed properly
  - Have seen harm to self
  - Bare assertions of risk or no risk without evidence
- Mitigation is not thorough
  - Recover documents
  - Obtain undertakings from receivers
  - Don’t leave loose ends

Communicating with affected parties

- Be open and honest
- Consider apologizing
- Explain what happened
- Identify risks so people can make their own decisions on how to protect themselves
- Tell them what you are doing to prevent similar problems in the future
- Let them know you have informed OIPC and other relevant authorities, such as police, professional regulators, etc.
- Make sure front-line staff are prepared to answer questions and even better a devoted person to answer specific questions, or develop FAQs.

Contents of the notification

- AB HIA/FOIP and BC FOIP/PIPA have no prescribed requirements.
- In AB PIPA – set out in section 19.1 of Regulations
  - (a) must be given directly to the individual, and
  - (b) include
    - description of circumstance
    - date or time period of loss or unauthorized access or disclosure
    - description of PI
    - description of steps taken to reduce risk of harm, and
    - contact information for a person who can answer questions on behalf of the organization

-When direct notification is unreasonable in the circumstances, indirect notification can be required.

What we are seeing

- Organizations are notifying individuals prior to notifying the Commission or during the Commissioner's investigation (about 75%)
- The Commissioner will not generally require an organization to re-notify individuals unless she finds the notice does not meet the requirements of the Regulation
- We have seen on numerous occasions where the notice does not meet the regulations.
  - The time period of the breach is not provided.
  - Only some of the personal information is listed.
  - Contact information not provided.

AVOIDING BREACHES

10 Overlooked Security Threats Claudiu Popa, Globe & Mail Update 09/12/2011

- Malware infections that lead to data and productivity losses.
- Malicious breaches that go on indefinitely.
- Hijacked domain names.
- Loss of accountability over employee accounts.
- Insider threats and disgruntled employees.
- Breaches caused by connecting (from) infected devices.
- Any data breach, interception or access confidentiality breaches.
- Business interruptions due to backup data issues.
- Physical breaches and theft.
- Trust abuses.

Most breaches are predictable and preventable

- Human error is the number one cause of breaches
- Theft is second
- Electronic systems compromises are third
- Failure to adequately control access to personal information is fourth

Prevention is key

- Collect only that PI that you absolutely need.
- Conduct privacy impact assessments for new systems, processes
  - Confirm privacy policies and privacy organization implemented
  - Confirm legal authority to collect, use and disclose personal information
  - Understand information flows
  - Identify and mitigate privacy risk
  - Review
- Use proper security to protect the PI – administrative, technical and physical controls.
- Audit and assess controls including ssecurity reviews/audits, penetration tests
- Build privacy protection into procedures and policy. Specifically, develop policies to support your CUD and security.
- Encrypt laptops & portable media devices.
- Secure destruction of PI when no longer required.
- Develop a breach response plan and practice it.
- Train and remind, then train and remind.
- Something bad may still happen – standard is reasonableness, not perfection

TAKE AWAYS & TRENDS

Learning from mistakes

- Review OIPC RROSH Decisions, Investigation Reports, to learn about:
  - Encryption on mobile devices
  - Faxing
  - Malware
  - Disposal
  - Misuse of personal information
- Encourage reporting and review of near-misses
  - Need internal culture, rewards to support this
- If you have a breach, communicate lessons learned internally

Take aways

- Do a thorough analysis to determine if there is a risk of harm to individuals.
- Ensure your report is comprehensive to allow the Commissioner to do a proper assessment.
- Make sure you have someone knowledgeable and available to answer questions about the breach.
- Evaluate contracts to ensure that service providers have an obligation to report to organization/custodian/public body that has control if there is a breach.
- Information sharing initiatives – in governance structure determine who is responsible for reporting a breach.

Take aways cont.

- Avoid re-notification by ensuring the contents of your notice meets the AB Regulation requirements. Also, notify individuals directly wherever possible.
- If notification is done verbally, keep a copy of the script and make sure the contents meets the requirements in the Regulation.
- Use the breach reporting resources on the BC, AB and federal OPC websites. Call if you ever have questions – we are here to help!

PIPA Resources

- OIPC
  - Website - http://www.oipc.ab.ca
- Service Alberta - Access and Privacy Branch
  - Website - http://www.pipa.alberta.ca
- OIPC - BC
  - Website - http://www.oipc.bc.ca
  - Guidelines for Social Media Background Checks
- OPC – Federal Privacy Commissioner
  - Website - http://www.priv.gc.ca/index_e.cfm

Alberta Breach Reporting Tools

- There is a
- Mandatory Breach
- Reporting Tool
- on the
- OIPC Website

Office of the Information and Privacy Commissioner of Alberta

Personal Information Protection Act

Mandatory Breach Reporting Tool

Purpose

The purpose of this Tool is to help organizations determine whether they are required to provide notice to the Information and Privacy Commissioner (Commissioner) of a breach under section 34.1 of the Personal Information Protection Act (PIPA).

Please contact the Office of the Information and Privacy Commissioner (OIPC) if you would like to speak to someone about a breach of personal information or if you have any questions about this Tool.

Breach Reporting Requirement

Since May 2010, the mandatory breach reporting requirement in section 34.1 of PIPA has been in effect and provides:

"34.1(1) An organization having personal information under its control must, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure".

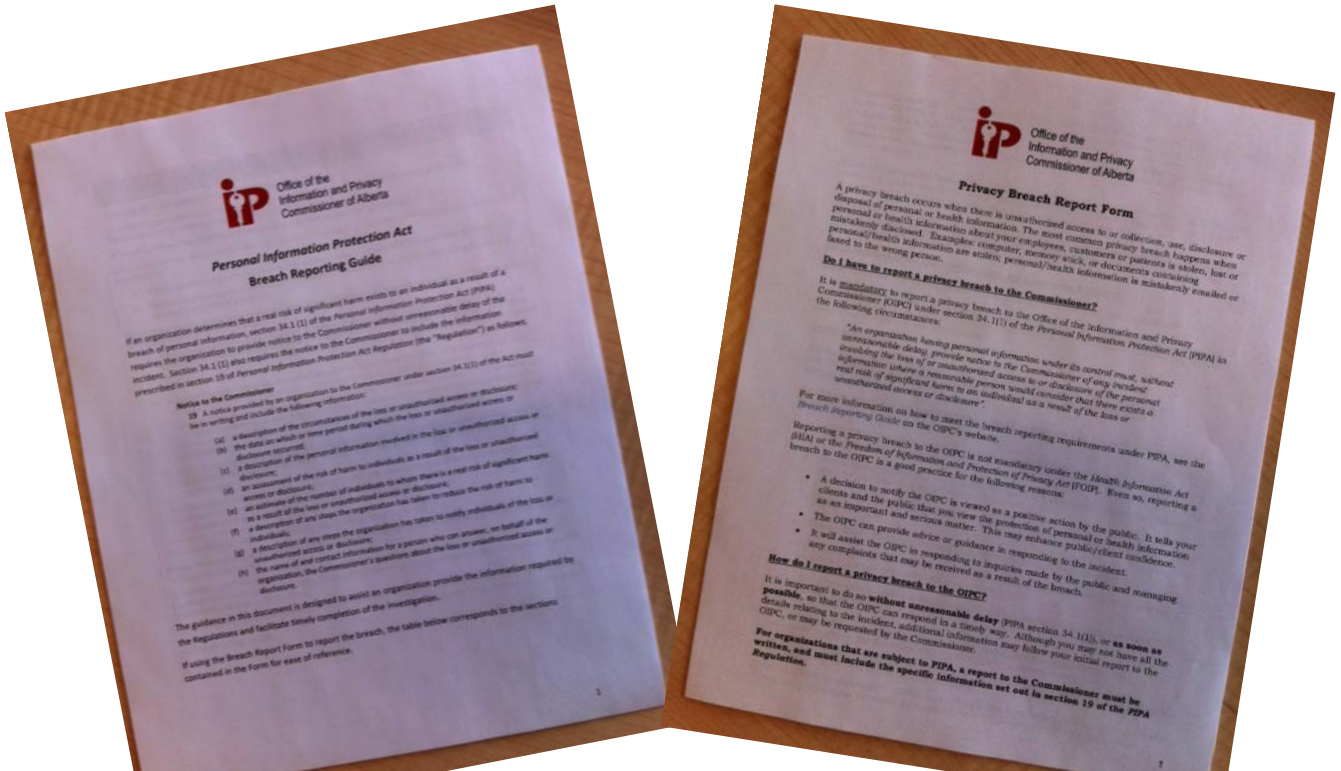
Privacy breaches can be reported under PIPA to the OIPC as follows:

Office of the Information and Privacy Commissioner
Suite 2460, 801 – 6th Avenue S.W.,
Calgary, Alberta T2P 3W2
Tel: (403) 297-2728
Fax: (403) 291-2711
Email: generalinfo@oipc.ab.ca

1

Forms Available to Assist Organizations

- There is a Breach Report Form and a Breach Reporting Guide on the OIPC website



BC Resources

- http://www.oipc.bc.ca/for-private-organizations.aspx

- “Privacy Breaches: Are you prepared?”
- “Privacy Breaches: Tools and Resources”
  - 4 Key Steps
  - 1) Contain the Breach
  - 2) Evaluate the Risks
  - 3) Notification
  - 4) Prevention

CASE STUDIES

You are the Chief Privacy Officer. Discuss and be prepared to advise your breach reporting team and the executive with respect to the following scenarios:

Case Scenario #1

- You are the PO for a provincial health authority. The IT Manager informs you of the following:
- As a result of an investigation into the failure of financial software, she discovered that the network had been infected with a “Trojan Horse.”
- The anti-virus software did not detect the malware as it is a “new” strain that was not yet detectable.
- The malware is designed to steal data from an infected computer and send it to server controlled by an unauthorized party.
- The malware affected a clinical internet application, Supreme Care Portal. The Portal contains a lifetime record a residents’ health information that is accessible via a website by authorized health service providers. Some or all of the following information about residents is contained on the website: patient demographic information (name, address, phone numbers, birthdates, health care id numbers), drugs, allergies or intolerances, immunizations, lab results, diagnostic imaging reports, other medical reports (discharge summaries & consultations.)
- The IT Manager informed you that she has contained the outbreak and removed the malware from over 3000 computers. The audit record did not indicate that data had been sent to the unauthorized external server address associated with the malware.
- However, 3 months later, the IT Manager contacts you again and reports as follows:
- As a result of firewall monitoring practices, an unusual increase in network activity, specifically activity involving the volume of information leaving the system, has been noted.
- Upon further investigation a second strain of the same malware involved in the above incident has infected the network.
- An audit confirms that the malware was sending data from infected computers to the same external unauthorized server address as the previous incident for approximately 16 days.
- The investigation reveals it is likely that the first infection resulted in the transmitting of the second new malware virus that activated several months later.
- This data included Supreme Care Portal data and perhaps any information entered by employees to log into personal banking or email accounts. The IT Manager is able to identity resident patient records affected (approximately 11, 000) and could pin point the affected computers.

Case Scenario #1

- What would you do first as PO after receiving this report? What instructions would you give to the IT Manager or recommendations to the Chief Information Officer?
- Would you 1) activate your breach management policy after the first breach – why or why or not? 2) activate your breach management policy after the second incident – why or why not?
- How would you evaluate the risks to the affected individuals?
  - rate the sensitivity of the personal information involved – low, low/medium, medium, medium/high, high for each category and how did you arrive at the rating?
  - What type of harm could come to the affected individuals? Describe. For example, financial harm, identity theft, physical harm or loss, hurt, harm or humiliation.
  - Is the harm significant?
  - What are some of the factors you would consider in your assessment of whether there is a real risk of the significant harm?
- Would you recommend your Organization report this incident to the Commissioner? Why or why not?
- Would you recommend that your Organization notify the affected individuals? Would you recommend notifying all residents that involve the patient information? Why? What about the employees who may have entered personal information into compromised work computers?
- What would you recommend to avoid this kind of situation from happening again?

Case Scenario #2

- You are the Freedom of Information and Protection Coordinator for a large university. An investigator with the Office of the Information and Privacy Commissioner contacts you and informs you that an individual has reported that a used server purchased from a wholesale retailer contained databases of personal information of thousands of students from the university. You get details of the purchase from the investigator and discover the following after conducting a review of records and interviews with the CI Officer::
- The university had used a non-profit society recycling business to deal with unwanted servers. The business offers a variety of services including picking up unwanted equipment, data wiping (onsite or off with certified software) and physical destruction. The non-profit business determines if it will destroy, donate or sell the items to a wholesaler equipment picked up from its members.
- The university was a member of the non-profit business in order that it may take advantage of its services. No written contract outlining services provided by the business was in place with the university.
- The invoices show that the business invoiced the university for picking up the server involved. There is no charge for destroying the data on the server on the invoice.
- The server contained some or all of the following information of approximately 183,900 university students and 3,500 employees from the period 1991-2010: names, email address, home address, phone number(s), date of birth, social insurance number, Alberta Education student numbers, credit card numbers with expiry dates, salary.
- The business had been used to decommission 21 university servers during the past 6 months, including the server involved.

Case Scenario #2

- What would you do first as PO after receiving this report?
- What steps would you recommend to contain this incident? Is there a danger that there could be other incidents of a similar nature?
- Would you activate your breach management policy – why or why not?
- How would you evaluate the risks to the affected individuals?
  - rate the sensitivity of the personal information involved – low, low/medium, medium, medium/high, high for each category and how did you arrive at the rating?
  - What type of harm could come to the affected individuals? Describe. For example, financial harm, identity theft, physical harm or loss, hurt, harm or humiliation.
  - Is the harm significant?
  - What are some of the factors you would consider in your assessment of whether there is a real risk of the significant harm?
- Would you recommend your Organization report this incident to the Commissioner? Why or why not? Which law applies to the incident – FOIP, PIPA, both? Has there been a contravention of the applicable law(s) in your opinion – why or why not?
- Would you recommend that your Organization notify the affected individuals? How would you recommend the Organization notify individuals - directly, indirectly. Draft a brief notification that you would recommend your Organization use if it decided to notify individuals.
- What would you recommend to avoid this kind of situation from happening again?

Case Scenario #3

- Due to an email error, the employees of an entire Organization (100) were carbon copied on an email that contained an attachment with the following personal information of 30 employees:
- Recruitment information – resumes and interview matrix of 15 applicants for a recent job opening, details concerning two candidates that were hired that included copies of offer letters with salary and employment details.
- Termination letters for 5 individuals no longer with the Organization that provided the terms of the termination in addition to the reason for termination.
- Payroll register – name, home contact information, SIN, DOB, salary and deductions for 1 biweekly payroll period (including garnishment if applicable).
- Salary bonus chart – chart of 30 employees and recommendations to management on amounts and reasons for receiving or not receiving bonus at next year end.

Case Scenario #3

- Is the above information personal information?
- How would you rate the sensitivity of the personal information involved – low, low/medium, medium, medium/high, high for each category and how did you arrive at the rating?
- What type of harm could come to the affected individuals? Describe. For example, financial harm, identity theft, physical harm or loss, hurt, harm or humiliation.
- Is the harm significant?
- What are some of the factors you would consider in your assessment of whether there is a real risk of the significant harm?
- Would you recommend your Organization report this incident to the Commissioner?
- Would you recommend that your Organization notify the affected individuals? Would you recommend the Organization notify even before the Commissioner makes a determination? Give reasons supporting your recommendation.

Case Scenario #4

- Payroll 123 provides payroll services to your organization. Payroll 123 receives the following information regarding employees: name, address, phone number, employee ID #, SIN, pay grade & salary details, bank account information.
- A hacker was able to obtain the credentials of an employee of your organization that has access to Payroll 123's systems. Your iPhone went off at 9:59pm, Sunday night with the following email:
- "From Systems Manager, Payroll 123." This is to advise that at 7:02 pm we identified an attempt to set up an unauthorized payroll period by one of your authorized users.
- During the course of this event, what we assume was an authorized third party was able to access all of the payroll records of your employees. Between 8:45 and 8:52, an unauthorized data download from the database occurred. At 9:23 the payroll database was physically taken offline by our staff and powered off entirely. We are assessing the incident and will provide further information as it becomes available".
- Payroll 123 cannot confirm exactly what information the hacker had access to. Audit records only show the hacker was in the system for approximately 15 minutes. Payroll 123 cannot confirm what if any information was actually accessed or disclosed.

Case Scenario #4

- Is the above information personal information?
- Does your Organization have control or custody or both of the information?
- How would you rate the sensitivity of the personal information involved – low, low/medium, medium, medium/high, high for each category and how did you arrive at the rating?
- What type of harm could come to the affected individuals? Describe. For example, financial harm, identity theft, physical harm or loss, hurt, harm or humiliation.
- Is the harm significant?
- What are some of the factors you would consider in your assessment of whether there is a real risk of the significant harm?
- Would you recommend your Organization report this incident to the Commissioner?
- What would you recommend to your Organization in terms of notifying the affected individuals?
- What would you recommend to avoid this kind of situation from happening again? Would you consider different contractual terms with respect to 123 Payroll with respect to auditing and breach reporting requirements?

Case Scenario #5

- A life insurance provider (the “Organization”) requires applicants to submit to several medical examinations and tests.
- The Organization mailed the medical lab results of two individual applicants. Coverage was denied due to positive lab test results. The lab results pertained to a type of communicable disease.
- The document contained the name, address, email address, description of the positive medical lab results, details of when and where the tests were taken, and a statement denying life insurance coverage.
- The lab results for one applicant were put in the envelope of another applicant by mistake and vice versa.
- Both individuals contacted the Organization and returned the lab results sent to them in error.
- The individuals reside in different cities in the same province.

Case Scenario #5

- Is the above information personal information?
- Does your Organization have control or custody or both of the information?
- How would you rate the sensitivity of the personal information involved – low, low/medium, medium, medium/high, high for each category and how did you arrive at the rating?
- What type of harm could come to the affected individuals? Describe. For example, financial harm, identity theft, physical harm or loss, hurt, harm or humiliation.
- Is the harm significant?
- What are some of the factors you would consider in your assessment of whether there is a real risk of the significant harm?
- Would your assessment of real risk of harm change if the Organization obtained a written undertaking from each individual that they did not copy or retain the information and would not use or disclose any information received in error?
- Would you recommend that your Organization report this incident to the Commissioner?
- What would you recommend to your Organization in terms of notifying the affected individuals?

Case Scenario #6

- An employee (the “Employee”) of a credit union (the “Organization”) took a laptop and paper files home concerning 5 customers and 1 Organization employee. The Employee left the bag containing the laptop and the files in a car parked outside the Employee’s residence. When the Employee went to retrieve the bag the next day, it had been stolen.
- The laptop was encrypted and no personal information was stored on the hard drive.
- The paper files contained the information of the 5 customers and one employee.
- The employee’s information included the following: name, SIN, DOB, home address, account number. The 5 customers information included the following: name, customer number, address (home and business), SIN, DL number, membership number, account transaction information including money wires and automated fund transfers.
- The paper files were returned to the Organization by a local newspaper. The newspaper had followed up on reports that the documents were found on a city street. The laptop was not recovered.

Case Scenario #6

- How would you rate the sensitivity of the personal information involved – low, low/medium, medium, medium/high, high for each category and how did you arrive at the rating?
- What type of harm could come to the affected individuals? Describe. For example, financial harm, identity theft, physical harm or loss, hurt, harm or humiliation.
- Is the harm significant?
- What are some of the factors you would consider in your assessment of whether there is a real risk of the significant harm?
- Would you recommend your Organization report this incident to the Commissioner?
- What would you recommend your Organization in terms of notifying the affected individuals?
-

Other issues to consider when dealing with a privacy incident:

- Discuss what you consider are the top 5 essential elements of a good privacy breach reporting and management system.
- Who is on your response team and why?
- How do you deal with someone on the executive who wants to put a particular “spin” on the breach – i.e. no big deal, no need to notify affected individuals?
- What would your team document and why?
- Can your response plan or how you deal with a breach be accessed by the public, media? How would this influence your approach?
- What would your advice be with respect to dealing with inquiries by affected individuals? Media?

Questions

THANK YOU!