Ready for November 1st: A Primer on the Impact of PIPEDA's Security Breach Notification Requirements

PROFESSIONAL DEVELOPMENT INSTITUTE, UNIVERSITY OF OTTAWA

Adam Kardash, Chair, Privacy and Data Management,
Osler, Hoskin & Harcourt LLP
Co-Lead, AccessPrivacy

November 1, 2018

OSLER

Presentation Overview

- Key Features of the Emerging Data Environment
- Security Incident Trends Experienced by Client Base
- Themes of Privacy Regulatory Authority Information Requests
- Narrative of Incident Response
- Statutory Safeguarding Obligations
- Current Security Breach Notification Requirements in Canada
- PIPEDA's Security Breach Notification Regime
- Notification and Record-Keeping Considerations
- Impact of PIPEDA's Security Breach Notification Regime
- Significance of Security Incident Readiness and Response Plan
- Common Elements of Breach Readiness and Response Protocols

Key Features of the Emerging Data Environment

- Rapid advances in information technology
- Proliferation of new data ecosystems
- Explosion in the volume of data
- High velocity of “data transactions”
- Data ubiquity – the data is “everywhere”
- Intensifying volume, breadth and sophistication of security threats

Common client mandate:

- Help us mitigate the expanding array of privacy, legal and other risks associated with our custody and control of data

Security Incident Trends Experienced by Client Base

- Clients are experiencing the following:
  - Over the past 24 months, marked increase in the volume, intensity, sophistication and breadth of security incidents, including:
    - State-sponsored/organized criminal attacks and (undetected) infiltration
    - Employee “snooping” incident spike
    - Incidents commonly (and increasingly) involving data in custody of third party service providers/vendors
    - Data extortion/ ransomware
  - Incidents arising from employee “mistakes” and complacency
    - Loss of data
    - Coding errors
    - Inadvertent disclosures

Themes of Privacy Regulatory Authority Information Requests

- During investigation of security incidents, privacy regulatory authorities commonly ask the following:
  - Demonstrate your information security governance program
  - Describe how you implemented your security incident response protocol
    - Demonstrate containment, risk evaluation, appropriate notification, continuous improvement
  - Show evidence of regular training and awareness
    - Demonstrate a “culture of privacy and security”
  - Show evidence of regular compliance monitoring
- Responses to above will also be important to responding to claims in negligence, tort, vicarious liability and breach of contract in private litigation

“Narrative” of Incident Response is Critical

- Office of the Privacy Commissioner of Canada Annual Report to Parliament, 2012

“2.11.1 LinkedIn moves quickly to stem damage from major cyber-attack

In June 2012 LinkedIn, a business networking site, had nearly 6.5 million user passwords stolen and posted online. While the breach exposed certain weaknesses in its information safeguards, LinkedIn was swift in its breach response and co-operative with our Office and our counterparts in British Columbia, Alberta and Quebec.

Its commitment to remediation clearly flowed from the top, with senior management authorizing a “Code Red” response that rendered the breach the top priority for the organization and triggered an immediate deployment of resources to deal with the breach.

Afterwards, LinkedIn followed up by reviewing their response, assessing what they learned, and further strengthening their information security measures.

LinkedIn, like many organizations, could have had better safeguards for information to begin with. But when we looked at the company’s breach response in the face of a cyber-attack, we found the organization had demonstrated due diligence and accountability.”

“Narrative” of Incident Response is Critical

- "In the immediate case, given that: (a) Home Depot apparently did nothing wrong; (b) it responded in a responsible, prompt, generous, and exemplary fashion to the criminal acts perpetrated on it by the computer hackers; (c) Home Depot needed no behaviour management; (d) the Class Members' likelihood of success against Home Depot both on liability and on proof of any consequent damages was in the range of negligible to remote; and (e) the risk and expense of failure in the litigation were correspondingly substantial and proximate, I would have approved a discontinuance of [the] proposed class action with or without costs and without any benefits achieved by the putative Class Members.“
  - *Lozanski* v. *The Home Depot, Inc.*, 2016 ONSC 5447 at para. 74

- "The case for Home Depot being culpable was speculative at the outset and ultimately the case was proven to be very weak. The real villains in the piece were the computer hackers, who stole the data. After the data breach was discovered, there was no cover up, and Home Depot responded as a good corporate citizen to remedy the data breach. There is no reason to think that it needed or was deserving of behaviour modification. Home Depot's voluntarily-offered package of benefits to its customers is superior to the package of benefits achieved in the class actions.“
  - *Lozanski* v. *The Home Depot, Inc.*, 2016 ONSC 5447 at para. 100

Safeguarding Requirements under Canadian Privacy Statutory Regime

- PIPEDA is one of 33 Canadian federal, provincial private sector, public sector and health statutes
- Canadian Private Sector Privacy Statutes
  - *Personal Information Protection and Electronic Documents Act* (Federal)
  - *Personal Information Protection Act* (BC)
  - *Personal Information Protection Act* (Alberta)
  - *An Act Respecting the Protection of Personal Information in the Private Sector* (Quebec)
- Statutes set out a regime for the protection of personal information, although each varies in scope, they contain substantively similar requirements.

Statutory Safeguarding Obligations

- In essence, safeguarding provisions require organizations to take reasonable / appropriate technical, physical and administrative measures to protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, modification or destruction.
- Policies, practices, procedures – part of information security governance framework
  - Part of broader privacy governance framework
  - Required by statutory obligations under “accountability” principle
  - Includes incident readiness and response protocol

What is a “reasonable” safeguard?

- “The reasonableness of security measures and their implementation is measured by whether they are objectively diligent and prudent in all of the circumstances. To acknowledge the obvious, “reasonable” does not mean perfect. Depending on the situation, however, what is “reasonable” may signify a very high level of rigour.”

  (See BC Investigation Report F06-01 and BC Order P17-01)

- A meaningful assessment of the required level of safeguards for any given personal information must be context based, commensurate with the sensitivity of the data and informed by the potential risk of harm to individuals from unauthorized access, disclosure, copying, use or modification of the information.

  (See PIPEDA #2018-001; #2016-005; #2014-015; #2014-010; #2014-004;#2014-003; #2013-001; #2012-009; #2003-180; #2003-177; #2002-72; #2001-5).

What is a “reasonable” safeguard?

- Findings by privacy regulatory authorities provide the following list of factors for organizations to consider when evaluating the reasonableness of their safeguards:
  - The sensitivity of the personal information;
  - The foreseeable risks;
  - The likelihood of damage occurring;
  - The medium and format of the record containing the personal information;
  - The seriousness of the harm;
  - The cost of preventative measures; and
  - Relevant industry standards of practice.
    - Note: Standards set “minimum” set of expectations.

  (See, for example, Alberta Investigation Reports P2006-IR-005 and P2008-IR-002; British Columbia Orders P15-01 and P17-01; and OPC and OIPC Alberta Report of an Investigation into TJX Companies Inc.)

Current Security Breach Notification Requirements in Canada

- Federal *Personal Information Protection and Electronic Documents Act*
- Alberta's *Personal Information Protection Act*
  - Includes statutory obligation to notify the Alberta Commissioner of a breach where there is a real risk of significant harm to an individual.
  - Alberta Commissioner has authority to require organizations to notify affected individuals of a breach.
  - All security breach decisions posted on OIPC website
- Eight health privacy statutes
  - Ontario's *Personal Health Information Protection Act*;
  - New Brunswick's *Personal Health Information Privacy and Access Act*;
  - Nova Scotia's *Personal Health Information Act*;
  - Newfoundland and Labrador's *Personal Health Information Act*;
  - Northwest Territories' *Health Information Act*;
  - Yukon's *Health Information Privacy and Management Act*;
  - Prince Edward Island's *Health Information Act*; and
  - Alberta's *Health Information Act*.
- Two public sector privacy statutes
  - Newfoundland and Labrador's *Access to Information and Protection of Privacy Act, 2015*; and
  - Nunavut's *Access to Information and Protection of Privacy Act*.

PIPEDA's Security Breach Notification Regime

- Amendments to the *Personal Information Protection and Electronic Documents Act* include new security breach notification requirements, in force as of November 1, 2018
- For certain "breaches of security safeguards", new security breach notification provisions contain a three-pronged notice requirement - (i) Report to the Office of the Privacy Commissioner of Canada, (ii) Notice to affected individuals, and (iii) Notice to other organization:
- Failure to comply with the breach notification provisions will be:
  - an offence punishable on summary conviction liable to a fine not exceeding $10,000, or
  - an indictable offence and liable to a fine not exceeding $100,000 (PIPEDA, s.28).

Definition of "Breach of Security Safeguards"

- "The loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's safeguards that are referred to in clause 4.7 of Schedule 1 or from a failure to establish those safeguards" (PIPEDA, s. 2(1)).

Reporting to the Commissioner

- Organizations required to report to the Commissioner any "breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates **a real risk of significant harm** (RROSH) to an individual" (PIPEDA, s.10.1(1)).

Definition of "Significant Harm"

- "Significant harm" includes "bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property" (PIPEDA. s.10.1(7)).

RROSH Factors

- Factors listed as relevant to determining whether a breach of security safeguards creates a real risk of significant harm include:
  - the sensitivity of the personal information involved in the breach;
  - the probability that the personal information has been, is being or will be misused; and
  - any other prescribed factor (PIPEDA. s.10.1(8)).
- Highly contextual assessment required.

RROSH Factors

In determining **the probability of misuse**, organizations should consider:

- What happened and how likely is it that someone would be harmed by the breach?
- Who actually accessed or could have accessed the personal information?
- How long has the personal information been exposed?
- Is there evidence of malicious intent (e.g., theft, hacking)?
- Were a number of pieces of personal information breached, thus raising the risk of misuse?
- Is the breached information in the hands of an individual/entity that represents a reputation risk to the individual(s) in and of itself? (e.g. an ex-spouse or a boss depending on specific circumstances)
- Was the information exposed to limited/known entities who have committed to destroy and not disclose the data?
- Was the information exposed to individuals/entities who have a low likelihood of sharing the information in a way that would cause harm? (e.g. in the case of an accidental disclosure to unintended recipients)
- Was the information exposed to individuals/entities who are unknown, or to a large number of individuals, where certain individuals might use or share the information in a way that would cause harm?
- Is the information known to be exposed to entities/individuals who are likely to attempt to cause harm with it (e.g. information thieves)? Has harm materialized (demonstration of misuse)?
- Was the information lost, inappropriately accessed or stolen?
- Has the personal information been recovered?
- Is the personal information adequately encrypted, anonymized or otherwise not easily accessible?

(OPC Guidance: *What you need to know about mandatory reporting of breaches of security safeguards*)

Timing and Content Requirements

- Reports to the Commissioner shall be made "as soon as feasible after the organization determines that the breach has occurred" (PIPEDA, s.10.1(2)).
- Reports must contain:
  - a description of the circumstances of the breach and, if known, the cause;
  - the day on which, or period during which, the breach occurred or, if neither is known, the approximate period;
  - a description of the personal information that is the subject of the breach to the extent that the information is known;
  - the number of individuals affected by the breach or, if unknown, the approximate number;
  - a description of the steps that the organization has taken to reduce the risk of harm to affected individuals that could result from the breach or to mitigate that harm;
  - a description of the steps that the organization has taken or intends to take to notify affected individuals of the breach in accordance with subsection 10.1(3) of PIPEDA; and
  - the name and contact information of a person who can answer, on behalf of the organization, the Commissioner's questions about the breach (*Breach of Security Safeguards Regulations*, s. 2(1)).

Notification of Affected Individuals

- Where a breach of security Safeguards gives rise to a RROSH organizations must notify affected individuals (PIPEDA, s.10.1(3)).
- The notice to individuals must be provided “as soon as feasible” and contain “sufficient information to allow the individual to understand the significance to them of the breach and to take steps, if any are possible, to reduce the risk of harm that could result from it or to mitigate that harm” (PIPEDA, s.10.1(4)).

Content of Notification to Affected Individuals

- Notification to affected individuals must include:
  - a description of the circumstances of the breach;
  - the day on which, or period during which, the breach occurred or, if neither is known, the approximate period;
  - a description of the personal information that is the subject of the breach to the extent that the information is known;
  - a description of the steps that the organization has taken to reduce the risk of harm that could result from the breach;
  - a description of the steps that affected individuals could take to reduce the risk of harm that could result from the breach or to mitigate that harm; and
  - contact information that the affected individual can use to obtain further information about the breach (*Breach of Security Safeguards Regulations*, s. 3).

Notification to Other Organizations

- Where a breach of security safeguards gives rise to RROSH, organizations must "notify any other organization, a government institution, or a part of a government institution of the breach," if the notifying organization believes that the other organization or institution "may be able to reduce the risk of harm that could result or mitigate that harm, or if any of the prescribed conditions are satisfied" (PIPEDA, s.10.2(1)).

Notification to Other Organizations

- Notification to other organizations could include:
  - "Notifying law enforcement when there is an attack on [the organization's] computer system where bad actors have accessed customers' information, if [the organization] believes law enforcement may be able to reduce the risk of harm that could result from the breach or mitigate the harm."
  - "Notifying an organization that processes [the organization's] payments, in the case of a breach affecting individuals' payment card information, if [the organization] believe[s] the [other] organization may be able to reduce the risk of harm that could result from the breach or mitigate the harm."

(OPC Guidance: *What you need to know about mandatory reporting of breaches of security safeguards*).

Record-Keeping Requirement

- Organizations are required to "keep and maintain a record of **every breach** of security safeguards involving personal information under its control" (PIPEDA, s.10.3(1)).
- Notably, this obligation applies to "every breach of security safeguards," not just to breaches that are deemed to create a "real risk of significant harm."
- Organization must maintain such records for 24 months after the day on which the organization determines that the breach has occurred (*Breach of Security Safeguards Regulations*, s. 6(1)).
- Record must contain any information that enables the Commissioner to verify compliance with breach regime.
- The Privacy Commissioner must be provided, with access or a copy of the record upon request (PIPEDA, s.10.3(2)).

Record-Keeping Requirement

- OPC guidance sets out the following minimum expectations for what a record should include:
  - date or estimated date of the breach;
  - general description of the circumstances of the breach;
  - nature of information involved in the breach; and
  - whether or not the breach was reported to the Privacy Commissioner of Canada/individuals were notified.
- In addition, OPC guidance provides that:

  "The record should also contain sufficient details for the OPC to assess whether an organization has correctly applied the real risk of significant harm standard and otherwise met its obligations to report and notify in respect of breaches that pose a real risk of significant harm. This could include a brief explanation of why the organization determined there was not a real risk of significant harm in cases where the organization did not report the breach to the Privacy Commissioner and notify individuals."

  (OPC Guidance: *What you need to know about mandatory reporting of breaches of security safeguards*)

Record-Keeping Requirement

- Record-Keeping Requirement
  - Designed to enhance OPC oversight, incentivize accountability and continuous improvement
  - Obligation to maintain record of “every breach” for specified period of time after day on which the organization determines breach has occurred – exceptionally broad, unqualified
    - Includes records maintained by service providers
  - Since records are accessible to OPC upon request, tactical approach for record-keeping required

Impact of PIPEDA's Security Breach Notification Regime

- Based on client experience stemming from introduction of US state security notification requirements and PIPA Alberta requirement, PIPEDA security breach notification regime will result in:
  - Enhanced transparency/reporting about security incidents within organizations
  - More notifications to affected individuals (and other persons) about security incidents
  - More media reports and general awareness about information security (or lack thereof)
  - More investigations/posted decisions by privacy regulatory authorities
  - Increased sophistication and expectations of privacy regulatory authorities
  - Increased litigation risk
  - More proactive efforts by organizations to address personal information security concerns
  - Increased costs to organizations due to all of the above

Significance of Security Incident Readiness and Response Plan

- Significance of effective security incident response plan cannot be overstated
- AccessPrivacy Thought Leadership Security Incident Workshops:
  - 300+ CPOs, privacy counsel, privacy compliance professionals attended workshops
  - 90% of participants indicated that their organizations had a data breach response plan, yet **only half** expressed confidence that their organization's response plan would be sufficient to respond to a public, large scale security incident

Common Elements of Breach Readiness and Response Protocols

- Identify who is responsible for the coordination and response to an incident
- Identify stakeholders on the response team
- Engage key service providers
- Clarify internal reporting/escalation structure
- Assess sufficiency of insurance coverage
- Conduct “tabletop” testing exercise
- Conduct breach training and awareness
- Outline approach to key steps in incident response process:
  - Discovery of nature and scope of the incident
  - Internal communications
  - Record keeping
  - Breach containment and preliminary investigation
  - Evaluation of risks to affected individuals, organization, other stakeholders)
  - External communications
  - Notification to affected individuals
  - Reporting/notification to regulatory authorities, law enforcement, other stakeholders
  - Action plan for future incidents