LexisNexis®

advancing
what's possible

How to Handle a Data Breach Like a Pro: complying with new requirements, without making things worse

Co-presented by:

Timothy Banks, Partner, nNovation LLP

Sarah Eisen, CIPP/C, CIPM, Content Lawyer (Corporate)
Lexis Practice Advisor Canada

Sarah Dale-Harris, Director of Content, Large and Mid-Law
Lexis Practice Advisor Canada

Tuesday, November 20, 2018

Preparing for data breaches

Timothy Banks
Partner
nNovation LLP

Today's speaker

Sarah Eisen
Content Lawyer (Corporate)
Lexis Practice Advisor Canada

Co-presenter

Sarah Dale-Harris
Director of Content
Large and Mid-Law Lexis Practice Advisor Canada
Co-presenter

Data breach laws are becoming the norm

- *Personal Information Protection Act* (Alberta)
- *Health Information Act* (Alberta)
- *Personal Health Information Protection Act* (Ontario)
- All 50 U.S. States
- E.U. General Data Protection Regulation

Breach of security safeguards

Breach of security safeguards means the **loss** of, **unauthorized access** to or **unauthorized disclosure** of personal information **resulting from** a breach of an organization's security safeguards that are referred to in clause 4.7 of Schedule 1 or from a failure to establish those safeguards.

Clause 4.7, Schedule 1

- Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.
- The methods of protection should include (a) physical measures, for example, locked filing cabinets and restricted access to offices; (b) organizational measures, for example, security clearances and limiting access on a “need-to-know” basis; and(c) technological measures, for example, the use of passwords and encryption.

Key obligations

- Create a record of each breach of security safeguards
- Assess whether there is a real risk of significant harm (RROSH) to an affected individual
- As soon as feasible after determining the breach has occurred, report breaches with a RROSH to:
  - the Office of the Privacy Commissioner of Canada
  - affected individuals
  - third parties (if it could reduce the risk of harm)

Who has to report?

- The organization that is in control of the personal information (there may be more than one)
- Ask:
  - Who decides what information is collected and how it is used?
  - To whom does the individual provide consent?
  - Does the service organization use the information solely on behalf of another organization or for its own purposes

Timelines for reporting

Law	Timeline
PIPEDA	“as soon as feasible after the organization determines that the breach has occurred”
Alberta PIPA	“without unreasonable delay”
GDPR	“without undue delay and, where feasible, not later than 72 hours after having become aware of it” Processors: “without undue delay after becoming aware “
California	“in the most expedient time possible and without unreasonable delay” Hosts: immediately following discovery

Traps!

- Blinders with respect to all of the potentially applicable laws
- Failing to take the record-keeping requirement seriously (and instituted comprehensive policies, procedures, education and vendor management)
- Not practicing or planning

Contents of the breach record

Sufficient detail for the OPC to assess whether an organization has correctly applied the RROSH standard and met its obligations. At a minimum:

- date or estimated date of the breach
- general description of the circumstances of the breach
- nature of information involved in the breach
- whether or not the breach was reported to the OPC and individuals were notified and brief reasoning

Mistakes lead to a loss of trust

- Getting stuck in denial
- Keeping critical internal stakeholders in the dark (the cloak of secrecy)
- Hesitating or being unclear about what you are going to do for affected individuals

Responding and earning trust

- Clear lines of reporting internally with pre-determined thresholds for board reporting, proactive public announcements, proactive discussions with OPC
- Clear communication that focuses on the individual
- Don’t feed the story with flip/flops or by prioritizing the press or the OPC – focus on the individual
- Spend the money on assisting individuals and plan for the ones who are sensitive or unable to help themselves

Get prepared now

- Map your data breach obligations to your business now
- Internal reporting chains and training
- Templates for employee communications and public communications in the event of a breach
- Estimate the cost of a breach and what you will need for different sized breaches

Questions?

Feel free to contact us at any time

Timothy Banks

Partner

nNovation LLP

tbanks@nnovation.com

Sarah Eisen

Content Lawyer (Corporate)

Lexis Practice Advisor Canada

sarah.eisen@lexisnexis.ca