



uOttawa

L'Université canadienne
Canada's university



Security Breach Notification

Philippa Lawson, Director
Canadian Internet Policy and Public Interest Clinic
University of Ottawa, Faculty of Law

www.cippic.ca

*BC FIPA Privacy and ID Theft Conference
Vancouver, B.C.
Nov.24-25th 2008*



The Problem

- Computer databases vulnerable to attack
- Organizations failing to take even basic measures to protect personal data
- Business incentive = to cover up
 - avoid reputational damage, lawsuits, etc.
- USA:
 - 446 disclosed security breaches in 2007
 - 449 disclosed breaches by Aug.22, 2008

History of SBN Laws

- 2003
 - Canadian consumer groups advocate
 - California adopts law
- 2005
 - Choicepoint breach
- 2005-2007
 - Most U.S. states adopt SBN laws
- 2007
 - ETHI Committee report advocates (PIPEDA)
 - Federal government announces intention to legislate
 - OPCC voluntary guidelines initiative
- 2008
 - Industry Canada consults on proposed legislative model



Why?

- Create stronger incentive for organizations to take effective security measures
- Allow individuals to mitigate potential harm
- Increase confidence in electronic marketplace
 - Industry Canada
- Provide basis for future policy, compliance actions
 - CIPPIC
- Improve functioning of marketplace through greater consumer awareness of risks
 - CIPPIC

Issues

- Definition of breach
- Threshold for reporting
- Responsibility for deciding
- Notification to whom?
- Timing of Notification
- Manner of Notification
- Content of Notification
- Penalties and Enforcement



Definition of data breach

- “an incident involving unauthorized collection, use, disclosure, loss, or access to personal information”
 - Industry Canada proposal (PIPEDA)
 - covers accidental loss as well as theft
 - does not cover loss/disclosure by individual, beyond control of organization (e.g., phishing, pharming)



Threshold for Reporting

- US laws:
 - must notify when specified “personal information” is reasonably believed to have been acquired by an unauthorized person
 - some exceptions where risk of harm unlikely
- Industry Canada proposal:
 - must notify when there is “a high risk of significant harm” resulting from the breach
 - list of factors to consider



Threshold for Reporting

	Significant Harm	Moderate Harm	Minimal Harm
High Risk			
Moderate Risk			
Low Risk			



Responsibility for Reporting

- Organization to determine
 - potential liability for not notifying
- Alternative:
 - Privacy Commissioner determines
 - in every case, or
 - upon request



Whom to Notify?

- affected individuals
- Privacy Commissioner
- Other?
 - Law enforcement (re: suspected crime)
 - Government agencies (re: relevant ID docs)
 - Banks, etc (re: relevant accounts)
 - Credit bureaus (to flag affected files)?

Timing of Notification

- Industry Canada:
 - “as soon as is reasonably possible following discovery of the breach”
 - delay permitted if law enforcement requests
- CIPPIC, PIAC:
 - specify maximum (e.g., 14 days); permit longer period if justified



Manner of Notification

- Industry Canada:
 - Directly to affected individuals, if possible
 - Email only where individual expressly consented to receive important messages that way
 - Not associated with any other communication

Content of Notification

- Industry Canada:
 - general description of incident
 - date or time frame
 - personal data involved
 - general account of actions taken
 - what the individual can do to mitigate
 - what the organization will do to help
 - contact info for org + OPC
 - whether breach was reported to OPC, other organizations



Reporting to OPC

- All “material breaches”
 - Factors to consider:
 - Magnitude (# individuals affected)
 - Sensitivity of data
 - Number of data elements
 - Whether data encrypted or otherwise unusable
 - Probability of misuse
 - Accidental vs. intentional
 - Other contextual factors
- “within a reas. period of time after detection”
 - preferably before notifying individuals



Role of OPC

- Oversight of organization compliance with SBN rule
- Compilation, analysis, reporting of aggregate data
 - CIPPIC, PIAC called for reporting requirement
- Availability of company-specific data
 - Organizations expressed concern about ATIP
 - CIPPIC, PIAC proposed public registry

Next Steps?

- Federal government
 - PIPEDA amendments?
 - Privacy Act reform?
- Provinces
 - PIPA amendments? (BC, Alta)
 - Other legislative initiatives?



www.cippic.ca



uOttawa

L'Université canadienne
Canada's university