



Proudly Presents...

Privacy Update

Hot Issues for Risk Professionals

Agenda

1. Privacy overview including PIPEDA & Privacy Commissioner's role
2. 2011 Trends & Issues
3. Coming Changes: Anti-Spam
4. Common and unexpected breach situations & lessons learned
5. Cyber Liability & Data Privacy – A Risk Management & Control Perspective
6. Risk Transfer – Key Considerations



Office of the
Privacy Commissioner
of Canada

Commissariat
à la protection de
la vie privée du Canada

Daniel Caron
Legal Counsel
Office of the Privacy
Commissioner of Canada

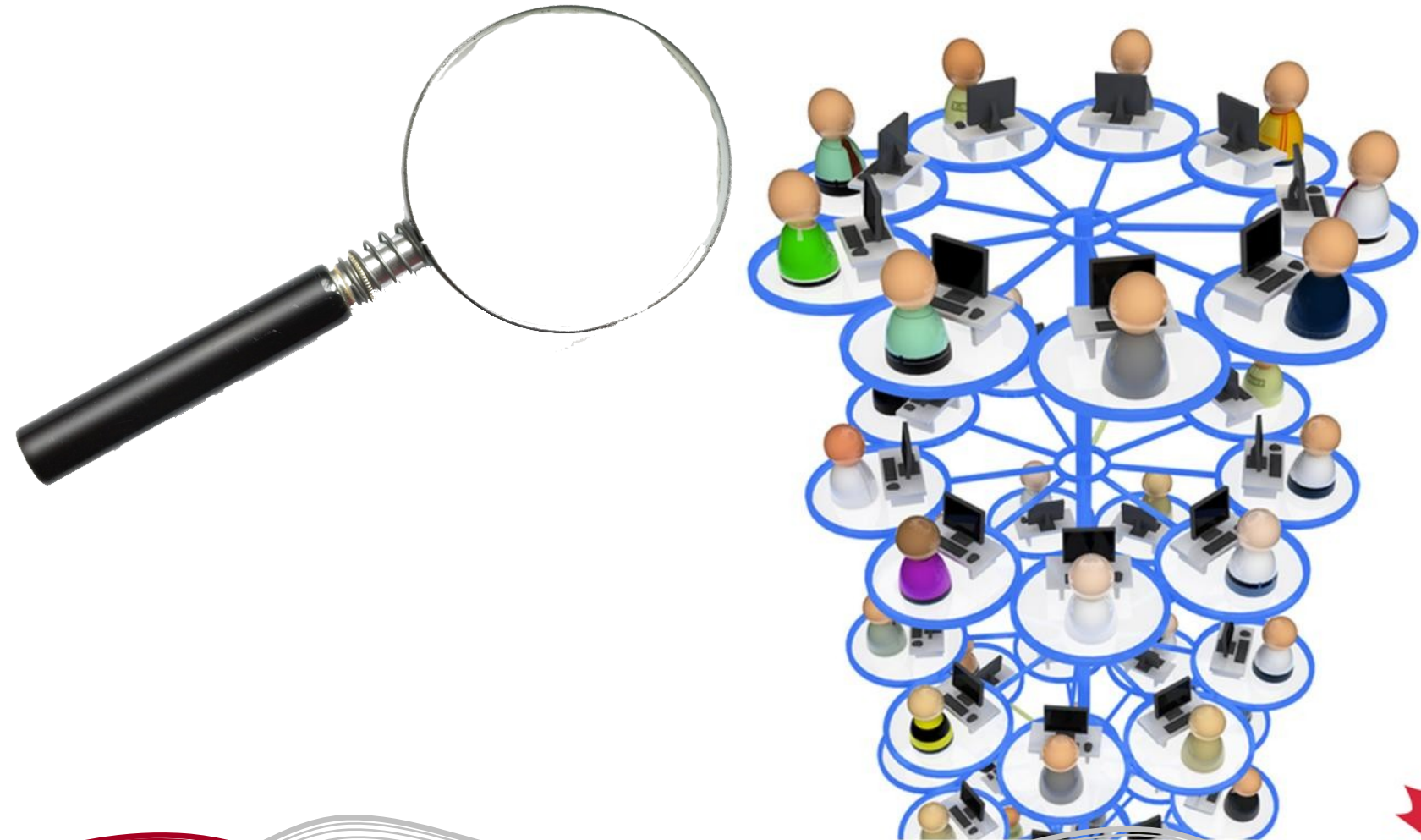
Privacy... Why Should You Care?

- A fundamental right in Canada
- Involves compliance with privacy legislation
- Can provide a competitive advantage
- Can minimize risks... both \$ and non-\$
- It's expected

So What is PIPEDA All About?

- PIPEDA is the federal private-sector personal information protection statute
- Accountability
 - Building privacy at the front-end to minimize risk at the tail-end
 - Disclosures v. transfers of personal information
- Knowledge and Consent, Appropriate Purposes, Limiting Collection, Safeguarding, and ... Notification?

The Role of the Office of the Privacy Commissioner



Dealing With the OPC

- The OPC is an ombuds office
 - Investigates complaints
 - Issues “findings and recommendations”
 - Possible follow-ups...
- Can go to Federal Court to seek enforcement
- Can make public information management practices if it is in the public interest
- Also interacts with stakeholders, organizations, the public, and international counterparts

Trends and Issues in 2011

- New platforms: social networking sites, mobile applications, cloud computing services
- New applications of technologies: facial recognition, geolocation
- The year of the data breach
- Government access to personal information
- International scope and cooperation

Margot Patterson, Counsel

Fraser Milner Casgrain LLP



Coming changes: Anti-Spam and PIPEDA

- What do the changes mean for organizations?
 - New and expanded responsibilities
 - Violations and penalties
 - Private right of action

Lessons Learned Part I: Breach situations

- The Expected
- The Unexpected
- The Impact of new requirements under Anti-Spam Legislation and PIPEDA:
 - How to prepare for the expected impacts and the unknown

Lessons Learned Part II: Best Practices

- Minimizing exposure
- Allocating risk

Scenarios:

- Cloud computing
- Social media

Aaron Konarsky

Director, Risk Management and Internal Controls, Canada Lands Company



CANADA LANDS COMPANY

SOCIÉTÉ IMMOBILIÈRE DU CANADA

Cyber Liability Challenges to Business & Government

Aon's Global Risk Management Survey 2011 found the following related risk rankings out of 49 risk descriptions:



Data & privacy breaches are everywhere and rising exponentially with larger losses due to exceptional growth of electronic data storage and communication.

Key Target Industries

- Financial Institutions
- Retailers
- Hospitality & Tourism (Food & Beverage)
- Payment Processors
- Government & Defense Industry
- Medical Facilities
- *Any entity with Personal Information on their systems of employees, customer/clients, third parties*


Sources of Losses/Exposures for Data Breach

- Forensic costs to determine what happened and how to prevent a recurrence of breach (highly specialized & technical work)
- Notification costs – content, printing mailing and follow-up
- Mitigation costs – credit monitoring, fines & penalties statutory/regulatory, PCI DSS (industry), other contractual
- Costs incurred in gathering information about breached data (related to first point)
- Defense & legal costs incurred in responding to complaints & litigation, third party claims (could include class actions)
- Regulatory/Law enforcement costs
- Reputational risk

Risk Assessment & Mitigating Exposures

Cyber risk needs to fit into enterprise risk management
planning

Steps to mitigate exposures:

1. *Identification and definition of risks & adoption of security measures to include – review of technical and information security policy safeguards, alignment of company processes with guidelines & relevant privacy laws; and detailed incident response & recovery plan;*
 2. *Contractual indemnity – outsourcers or service providers with access to customers systems & data should have hold harmless or indemnity obligations respecting loss or theft of customer's personal information;*
 3. *Insurance coverage – review or audit of company's existing insurance program to determine coverage and gaps due to new or unexpected privacy & data breaches (traditional insurance may not be able to respond adequately)*
- 

Payment Card Industry Data Standards (PCI DDS)

Requirements for Compliance with Control Objectives

Source: Adapted from PCI Security Standards Council

Control Objectives

1. *Build and Maintain a Secure Network*
2. *Protect Cardholder Data*
3. *Maintain a Vulnerability Management Program*
4. *Implement Strong Access Control Measures*
5. *Regularly Monitor and Test Networks*
6. *Maintain an Information Security Policy*

PCI DDS Requirements

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks
5. Use and regularly update anti-virus software on all systems commonly affected by malware
6. Develop and maintain secure systems and applications
7. Restrict access to cardholder data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security

What are Industry Standards for Payment Cards?

- Data Security Standards apply to all organizations that hold, process or pass payment cardholder information
- Fines & Penalties for Non-Compliance (VISA, MC, etc)
- Contract between the card companies and merchants/service providers
- Non-compliance can be viewed as evidence of negligence

Specialty Risk Transfer for Cyber Liability Exposures

Most traditional insurance policies (crime bond, property, general liability, E & O) do not cover these 'intangible' risks.

The specialty insurer's underwriting application process serves as an excellent & robust internal control questionnaire as its designed to address the risks

Brian Rosenbaum LL.B

**Director, Legal & Research Practice, Financial
Services Group**

Aon Reed Stenhouse Inc.



Coverage in Traditional Insurance Policies

Commercial General Liability Policy

- Bodily injury/property damage trigger limits applicability
- Advertising & personal injury provisions may not apply to lost data

Property Policy

- Coverage limited to damage to tangible property

Professional and Media Liability Policy

- Coverage limited to economic damage arising from negligence in providing professional services
- Media liability coverage must be very broad to account for privacy breach exposures

Coverage in Traditional Insurance Policies

Commercial Crime/Fidelity Policy

- Limited to employee theft of tangible property and computer fraud
- No 3rd party liability coverage

Kidnap, Ransom and Extortion Policy

- Limited to extortion threats with ransom demands

Directors and Officers Policy

- Limited to wrongful acts of directors/officers
- Bodily injury and property damage, intentional acts excluded

Differences Between First and Third Party Coverage

Third Party Costs

- Legal fees, settlements and judgments arising from civil suits brought by business partners, customers/clients and employees
- Legal fees, fines, penalties and damages arising from regulatory investigations and proceedings

First Party Costs

- Damage to data and property
- Investigative costs
- Lost employee productivity
- Mitigation expenses including notification, call centre, credit monitoring and public relations
- Damage to reputation and loss of public, customer/client confidence
- Damage to business relationships
- Recovery and restoration expenses
- Loss of intellectual property
- Business interruption
- Loss of business opportunity/future revenues

Specialized Privacy/Cyber Insurance

·State of the Market

- many new market entrants and forms
- competition is increasing
- forms can be very different in structure and approach which makes comparisons challenging

·Carriers

- Everest
- Chartis
- Chubb
- Ace
- London Markets

·Capacity and Limits

- primary limits available in the \$1-10 million range
- multi-layer programs can be written
- limited loss history and diverse underwriting variables makes benchmarking challenging

·Deductibles

- levels vary and depend on many factors
- for typical program with limits of \$2-5 million deductibles range from \$25,000 to \$50,000
- however, for certain risks and limits of \$10 million and up, deductibles can be \$250,000 and more

·Third and First Party Coverage

- ensure coverage provides both 1st and 3rd party coverage (not all forms do)

·Pricing

- overall rates are slowly declining
- average premium rates range between \$5-12,000 per million for primary layer

Coverage Issues and Options

- Coverage trigger
- Scope of data
- Insider acts coverage
- Employee claims
- Off-site breaches
- Regulatory Proceedings Coverage
- Fines and penalties
- PCI holdbacks
- Independent contractors' coverage
- Event management coverage
- Business interruption coverage
- Loss of corporate information
- Geographic Scope

Panel Discussion & Questions

Thank you for attending the
Ottawa Capital Connexions
Conference