Cybersecurity and Data Protection in Canada

Kim Ozubko
Partner
Miller Thomson LLP
Toronto, Ontario
Agenda

1. Introduction
2. Legal Landscape
3. Best Practices
4. Steps to Reduce Liability
Introduction

• What is data protection?
• What is cybersecurity?
• Cybercrime in Canada
  – Data breach examples
• Are pension and benefit plans at risk?
  – Points of vulnerability
What is Data Protection?

“The process of safeguarding important information from corruption, compromise or loss. The importance of data protection increases as the amount of data created and stored continues to grow at unprecedented rates.”

–Tech Target Network (2019)
What is Cybersecurity?

“The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.”

– Oxford Dictionaries, 2018

“The process of protecting information by preventing, detecting and responding to attacks.”

Cybercrime in Canada

• Types of cybercrime (examples)
  – Untargeted attacks
    • Ransomware
    • Phishing
    • Water holing
  – Targeted attacks
    • Spear-phishing
    • Botnet
    • Disrupting the supply chain
  – Inside attacks
Cybercrime in Canada

• Impact of cybercrime
  – Canadian Survey of Cyber Security and Cybercrime (Statistics Canada 2018)
    • In 2017, 21% of Canadian businesses reported that they were impacted by a cybersecurity incident that affected operations
    • Large businesses (41%) were more than twice as likely as small businesses (19%) to have identified an impact
Data Breach Examples

• Capital One (2019)
  – Former employee of Amazon Web Services, which hosted Capital One database, hacked into server containing personal information
  – Hacked information included names, addresses, phone numbers, postal codes, email addresses, social insurance numbers, birthdates and self-reported income
  – 6 million Canadians and 100 million Americans impacted
### Data Breach Examples

- **Desjardins Group (2018-2019)**
  - Employee improperly collected information about customers and shared information with third party
  - Leaked information included names, addresses, birth dates, SINs, email addresses
  - 2.7 million people and 173,000 businesses impacted
  - Proposed class action filed in Quebec Superior Court alleging negligence
Data Breach Examples

• Condon v. Canada
  – Loss of portable hard drive in 2013 that contained dates of births, addresses, SINs and student loan balances of approximately 583,000 borrowers in Canada Student Loan Programs
  – Class action against Canadian federal government for claim of “intrusion upon seclusion” settled in 2018
    • $17.5 million settlement
Are Pension and Benefit Plans at Risk?

- Pension and benefit plans hold significant amounts of personal data that is of value to the plan, members and beneficiaries and hackers
  - Names, addresses, SINs, DOB, phone numbers, passwords, security questions, personal identification numbers, bank account numbers, healthcare information, salary information
Points of Vulnerability

• Plan sponsors and administrators
  – Data management
  – Technology management
  – Service provider management
  – People issues

• Members and beneficiaries
  – Use of passwords
  – Social networking sites

• Service providers
## Legal Landscape

- Privacy and data management laws
- Statutory torts
- Pension standards legislation
- Common law
Privacy and Data Management Laws: Public Sector

• Federal
  – Privacy Act (Canada)

• Provincial
  – Every province and territory has its own laws that apply to provincial government agencies and their handling of personal information (e.g., Freedom of Information and Protection of Privacy Act (Ontario))
Several provinces have health related privacy laws

- e.g., *Personal Health Information Protection Act* (Ontario)
  - Applies to personal health information that is collected, used and disclosed by health information custodians
- e.g., *Personal Health Information Privacy and Access Act* (New Brunswick)
  - Applies to personal health information that is collected, maintained or used by a custodian
Privacy and Data Management Laws: Private Sector

- **Personal Information Protection and Electronic Documents Act (Canada) ("PIPEDA")**
  - Applies to the collection, use, disclosure and protection of employee personal information by federally regulated employers
  - Applies to the collection, use, disclosure and protection of personal information in the course of commercial activities in all provinces and territories that do not have substantially similar legislation
  - Currently only BC, Alberta and Quebec have substantially similar legislation
Privacy and Data Management Laws: Private Sector

- PIPEDA amended by *Digital Privacy Act*
  - Effective *November 1, 2018*, organizations subject to PIPEDA must report breaches of security safeguards and notify affected individuals where it is reasonable to believe breach creates “real risk of significant harm”
  - Record of data breaches must be maintained for at least 24 months after breach
  - Potential fine of up to $100,000 for breach of legislation
Privacy and Data Management Laws: Private Sector

- Application of PIPEDA to plan member information—plan administrator
  - Is plan administrator under federal jurisdiction (e.g., a bank)?
  - Is plan member employed in province with legislation substantially similar to PIPEDA?
  - Is plan administration activity a “commercial activity”?
Privacy and Data Management Laws: Private Sector

- Application of PIPEDA to plan member information—third party service providers
  - Is plan member employed in province with legislation substantially similar to PIPEDA?
  - Is plan administration activity a “commercial activity”? 
Statutory Torts

• Statutory breach of privacy under legislation in British Columbia, Saskatchewan, Manitoba and Newfoundland and Labrador
  – Generally actionable where a person wilfully violates another person’s privacy
  – Degree of privacy depends on what is reasonable in the circumstances
Pension Standards Legislation

- No express reference to cybersecurity or data protection under pension standards legislation
- But plan administrators subject to:
  - General standard / duty of care
  - Duty with respect to selection and supervision of agents
- Potential penalties for breach of legislation
Common Law—Potential Claims

- Breach of fiduciary duty: Well established principle that pension plan administrator is in a fiduciary relationship with plan members and other plan beneficiaries
- Negligence
- Intrusion upon seclusion
- Privacy-related tort
- Class actions
Best Practices

• Regulatory Guidance (Canada)
  – Financial Services Regulatory Authority of Ontario
    • The importance of cyber security (2016)
    • Seven ways to reduce the risk of a cyber-attack
  – Office of the Superintendent of Financial Institutions
    • Cyber Security Self-Assessment Guidance for federally regulated financial institutions (2013)
Best Practices

• Regulatory Guidance (Canada)
  – Canadian Association of Pension Supervisory Authorities Strategic Plan (April 2019-March 2022)
    • Research and develop guidelines that will assist stakeholders in developing and building robust cybersecurity plans
  – Canadian Standards Association Model Code for the Protection of Personal Information (adopted in Schedule 1 of PIPEDA)
    • Outlines 10 privacy principles, including principles of safeguards and limiting collection
Best Practices

• Regulatory Guidance (Other)
  – General Data Protection Regulation (“GDPR”) (UK)
    • Regulates the collection and processing of personal data of EU subjects
    • Significant fines for breach of GDPR
  – The Pensions Regulator (UK)
    • Guidance for trustees: Cyber security principles for pension schemes (April 2018)
Steps to Reduce Liability

• Cybersecurity plan
  – Design a cybersecurity plan
    • Assess and understand the risk; address the weakest link
    • Understand your supply chain/service providers
  – Test the cybersecurity plan
    • Put controls in place
  – Follow the cybersecurity plan
    • Monitor and report
Steps to Reduce Liability

• Service provider monitoring and supervision
  – Engage in thorough review of service providers
    • What are service provider’s data protection and cybersecurity standards?
    • What is service provider’s cybersecurity breach incident plan?

• Cybersecurity insurance
  – Consider third-party insurance
    • Generally separate from general commercial liability insurance
Key Takeaways

• It is not a matter of if but when . . .
  – Potential liability to plan administrator or sponsor under legislation and common-law if a data breach occurs
  – Potential liability to plan administrator or sponsor under legislation and common law if a breach of service provider data occurs

• Exercise due diligence, understand your risks and have a plan