Cyber Liability: What you need to know in 2018

Canada's New Mandatory Privacy Breach Reporting Obligations and Claims Examples; GDPR

For The CYBER Exchange

Presented by Gerry Gill

October 2, 2018

Our Firm

Dedicated exclusively to insurance law

Offices in:

- Toronto
- Vancouver
- Calgary
- Kelowna

What We Will Cover

- Canada-Wide Mandatory Breach Notice
- Top 5 Canadian Class Action Settlements
- Claims Examples

Canada-Wide Breach Notice

Notice Goes Canada-Wide

- Alberta already has mandatory notice
- Elsewhere "voluntary", but practically required to satisfy Privacy Commissioners
- Will now be required of:
  - Companies anywhere in Canada subject to federal jurisdiction
  - Private companies in provinces other than BC, Alberta and Quebec
- Will likely prompt new legislation in other provinces

Notice Goes Canada-Wide

- **Alberta** - failure to notify is offence with fines up to $100,000
- **PIPEDA current** – failure to cooperate with Commissioner is an offence
- **PIPEDA Nov. 1, 2018** – include two new offences if fail to meet requirements
  - Failure to issue **notice of data breach**
  - Failure to **keep records** of all breaches
- PIPEDA penalties/offences up to $100,000

New Notice Requirements

WHEN?

- If there is a "real risk" of "significant harm"

WHY?

- Inform affected individuals
- Enable them to protect themselves

TO WHOM?

- Federal Privacy Commissioner
- Any individuals at "real risk of significant harm"
- Anyone else who can mitigate risk or harm

Real Risk

More than mere speculation/conjecture

Cause and effect relationship between breach and harm

Depends upon:

- Sensitivity/type of information
- Malicious intent (loss v. theft)
- Probability information might be misused to inflict harm
- Encrypted

Significant Harm

- Bodily harm
- Humiliation, damage to reputation or relationships
- Employment, business, or professional loss
- Financial loss and property damage
- Risk of identity theft or damage to credit
- LOW HURDLE

When is there a "Real Risk"?

Church (P2017-ND-46)

- Laptop computer stolen from locked office during break-in
- PI: name, address tel number, email, church hall rental contracts for 125 individuals
- Laptop was password protected but not encrypted and never recovered

FOUND: **There was real risk of significant harm**

- Factors: risk of phishing, laptop not recovered, malicious intent, vulnerable population (seniors)

When is there no "Real Risk"?

Third party vendor sent broker's client list to wrong brokerage

- Accidental disclosure of PI of 80 Albertans

FOUND: **no "real risk" of significant harm**

- Detected immediately and deleted same day
- Only one person viewed the list and deleted upon realizing not their clients
- Confirmation not further disseminated, not copied and not accessed by others
- No malice – accidental

Notice Content

To Privacy Commissioner	To Affected Individuals
Circumstances of the breach	Circumstances of the breach
Date or period of time when breach occurred	Date or period of time when breach occurred
Personal information affected	Personal information affected
Steps taken to reduce risk of harm	Steps taken to reduce risk of harm
# of affected individuals and steps taken to notify them	Contact info to ask questions (toll-free number or email address)
Contact information for someone who can answer questions	Organization's complaint process & the right to file a privacy complaint **(Commissioner Recommended)**

Breach Coach

- Emergency contact
- 1-800 service 24/7
- 60 minutes free legal advice
- Ongoing retainer optional – by insurer or insured

Role of Breach Coach

- Conduct **legal analysis** to determine:
  - Jurisdiction
  - Notification obligations and notice content
  - Contractual obligations
- **Negotiate** with Privacy Commissioners
  - notification and content
  - investigations and audits – avoiding an Order!
  - voluntary Compliance Agreements
- Coordinate with third party **clients/stakeholders**
- Breach Legal Counsel can become **Defense Counsel**

Top 5 Canadian Class Action Settlements in 2017

Condon v. Canada
Federal Court, 2015

- Lost hard drive containing student loan data
- 583,000 Canadians' name, address, date of birth, student loan balance, SIN number
- Proposed settlement for $17.5 million reached
  - $60 for each person for inconvenience
  - fund for class members that allege financial harm to be assessed by Arbitrator
  - class counsel fees of $5.25 million

Evans v. Bank of Nova Scotia Ontario, 2016

- Employee stole 645 customers' info, gave to girlfriend, sold for fraudulent purpose
- Customers notified, some victims of fraud, bank reimbursed & gave credit monitoring pre-lawsuit
- Certified 2014
- Settled 2016:
  - $7,000 paid to each class member
  - Bank max payment $1.155 M
  - $444,000 for class counsel fee

Hemeon v. South Western Nova District Health Authority
Nova Scotia, 2017

- Hospital employee accessed patient medical records. Hospital notified patients in 2012 and class action was commenced
- Certified: intrusion upon seclusion, negligence, vicarious liability
- Settled: $1,000 per person, $1 million total

Drew v. Walmart
Banadyga v. Walmart
Ontario and Saskatchewan, 2016

- Photo customers' PII accessed by service provider
- 60,000 customers
- 1 year credit monitoring, up to $350,000
- Out of pocket expenses, up to $400,000
    - $5,000 per customer
    - $15/hr up to 5 hours for personal time if documented, 2 hours undocumented
- Defence counsel fee - $250,000 each, plus $250,000 administration fees – approved May 30, 2017

Lozanski v. Home Depot
Ontario 2016

- 6 actions, 5 jurisdictions, 500,000 affected
- Certified for settlement - $920,000
  - Up to $250,000 for out of pocket expenses
    - $5,000 per customer
    - $15/hr up to 5 hours for personal time if documented, 2 hours undocumented
  - Free credit monitoring up to $350,000
  - $120,000 plaintiffs' counsel fee

Claims Examples

The Honda Case

5 Person IT firm contract to update website

Employee steals customer list for personal use

Lawsuits in Canada and US to recover data and seeking damages

Class action settled

Damages

- $185,000 - Computer forensics expenses
- $326,000 - Legal costs in USA to stop spread & misuse of data
- $200,000 - Mailing notice to 120,000 Canadian auto owners
- $450,000 – Manufacturer's legal costs to defend class action and Privacy Commissioner
- $300,000 - IT firm's defence costs in USA and Ontario
- Undisclosed settlement paid to settle class action (Confidential)

http://www.bhmpics.com/walls/money_pic-wide.jpg

Ransomware:
The Intruder's Flavour of the Month

- Entry/intrusion – usually by phishing email
- Intruder encrypts all data
- Unable to access/open
- Typically has a ransom note
- Currency of choice: bitcoins (neutral facilitator and untraceable)

Ransomware

- Issue: has there been "snooping" such that subject of encrypted data may have a claim for unauthorized access
- Cost to fix: requires special protocol - $120,000 for a 30 lawyer firm
- Solution: some forensic firms can unencrypt without paying the ransom, depending on sophistication of encryption

Ransomware at Law Firm

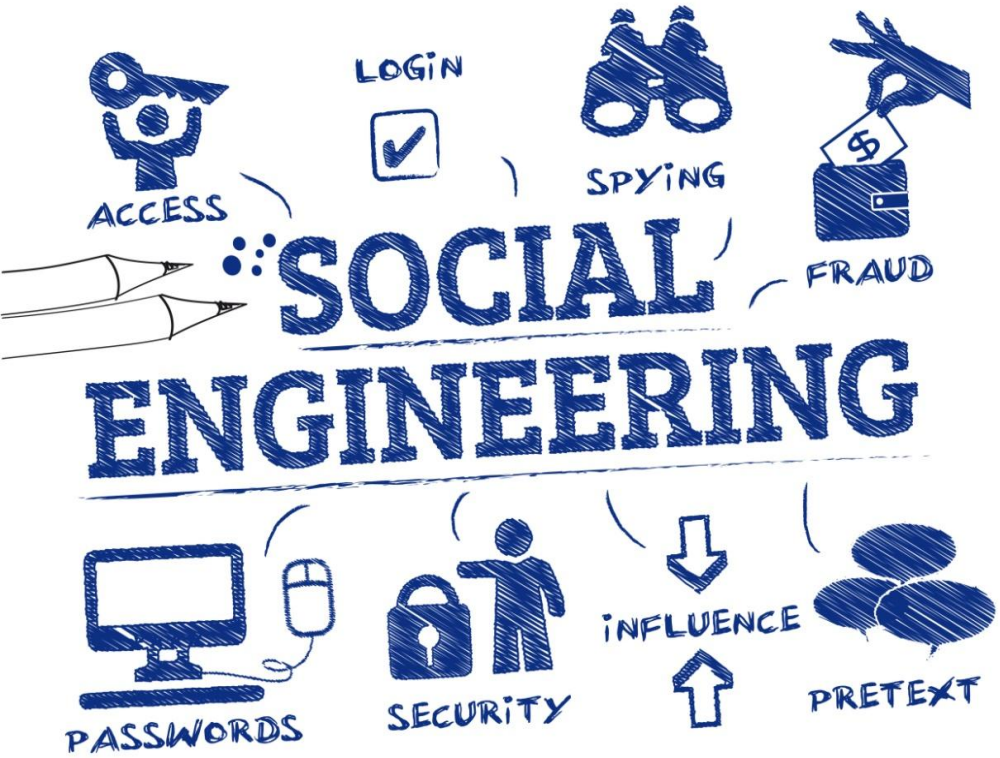
- Hackers access law firm's server month before ransomware attack & shut down auto backups
- Process to encrypt was unsuccessful
  - Due to performance issues
- IT department inadvertently deleted logs in attempt to resolve performance issues
- Forensics unable to determine if there was privacy breach due to lack of evidence BUT dark web search was negative
- No reporting to individuals or Commissioner
- Costs:
  - Forensics $40K for breach response and vulnerability assessment
  - Dark web search $5K to $10K
  - Legal $9K

Security Breach: Ransomware at Manufacturing Plant

- Ransomware attack on Friday of long weekend
- Ransomware encrypted **operations and backups**
  - 70 servers and 800 computers
  - 30 plant locations in Canada & USA
- Some sites able to work out existing orders manually for 24-48 hours before incurring BI loss
- Retained specialist **ransomware forensics firm** – discovered double encryption (on servers and virtual machines)
- Paid ransomware demand 17 bitcoins (approx. $200,000)
- **Retained PR firm** to assist with internal/external messaging
- Decryption successful and able to restart operations with minimal loss & no privacy breach

Security Breach: Ransomware at Manufacturing Plant

- Legal - $11,000
- No PI/no notification required
- Forensics - $60,000 – decryption, remediation, vulnerability assessments
- PR Firm who assisted with internal and external messaging - $9,000
- Ransomware demand 17 bitcoins (approx. $200,000)



Tricking people to disclose confidential information or perform acts for a fraudulent purpose

- email and telephone scams
- using information obtained through social media or purchased

Social Engineering Fraud

Type	Explanation
Phishing	Criminals persuade victims to hand over personal details or transfer money by sending spoof emails
Spear phishing	Targeted phishing email aimed at a specific person
Vishing	Criminals persuade victims to hand over personal details or transfer money, over the telephone
SMiShing	Criminals persuade victims to hand over personal details or transfer money, by way of spoof SMS text messages

Privacy Breach: Spear Phishing at Care Home

- Phishing attack targeted CFO
  - Send phishing email to contact list (and responded to inquiries)
  - Office 365 settings changed to divert all incoming email – 790 emails over 3 weeks
- IT Provider did not catch forwarding rule until a month later – failed to inform Care Home
- Of 790 emails diverted, 130 had personal information (residents, employees, job applicants, directors)
- Contract with hospital – terminated access to database causing BI loss
- Reported to Privacy Commissioner, notified 130 affected individuals
- Database access restored

Privacy Breach:
Spear Phishing at Care Home

- Legal $33,000 – analysis of affected email, notification, Privacy Commissioner negotiations
- Forensics $72,000 – breach response and forensic analysis
- Handled notifications internally
- No credit monitoring provided

Social Engineering Example: Accounting Firm & Financial Info

- Accounting firm receive phishing email
- "Go to assist" credentials harvested
- Hackers watched accountants work and stole access info for clients
- Used "Go to Assist" to access clients and steal from bank accounts
- Corporate info is not personal information

General Data Protection Regulation "GDPR"

What is GDPR

- **Single, overarching privacy regulation that governs the European Union ("EU")**
- **Came into force on May 25, 2018**
- **Fair to say – most stringent privacy legislation**
  - **penalties for non compliance:**
    - **$30M CDN; or 4% of annual revenue**
    - **$15m CDN or 2% of annual revenue**

Key Features of GDPR

Consent

- "Opt-Out: not permitted

- Must be specific, informed and "given through clear action"

- Children under 16 need parental consent

- e

Key Features of GDPR

Accountability

- Must appoint data protection officers

- Positive obligations to implement data protection- must demonstrate compliance

- Must carry out privacy impact assessment

Key Features of GDPR

Data Rights

- Right to be forgotten

- Right to information about process

- Right to object to direct marketing

Key Features of GDPR

Notification

- Mandatory
  - unless the breach is unlikely to impact the rights and freedoms of individuals.
- Within 72 hours

- Data Processers must report to Controllers

GDPR APPLIES TO CANADA

- If established in EU or control or process data in connection with
  - Offering goods and services
  - Monitoring behavior
  - If there is a "real risk" of "significant harm"

- **Processing -** any operation performed on personal data, including collection, use, disclosure and storage

GOOD NEWS?

- Canadian privacy laws similar in scope
  - Notification
  - Record retention policy
  - Privacy by design

- Ready for Canada = Ready for GDPR???

Questions?

DOLDEN WALLACE FOLICK LLP

Insurance Lawyers

Vancouver | Kelowna | Calgary | Toronto