Cyber Liability: What you need to know in 2019

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

The CYBER Exchange

Presented by Gerry Gill

May 22,2019

Our Firm

Dedicated exclusively to insurance law

Offices in:

- Toronto
- Vancouver
- Calgary
- Kelowna

What is Cyber Liability

- **Encompasses information security and privacy (Privacy Breaches – "technology as instrument")**
- **Encompasses system sand network security (Ransonware – "technology as target")**
- **Not limited to digital world or technology (Loss of paper files)**

Breach of Privacy
Statutory Cause of Action

- **Provincial Privacy Acts create cause of action for breach of privacy**
  - **British Columbia, Manitoba, Newfoundland and Labrador and Saskatchewan**
- **Intentional act**
- **No need for proof of actual damages**
- **Contextual – degree of privacy afforded depends on context**
- **No Privacy Commissioner**

Intrusion Upon Seclusion

- **Nominal damages capped at $20,000**
- **Elements:**
  - **Intentional conduct, can be reckless**
  - **Invaded private affairs without justification**
  - **Reasonable person regard as highly offensive invasion causing distress, humiliation or anguish**
  - **Possible Aggravated or punitive damage**

    - *Jones v. Tsige* (ONCA) awarded $10,000

http://static-assets.komando.com/wp-content/uploads/2014/11/invasion-of-privacy.jpg

Personal Information Protection and Electronic Documents Act ("PIPEDA")

- **Statutory duty with respect to use, collection, disclosure of information (legal framework for damage claim). Statutory duty regarding security frameworks.**

- **Applies to federal industries and Provinces that do not have Provincial Equivalent**
  - **BC, AB, MB have equivalent statutes**
  - **Other legislation – Health Statutes**

PIPEDA

- **Manner of Breach irrelevant: breach of duty regardless of how information is disclosed**
- **Right to sue conferred by PIPEDA (s. 16) – but must first obtain ruling from Privacy Commissioner (s.14)**
- **Cases under PIPEDA filed in Federal Court**

Privacy Law in Canada After November 1, 2018

- After November 1, 2018, is now required of:
  - Private organizations anywhere in Canada subject to federal jurisdiction that engage in "commercial activities"
  - Private organizations outside of BC, Alberta and Quebec
- May prompt amendments in BC and Quebec to maintain "substantially similar" status to PIPEDA

Mandatory Notice Requirements (PIPEDA and Alberta PIPA)

When?	• If there is a "real risk of significant harm"
How?	• Direct notification – email, phone, letter • If direct not possible, indirect may be acceptable – website, newspaper
How soon?	• "as soon as feasible" (PIPEDA) • "without unreasonable delay" (Alberta PIPA)
To whom?	• Privacy Commissioner(s) • Any individual who is at "real risk of significant harm" • Third parties who can mitigate risk of harm (e.g., police)

Offences and Penalties

- Alberta - failure to notify is offence with fines up to $100,000
- PIPEDA before Nov. 1, 2018 – failure to cooperate with Commissioner is an offence
- PIPEDA current – includes 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

Real Risk of Significant Harm

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**

What is 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"?

Chartered Accountants (P2017-ND-143)

- **Client mistakenly given a printed tax return of another client**
- **PI – name, address, birthdate, SIN, income and personal deductions**
- **Recipient discovered error, notified accountants and mailed list back**

FOUND: There was real risk of significant harm

- **No confirmation that unintended recipient did not copy the information**

When is there no "Real Risk"?

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

- **Accidental disclosure of 80 Albertans' PI**

FOUND: no "real risk" of significant harm

- **Detected immediately same day**
- **One person viewed the list**
- **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 and if known, the cause	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 and steps individuals can take
# 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)**

PIPEDA Breach Log Requirements

- **Keep a "record" of every "breach of security safeguards" involving personal information**
  - **Even where there is NO real risk of significant harm**
- **Keep for 2 years from date of discovery of the incident**
- **Federal Privacy Commissioner can audit**
- **Failure to keep breach log can result in penalties/offences up to $100,000**

What to Include in the Breach Log?

- **Any information that enables Privacy Commissioner to verify compliance and assess the real risk of significant harm**
- **Date or estimated date of the breach**
- **General description of the circumstances**
- **Nature of information involved in the breach and**
- **If notification was required and carried out**
- **DO NOT include privileged information (legal opinion, data forensic investigation report, etc.)**

What to Include in the Breach Log?

- **If breach is reported, the report to the Privacy Commissioner can constitute the breach log**
- **Privacy Commissioner will keep breach log confidential, unless in the public interest**
- **Breach log protected by privilege?**

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**

http://foreclosureshelper.com/when-to-hire-a-foreclosure-attorney/

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

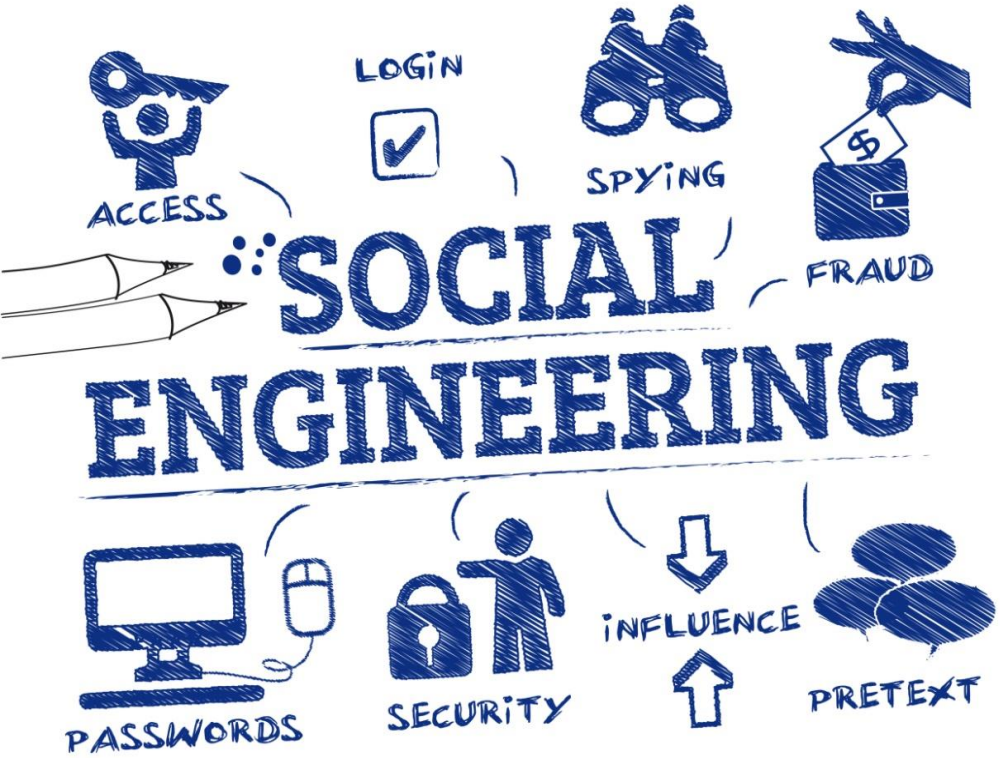
- Hackers access law firm's server month before ransomware attack & shut down auto backups
- Process to encrypt was unsuccessful
  - Due to performance issues
- IT department inadvertently deleted logs in attempt to resolve performance issues
- Forensics unable to determine if there was privacy breach 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
  - Need for privacy officer
  - Notification
  - Record retention policy
  - Privacy by design

- Ready for Canada = Ready for GDPR???

Questions?

DOLDEN WALLACE FOLICK LLP

Insurance Lawyers

Vancouver | Kelowna | Calgary | Toronto