Cyber Liability Issues Affecting Municipalities

A Presentation
to the AMM
April 16, 2021

Mouna Hanna

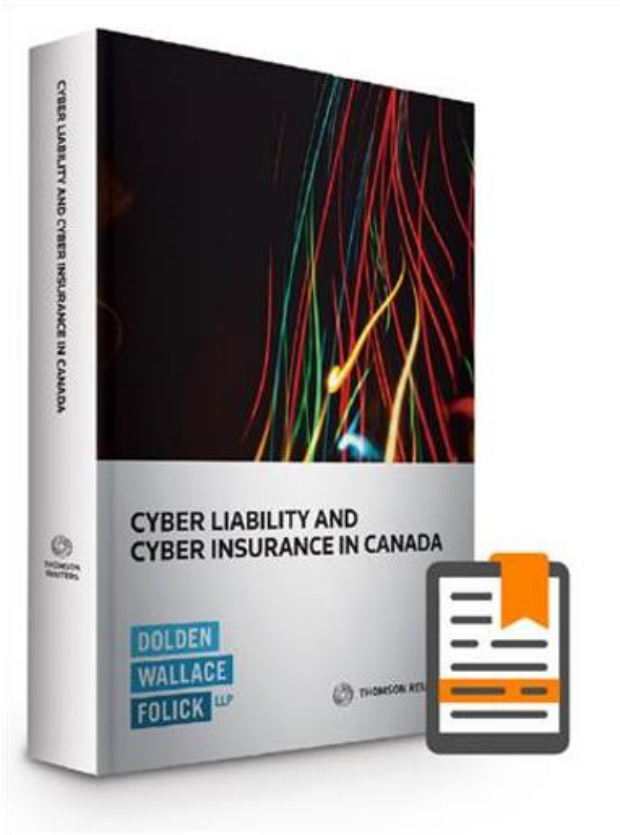
Our Firm

Dedicated exclusively to insurance law

Offices in:

- Toronto
- Vancouver
- Calgary
- Kelowna

Released - February, 2020



Overview

1. Ransomware & Trends in 2020/2021
2. Public Sector Privacy Law – FIPPA and PHIA
3. Cyber & Privacy Breaches
4. Breach Reporting
5. Role of a Breach Coach
6. Risk Management Strategies
7. Questions?

In The News

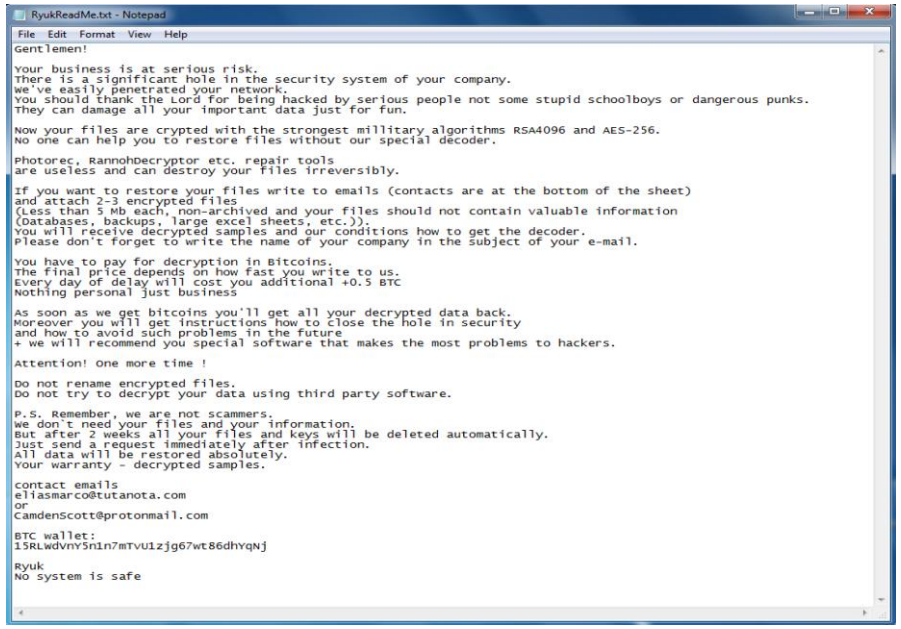
"Municipalities are an appealing target for cyberattackers for the sheer quantities of data they have access to…"

(CBC News – April 15, 2019: https://www.cbc.ca/news/canada/kitchener-waterloo/hack-cyber-attack-stratford-1.5098407)

"Ontario has the highest number of incidents as compared to other provinces….Smaller municipalities are being targeted because their IT budgets are smaller with a smaller staff so they don't have the resources to provide a higher level of protection that larger municipalities can afford…. But larger municipalities have been hit [too]" - OPP

(Simcoe.com – January 24, 2019: https://www.simcoe.com/news-story/9129023-ontario-municipalities-hit-hardest-by-cyber-attacks-says-opp-investigator/)

Spotlight: Ransomware



Spotlight: Ransomware

Average Ransom Demand Q4 of 2020

Average Ransom Payment

$154,108

-34% from Q3 2020

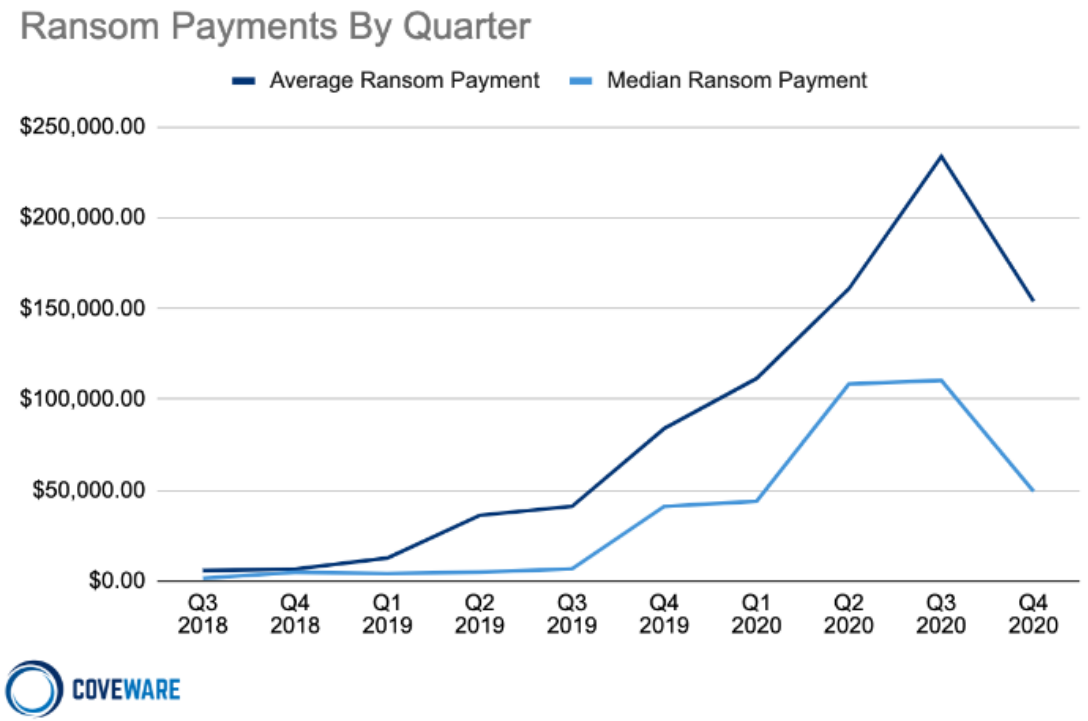
Median Ransom Payment

$49,450

-55% from Q3 2020

Source: Coveware (https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020)

Spotlight: Ransomware



Source: Coveware (https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020)

Contain & Investigate

Spotlight: Ransomware

- Determine how many systems affected
- Secure and disconnect
- Determine point of entry
  - Did someone click a fraudulent link?
  - Did the threat actor enter through an open RDP port?
- Identify whether critical data, personal information or services implicated
- Rebuild/restore from back ups vs. payment of ransom demand
  - Philosophy and stance on payment of ransom demand?
  - Risk: you may pay for the decryption key that may not work
  - "Good cyber criminals" vs. "bad cyber criminals"

Ransomware Trends in 2020/2021

- Ransomware on the rise post COVID-19
- Email phishing – top attack vector and point of entry
- Threat to leak stolen data if ransom demand not paid
- Rise in data leak websites
- Data not always destroyed when threat actor says it has been (risk of double extortion)
- Irreversible data destruction as an attack method – growing trend
- Big problem for small organizations
  - 2020 Q4 – Public sector made up approximately 10% of ransomware targets (Health care highest at 17.9%)

Show Me The Money

Example:

- Bitcoin:
  - $79,179.39 CAD per BTC
- Threat Negotiation Expenses:
  - $7,500
- Forensic Investigation:
  - $50,000
- Notification Expenses:
  - $5,000
- Credit Monitoring & ID Theft Expenses:
  - $12 per person
- Public Relations:
  - $5,000
- Breach Coach/Legal:
  - $15,000

Case Study: Wasaga Beach

- Town of Wasaga Beach - 20,675 residents
- Victim of a ransomware attack in April, 2018 whereby all municipal data was encrypted
- 7 weeks of recovery efforts (including weekends)
- After consultation with legal department and negotiation with threat actors, ransom payment: $34,950 (initial demand was $143,000/11 bitcoin)
- Costs incurred: $250,000 + $95,000/year ongoing

Case Study: Midland

- Town of Midland – 16,864 residents
- Victim of a ransomware attack in September, 2018 resulting in the encryption of several systems, including financial systems
- Town paid 6 bitcoin however threat actor did not release all of the decryption keys
- Town paid an additional 2 bitcoin for the remaining keys
- Town had a cyber policy

Common Cyber and Privacy Breaches

- Ransomware
  - With or without threat of exposure of data (ie. “double extortion”)
  - Rise in popularity - publishing data on data leak sites (ie. Conti News)
  - Increase post COVID-19
- Business Email Compromise
  - Phishing
  - Manipulation of invoices, spoofed emails, redirection of funds to “new” bank account
- Website Manipulation and Credential Harvesting
  - Credit card skimmers
- Employee Misconduct & Error
  - Theft of personal information (ie. Desjardins)
  - Adding emails to CC line instead of BCC line
  - Failing to secure IT environment or cloud related security exposing data to the public domain

Freedom of Information and Protection of Privacy Act ("FIPPA")

- Applies to all records in the custody or control of a public body in Manitoba
  - Municipalities, local government bodies, schools, hospitals, health boards, crown corporations
- Required to designate an Access and Privacy Officer to oversee privacy and freedom of information compliance program

Personal Health Information Act ("PHIA")

- Applies to health information in the custody and control of "trustees", which include Municipalities

Disclosure of Personal Information

Obligations:

- may only disclose personal information:
  - with consent, for a consistent purpose, to comply with legislation or for law enforcement
  - authorized under section 44(1)(a)-(dd) of FIPPA
- must protect personal information from inadvertent disclosure or authorized access

What is a Privacy Breach?

Privacy Breach:

- Unauthorized collection, use, disclosure or disposal of personal or personal health information. Such activity is "unauthorized" if it is not permitted by the FIPPA or PHIA

Unauthorized **access**:

- Snooping
- Hacking

Unauthorized **disclosure:**

- Loss or theft of devices (eg. USB keys, phones, laptops, cameras, external hard drives)
- Improper disposal of records
- Inadvertently sending communications to the wrong recipient due to human error

Breach Reporting under FIPPA

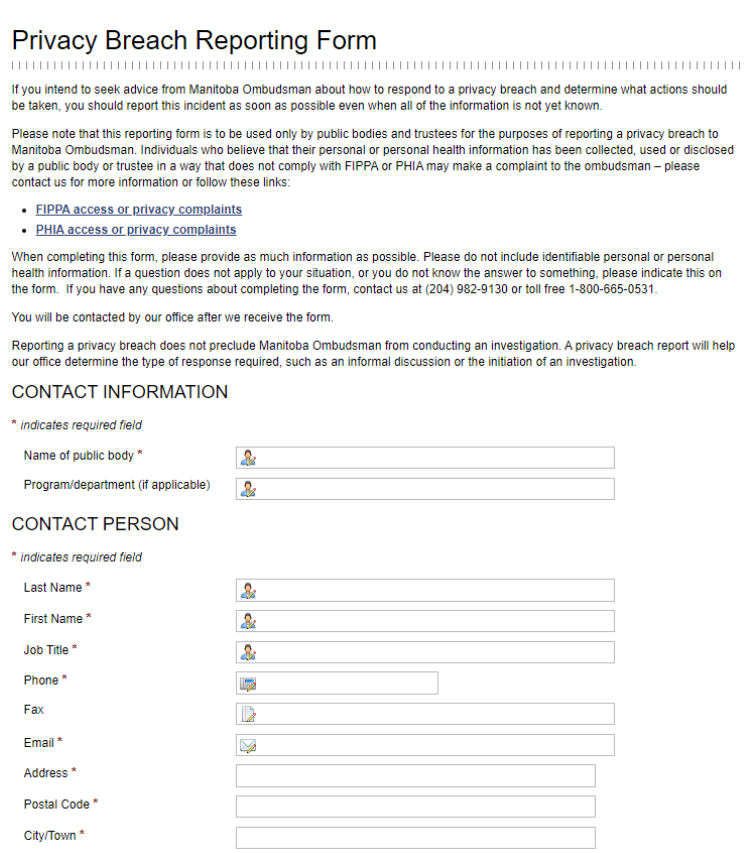
- No mandatory breach reporting to the Manitoba Ombudsman, however recommended and encouraged
- Consider possible complaints by affected individuals to the Ombudsman
  - Get ahead of the cyber incident and/or privacy breach and control the message
  - Media impact
- Consider the risk of harm to affected individuals

Risk Assessment

- Manitoba Ombudsman Practice Note
- "reasonable risk of harm"
- Number of people affected

Risk Factor	Low	Medium	High
Nature of personal and/or personal health information	▪ Publicly available personal information not associated with any other information	▪ Personal information unique to the organization that is not medical or financial information	▪ Medical, psychological, counselling, or financial information or unique government identification number ▪ Information relates to a vulnerable individual (ex. youth or seniors)
Scope of the breach	▪ Very few affected individuals	▪ Identified and limited group of affected individuals	▪ Large group or entire scope of group not identified
Relationships	▪ Accidental disclosure to another professional who reported the breach and confirmed destruction or return of the information	▪ Accidental disclosure to a stranger who reported the breach and confirmed the destruction or return of the information	▪ Used by or disclosed to an individual with some relationship to or knowledge of the affected individual(s), particularly disclosures to ex-partners, family members, neighbours or co-workers ▪ Theft by a stranger
Cause of the breach	▪ Technical error that has been resolved	▪ Accidental loss or disclosure	▪ Intentional breach ▪ Cause unknown ▪ Technical error (if not resolved)
Containment efforts	▪ Data was adequately encrypted ▪ Portable storage device was remotely wiped and there is evidence that the device was not accessed prior to wiping ▪ Hard copy files or device were recovered almost immediately and all files appear intact and/or unread	▪ Portable storage device was remotely wiped within hours of loss but there is no evidence to confirm that the device was not accessed prior to wiping ▪ Hard copy files or device were recovered but sufficient time passed between the loss and recovery that the data could have been accessed	▪ Data was not encrypted ▪ Data files, or device have not been recovered ▪ Data at risk of further disclosure particularly through media or online
Possible harm from the breach	▪ No foreseeable harm from the breach	▪ Loss of business or employment opportunities ▪ Hurt, embarrassment, damage to reputation or relationships ▪ Social/relational harm ▪ Loss of trust in the public body/trustee ▪ Loss of public body/trustee assets ▪ Loss of public body/trustee contracts or business ▪ Financial or legal exposure to public body/trustee	▪ Security risk (ex. physical safety) ▪ Identity theft or fraud risk ▪ Hurt, embarrassment, damage to reputation may also be high risk depending on the circumstances ▪ Risk to public health or safety

Breach Reporting



Privacy Breach Reporting Form

If you intend to seek advice from Manitoba Ombudsman about how to respond to a privacy breach and determine what actions should be taken, you should report this incident as soon as possible even when all of the information is not yet known.

Please note that this reporting form is to be used only by public bodies and trustees for the purposes of reporting a privacy breach to Manitoba Ombudsman. Individuals who believe that their personal or personal health information has been collected, used or disclosed by a public body or trustee in a way that does not comply with FIPPA or PHIA may make a complaint to the ombudsman – please contact us for more information or follow these links:

- FIPPA access or privacy complaints
- PHIA access or privacy complaints

When completing this form, please provide as much information as possible. Please do not include identifiable personal or personal health information. If a question does not apply to your situation, or you do not know the answer to something, please indicate this on the form. If you have any questions about completing the form, contact us at (204) 982-9130 or toll free 1-800-665-0531.

You will be contacted by our office after we receive the form.

Reporting a privacy breach does not preclude Manitoba Ombudsman from conducting an investigation. A privacy breach report will help our office determine the type of response required, such as an informal discussion or the initiation of an investigation.

CONTACT INFORMATION

* *indicates required field*

Name of public body *

Program/department (if applicable)

CONTACT PERSON

* *indicates required field*

Last Name *

First Name *

Job Title *

Phone *

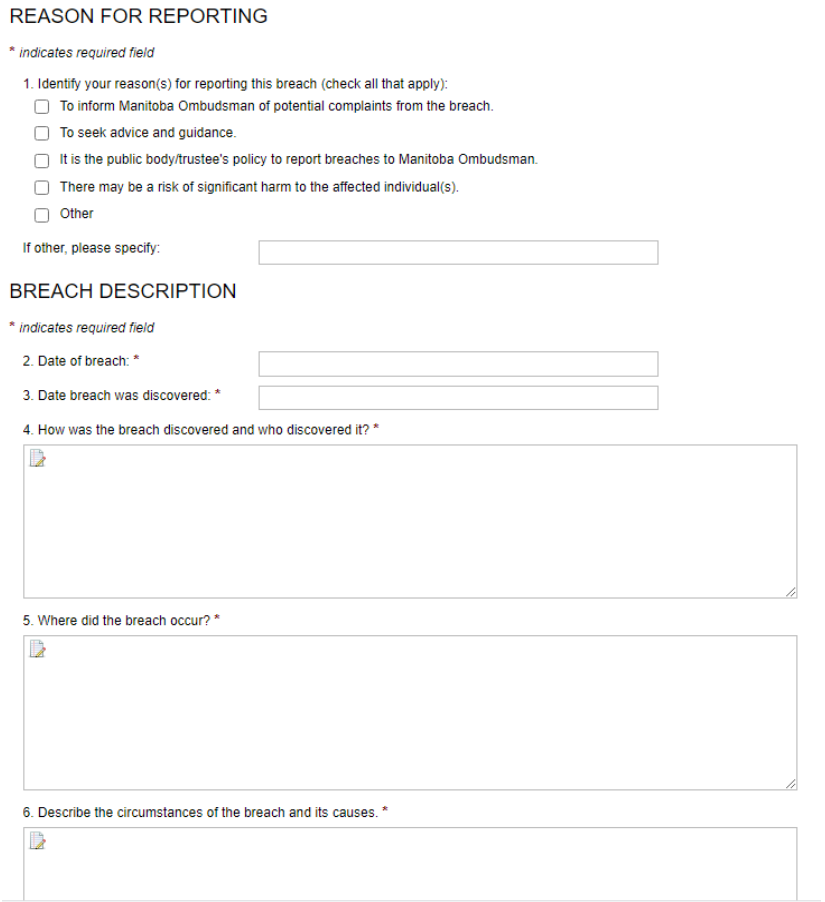
Fax

Email *

Address *

Postal Code *

City/Town *



REASON FOR REPORTING

* *indicates required field*

1. Identify your reason(s) for reporting this breach (check all that apply):
   - ☐ To inform Manitoba Ombudsman of potential complaints from the breach.
   - ☐ To seek advice and guidance.
   - ☐ It is the public body/trustee's policy to report breaches to Manitoba Ombudsman.
   - ☐ There may be a risk of significant harm to the affected individual(s).
   - ☐ Other

If other, please specify:

BREACH DESCRIPTION

* *indicates required field*

2. Date of breach: *
3. Date breach was discovered: *
4. How was the breach discovered and who discovered it? *
5. Where did the breach occur? *
6. Describe the circumstances of the breach and its causes. *

Source: Manitoba Ombudsman https://www.ombudsman.mb.ca/breaches/privacy-breach-reporting-form.html

Urgent Decisions: Initial Call

1. Do you have an Incident Response Plan?
2. Dispatch computer forensics or data restoration experts?
3. What data has been affected? Whose personal information (PI) is at risk?
4. Has data/PI been accessed, copied or exfiltrated?
5. What needs to be done to avoid/reduce business interruption?
6. Does the Ombudsman need to be notified?
7. Is this going to hit the media?
8. Do affected individuals need to be notified?
9. Contractual obligations to partners, vendors etc?

Role of Breach Coach

- Crisis Management: guidance through an emergency
- Investigate the circumstances around the breach: date of the breach, how it happened, when it was discovered etc.
- Coordinate Response: computer forensics, regulatory compliance, public/client relations, credit monitoring police
- Notification assistance: affected individuals, clients, business partners, vendors
- Minimize potential harm and liability

Benefits of using a Breach Coach

- Coordinated response to the cyber incident
- Claims frequency and costs drop with involvement of a Breach Coach
- Early preparation for the defence of a claim
- Minimize chance of regulatory investigation or lawsuit
- Establish and maintain lawyer client/litigation privilege
- Recouping damages from third parties

Risk Management Strategies

- IT Systems
  - Keep them current and backed up
  - Test your back ups
  - Ensure security controls, anti-virus, firewalls, patches etc. are current
  - Limit access to critical data and information on a “need to know” basis
  - Consider encryption of all critical and sensitive data
  - Multi-factor authentication
  - Network diagrams
  - Understanding where you keep sensitive and critical data

Risk Management Strategies

- Employee and Staff Awareness
  - Cyber awareness and privacy training – ongoing
  - Educate on emerging risks
  - Forced password resets
  - Promote a culture of security and fraud awareness – must come from senior leadership
  - Encourage staff to come forward if they detect suspicious activity and provide them with an emergency contact in the IT department
  - Confirm any payment instructions or changes to account information via telephone or in person (ie. with vendors, service providers, payroll etc.)
  - Avoid using public WiFi networks

Example: Ransomware

Non-Profit Organization

- Non profit organization suffered a ransomware attack on Christmas eve with threat of publication by CONTI group
- Viable back ups however logging insufficient
- Threat actor provided confirmation of data exfil
- Retained threat negotiators and forensic experts
- Paid ransom in exchange for return of exfil data, proof of deletion and promise of not to publish
  - "Honour among thieves"
- No notification required

Example: Ransomware

Non-Profit Organization

- Ransom - $180,000
- Threat negotiation expenses - $6,500
- Forensic experts - $25,000
- Remediation - $18,000
- Legal -$10,000

Questions?

THANK YOU!

Canada's Specialty Insurance Firm

VANCOUVER KELOWNA CALGARY TORONTO WWW.DOLDEN.COM

DOLDEN WALLACE FOLICK LLP