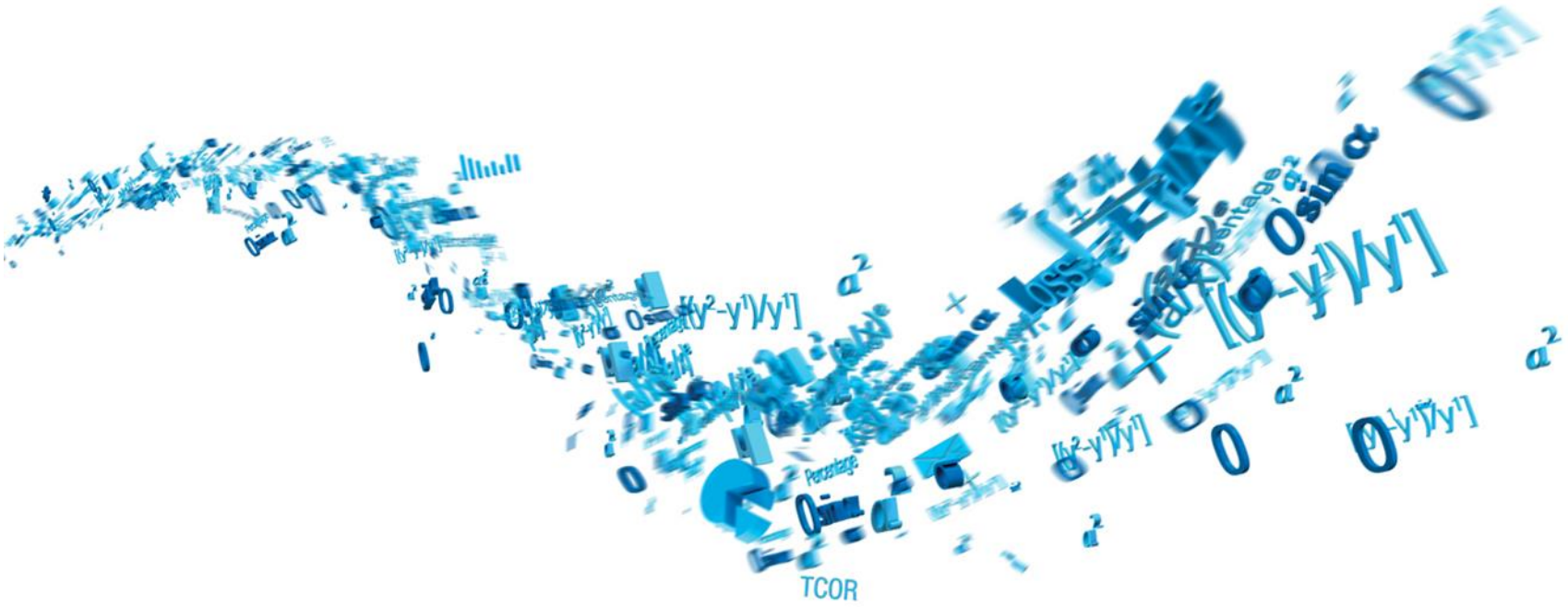


Can you really insure against Cyber Fraud?

Prepared by Alyssa Unrau
Account Executive, Risk Management Practice
Aon Reed Stenhouse Inc.

September 2018

Empower Results®

Agenda

About Aon
What is Cyber Fraud?
Cyber Statistics
Cyber Fraud – Top Causes of Loss
Unique Challenges faced by Municipalities
Most Common Cyber Exposures
Cyber Risk Management
Risk Mitigation Measures – Transferring the Remaining Risk
Cyber Liability Insurance
- First Party Coverage
- Third Party Coverage

Claims Examples
Risk Mitigation Measures – Develop an Incident Response Plan

About Aon

- Aon is Canada’s oldest insurance broker
- We have 1,600 employees in 22 offices across Canada
- Globally Aon has 50,000 employees in 500 offices in 120 countries
- We have $290 billion in premium placements worldwide
- Leader in the placement of insurance for Public Sector clients for 40+ years.
- Specialized team dedicated to addressing gaps in coverage and changes in laws

What is Cyber Fraud?

- Any type of intentional deception that involves the internet

- Types of Losses include:
  - Hackers
  - Malware/virus
  - Lost or stolen device
  - Human Error
  - Paper records
  - Rogue employee(s)
  - System glitch
  - Theft of money

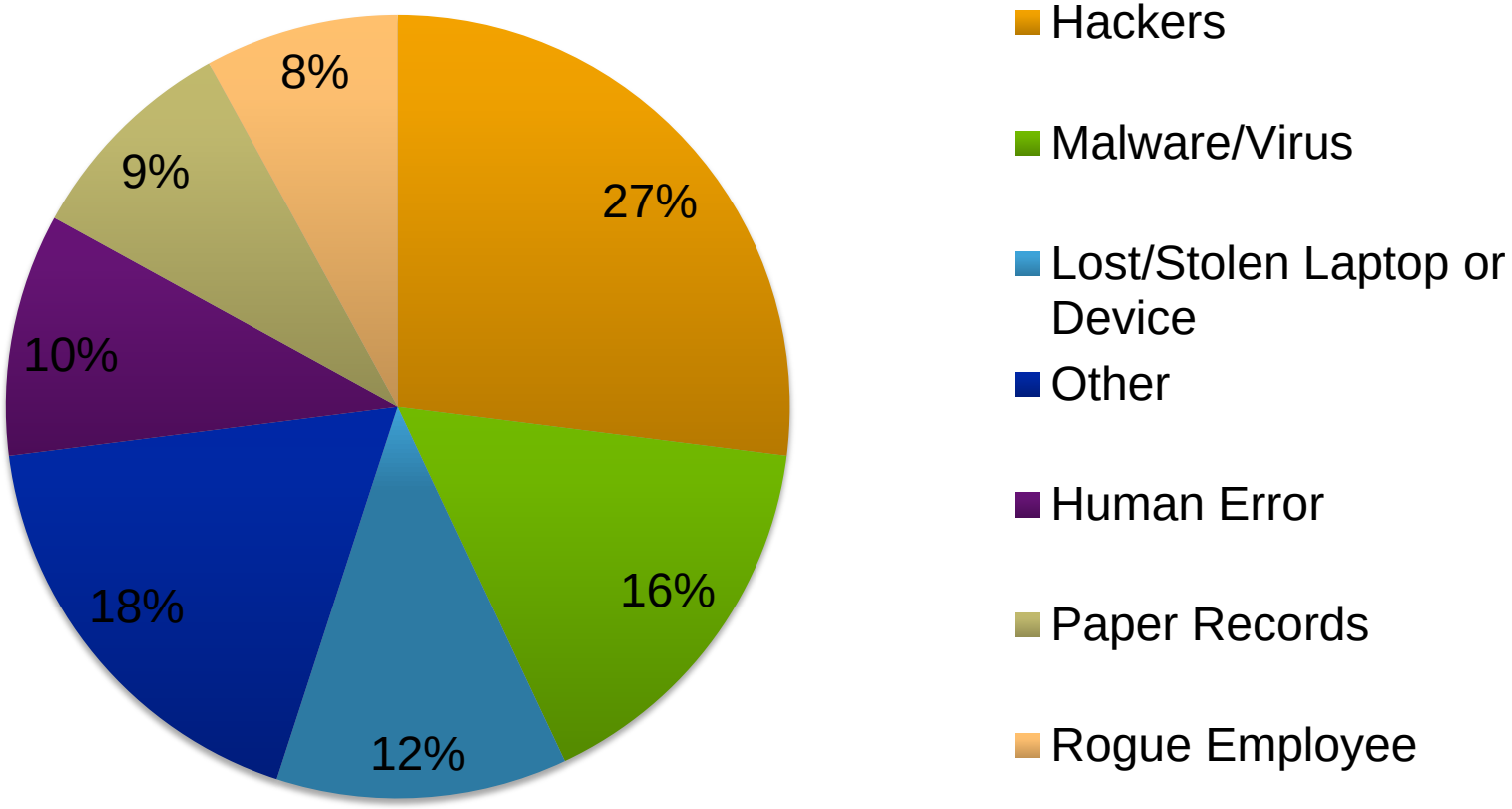
Cyber Statistics

- Small to mid-sized organizations experienced the most incidents, while large organizations lost the most records per breach. The more records lost, the higher the cost of the data breach.
- The faster the data breach can be identified and contained, the lower the costs
- Detection and escalation costs are highest in Canada. The average was USD 1.46 million.
- Data breaches are most expensive in the United States and Canada. The average per capita cost is USD 225 in the United States and USD 190 in Canada.
- Hackers and criminal insiders cause the most data breaches. The average cost for these attacks in Canada is USD 201 per record.
- Health care organizations had an average cost of USD 380 and public sector had the lowest average cost per lost or stolen record at USD 71.
- Companies in the Middle East and Canada have the highest direct per capita costs at USD 81

Ponemon Institute 2017 Cyber Breach Study

Cyber Fraud – Top Causes of Loss

Percentage of Claims By Cause of Loss



2017 NetDiligence Claims Cost Report

Unique Challenges Faced by Municipalities

1. **Budget Constraints**
   i. More significant than those in the private sector
   ii. Impact on ability to train staff, maintain, upgrade, monitor and test computer systems
2. **Outsourcing of IT Operations**
   i. Outsourcing a large percentage of IT operations to third parties (ie. cloud service providers) can increase risks in some cases
3. **Target for Hackers**
   i. Local governments can be a target for hackers and extortionists for monetary gain or political reasons
4. **Public Scrutiny**
   i. Municipal government tends to be subject to greater public scrutiny with respect to cybersecurity and the use and protection of personal identifiable information
5. **Long Information Retention Periods**

Most Common Cyber Exposures

- **Personal Identifiable Information**
  - Employment histories, health records, salary and payroll information (even if outsourced)
  - Resident names, addresses, property tax information, banking information, police interactions, court records
- **Corporate confidential information**
  - Third party intellectual property
- **Network Interruption:** security breaches causing operational downtime
  - Dependent Business Interruption: key service providers experience security breaches that in turn interrupt the insured's business
- **Cyber Extortion:** threats made against an organization to disclose confidential information "or else"
- **Physical Damage to Property or Personal Injury:** resulting from cyber breach

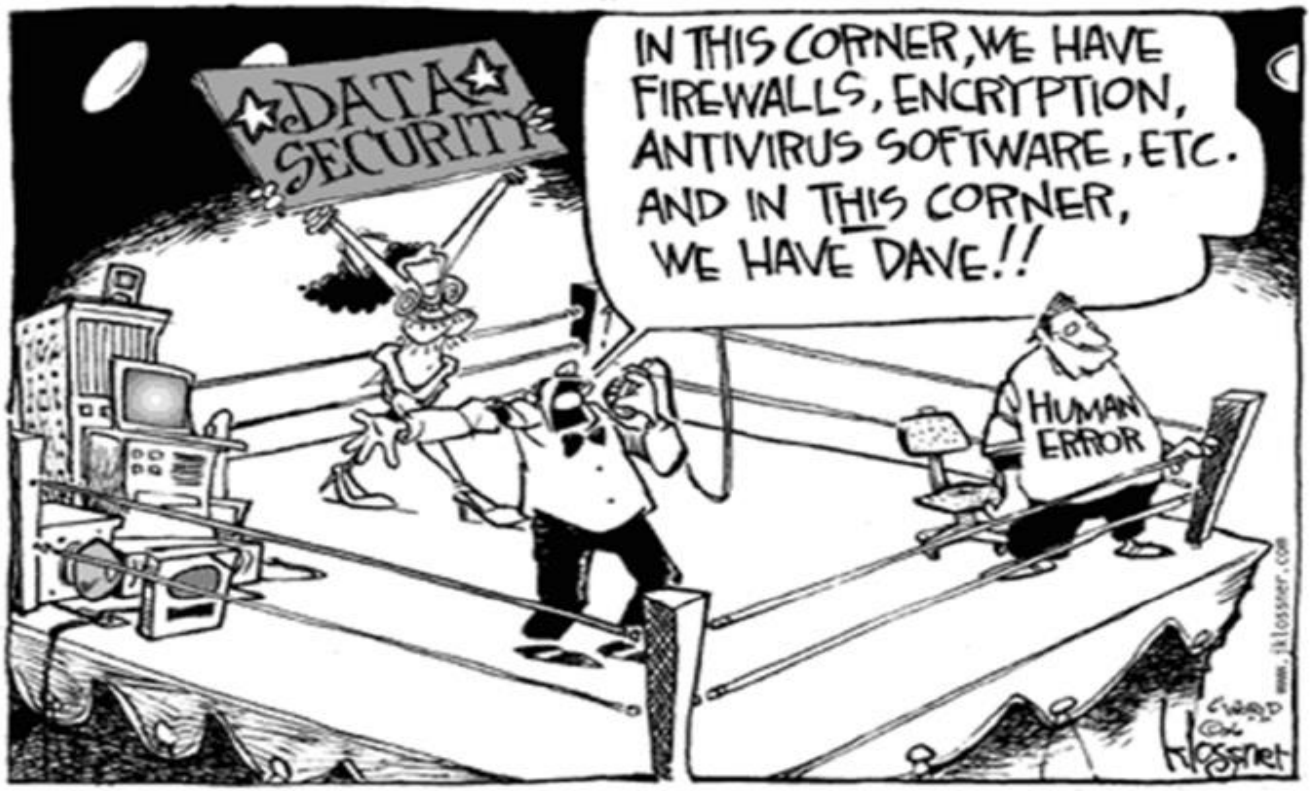
Cyber Risk Management

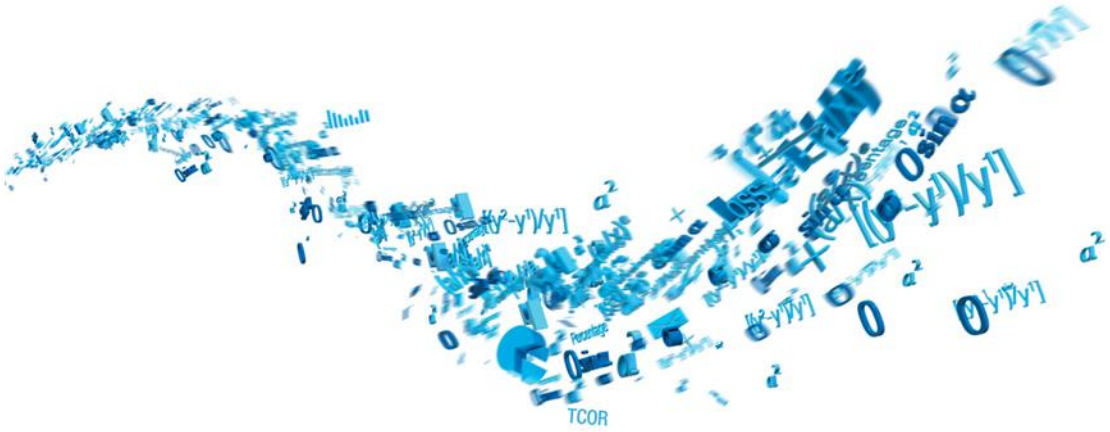
1. **Understand the type of information that is crucial to protect.** Conduct a risk assessment to see where there are gaps in information security.
2. **Utilize IT data security tools such as firewalls, anti-virus software, encryption, and strong passwords.** In addition, ensure proper physical security of all sensitive data.
3. **Establish a culture of data security.** Take steps to enforce compliance.
4. **Train staff.** Increase awareness of security policies and procedures as well as tricks and techniques often used by fraudulent individuals to gain access to confidential information.
5. **Put an incident response plan in place.** Establish what should be done in the event of a cyber breach.
6. **Utilize risk management tools such as Cyber Liability Insurance to transfer remaining risk.**

Risk Mitigation Measures – Transferring the Remaining Risk

- There are two Cyber Frauds that no organization can completely control:

1. The ever increasing sophistication and determination of hackers; and
2. The human element, or…Dave





Cyber Liability Insurance

What Does a Cyber Liability Insurance Policy Cover – First Party Costs

- **Privacy Breach Costs**
  - Notification costs (not required to be statutorily mandated)
  - Legal advice
  - IT forensics (sometimes needed to determine whether a breach has even taken place)
  - Public Relations and brand damage management
  - Credit and Identity Theft monitoring for affected individuals
- **Business Interruption**
  - Extra expenses incurred because of loss
  - Ordinary payroll expenses while business interruption is ongoing
  - Lost income
- **Digital Asset Restoration**
  - Cost of labour to recreate digital records
  - Cost to replace damaged hardware and software
- **Cyber Extortion**
  - Expenses resulting directly from insured surrendering funds or property to a person who makes a threat and costs to terminate the threat

What Does a Cyber Liability Insurance Policy Cover – Third Party Costs

- **Your liability to third parties arising out of:**
  - Network security breaches to your computer system
  - Network security breaches to the network of a third party service provider
  - Privacy breaches – your failure to protect confidential information
  - The transmission of malicious code to third parties
- **Regulatory Investigations, Proceedings and Penalties:**
  - Fines and penalties levied by privacy regulatory bodies
  - Civil awards made by regulatory bodies
  - Costs of regulatory investigations
  - Payment Card Industry fines, penalties and investigations (with added endorsement and additional premium)

Claims Examples – U.S.

- **City of Atlanta**
  - In March 2018, a ransomware attack on the City of Atlanta rendered their computer systems unusable
  - The bitcoin ransom demand amounted to approximately USD 51,000 (at the time)
  - Little to no evidence that personal data had been compromised
  - Years worth of data was destroyed – legal documents and police dash cam footage was deleted
- **U.S. Regional Healthcare System**
  - Lost 19 unencrypted computer back-up tapes, containing medical records of 14,000 patients
  - Four separate state and federal regulators initiated regulatory proceedings
  - Cyber Insurance had been purchased and responded
  - The Insurer paid over USD 375,000 for civil penalty, defense costs and breach response costs

Claims Examples – Canadian

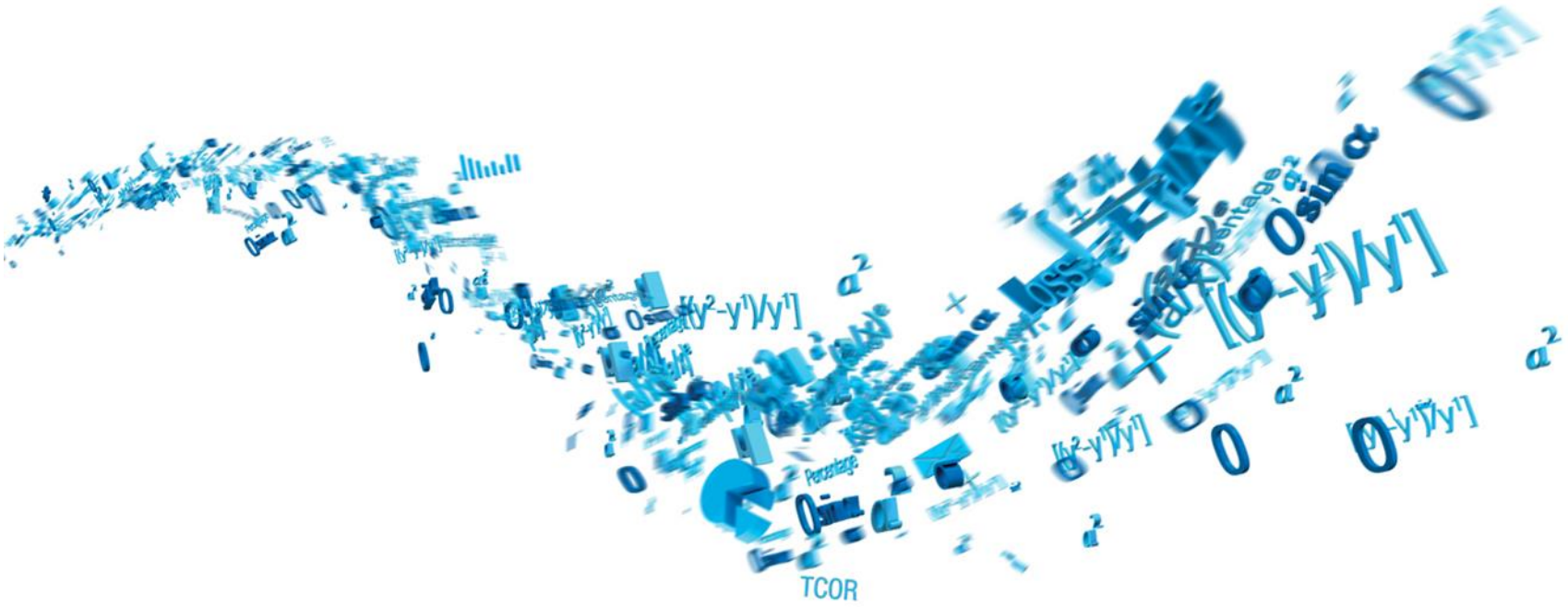
- **Small Canadian Municipality**
  - Operate two seasonal campgrounds and a small store with 15 employees
  - Declined to purchase Cyber Insurance
  - Break-in at the store where 2 walkie talkies and a desktop computer were stolen
  - Privacy Commissioner required that all 22,500 individuals be notified
    - As the 22,500 individuals were not affected, they were only giving a warning
  - After the incident they, again, declined to purchase Cyber Insurance, after a change in management they finally purchased the coverage
  - In 2018, their finance software was victim to a trojan horse

Claims Examples – Canadian

- **B.C. Liberal Government**
- **City of Calgary**
- **Canadian College**
- **City of Ottawa**
- **Canadian Federal Government**
- **B.C.’s PharmaNet**
- **Municipal District of Opportunity No. 17, Wabasca, Alberta**
- **District of West Vancouver**
- **Ontario Ministry of Education**
- **University of Calgary**
- **Eastern Health Authority, Newfoundland and Labrador**
- **Ontario Crown Agency**
- **Nova Scotia Office of Privacy Commissioner**
- **A Federal Ministry**

Risk Mitigation Measures – Develop an Incident Response Plan

- Develop an incident response plan that sets out what should be done in the event of a cyber breach
- Identify an individual or department that will act as a central location for all information and to which a breach should be reported
- Put in place a plan regarding how and what to communicate to individuals affected by a breach
- Identify third party service providers that you will contact in the event of a breach
  - Many of these service providers are very busy and may have trouble responding on short notice where there is no previous relationship or retainer in place
- Purchase Cyber Liability Insurance



Questions/Thank you

Empower Results®