MARSH

What do Housing Providers need to know about managing cyber risk?

Prepared for the Housing Sector in Partnership with HSC

Webinar on June 10th 2020

MARSH RISK CONSULTING
RISK. DISPUTES. STRATEGY.

MARSH & McLENNAN COMPANIES

Introduction

- Context
- Panelists presentation
- Agenda

CONTENT

Evolution of IT practices changes cyber risk exposure

Acceleration or expansion of telework	The number of entry points (i.e. attack surface) for attackers has increased with the number of remote connections
Change in systems and configurations	Due to change management needs, IT teams might have had less time to focus on security - and home networks are less secure
Development of online sales and new services	The quick development of online services and new solutions might have needed to trade off some security for velocity
Modification of business processes and models	The modification or simplification of business processes is introducing a higher uncertainty in incident detection and handling

Cyber threat landscape has also evolved

Medical research and pharmaceutical industry highly targeted by advanced attackers

Massive phishing & social engineering using COVID-19 as hook

Increase in fund transfer fraud leveraging change in context and processes

Some ransomware attack plans have developed faster, trying to take advantage of the context

Cyber threat landscape has changed and exposure has slightly increased

Change in cyber exposure is limited for Housing Sector

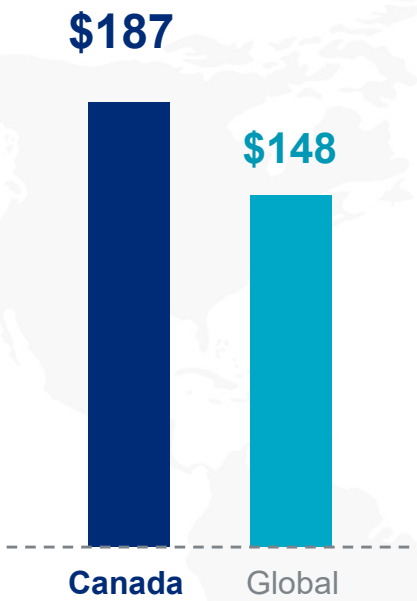
In the COVID-19 context, the cyber risk exposure of the Housing Sector to cyber risk has evolved similarly to the average of other industries

- Increased “attack surface” and vulnerabilities due to remote working
  -> More entry points for attackers; Less secure home networks
- Increased exposure due to a context with higher uncertainty
  -> Enhanced COVID-19 social engineering
- Lower protection due to a context with changed processes and systems
  -> Possible lack of responsiveness or unexpected situations

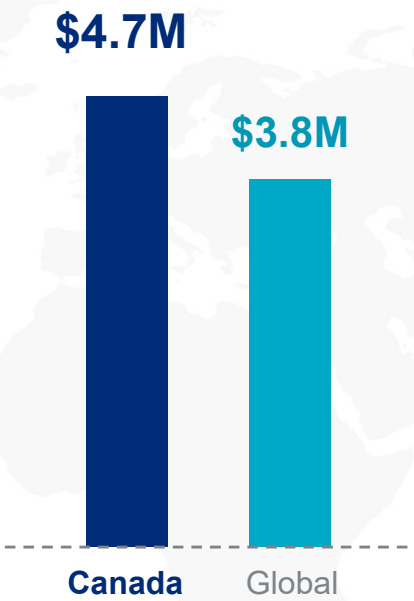
Ensuring cybersecurity program effectiveness is even more important now

CONTENT

Cyber Insurance Overview
Cost of a Data Breach



AVERAGE COST OF A DATA BREACH PER CAPITA



AVERAGE TOTAL COST OF A DATA BREACH

AVERAGE NUMBER OF BREACHED RECORDS

Source: (1) "*2019 International Cost of Data Breach Study: Canada*"; Ponemon Institute

Cyber Insurance Overview
Cost of a Data Breach (Cont.)

241 Days

Mean time for a Canadian company to **identify** a data breach

> *Companies that **identified** a breach in **less than 100 days saved more than $1,000,000** as compared to those that took more than 100 days.*

69 Days

Mean time for a Canadian company to **contain** a data breach

> *Companies that **contained** a breach in **less than 30 days saved more than $1,000,000** as compared to those that took more than 30 days.*

*The **Faster** a Data Breach can be Identified and Contained, the **Lower** the Cost will be.*

Source: (1) "*2019 International Cost of Data Breach Study: Canada*"; Ponemon Institute

Cyber Insurance Solutions: 1st Party Coverage

Direct loss and out of pocket expense incurred by the insured

Coverage	Description	Covered Costs
Business Income/ Extra Expense 	Interruption or suspension of computer systems due to a network security breach. Coverage may be added to include system failure.	• Loss of Income. • Costs in excess of normal operating expenses required to restore systems. • Dependent business interruption. • Forensic expenses.
Data Asset Protection 	Costs to restore, recreate, or recollect your data and other intangible assets that are corrupted or destroyed.	• Restoration of corrupted data. • Vendor costs to recreate lost data.
Event Management 	Costs resulting from a network security or privacy breach.	• Forensics / investigation costs. • Notification to individuals. • Credit Monitoring. • Call Center. • Costs related to public relations efforts.
Cyber Extortion 	Network or data compromised if ransom not paid	• Forensics. • Investigation. • Negotiations and payments of ransoms demanded.

Cyber Insurance Solutions: 3rd Party Coverage

Defense and liability incurred due to harm caused to others by the insured

Coverage	Description	Covered Costs
Privacy Liability 	Failure to prevent unauthorized access, disclosure or collection, of confidential personal information or for the failure to properly notify of a privacy breach.	• Liability and defense.
Network Security Liability 	Failure of system security to prevent or mitigate a computer attack. Failure of system security includes failure of written policies and procedures addressing technology use.	• Liability and defense. • Bank lawsuits. • Consumer Lawsuits.
Privacy Regulatory Defense Costs 	Privacy breach and related fines or penalties assessed by regulators.	• Liability and defense costs. • PCI / PHI / regulatory fines and penalties. • Prep costs to testify before regulators. • Consumer / bank lawsuits.

Cyber Insurance Solutions: Exclusions and Limitations

Exclusions and Limitations

- Coverage excluded for failure of power, utility, mechanical, or telecommunications (including internet) infrastructure not under the insured's direct operational control.
- Coverage may only apply to voluntary shutdowns to prevent the spread of malware or limit damage.
- Computer system/network definitions may be limited.
- Policies may require:
  - Human or programming "error."
  - Proof of testing or patches.
  - Proof of system use prior to failure.

Cyber Insurance Claim Trends

- Total number of data breaches reported under Canadian privacy legislation in 2019 was 680 (six fold increase)

- Leading causes of breach:
  - Ransomware
  - Business e-mail compromise
  - Social engineering scams
  - Rogue employees employee error
  - Lost or stole laptops

- The cost of data breach or impact of an extortion claim for Canadian firms has reached $1M on average

Cyber Insurance Value

Pre Loss Services:

- Education and Knowledge
- Training and Compliance
- Threat Intelligence
- Expert Advice and Consultation

Post Loss Services:

- Access to experts for incident management
- 24/7 Guidance
- Legal and Forensic Services
- Notification, Credit and ID Monitoring Call Center
- Crisis Communication Experts
- Ransom payment and negotiations
- Forensic accounting

CONTENT

Corporate Cybersecurity Considerations

RISK GOVERNANCE

- ✓ Provide employees with **regular communication and awareness messages**, including security knowledge:
  - Beware of **COVID-19 phishing** scams
  - Know working from home “DOs & DON’Ts”
  - Ensure home Wi-Fi is secure
  - Always use VPN (Virtual Private Network) on public Wi-Fi
  - Etc.
- ✓ Provide channel/ email address to **forward suspicious emails**
- ✓ Update your company’s Acceptable Use Policy
- ✓ Adapt **incident response** and disaster recovery plans
- ✓ Ensure **sufficient service desk** availability

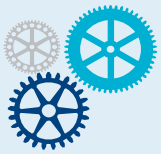
TECHNOLOGY MANAGEMENT

- ✓ Provision **protective technology on endpoints** (hardening, anti-virus, endpoint detection and response, etc.)
- ✓ Utilize a **password manager** or run password audits
- ✓ Tighten and test **access control** procedures
- ✓ Provide **VPN access**
- ✓ Enable **multi-factor authentication** everywhere, especially on email accounts
- ✓ Use **MDM solution (Mobile Device Management)** and enforce remote software updates
- ✓ Provide **home security checks** for employees through phone technical support

Home Environment Security Considerations

ENVIRONMENTAL & BEHAVIORAL

- ✓ **Keep your work separate** – don't use work laptop for personal matters, let family members use it, or use personal laptop for work
- ✓ **Never leave your laptop** and other mobile devices **unattended** in public space or unlocked at home
- ✓ Mute or **shut down any digital assistants** (e.g., Alexa, Google Home, etc.) where you're working
- ✓ Maintain a **clean work area** and enable a 5 minutes screen lock
- ✓ **Store any paper documents securely** and dispose of by using a shredder



TECHNOLOGY & SECURITY

- ✓ Reset default home **Wi-Fi router passwords**
- ✓ Enable **WPA2 encryption** (Wi-Fi Protected Access)
- ✓ **Avoid the use of USB sticks** and other removable storage
- ✓ Use **company pre-approved cloud or data center storage** instead of local or personal storage
- ✓ When necessary, **save VPN bandwidth** for your organization
- ✓ Review logs

How to improve cyber risk management: recommendations

	Short Term	Long Term
Small to Medium Size Organization	• Review remote working security controls and take action • Conduct security tests • Consider cyber insurance	• Review cyber security program against a framework like “NIST CSF” or the “Baseline Security Controls” of Canadian Cyber Security Center
Larger Organization	• Re-prioritize cybersecurity improvement plan based on context • Quantify cyber risk	• Leverage use of cyber security framework like NIST or CSC 20 • Optimize cyber risk management cost utilizing a mix of mitigation, retention and insurance

CONTENT

Contact Information & Resources

Ruby Rai
Cyber Practice Leader
+ 1 416 349 4729

Julien Ducloy
Cyber Risk Consulting Lead
+ 1 647 229 4703

RESOURCES:

- Coronavirus Risk Hub which includes Cyber Risk Management resources: https://coronavirus.marsh.com/ca/en/canada.html
- Cybersecurity article which includes Marsh's point of view: https://businessinedmonton.com/featured/inside-job-the-threat-to-your-cyber-security-isnt-always-external/
- Insights and perspectives from Marsh, Guy Carpenter, Mercer and Oliver Wyman: https://www.mmc.com/insights/coronavirus.html

THANK YOU FOR YOUR TIME