



FOSTER PARK  
BROKERS INC.



# **Limiting Your Exposures Through Risk Management and Insurance**

# ***Todays Session***

- **Overview of your CL Insurance Program**

- *What and Who does it cover?*

- *Extensions of coverage for:*

- Programs & Events*

- Volunteers, Employees and Board Members*



- **Property**

- *Easy ways to help protect your physical assets*

- **Liability**

- *Due Diligence by the League and their Board*

- **Cyber**

- *All new... What to know*



# Your Community League Insurance Program

## Commercial Package Policy:

*Property – Building & Contents (individual to each league)*

*Crime & Accident*

*General Liability (\$5MM - including Events & Host Liquor Liability)*

## Directors & Officers Liability Policy:

*Coverage for the Board of Directors & Officers*

*(\$2,000,000 Limit)*

# ***Lets Talk Property ...***



**There are a number of ways to manage risk at your hall and buildings**

- ✓ Regular activity on premises – hall rentals & events
- ✓ Ample lighting throughout the property
- ✓ Security/Alarm Systems – monitored or not
- ✓ Proper/Visible Signage (potential hazards etc.)
- ✓ *“Tight”* Rental Agreements - Including: Damage Deposit clause and requirement of proof of Renters Insurance



# ***Liability is a Common Question And ...***

***“Due Diligence” can often be the answer***

- ✓ Ensure Police Checks are completed on a regular basis and Waivers are signed when deemed necessary
- ✓ Certificates of Insurance are obtained from Contractors and Third Party Facility Renters

A well drafted rental agreement  
can also limit your liability  
exposure





✓ Board Executive & Members to know and understand their Roles, Duties & Responsibilities in their board capacity

✓ Accurate-up to date Financial and Governance documents kept; along with regular reviews of each

✓ 2 Executive Signatures required on all CL cheques

✓ Petty Cash to be held at a minimum

eg: under \$200 to minimize the potential for employee/internal theft



## ✓ Proper / Visible Signage

for example: - Rink Safety/Usage Rules  
- Slippery / Wet Floors



# THIS ... is NEW to YOU & ME



DID YOU  
**KNOW**



# Cyber Claims

Cybersecurity incidents in Canada have increased by 160% year over year according to PwC Canada's 2016 Global State of Information Security Survey



# Cyber Overview

- Worldwide Cyber premium is set to go from \$2.5 Billion today to over \$75 Billion by 2020
- 51% of Canadian respondents have experienced loss or exposure of sensitive information (Ponemon Institute 2016)
- 90% of organizations experienced a hack last year (BI&I 2017).
- RCMP's CPIC system has been breached 480 times over the past 3 years
- It's not a matter of if you get breached – it's how long it takes you to figure out that you were (FBI 2016)
- Average discovery period is now 220 days

YOU HAVE BEEN  
HACKED !

# Cyber Statistics

- 50% businesses report knowing/suspecting they have experienced fraud or scams in the last year (Ipsos 2017)
- In Canada 54% of all breaches due to hackers & criminal insiders
- 8 out of 10 households in Canada have a home data network
- 33% of Canadians attach their gaming consoles, TV's, thermometers, or security systems to the Internet



- 50% of businesses have been infected with Ransomware in the past year (IBM 2017)
- Half of these paid \$10,000 to retrieve their data
- Cost to known victims in the first half of 2016 was \$209 million
- Cost in 2015 - \$24 million
- Fastest growing area of Cyber loss



**“I rob banks because that’s where the money is ...”**

- Bank Robber *“Slick Willie Sutton”*

Data thieves and cyber criminals have the same strategy ... except they go where the ***data*** is

It has been noted that,

- Since 2015, more than 50% of the world’s data has been created and;
  - Since 2015, cyber attacks have increased four fold
- ... interesting - but scary!

# Ransomware Examples

- University of Calgary had some computers locked down by Ransomware and a demand for \$25,000 to be paid to restore the systems
- With Ransomware the files remain on your computer - encrypted
- This was paid by a professor
- Kensington Wine Market – Calgary
  - Paid \$500 in Bitcoins
  - Quoted \$6,000 for outside help



**SO WHAT DOES  
IT ALL MEAN**

**?**

Your organizational security is only as strong as your weakest link.



# What is Cyber?

- Cyber means different things to different people.
- There is no agreed definition of what cyber is (which is part of the problem)
- Cyber is not a very accurate definition of many of the exposures – more accurate is probably data and network protection
- In reality privacy, computer and network security are not just internet issues
- Any entity that transacts business using a computer or network is impacted because confidential information is at risk



# How can a claim occur

- Employee loses unencrypted USB Device
- Email + attachment sent to wrong party
- Programming error
- Stolen or lost laptop
- Confidential information not destroyed according to protocol
- Laptops not wiped clean when discarded
- Vendors
- Unauthorized access to records



# Stats

- Cybercrime has become a more lucrative criminal industry than the illicit drug trade, generating over **\$100B US annually**
- An estimated 7 million people in Canada have been victims of cybercrime in 2013
- The average cost per victim in Canada was roughly \$380

- 2013 Norton Report

# What is a 'Privacy Breach'


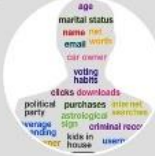


- A privacy breach is the result of an unauthorized access to, or collection, use or disclosure of personal information
- Such activity is “unauthorized” if it occurs in contravention of applicable privacy legislation



- Some of the most common privacy breaches happen when personal information is stolen, lost or mistakenly disclosed. A privacy breach may also be a consequence of faulty business procedure or operational breakdown

- Office of the Privacy Commissioner of Ontario

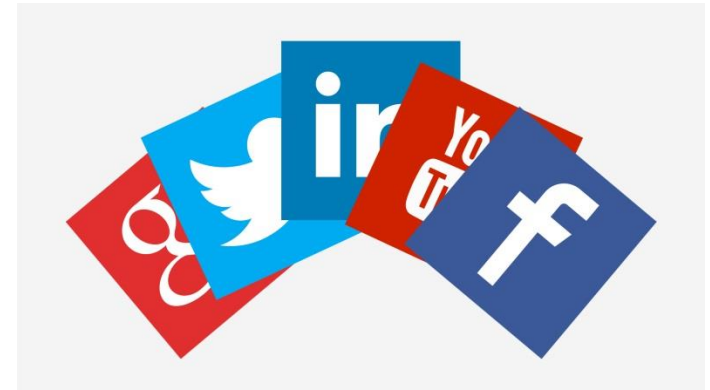
## What Personal Information Is Stolen by Identity Thieves?

			
<b>Name</b> <b>Address</b> <b>Date of birth</b> <b>Social Security number (SSN)</b> <b>Health insurance ID number</b>	<b>Mother's maiden name</b>  <b>Username and passwords for web sites</b>  <b>Driver's license</b>	<b>Personal identification numbers (PINs)</b>  <b>Credit card information (numbers and expiry dates)</b>	<b>Bank account numbers</b>  <b>Signature</b>  <b>Passport number</b>

12

# What are the Key Risk Areas or “Threat Environments”?

- Social Media / Networking
- Internal
  - Rogue Employees/ disgruntled employees
  - Careless Staff
  - Human error
  - Lost, stolen or discarded devices
  - Mobile devices – prone to loss and theft; also, they are always on, so more vulnerable to network attacks



- External
  - Organized Crime (foreign & domestic)
  - Hackers



- Technology
  - Viruses
  - Structural vulnerability & Systems error
  - New technology risks
    - Cloud computing - shared public infrastructure, limited control of services/ data flow
    - BYOD – use of personal devices on organizations network
    - Working from home - what sort of security/ management is in place

# Understanding the Risks That We Face?

- This area is not only difficult for the general public, but is also a challenge for brokers and insurers
- New exposure – limited technical expertise
- Ounce of prevention definitely worth a pound of cure
- Depending on the business, there can be complex interaction between General Liability; Crime; Errors & Omissions and Cyber policies
- Determining a correct limit can also be tough

Single  
Engaged  
Divorced  
✓ It's Complicated  
Separated  
In a Relationship  
Married

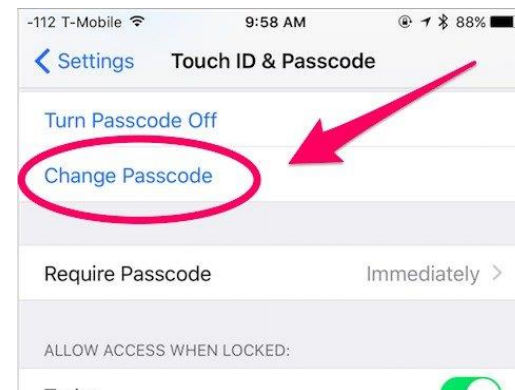
**We must work together to put in place the best risk management and cyber coverage possible**

# Mitigating the Risk



- Assess your current level of preparedness
- **Apply software with the most recent security** releases as quickly as possible
- Identify, prioritize and **protect confidential/essential data**
- Determine what information you're collecting and why you're collecting it
- Determine who can access certain data & reduce the # of users with administrative privilege
- **Vendor Management**
- Develop effective cyber security practices
- **Educate your Board members, staff and volunteers**
- **Require strong passwords;** regularly changing passwords
- Encryption

- **Examine internal practices**
- **Change passcodes** when people leave, i.e. Admin passcode when IT staff leaves
- **Educate your Board members, staff and volunteers**
- **Screen potential employees**, have strong non-disclosure clauses in your employment agreements
- PCI Security Standards Council, look to them anytime you are accepting a credit card payment
- **Have policies and procedures in place that deal with privacy, cyber risks and what to do when a breach occurs**
- Develop effective cyber security practices
- **Require strong passwords**; regularly changing passwords



# Preventing Cybercrime Exposure

1. Install and maintain anti-virus software
2. Install and enable firewalls
3. Install passwords but be sure to:
  - a) Change all default passwords
  - b) Do not allow passwords to be based on personal information
  - c) Incorporate lowercase and capital letters
  - d) Utilizing a combination of letters and numbers
  - e) Use different passwords on different systems
  - f) Ensure employees change their passwords every 30 days



4. Analyze business operations to identify areas vulnerable to IT risks
5. Develop strong business continuity plans
6. Practice regular diagnostic testing and monitoring
7. Install software patches as soon as possible
8. Use anti-spyware tools
9. Use caution with e-mail attachments
10. Remove unused software



# What Can I Do to Protect My Business From a Cyber Attack ??



... include a ***Cyber Policy*** in your  
Commercial Insurance Program

# Cyber Liability

## AKA – Data & Network Protection

### Exposures

- Theft
- Hactivism
- Denial of Service
- Spear Phishing
- Cyber-extortion



- Human Error
- Data on Cloud
- Reputational Risk
- Cost of data breach
- Business Interruption



# Social Engineering

- Very targeted approach – ex: email from CEO for rush payment or phone call updating Account information for a vendor

## Claim Example:

### McKnight Hockey Club- Calgary

- Treasurer received request from “President” and “Vice President”
- Fraudulent wire transfer in the winter of 2017 - **\$98,000**
- 10 other Hockey associations have also been targeted – but successfully identified the fraudulent emails



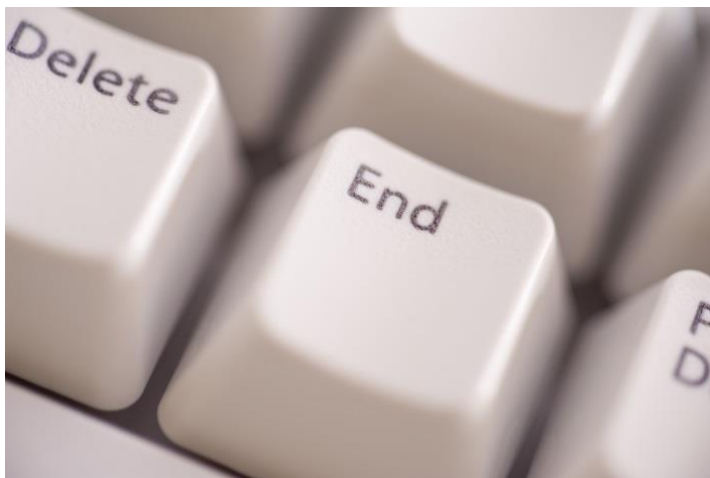
# Insurance Coverage

In order to properly protect your organization against these direct attacks, appropriate insurance coverage should be secured

These can include:

**Computer Violation, Identity Theft  
Computer Fraud & Funds Transfer**





## The bottom line ...

- Cyber is the fastest growing area of crime today – low risk, high payoff
- Implementing appropriate controls will reduce your risk
- Cyber policy will transfer much of your remaining risk
- **Cyber solutions are best implemented by clients, their broker and their insurer working together**

# Your Community League



And you ...

We know that almost all of the people involved with community leagues are volunteers. Although we do our very best to serve the organization and its community members, it's impossible for anyone of us to foresee *if* or *when*, a circumstance or claim may arise. We can however, strive to be **educated**, take advantage of the **resources** available to us and use **common sense**. Many incidents can be avoided by incorporating these simple concepts.

# ***Any Questions***





**Expert Advice. Trusted Solutions.**

**For more information contact:**

***Wanita Quaia***

**[wanita.quaia@fpb.ca](mailto:wanita.quaia@fpb.ca)**

**780-930-4399**