COMMERCIAL INSURANCE Profile

Workplace and safety tips brought to you by: Beyond Insurance Brokers Inc.

DID YOU KNOW

Following a data breach resulting in major data loss, 93 per cent of companies go out of business within five years. Additionally, 30 per cent of business that back up their data do so because of a previous data breach.

How to Mitigate Your Winter Slip and Trip Risk

Winter weather presents a multitude of liability risks for you as an employer. With snow and ice covering your property, it's important to keep in mind strategies for mitigating the risk of slips and trips—both inside and outside of your building.

It can be difficult to keep up with shoveling snow and salting icy sidewalks, but you could be held liable for employee injuries if you fail to keep your workplace safe. You are also responsible for any injury a pedestrian or customer suffers due to snowy or slippery sidewalks, entryways or hallways.

Here are a few tips for preventing employees and passersby from getting hurt:

- Utilize an inspection and maintenance policy to keep track of who is responsible for ensuring that high-risk areas are safe. Be sure to include who is responsible for carrying out the inspection, how often it should be carried out and any disciplinary action that will be taken if the inspection is not conducted.
- Perform inspections on a regular basis, and be sure to record results on a designated form. For example, snow and ice create slippery areas near doorways. If this is a common occurrence, you should make note of it and develop a maintenance schedule in order to mitigate the risk of anyone slipping in that area.
- If a hazard is present, inform your employees and customers by posting warning signs, placing barriers around the hazard, repairing the hazard or removing the hazard.

BEYOND INSURANCE BROKERS INC

Hidden Risk: Business Interruption Costs Associated with a Data Breach

On Nov. 24, 2014, Sony Pictures Entertainment experienced a major data breach that forced the company to shut down entirely for almost two days. A few days later, a number of Sony's movies that were not yet released were distributed by the hackers across the Internet, allowing millions of people to view them. Employees' personal information was also leaked.

In light of the growing number of high-profile data breaches that have occurred in the last year, more and more companies are purchasing cyber liability insurance and creating plans for their responses to data breaches. While this is a step in the right direction, the Sony example highlights an exposure that many business owners have not yet considered: business downtime in the event of a technology failure or cyber attack.

Most standard commercial insurance policies do not cover business interruption time that occurs as a result of cyber-related circumstances or a technology failure. This means that any losses a company experiences during the time spent trying to get the company back on track would not be covered. In Sony's case, employees were unable to work during the two days the system was shut down, and potential sales were lost during that time. However, payroll and other expenses that the company was expected to provide were still taken out. Without any output and subsequent profit, employee paycheques and other bills can add up quickly during a business interruption—especially if it lasts for a month or longer.

The professionals at Beyond Insurance Brokers Inc. can help you customize your policy in order to best reflect your coverage needs. Additionally, Beyond Insurance Brokers Inc. has access to business continuity planning materials, which can help mitigate the uninsurable risks associated with a business interruption. For more information, contact your Beyond Insurance Brokers Inc. representative today.

According to IT World Canada, the average total cost of a data breach has increased by

15 per cent

costing companies an average of **$145 per lost or stolen record.**

For major companies with many customers, this could easily mean paying **$3.5 million**

Companies who were able to bounce back quickly after a breach had the following characteristics in common:

- The companies had strong security in place prior to the attack
- They had a solid response plan
- One person was employed as the chief information security officer

Factors affecting high costs after the breach included:

- Whether the breach was a result of corporate devices being lost or stolen
- Whether anyone outside the company was involved
- How quickly customers were notified
- The use of consultants after the breach

Source: IT World Canada

COMMERCIAL INSURANCE Profile

Workplace and safety tips brought to you by the insurance professionals at:
Beyond Insurance Brokers Inc.