OPTIMUM®
General Insurance

“ Protecting our policyholders and their assets with creative and tailored solutions ”

Prevention Capsule

Cyber Security – The importance for a business to be vigilant about data protection

Even though most companies have had security systems for their computer networks in place for some time, it is also very important to make sure your internal teams are well aware of and prepared for the many risks associated with cybersecurity. A simple mistake can severely damage your company’s public image as well as it’s professional bond of trust with your clients and customers for many years into the future.

Limit the impacts of a data breach or computer attack on your business by adopting appropriate preventive measures.

Explanation of terms related to cyber security

Data breach

What exactly does a data breach mean? It is the unauthorized access to, viewing, copying, stealing, transmitting, or exposure of information that can identify an individual person or group of people.

Computer attack

A computer attack (or cyberattack) can occur either by an unauthorized person gaining access to a computer system, or by an authorized person gaining access to the computer system for unauthorized purposes, or by a malware attack, or by a denial of service (DDS) attack.

Here are some prevention tips that will help reduce the risk of cyberattacks for all types of companies:

- First and foremost, as part of your risk management make sure you have a specialized team set up for security and prevention as well as **duly designated and accountable manager(s)** for the department or team. As your company grows in size and technological needs, this team should logically also grow on a proportionate basis.
- In addition to the security and prevention team, it is also very important to offer ongoing security awareness and preventative measures training to all your employees. In most cases it is often the employees who are commonly exposed to security threats including malware or phishing attacks via email etc. Having your employees well trained and able to identify potential threats as a first line of defence is always strongly recommended.
- Third-party risk management: If your networks, systems, or data are managed by third parties, it is recommended that you evaluate their strategic approach to the security of your data, **as well as their IT protocols directly related to IT security**.
- Prioritize security updates to your systems, **as well as updates to the various software used**.
- Create and **internally communicate** a pre-prepared intervention plan that covers several different scenarios should your business suffer an attack. This will allow for optimal crisis management. At the time of an unfortunate situation, it can easily disorient one’s judgment and cause them to be more reactive when making important decisions. With a pre-prepared plan in place, the approach to decision making and management will be calmer and clearer.
- Purchase cyber insurance to protect your business’ assets, resources, and confidential data. The costs to recover after a cyberattack can be significant. You should also think about the following:
  - Brand image management and its costs, mainly related to public relations;
  - The requirement to send bulk mailings to affected individuals of a data breach as well as other required and related procedures and communications **that are necessitated by the Personal Information Protection and Electronic Documents Act (PIPEDA)**;
  - Legal expenses and the potential impact to your business of a judicial investigation, as well as any other associated legal costs **such as fines or penalties that may be imposed on the business if it is found to be legally liable under applicable provincial or federal legislation**.

For more details about the cyber insurance products offered by Optimum General Insurance, visit our website www.optimum-general.com.

2023-05

optimum-general.com

optimum-general.com/linkedin