
# Cyber Liability Insurance for Business

Gone are the days when cybercriminals only targeted companies that were treasure troves of credit card or health information. In today's interconnected society, everybody and every business is vulnerable. Cyberattacks and data breaches can happen to the most unsuspecting victims. As Canadians reap the benefits of the Internet of Things (IoT) and connected technology in both the personal and commercial spheres, they're unknowingly creating long, connected access routes for cybercriminals to exploit. As fast as our technology evolves, cyber threats also evolve.

## 3 Ways to Mitigate Cyber Risks for Business

In our businesses we can proactively do three things:

1. Understand cyber risk.
2. Take preventative action.
3. Consider a Cyber Liability Insurance policy.

# Understanding Cyber Risk

### How does a cyber attack happen?

Essentially there are 3 ways a cyber attack may happen.

**1. Phishing.** The most common way for bad actors to get access to a personal or business computer system is by 'phishing'. This is done by sending an apparently authentic request for a response, information, or a password to you. If an email looks legitimate but asks for personal information or money transfers, or is a strange request from what appears to be a familiar source, this is likely a fraudulent email and should be deleted or at least brought to the attention of someone who can assist in this determination. The simplest protection from this is to follow an absolute rule to not open email from sources you don't know or sources you are not expecting an email from. Everyone in business-all employers and employees-should follow that simple rule. It is a MUST.

**2. Hacking.** The second way for bad actors to get access to a personal or business computer system is a serious and intentionally focussed programming 'hack' or attack on a computer system. This is more sophisticated and our protections rely on virus protection software which most businesses must continually update and monitor. Consumers' computer software usually comes with some protection and more can be purchased with advice from your technology provider.

**3. The Insider.** The third way for bad actors to get access to a personal or business computer system is good old-fashioned theft. This would be someone on the inside of a business or someone personally close to an individual who would share access credentials or passwords with an outsider. The theft of credentials could be the result of an innocent or naïve error, or it could be intentional.

## Taking Preventative Action

Like most things in life, being careful and being smart about how we go about our on-line lives is the most effective way to protect our information from theft, misuse, or damage. Having a very secure property doesn't mean no one will break in, but it does discourage the act, and makes us less of an 'easy target'. The same applies to cyber security. Here's some quick tips:

1. Watch out for 'phishing'. Have strict rules both personally and in business about not opening and deleting suspicious email.
2. Change passwords frequently on all devices as much as this is a pain to do. Smart folks are now transitioning to multi-factor authentication now. (see separate info on this subject on our News & Info page).
3. Have an expert periodically check your computer(s) for bugs, malicious files, and general clean-up and maintenance.
4. Keep your work computer and work-related documents and files in an area at home that is physically separate from your family life.
5. Use your work computer for work only and limit the use of your personal devices for work-related purposes.
6. **DON'T:**
    - ❖ Provide business or personal information, even seemingly innocuous information, to requestors you cannot verify with certainty.

- ❖ Use the pandemic as an excuse to bypass regular work processes, such as authorizing payments.
- ❖ Disable security software or automatic updates on your work computer.
- ❖ Leave work-related files with sensitive information lying around openly at home.
- ❖ Give family members or other individuals access to your work computer.
- ❖ Use your work computer for private business.
- ❖ Email business documents to your personal email account.
- ❖ Use any cloud services or install any software on your work computer that your company hasn't authorized for business use.

## A Cyber Liability Insurance Policy

In business, risk trips us up when we least expect it. One such risk are your cyber exposures. Be it stored customer data or website content, cyber exposures are vast and require the best business insurance options. However, a standard business liability policy is unlikely to protect against most cyber exposures and in fact, often **explicitly excludes** such coverage.

Just one malicious cyber attack could bring the day-to-day activities of your small business to a standstill. Damage could be caused by:

- An attack that cuts off access to your website, a DDoS (distributed denial of service).
- A malicious code that renders your website unusable.
- Viruses or worms that delete vital operational information.

Exploiting weaknesses in corporate computer systems, whether through traditional hacking methods or social engineering is a full-time job. Hackers, thieves, and other unauthorized individuals are now adept at finding ways to compromise security – this is where business insurance and cyber liability insurance can provide the coverage you need. If your data is compromised and normal operations are halted, business insurance and cyber liability insurance coverage can help pay for interruption related expenses such as:

- Operating expenses, such as utilities, that must be paid even though business has temporarily ceased
- Profits that would have been earned had the hacking situation not occurred
- Lost income due to the cyber attack event
- Rented or leased equipment

With **Cyber liability coverage** as part of your business insurance program, you could also have protection from:

- Cyber extortion, including ransomware, which is malicious code installed into a computer on your network that prevents you from accessing it until a ransom is paid
- Data breaches, including costs for customer notification, some legal costs and credit monitoring for those affected

- Data or code loss due to a natural disaster or malicious activity.
- Damages to third-party systems if, for example, an infected email from your servers crashes the system of your small business clients or suppliers

Understanding Cyber Risk, Taking Preventative Action, and considering a Cyber Liability Insurance Policy as part of your insurance program are all part of managing business risks toady. Talk to us at Gateway Insurance Group. We can help you find sensible solutions for your insurance needs!

***To find out more, contact us anytime at 1-855-390-9300 or info@gatewayinsurance.ca.***