Cyber Risks & Liabilities

Cyber Risk. What is it? Why should we be concerned? Can it happen to anyone? What should we do to protect ourselves and our businesses? Can anyone answer this question in straightforward language? All good questions.

Cyber Risk. First, most of us are connected to the outside world one way or another. From smart appliances at home, to personal email services, to our cell phones, to more sophisticated computer systems in our work lives. All these connections make us vulnerable to electronic or 'cyber' attack by persons who do not care about our circumstances or the damage they might inflict on you or your colleagues, friends, or clients. Personal and business information is therefore at risk. It can disappear, be corrupted, or used maliciously causing damage or cost to you and to others and creating liabilities for individuals and businesses. Depending on what information is exposed to an attack, these costs and liabilities can be significant.

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.

How do we protect ourselves?

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.

What Role Does Cyber Insurance Play in our Protection?

No surprise, this is a fast-changing landscape with insurers reacting to cyber risks by extending insurance coverages, then adding, withdrawing or changing the coverages. Generally, expect increasing costs for cyber insurance as the threats and claims multiply. Many home insurance policies may now carry a basic coverage or coverage option for some recovery of costs incurred in a personal cyber breach. Business insurance options for cyber coverage ranges in its depth by type of business and type of policy. The best advice is to have a discussion with one of our brokers at Gateway to find out what is available and sensible for your particular personal or business needs. See our News & Information Page for more on this subject.

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