KRGinsure

Technology over the past few decades has transformed how we lead our personal and professional lives. With increased access to information at our fingertips, more and more organizations are being exposed.

A recent cybersecurity study revealed that 43 percent of Canadian businesses had experienced one or more cyber-attacks during the course of the year, which infiltrated networks or enterprise systems.

What is cyber risk?

Cyber risk refers to any risk of financial loss, disruption or damage to the reputation of an organization resulting from the failure of its information technology systems. This could materialize in a variety of ways:

- Deliberate and unauthorized breaches of security to gain access to information systems
- Unintentional or accidental breaches of security
- Operational IT risks due to poor systems integrity or other factors.

How cyber risk affects your business?

Whether you're a small business or a multi-million dollar corporation, you're not immune to cyber risks. All businesses face the risk of a cyber breach at some point during their life cycle, but understanding the threat and its severity can go a long way to helping control for its consequences.

Ways you can become a victim of a cyber-attack:

- Cyber criminals are increasingly walking amongst us as company employees
- Employees are the weakest link due to phishing and social engineering
- Cyber criminals target organizations with computing resources that they can rent out
- Hackers are using email notifications to send payments to criminals
- Blended attacks (using any and all opportunities) are becoming common practice
- Extortion, where data is held ransom, is a common cyber-criminal activity

Ways you can try to control for cyber-attacks:

- Provide security awareness training to all employees
- Segment networks to ensure only authorized employees are able to access appropriate data sets
- Keep all software up to date to ensure criminals have fewer weaknesses to exploit
- Establish good data governance policies and processes

KRGinsure

What you need to know about the Digital Privacy Act – November 1, 2018

The Digital Privacy Act (known as Bill S-4) reformed the Personal Information Protection and Electronic Documents Act (PIPEDA). There are some implications that businesses need to be aware of such as: fines & penalties associated with a reporting a breach, the need to inform clients, proper record keeping requirements, and change to consent.

Fines & Penalties

Organizations are now obligated to record and report any breaches of their security safeguards. They also can't obstruct an investigation or audit into a breach, or they will be liable for fines up to $100,000 for an indictable offence, or a fine of up to $10,000 for offences punishable on summary conviction.

Notifying clients in the event of a breach

Organizations are also required to notify individuals that are affected by the breach if it could cause harm to the individual. Harm is broadly defined as anything that includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identify theft, negative effects on the credit record, and damage to or loss of property. The organization also has to notify the Office of the Privacy Commissioner of Canada.

Breach Record Keeping Requirements

Organizations are required to keep record of every breach of security that involves personal information under control. These records must be provided to the Privacy Commissioner when requested. There are currently no details on how long the records need to be retained, how the records must be designed and maintained, and the level of detail required in the report. It is a good idea for organizations to keep a record of a breach no matter how trivial or inconsequential they may seem.

Changes to Consent

Obtaining valid consent from customers, clients or users when obtaining their data or personal information, has also changed under this new bill. While organizations were always required to obtain consent, the new legislation emphasizes the need for the user to understand the nature, purpose and consequence of the data collection. Privacy policies should be written in clear and simple language to ensure that consent is valid.

Next steps for businesses – Digital Privacy Act

Businesses that handle or collect personal information should:

- Review privacy policies and security safeguards to ensure compliance.
- Board of Directors should review their risk management and allocation of risk surrounding the new monetary penalties.
- Review or develop new response plans and continuity plans that comply with the new reporting and notification requirements.