

FACTS ABOUT CYBER CRIME

Cyber crime typically involves an attack on an organization's electronic infrastructure and/or gaining unauthorized access to data with the intent of stealing it. **These attacks are not only inconvenient and expensive, they can present an existential threat to a business or organization.**

Criminal hackers are working around the clock to find new ways of compromising the security systems of organizations regardless of their size. Individuals, complex cyber criminal networks and even foreign governments are engaging in cyber crimes. **No one is immune.**

Questions about insurance? Call us.

Insurance Bureau of Canada
Toll-free: 1-844-2ask-IBC
(1-844-227-5422)

ibc.ca

- @InsuranceBureau
- facebook.com/insurancebureau
- youtube.com/insurancebureau

Insurance Bureau of Canada is the national trade association for Canada's private home, car and business insurers.



© 2018 Insurance Bureau of Canada. All rights reserved.

The information provided in this brochure is intended for educational and informational purposes only. Please consult the appropriate qualified professional to determine if this information is applicable to your circumstances.



BUSINESS INSURANCE → VISIT IBC.CA



How big is the problem?

Cyber crime creates problems that are significant and costly.

- ▶ Worldwide, incidents of cyber crime cause **almost \$600 billion in losses every year.**¹
- ▶ Cyber attacks can be fatal to businesses. Approximately **60% of small businesses go out of business within six months of a cyber attack.**²
- ▶ In Canada, the **average cost of a data breach is \$4.74 million.**³
- ▶ Every year, Canada loses 0.17% of its gross domestic product to cyber crime – the **equivalent of \$3.12 billion per year.**
- ▶ In 2016, **fraud accounted for 47.5% of cyber crimes** reported by Canadian police services.⁴
- ▶ Identity theft and identity fraud accounted for **1.1% and 3.5%**, respectively, of cyber crimes in 2016.⁵
- ▶ The average **data breach detection and escalation cost** in Canada - which include forensic and investigative activities, assessment and audit services, crisis team management and communications and credit monitoring - is **\$1.78 million.**⁶



¹ McAfee 2018, The Economic Impact of Cybercrime: No Slowing Down

² Canadian Federation of Independent Business

³ Ponemon Institute July 2018 study on the cost of data breaches

^{4,5} Statistics Canada

⁶ Ponemon Institute July 2018 study on the cost of data breaches



How your business or organization can be attacked

Security doors and bank vaults of yesterday have been replaced by password-protected computers and encryption. Criminals have changed with the times and found new ways to undermine organizations and access their information. While criminal hackers are devising new techniques all the time, here are a few common ways in which organizations can come under attack.

- ▶ **Denial-of-service attack:** Flooding a website with more traffic than it was built to handle overloads the website's server, making it impossible for legitimate visitors to access the site.
- ▶ **Phishing:** An attacker pretends to represent a trusted organization as a way to trick a user into taking an action (opening a malicious attachment or clicking on a bogus link) that he or she would normally not take.
- ▶ **Malware:** This harmful software takes control of a machine, monitors user actions and keystrokes, and/or sends confidential data from the infected computer or network to the attacker's home base.
- ▶ **Ransomware:** This software encrypts files to prevent users from accessing them and then demands payment for their safe recovery. These attacks can occur after clicking on a phishing link or visiting a compromised website. Ransom payments are usually requested in untraceable, crypto currencies, such as bitcoin.
- ▶ **Spoofing:** Once a cyber criminal gains access to a network, he or she impersonates another user or device in order to attack network hosts, steal information, spread malware or bypass access controls.
- ▶ **Brute force:** This type of attack uses trial and error to decode encrypted data by trying as many combinations as possible, as fast as possible. With recent improvements in computing power, this tactic can be highly effective.

What can a cyber attack cost your organization?

Multiple expenses may be associated with a cyber attack.

- **Regulatory defence expenses:** Expenses and civil fines incurred in responding to a regulatory proceeding resulting from a privacy or network security breach
- **Legal and civil damages:** Includes the cost of legal representation and possible damages related to a privacy or network security breach
- **Security breach remediation and notification expenses:** Costs to notify and manage a privacy incident
- **Crisis event management expenses:** Public relations expenses to manage the damage to your company's reputation as a result of a breach or cyber attack
- **Forensic investigations expenses:** Costs for hiring a breach response firm
- **Computer program and electronic data restoration expenses:** Expenses to restore or recover damaged or corrupted data caused by a breach, denial-of-service attack or ransomware
- **E-commerce extortion and reward payments coverage:** Costs paid to the person or organization extorting you or your company
- **Business interruption and additional expenses:** The income your business loses and the costs it incurs due to an interruption in services.



Learn more about cyber insurance

Cyber insurance is a prudent option to consider in case other preparations against potential cyber attacks fail. **It can cover your losses and your liability for the losses of others that arise as a result of the electronic activities of your business.** Policies can cover liability associated with holding personal information in both hard and soft formats.

Cyber insurance may not be included in a traditional business or commercial policy and may need to be added as a separate coverage.

To understand what risks your business may be exposed to and what coverage can best protect your business, contact your insurance representative.