THE TRUE COST OF CYBERCRIME

As technology advances, so do the risks that businesses face.

"Cybercrime is one of the greatest threats that businesses of all sizes and in all sectors face today," says Lee Rogers, President of the Rogers Insurance Group of companies.

In 2021, cyber incidents were nearly twice as likely to impact businesses as natural disasters and theft combined. (Source: Allianz) Further proof: Ransomware attacks increased by 151 per cent globally in 2021, compared to the first half of 2020. (Source: Canadian Centre for Cyber Security) The rapid escalation of this trend is expected to continue as cybercriminals consistently increase the frequency and sophistication of their attacks, often utilizing emerging and maturing technologies such as internet of things (i.e., smart objects like security systems that connect and exchange data with the Internet), machine learning, artificial intelligence and the recent implementation of 5G.

CYBERCRIME BY THE NUMBERS

4,600+
The number of cybercrime incidents reported in Canada in 2021.
(Source: Emsisoft)

Every 39 seconds
How often hackers launch an attack.
(Source: University of Maryland)

54%
The percentage of email scams and phishing attacks that target small businesses.
(Source: Canadian Broker Network Cyber Crime Report)

60%
The number of small- to medium-sized organizations that go out of business within six months of a cyberattack.
(Source: Cybercrime Magazine)

Did you know?

The average business interruption cost following a cyberattack is 24 times greater than the average ransom amount. (Source: Canadian Broker Network Cyber Crime Report)

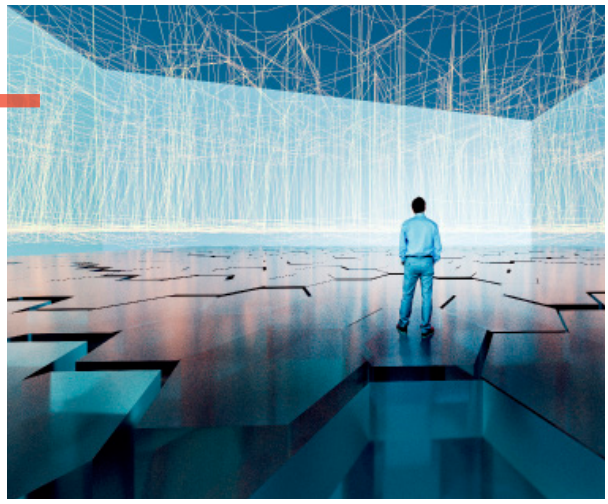
CYBERCRIME: MORE THAN MEETS THE EYE

The financial hardship a business faces after falling victim to a cyberattack is much higher than just the ransom or fraudulent fund transfer amount.

Additional losses and expenses that can result from a cyber breach include:

- Business interruption
- Digital assets restoration
- Forensic investigation
- Lawsuits
- Regulatory fines and penalties
- Replacing devices permanently impacted by malware
- Reputational repair and crisis management

A comprehensive cyber liability policy can help businesses cover such losses. Waiting to obtain this coverage until after experiencing a cyber breach will not only hinder a company's ability to respond to the incident but it will also make getting cyber liability insurance in the future more prohibitive. In most cases, it's likely the policy will offer less coverage, but the rate will be more expensive.



> "**Cyber liability insurance** is just as critical as other traditional commercial coverages," says David Edgar, Chief Broking Officer, CapriCMW.

What are Businesses to do?

Businesses can no longer afford to view cyber liability insurance as a nice-to-have; it is a necessity.

Even though cybercrime has been escalating at an alarming rate, most organizations' cybersecurity budgets have remained fairly flat (Source: Cybercrime Magazine), or were even cut in response to the COVID-19 pandemic (Source: Canadian Broker Network Cyber Crime Report).

To truly protect themselves, businesses must prioritize allocating more of their budget to cybersecurity. This includes investing in:

Cyber Liability Insurance

Insurers are increasing their cyber liability rates in response to the rapid rise in frequency and severity of claims. But this should not dissuade a business from getting or maintaining this coverage, as it provides a critical safety net from the skyrocketing costs of a cyberattack. For example, according to cyber insurer Coalition's H1 2021 Cyber Insurance Claims Report:

- The average ransom demand in 2021 was $1.2 million — an increase of 170 per cent compared to the year prior.
- The average amount stolen via fraudulent fund transfer in 2021 was over $326,000 — an increase of 179 per cent compared to the year prior.

Bear in mind, these figures do not factor in additional costs that arise from a cyberattack — such as business interruption, which some estimates state will increase by as much as 75 per cent year-over-year as cyberattacks become even more complex.

(Source: Canadian Broker Network Cyber Crime Report)

Cyber Hygiene

Risk management and mitigation should always be a business's first line of defence against any risk. In the cyber realm, this means practicing good cyber hygiene — the routine maintenance and regular improvements that strengthen digital security.

Common best practices include, but are not limited to:

- using multi-factor authentication;
- closing all unnecessary remote desktop protocols;
- regularly conducting employee training;
- using email filtering software; and,
- properly protecting and storing data backups.

Good cyber hygiene not only makes a notable difference in minimizing an organization's cyber risk, but it also improves the odds of obtaining cyber liability coverage at a more favourable rate.

Contact your broker today to discuss how cyber liability insurance can protect your business.

Acera INSURANCE | Rogers INSURANCE LTD. A human approach to insurance | CapriCMW CUSTOM INSURANCE SOLUTIONS

Rogers STIEG TRANSPORTATION INSURANCE Ltd. | Rogers INSURANCE CANADA | Sylvan AGENCIES | Megson FitzPatrick INSURANCE SERVICES | CCV INSURANCE & FINANCIAL a division of Rogers Insurance Canada Ltd. | Rogers McLEAN SHAW INSURANCE BROKERS LTD. | AgPro INSURANCE BROKERS Natural Expertise | RV DIRECT INSURANCE | A-WIN INSURANCE

bullfrog INSURANCE | EASYCOVER WORK WITH CONFIDENCE | Sharp INSURANCE | SMITH PETRIE CARR & SCOTT INSURANCE BROKERS LTD. | KAERUS GROUP RISK SOLUTIONS INC. | FAIRFIELD WATSON committed to people

Interested in learning more about cybercrime trends?

CanadianBrokerNetwork

Click here to read the Canadian Broker Network Cyber Crime Report or go to canadianbrokernetwork.com/cbn-cyber-crime-report-january-17-2022/