



CYBER INSURANCE AND WHY YOUR SMALL BUSINESS NEEDS COVERAGE

It's no secret that cybercrime is on the rise. A recent study indicates cybercrime is now the most serious threat to small businesses, accounting for roughly half of all attacks.[1]

There are many steps businesses can take to prevent a cyber incident, such as investing in robust cybersecurity measures. However, if an incident does occur, having cyber insurance can help you financially recover.

What is cyber insurance?

Cyber insurance covers financial losses that result from cyber events such as data breaches, cyber theft, ransomware and more.



- Cyberattacks are now a serious threat to small businesses because they typically lack enterprise-level protection.
- Cyber insurance is not typically included within general insurance and must be purchased separately.
- Each company offering a policy form has a unique list of coverage options available as well as exclusions, leading to a plethora of options.
- If your business handles or stores personal/sensitive information online, cyber insurance should be a top priority.

Why do small businesses need cyber insurance?

80%

Over 80% of small businesses are not properly equipped to recover from a cyber incident.[2]

10%

Less than 10% of small businesses have proper cyber insurance coverage.[2]

03
Per Day

There were over 1,200 publicly disclosed cyber incidents last year, i.e., almost three incidents per day.[2]

15%

Less than 15% of small businesses consider their cyber incident prevention and response strategy as effective.[2]

50%

Over 50% of small businesses do not have a cybersecurity expert in-house.[2]

What does cyber insurance cover?

It is always better to contact your insurer to get the exact details of what they cover. Typically, this is what cyber insurance covers:

- Cost of recovering data
- Cost of legal proceedings
- Cost of notifying stakeholders about the incidents
- Cost of restoring the personal identities of those affected



Top 5 reasons cyber insurance is denied



- **Companies have poor prevention practices in place**
- **Companies fail to document preventative measures**
- **A third party or contractor is at fault**
- **Accidental errors and omissions**
- **Coverage does not extend beyond the interruption timeframe**

Sources:
1 - National Cybersecurity Alliance
2 - IT Governance EU

Cyber insurance is a vital tool in protecting businesses from financial fallout in the aftermath of a cyberattack. However, many insurance providers are reluctant to offer coverage due to the perceived risks. While that may sound like bad news, don't worry — it's possible to get and keep coverage with the help of an experienced IT service provider.

Schedule a no-obligation consultation to learn more about how we can help you stay compliant with your policy.

claritech

Dan Frederick
dan@claritech.ca
(587)-600-9886
https://claritech.ca