Northbridge®
Insurance

CYBER COVERAGE

BUILT FOR YOUR BUSINESS

Cyber threats are on the rise, with over 20% of Canadian businesses having experienced a cyber incident.[1]

While big company breaches tend to make headlines, the fact is that cyber criminals target businesses of all sizes, across every industry.

If you're hit, recovering can be costly and time consuming.

That's why we offer comprehensive cyber insurance designed to meet today's evolving cyber risks.

WHETHER:

- You've downloaded a virus and no longer have access to critical data
- An employee has lost a device with sensitive information
- A critical database has become corrupted by malware
- You've fallen victim to ransomware

Our policy provides first and third party protection, and coverage of data stored on your system or a service provider's system—anywhere in the world.

Plus our Cyber Assist* service can help you with proactive measures to protect your data, and reactive assistance in the event of a breach.

It's all part of our commitment to keeping you safe in an increasingly digital world.

WHY CONSIDER CYBER INSURANCE?

- Small and medium sized businesses account for 61% of all cyber attacks[2]
- Cyber incidents impact companies across every industry
- The average cost of a breach response is $6.11 million[3]
- Average business downtime from a breach is 23 hours[1]
- Failure to comply with Canada's mandatory privacy breach reporting and record keeping laws could result in a fine of up to $100,000

MORE THAN JUST A POLICY

We've partnered with CyberScout, a leading data risk management service provider, to provide our customers with Cyber Assist services.

Included at no additional charge with our cyber risk policies:

- Pre and post privacy breach services
- Risk management resources
- Incident response planning
- Crisis management support
- Notification assistance
- Media relations consulting

[1] Stats Canada – Impact of cybercrime on Canadian businesses, 2017; Released 2018-10-15

[2] Verizon 2017 Data Breach Investigations report

[3] IBM Ponemon Institute's Cost of Data Breach study, 2017

COVERAGE OPTIONS

Standard Package:

Our standard package is available to any business with under $15 million in revenue and with coverage limits up to $1 million.

Custom Solutions:

We offer custom cyber risk solutions for businesses with over $15 million in revenue or requiring higher limits.

Coverage/Feature	Explanation	Standard Package	Custom Solutions
FIRST PARTY COVERAGE			
Incident Response Expense	Costs to notify and manage a privacy incident, including public relations expenses to manage reputation harm.	✓	✓
Data Recovery Expenses	Expenses to restore or recover damaged or corrupted data caused by a breach.	✓	✓
Business Interruption	Coverage for business income lost as a result of an interruption in services such as malware or a denial of service attack.	✓	✓
Extortion	Expenses to prevent an extortion event from impacting business operations.	✓	✓
THIRD PARTY COVERAGE			
Network Security & Privacy Liability	Coverage for incidents resulting from unauthorized access or snooping of information. Coverage for incidents involving the transmission of malware or participation in a denial of service attack.	✓	✓
Internet Media Liability	Coverage for personal injury and infringement resulting from content posted online.	✓	✓
Regulatory Expenses	Expenses and civil fines incurred in responding to a regulatory proceeding resulting from a privacy or network security breach.	✓	✓
Limits	Maximum available aggregate limit of insurance.	$1 million	$10 million
Minimum Price		$175	Negotiable
Cyber Assist	Access to consultation on proactive measures to protect their business, as well as reactive assistance in the event of a privacy breach.	Included at no additional charge	Included at no additional charge

CYBER RISK CLAIMS EXAMPLES

Rogue Employee | $ Millions

An employee violated company policy, accessing and selling information on thousands of customers to a third party marketing company. When the employer became aware of this, it launched an internal investigation during which time additional records were accessed and sold.

A public relations firm was hired to help communicate with customers and the general public about the incident. The rogue employee was fired and subsequently criminally charged and fined. The company faces a potential multimillion dollar class-action lawsuit from the affected customers.

Business Interruption | $200,000

A mid-sized manufacturer of metal component parts had its network breached. Malware infected its computer network, including automation systems. The company's IT contractor spent two days recovering electronic data from corrupted storage devices, but not all data was recoverable. While data backups were only a month old, the integrity had not been verified and so the data was useless. It took an additional 48 hours of reinstalling, repairing and reconfiguring the company's computer systems before the company was again operational.

Business income was lost over the four days the company could not operate. As a result of the interruption, the business also experienced contract performance delays causing vendors to experience lost income and delays of their own.

The manufacturer experienced an insured first party loss of $209,000 ($4,000 for forensic investigation and assistance, $5,000 for legal expenses and $200,000 for business income loss).

Denial of Service Attack | $34,000

A small professional services company was hit by a distributed denial of service attack that impacted its systems to the point that it needed to shut them down for a few days to complete remediation.

Much of the work related to fixing the software was covered by its cyber policy. There was also physical damage to its network, which was also covered under its property policy.

Malware | $4,000

Over the weekend, malware infected the computer network of a local veterinarian's office. On Monday, the office staff was locked out of the CRM and vaccination software and unable to service customers or contact them to reschedule appointments.

IT forensics was called in and able to unencrypt the computer system in 10 hours. It was also determined that no customer information had been accessed or stolen.

ABOUT US

Northbridge Insurance is a leading Canadian commercial insurer. Working closely with our broker partners and leveraging our in-depth industry expertise, we help businesses operate more safely so you can worry less about risks and focus on opportunities. Learn more at www.nbins.com.

3818-004-ed02E | 08.2020