CYBER INSURANCE

CyberOne® Coverage

Why is coverage needed?

Virtually every business relies on data and computer systems. When these systems experience a virus or other computer attack, a business is at risk of losing critical information. This information can be essential to daily operations. Some businesses rely on data, systems and the internet as a primary means of conducting business. Others depend on data and systems as a support function within the organization.

Computer viruses are a growing problem, and a cyber-attack can significantly impact a business' bottom line. System and data recovery can result in lost income, and can generate thousands in recovery costs. What's more, liability from insufficient systems security can lead to expensive litigation.

How does CyberOne® Coverage meet this growing need?

CyberOne® Coverage is designed to help pay for the costs associated with restoring computers and recovering data.

This coverage also protects against lawsuits brought against a business as a result of a failure of its system security.

Highlights of CyberOne® Coverage

A) Computer Attack

Coverage is provided for the cost of an outside professional firm hired by the insured to restore its computer system to its pre-attack level of functionality by replacing or reinstalling software, removing malicious code and correcting the configuration of the insured's computer system. Coverage is also provided for the cost of a professional firm hired by the insured to replace lost or corrupted data from electronic sources. Coverage is triggered by a "computer attack" such as:

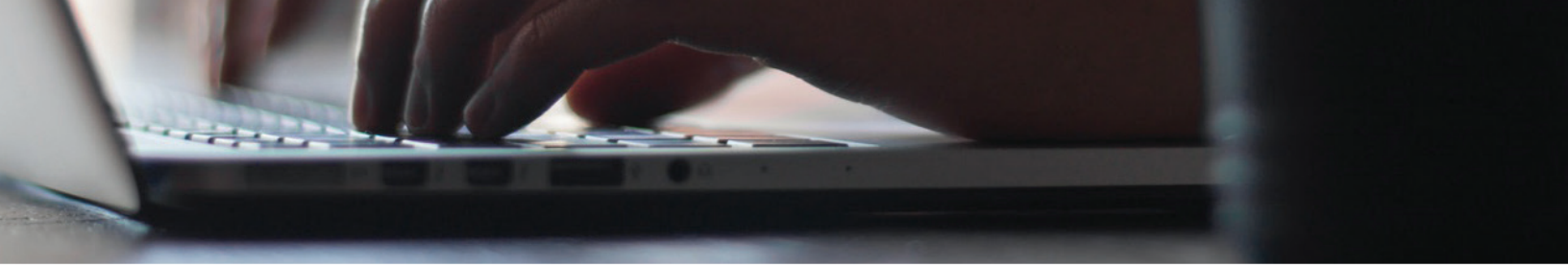
- A hacking event or other instance of an unauthorized person gaining access to the insured's computer system.
- An attack against the system by a virus or malware.
- A denial of service attack against the insured's system.

Computer Attack extensions of coverage

- Loss of Business: coverage for business income lost by the insured and extra expenses incurred by the insured during the period of time when system and data recovery activities are taking place. A sublimit of 20% of the Computer Attack limit applies.

Wawanesa Insurance

wawanesa.com



- Public Relations Services: coverage for assistance from a professional public relations firm in communicating with outside parties concerning the Computer Attack and the insured's response. A sublimit of 10% of the Computer Attack limit applies.
- Data Recreation Costs: coverage for the cost of a professional firm hired by the insured to research, recreate and replace lost or corrupted data from non-electronic sources. A sublimit of 10% of the Computer Attack limit applies.

These coverage extensions are included in, and not in addition to, the Computer Attack limit.

B) Network Security Liability

In the event of a lawsuit against the insured based on an alleged negligent security failure or weakness with regards to owned/leased computer equipment, Network Security Liability coverage covers defence, settlement and judgment costs. Defence is provided within the coverage limits. Network Security Liability coverage is triggered by a "network security liability suit" – a civil proceeding, an alternative dispute resolution proceeding or a written demand for money alleging that a negligent failure of the insured's computer security allowed one of the following to occur:

- A breach of third party business data
- An unintended propagation of malware
- A denial of service attack in which the insured unintentionally participated

CyberOne® Coverage options

A) Computer Attack

- Available coverage limits: $50,000 and $100,000

B) Network Security Liability

- Must be purchased in conjunction with Computer Attack coverage.
- Limit and deductible must be the same as the Computer Attack limit and deductible.

What could go wrong?

Insufficient systems security at one of the insured's contacts can make them vulnerable to a computer attack. Flaws in the insured's own system security can open their customers, vendors and others, with whom they do business, to potential damage and can lead to costly litigation.

Disgruntled Employee: A transportation contractor failed to change passwords after a disgruntled employee left. Shortly afterwards, the system began to act erratically: crucial software programs were unavailable and large amounts of data appeared to have been deleted. The firm's IT contractor spent 30 hours recovering electronic data from damaged storage devices. Not all of the data could be recovered, however, so the firm paid to have some of its historical records, still maintained in paper form, inputted manually. The contractor spent 45 hours reinstalling software, re-configuring the firm's servers and repairing other damage to the firm's computer system. In addition, the firm replaced various pieces of cargo tracking software that had been damaged or destroyed. Business income was lost over the course of several days while system issues were being addressed. A public relations firm was hired to help the contractor communicate with its customers about the incident. Insured losses: $43,850 (Computer Attack).

Computer Virus: The customers of an equipment dealer received strange emails appearing to have come from the firm. Worried, the firm's owner called an outside IT consultant who investigated and fixed the problem. The dealer's computer had been infected by a virus, but it had been easy to remove. Several weeks later, the dealer received a lawyer's letter alleging a customer had been infected by a virus received in the email message sent by the dealer. According to the letter, the customer had suffered a variety of different kinds of harm related to the virus and had incurred significant cost to have the virus removed. The equipment dealer engaged an attorney of its own and by the time the matter had been resolved, the dealer had written a $30,000 cheque to settle the dispute with the customer, while its own attorney had left a bill for 18,000. Insured Losses: $48,000 (Network Security).

Online Assistance Anytime

As a value added service for our CyberOne® policyholders, Wawanesa insurance offers an online risk management website with a number of tools and sources of information that can help them assess and manage the risk of a cyber-attack. Key features of the portal include: Steps a business can take following an incident, training modules, self-assessments and the latest news. It is designed to help the customer to better understand their risks and establish a response plan. With a response plan and instant access to informative resources they'll be ready to more efficiently and cost-effectively respond to and recover from a computer attack.