Loss Examples

Equipment dealer's virus infected external customer computers

The customers of an equipment dealer received strange emails appearing to come from the firm. The firm's owner called an outside IT consultant who investigated and fixed the problem. The dealer's computer had been infected by an easy to remove virus. The consultant left a bill for $200.

Several weeks later, the dealer received a lawyer's letter alleging a customer had been infected by a virus received in an email from the dealer. According to the letter, the former 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: First party: $200, Third party: $48,000

Small law firm becomes victim of mass-injection attack

Hackers gained access to the servers running databases behind the website of a small law firm.

The firm learned of the attack when Google notified that the site had been infected and had blocked access to it.

An outside IT firm was hired to find and delete the malicious code - three times. The first two fixes lasted only a week before the infection recurred.

Insured losses: IT work and lost business: $16,000

PEACE HILLS
INSURANCE

Head Office
Edmonton, AB

Offices
Calgary, AB
Vancouver, BC
Winnipeg, MB

CyberOne® COVERAGE

www.peacehillsinsurance.com

Represented by:

PEACE HILLS
INSURANCE

Printed 09/17

Cyber risk is a growing issue

Virtually every business relies on data and computer systems. When these systems experience a virus or other computer attack, a business is at real risk of losing critical information that is essential to daily operations and potentially exposing itself to third party lliability.

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

How does CyberOne® coverage meet these needs?

CyberOne® is comprised of first party coverage that is designed to respond to a computer attack that damages the insured's data and systems and helps pay for the costs associated with restoring computers and recovering data. In addition, this coverage is also comprised of third party coverage designed to provide defense and settlement costs in the event of a suit alleging that a system security failure on the part of the insured caused damage to a third party.

Highlights of CyberOne® coverage

Eligible Risks:

Most commercial risk classes with the exception of the following: financial institutions, adult business, gaming/gambling, hospitals, collection agents, credit reporting agencies, credit card/financial transaction processing, educational institutions and municipalities.

Option 1 – Computer Attack Coverage is triggered by the insured's discovery that a computer attack has affected a computer system owned or leased by the insured and under the insured's control. A computer attack may be a hacking event or other instance of an unauthorized person gaining access to the computer system; may be an attack against the system by a virus or other malware or it may be a denial of service attack against the insured's system. Coverage for costs for data restoration, data recreation, system restoration, loss of business and public relations is provided.

Computer Attack Coverage Limit Options, Sub-limits & Deductibles

Coverage limits available:

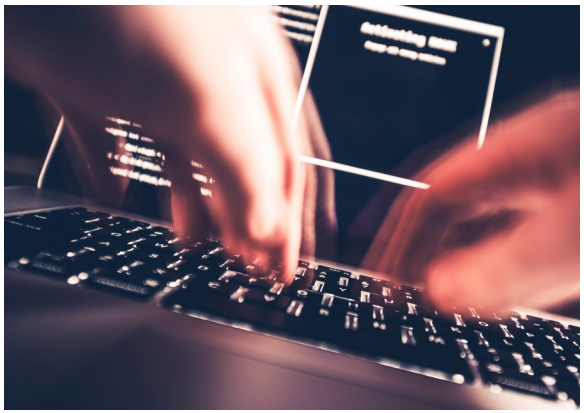
- $50,000 or $100,000 annual aggregate

Deductible of $1,000 is the minimum with options available:

- $ 2,500, $5,000, $10,000, $25,000 or $50,000

Computer Attack Sublimit:

- 10% of the Computer Attack Limit, per occurrence for Data Recreation
- 20% of the Computer Attack Limit, per occurrence for Loss of Business
- 10% of the Computer Attack Limit, per occurrence for Public Relations



Option 2 – Network Security Liability Coverage provides third party coverage 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

In the event of a network security liability suit, third party coverage would cover the costs of defense, settlement and judgements. (Defence is provided within the coverage limits). Receipt of the notice must occur during the policy period, and the suit must arise from an event that occurs after the first inception of the coverage. Third party coverage must be purchased in conjunction with the first party Computer Attack Coverage and the limits and deductibles would only be offered at the same limit and deductible as the first party coverage.

Examples of events that can lead to losses:

- Malicious insider
- Denial of service attack
- Malicious code
- Worms, viruses, Trojans
- Social engineering, phishing, pharming, spear phishing
- Website takeover via mass-injection attack, ransomware, spyware,
- Espionage: theft of trade secrets
- Social hacktivism
- Cyber terrorism

Subject to terms, conditions and exclusions of the policy

eRiskHub®

Insureds purchasing CyberOne® Coverage can be given access to a risk management portal. This web portal is provided as a value added service to customers to establish an incident response plan roadmap, online training module access, risk management tools, eRisk Resources, News Centre and Learning Centre.

Contact your independent insurance broker for other eligibility and minimum insurance requirements.