Data Protection and Cyber Liability

BY SHERRY D. SAMSON

Each day brings more news reports of data theft or system infiltration by outsiders that result in massive expenses to the affected businesses. Cyber liability is the most common term for policies intended to insure against a security breach that results in the theft, loss or unauthorized disclosure of confidential or personally identifiable information. But the terminology isn't consistent and the policies are not standardized.

The largest expenses incurred by businesses that are victims of a security breach include:

Remediation

- Costs to notify affected customers when a breach of a network results in unauthorized access to personally protected or confidential information. A policy should also include non-electronic records such as paper files.
- Credit monitoring: Although not required by most states, this service is typically covered, along with the cost of call centers for customer support.
- Forensic costs to investigate the nature and extent of the breach and determine what actions are necessary to correct any vulnerabilities.
- Costs to restore system and data.
- Costs for public relations services.

Fines and Penalties

- Regulatory action defense and penalties: Some policies provide only defense costs, others additionally provide coverage for civil fines to the extent insurable by law, and some do not offer this coverage at all. Coverage doesn't include criminal penalties or fines and is typically subject to a sublimit.
- Payment Card Industry Data Security Standard assessment coverage: This coverage is not available from all carriers.

Business Interruption

- The reduction in business income when a data breach affects revenues. Coverage is limited to a specified duration of time and there is a time-dependent deductible, e.g., two weeks.

Other Coverage

Cyber liability can provide coverage for claims made against an organization by its customers or other third parties, including:

- Bodily injury or property damage claims alleging damages as a consequence of personally protected information being accessed by an unauthorized party.
- Claims alleging transmission of malicious code including viruses, Trojan horses, spyware, etc., from a computer system.
- Claims alleging libel, slander, product disparagement, invasion of privacy, plagiarism, copyright infringement, etc., arising from a website, social media or other media material.

Cyber liability policies may also include computer crime coverage:

- Cyber extortion: Expenses and ransom when a business is the victim of a demand for money threatening damage or destruction of an IT system or data.
- Social engineering: An employee improperly transfers funds to a third party on the basis of an email request from someone purporting to be a person of authority within a company.
- Financial fraud: Through unauthorized access to the system, a third party transmits an unlawful instruction to the bank to disburse funds from the account.
- Phishing attack: A third party impersonates the company via fraudulent emails or malicious websites to solicit personal information.
- Cyber terrorism: Unauthorized access to a computer system with the intent to intimidate or cause destruction or harm and further social, ideological, religious, political or similar objectives.

With an average cost of $230 per record to resolve a malicious or criminal act (Ponemon Institute LLC, May 2015), data breaches present a significant financial risk for most businesses. Discuss exposures with an insurance agent. PB

Sherry D. Samson
Executive Vice President, Vaaler Insurance
Grand Forks, N.D.
701.787.3214
ssamson@vaaler.com