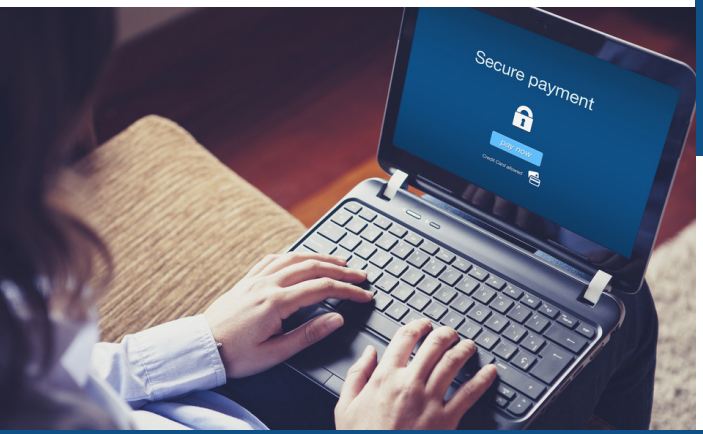
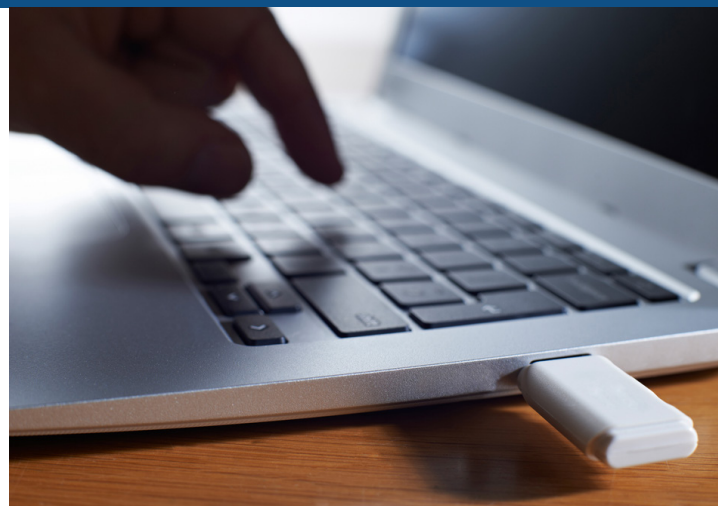


PEACE HILLS
INSURANCE

Head Office
Edmonton, AB

Offices
Calgary, AB
Vancouver, BC
Winnipeg, MB



DATA COMPROMISE COVERAGE

www.peacehillsinsurance.com

Represented by:

PEACE HILLS
INSURANCE

Printed 09/17

Data breach is a growing public issue

Virtually every business has data on clients, employees and others which can be stolen, electronically "hacked" or lost through accidental or inadvertent release.

71 percent of data breaches occur in businesses with 100 employees or less[1].

When asked which type of lost or stolen data was more likely to harm their business, 70 percent agreed the loss of personally identifying information was more damaging than confidential company data.[2]

How does Data Compromise coverage meet these needs?

This coverage was designed for small to medium sized businesses to help deal with the financial burden and service expectations of a data breach, discovered during the policy period and occurring after the first inception of coverage.

Data Compromise coverage will also: help the business to notify and assist affected individuals following a breach of personally identifying information; assist the insured in complying with data breach notification laws and requirements; offer credit flagging and case management to affected individuals; pay for defense and liability costs for actions brought by affected individuals as a result of a breach of personal information.

Highlights of Data Compromise 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 – Response Expenses Coverage provides for payment of first-party expenses in response to the personal data breach which includes the theft of electronic files, theft of physical files, accidental loss or release and voluntary release due to fraud. This would include expenses for notification to the affected individuals, outside legal counsel, forensic IT review, public relations costs, fraud alert assistance and identity restoration services to the affected individuals. Coverage is triggered by the discovery of the breach of personal information that is in the insured's care, custody or control or a third party with whom the insured has a direct relationship and has directly turned over such data.

Response Expenses Coverage Limit Options, Sub-limits & Deductibles

Coverage limits available: $25,000, $50,000, $100,000*, $250,000*, $500,000* & 1,000,000* annual aggregate

Sub-limits: (included in & not in addition to the Response Expenses Coverage limit)

- 10% of the Response Expenses limit applies per breach for Legal Review
- 10% of the Response Expenses limit applies per breach for Forensic IT Review
- 10% of the Response Expenses limit applies per breach for Public Relations Assistance

Deductible of $1,000 is the minimum with options available: $2,500, $5,000, $10,000

* Available to qualified insureds only

Option 2 – Defence and Liability Coverage provides third party coverage in the event the Insured receives notice of a third party suit or claim arising out of the first party personal data breach. In order for this coverage to apply you must first purchase the Response Expenses Coverage and the limits and deductibles must be the same as the Response Expenses Coverage. This coverage would include costs of defence and costs of settlement or judgement.

Examples of events that can lead to losses:

- Malware
- Hacking
- Inadvertent employee or contractor mistakes
- Injection of SQL
- Malicious insider
- Lost, stolen or highjacked devices

Subject to terms, conditions and exclusions of the policy.

1 National Cyber Security Alliance, 2015
2 HSB Group/Ponemon Institute poll 2013

eRiskHub®

Insureds purchasing Data Compromise Coverage can be given access to a data breach risk management portal. This web portal will assist customers to understand their information exposures, establish an incident response plan to manage the costs and minimize the effects of a data breach.

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

Loss Examples

Gas Station
Identity thieves used card skimmers at a gas station to steal bank account numbers with PIN codes from 550 customers. The thieves then created false debit cards, using the stolen information at ATMs to drain funds from client accounts.
Cost of notification and services: $19,250

Physician's Office
Three external back-up hard drives with private personal records from 300 patients were stolen from a locked physician's office. Notifications were sent to affected individuals advising them to place a fraud alert with credit bureaus and to monitor their credit reports and other financial statements.
Cost of notification and services: $10,500

Accountant's Office
A burglar broke into an accountant's office and stole a computer with the tax records of 800 clients. Clients were urged to contact their banks and place fraud alerts on their credit files.
Cost of notification and services: $28,000

Apartment Building
A box of rental applications with the name, address and Social Insurance numbers of 2,600 individuals was stolen from an apartment building office.
Cost of notification and services: $91,000

PEACE HILLS
INSURANCE