COVERAGE COMPARISON

Event Insured Against:
- **Data Compromise** - data breach
- **CyberOne®** - computer attack

Intent:
- **Data Compromise** - helps businesses notify and assist affected individuals following a breach of personally identifying information
- **CyberOne® ®** - protects businesses against damage to electronic data and computer systems from a computer attack

Coverages:
- **Data Compromise**
  - Responds to the breach, theft or unauthorized disclosure of personal information
  - The policy assists the insured in complying with data breach notification laws and requirements.
  - Offers services to affected individuals such as credit flagging and case management
  - Pays for defense and liability costs for actions brought by affected individuals as a result of a breach of personal information
- **CyberOne®**
  - Responds to events that damage or degrade data and systems
  - Coverage pays for defense and liability costs for the business's security system failure, including the breach of third-party business information

First-Party Coverage:
- **Data Compromise** - personally Identifying Information relating to individual people, including employees, customers and vendors
- **CyberOne®** - business operational software, operating systems and electronic data

First-Party Trigger:
- **Data Compromise** - loss, theft or inadvertent release of personal information
- **CyberOne®** - damage or destruction of business operational data and software by way of a computer attack

How Can an Event Happen?:
- **Data Compromise**
  - Electronic theft
  - Physical theft of electronic data
  - Physical theft of hard copy files
  - Procedural errors
- **CyberOne®**
  - Hacking
  - Virus or other malicious code
  - Denial of service attack

Summary of First-Party Coverage Response:
- **Data Compromise**
  - Forensic I.T. and legal consultation expenses
  - Expenses related to notifying affected individuals and regulatory authorities
  - Credit flagging and case management services to affected individuals
  - Public relations expenses
- **CyberOne®** - costs of recovering from a computer attack, including:
  - Recovery of data
  - Repair of systems
  - Loss of business
  - Public relations expenses

Third-Party Trigger:
- **Data Compromise** - insured's receipt of a third-party suit or claims arising out of the first-party triggering event
- **CyberOne®** - insured's receipt of a third-party suit or claim alleging that a failure of the business's computer security allowed one of the following to occur:
  - Breach of that third-party's business information
  - Transmission of malware to that third-party
  - Denial of service attack targeting that third-party

Summary of Third-Party Coverage Response:
- **Data Compromise** - costs of defense, costs of settlement or judgement
- **CyberOne®** - costs of defense, costs of settlement or judgement

Examples of Events Leading to Losses:
- **Data Compromise**
  - Malware
  - Inadvertent employee or contractor mistakes
  - Hacking
  - Injection of SQL
  - Malicious insider
  - Lost, stolen or hijacked device
- **CyberOne®**
  - Malicious insider
  - Denial of service attack
  - Malicious code
  - Worms, viruses, Trojans
  - Social engineering, phishing, pharming, spear phishing
  - Website takeover via mass-injection attack
  - Espionage: theft of trade secrets
  - Social hacktivism

For presentation purposes only. For all coverages, terms, conditions and exclusions, please refer to actual insurance policy.

SASKATCHEWAN MUTUAL INSURANCE COMPANY

www.saskmutual.com

Cyber Coverage

Data Compromise & CyberOne®

279 3rd Avenue North
SASKATOON SK S7K 2H8
Ph: (306) 653-4232
Fx: (306) 664-1957
1-800-667-3067

headoffice@saskmutual.com
www.saskmutual.com

BROKER:

M263 (12/18)

CYBER RISK IS A GROWING CONCERN

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 liability.

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 amount to thousands in recovery costs. Also, liability from insufficient systems security can lead to expensive litigation.

Federal mandatory data breach notification laws came into force November 1, 2018. "The Digital Privacy Act (Bill S-4)" amends the "Personal Information Protection and Electronic Documents Act" (PIPEDA), making it mandatory for all businesses, including non-profit organizations, to report data breaches to affected individuals and the Office of the Privacy Commissioner of Canada. Prescribed regulations accompany the legislation and outline requirements for data breach notification and record-keeping.

DATA BREACH RISKS

Virtually every business has data on clients, employees and others which can be stolen, electronically "hacked" or lost through accidental or inadvertent release. When asked which type of lost or stolen data was more likely to harm their business, 70% agreed the loss of personally identifying information was more damaging than confidential company data.

FACT: 71% of security breaches target small businesses *

COVERAGES TO HELP INSURE THESE RISKS

Heavy reliance on today's computer and data technology has heightened every business's exposure to data breach and cyber attack risks. Both have become increasingly frequent, costly and complex.

'Data Breach' and 'Cyber Attack' coverages are often used interchangeably but they remain distinct in terms of their definitions, triggers, losses and affected parties. SMI recognizes the important role that insurance can play in a business's overall risk management strategy. Therefore, we are offering two important coverages to protect business systems from harmful cyber attacks - Data Compromise and CyberOne® .

DATA COMPROMISE COVERAGE

Data Compromise is designed to help businesses respond to the financial burden and service expectations of a data breach. Businesses should be able to notify all parties affected by a breach, effectively communicate the scope of the possible damage and provide fraud alert assistance and identity restoration case management to those affected by the breach.

Highlights of Data Compromise Coverage:

First-Party Coverage - payment of first-party expenses in responding to a personal data breach including:

- Outside legal counsel
- Forensic IT review
- Public relations costs
- Notifications
- Fraud alert assistance
- Identity restoration services to affected individuals

Third-Party Coverage - defense and liability coverage designed to provide defense and settlement costs in the event of a suit

Covered Events Include:

- Theft of electronic files
- Theft of physical files
- Accidental loss or release and voluntary release due to fraud

Coverage Trigger - discovery of breach by the insured

Limits Options - various limits available up to $1,000,000

Deductible - $1,000

Eligibility - most businesses are eligible for Data Compromise coverage

CYBERONE® COVERAGE

CyberOne® helps pay for the costs associated with restoring computers and recovering data. This coverage also protects against third-party liabilities a business might have as a result of the failure of its system security.

Highlights of CyberOne® Coverage:

First-Party Coverage - triggered by a "computer attack" caused by:

- An unauthorized person gaining access to the business's computer system
- A malware attack
- A denial of service attack

In the event of a computer attack, payment available for:

- Data Restoration from electronic sources
- Data Recreation from non-electronic sources
- Systems Restoration
- Business Income
- Public Relations

Third-Party Coverage - triggered by a "network security liability suit" (ie: a civil proceeding, an alternative dispute resolution proceeding or written demand for money) alleging that a negligent failure of the business'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 business unintentionally participated

In the event of a network security liability suit, CyberOne® covers costs of defense, settlement and judgment. Defense is provided within the coverage limits.

Limit Options - various limits available up to $100,000

Deductible - $1,000

Eligibility - most businesses are eligible for CyberOne® coverage except the following classes of business:

- Adult Business
- Gambling or Gaming
- Financial Institutions
- Municipalities
- Schools, Colleges and Universities

* National Cyber Security Alliance 2015