Data Compromise and CyberOne® Coverage – Why You Need Both

Did you know...

54% of companies have experienced one or more cyber attacks that have compromised their computer systems and data? SGI CANADA's CyberOne® and Data Compromise coverages can play an important role in your organization's overall risk management strategy. With their distinct definitions, triggers, losses and affected parties, they cover different situations, working together to protect your business from all angles.

Here's why businesses need them both:

	Data Compromise Coverage (data breach)	CyberOne® Coverage (computer attack)
What's the intent of the coverage?	Helps businesses and organizations notify and assist individuals impacted by a data breach of personally identifying information.	Protects businesses and organizations against damage to computer systems and electronic data from a computer attack.
Coverages	• Responds to the breach, theft or unauthorized disclosure of personal information. • Assists the business in complying with data breach notification laws and requirements. • Offers services to impacted customers such as credit flagging and case management. • Pays for defense and liability costs for actions brought by impacted customers as a result of a breach of personal information.	• Responds to attacks that damage or degrade data and systems. • Pays for defense and liability costs for security system failure, including the breach of third-party business information.
What triggers the coverage? (first-party trigger)	Loss, theft or accidental release of personal information, due to: • electronic theft • physical theft of electronic data • physical theft of hard copy files • procedural errors	Damage or destruction of business operational data and software due to a computer attack, including: • hacking • virus or other malicious code • denial of service attack
How does the coverage respond?	It covers the costs of: • forensic IT and legal consultation expenses • expenses related to notifying impacted customers and regulatory authorities • fraud alert and case management services for impacted customers • public relations expenses	It covers the costs of recovering from the computer attack, including: • recovery of data • repair of systems • loss of business costs • public relations expenses
What triggers further coverage? (third-party trigger)	The business is named in a lawsuit or claim arising out of the data breach.	The business is named in a lawsuit or claim arising out of the cyber attack.