

# Data Compromise vs CyberOne® Coverage Comparison

With the heavy reliance on today's computer and data technology, it has heightened every business's exposure to both data breach and cyber-attack risks. These risks are distinct in terms of definitions, triggers, losses and affected parties. We, at Peace Hills recognize the important role both play in a business's overall risk management strategy. We've tailored two complementary products to assist you in providing your small to medium sized insureds with solutions to managing these exposures - Data Compromise and CyberOne® Coverage.

	<b>DATA COMPROMISE COVERAGE</b> <b>*Response Expenses</b>	<b>CYBERONE® COVERAGE</b> <b>*Computer Attack</b>
<b>Event insured against</b>	Data Breach	Cyber/Computer Attack
<b>Intent</b>	Helps businesses notify and assist affected individuals following a breach of personally identifying information.	Protects businesses against damage to electronic data & computer systems from a computer attack.
<b>First Party Coverage</b>	Personally identifying information related to individual people such as customers, employees and vendors	Business operational software, operating systems and electronic data.
<b>First Party Trigger</b>	Discovery of the loss, theft or inadvertent release of personal information by electronic theft, physical theft of electronic data/ hard copy files or procedural errors.	Damage or destruction of business operational data and software by way of a computer attack through malware attack, unauthorized person gaining access to the computer system or a denial of service attack.
<b>Coverage: (First Party)</b>	Covers costs and expenses for the following: <ul style="list-style-type: none"> <li>• Forensic I.T. and legal consultation expenses</li> <li>• Expenses related to notifying affected individuals and regulatory authorities</li> <li>• Services to affected individuals</li> <li>• Public relations expenses</li> </ul>	Covers costs of recovering from the computer attack including: <ul style="list-style-type: none"> <li>• data restoration</li> <li>• data recreation</li> <li>• system restoration</li> <li>• public relations expenses</li> <li>• loss of business</li> </ul>
	<b>DATA COMPROMISE COVERAGE</b> <b>*Defence and Liability Coverage</b> ( <i>Third Party</i> Coverage is only available if First Party Response Expense coverage is carried and must have the same limits & deductibles)	<b>CYBERONE® COVERAGE</b> <b>*Network Security Liability Coverage</b> ( <i>Third Party</i> Coverage is only available if First Party Computer Attack coverage is carried and must have the same limits & deductibles)
<b>Third Party Trigger</b>	Insured's receipt of a third party suit or claim arising out of the First Party triggering event.	Insured's receipt of network security liability suit alleging a negligent failure of the insured's computer security allowed one of the following to occur: <ul style="list-style-type: none"> <li>• breach of third party business data</li> <li>• an unintended propagation of malware</li> <li>• a denial of service attack in which the insured unintentionally participated.</li> </ul>
<b>Third Party Coverage</b>	Covers the defence costs and liability, costs of settlement or judgement.	Covers the costs of defence, costs of settlement or judgement.
<b>Events that can lead to losses</b>	<ul style="list-style-type: none"> <li>• Malware</li> <li>• Hacking</li> <li>• Inadvertent employee or contractor mistakes</li> <li>• injection of SQL</li> <li>• Malicious insider</li> <li>• Lost or stolen or hijacked devices</li> </ul>	<ul style="list-style-type: none"> <li>• Malicious insider</li> <li>• Denial of service attack</li> <li>• Malicious code</li> <li>• Worms, viruses, Trojans</li> <li>• Website takeover via mass-injection attack</li> <li>• Social Engineering, phishing, pharming, spear phishing</li> <li>• Ransomware, spyware</li> <li>• Espionage: theft of trade secrets</li> <li>• Social hacktivism</li> <li>• Cyber terrorism</li> </ul>

Subject to terms, conditions and exclusions of the policy