TRAVELERS

Travelers Canada CyberRisk™ Coverage Checklist

TRAVELERS CANADA

Why businesses need our protection.

In today's data-driven world where sensitive information is stored and transferred electronically, organizations of all sizes are vulnerable to costly and damaging liabilities from data security breaches that are occurring at alarming and growing rates.

Whether data is compromised by a hacker, virus, cyber thief, or simply because of lost or stolen computers, laptops, flash drives or smart phones, a breach can have serious ramifications. There are substantial financial costs involved in finding and remedying a breach, including the cost of notifying customers, possible fines and legal expenses. Breach notification is legally mandated in the province of Alberta and, with respect to personal health information, in the provinces of Alberta, Ontario, New Brunswick, and Newfoundland and Labrador. The company can also suffer immense damage to its reputation and from the interruption to business.

Travelers Canada CyberRisk™ coverage delivers a truly comprehensive coverage solution in a single policy. The following checklist illustrates key coverages and features every organization should have as part of its insurance program to protect against data breaches and related technology exposures:

	CyberRisk™	Other policy
Third party (liability) and first party coverage – protecting the insured for its liability to others and reimbursing the insured for expenses incurred	✓	
Worldwide coverage – applies to claims made or events occurring anywhere in the world	✓	
Ten distinct insuring agreements – with the ability to set limits and retentions for each insuring agreement	✓	
Defence option – option to select duty to defend or reimbursement coverage at policy inception	✓	
Maximum retention cap – for claims covered under more than one liability insuring agreement or events covered under more than one first party insuring agreement	✓	
Non-cancellable by insurer – except for non-payment of premium	✓	
Extended reporting period – applies to crisis event management and security breach expense coverage	✓	
Automatic 90-day extended reporting period – for first party coverages	✓	
First party coverage for computer program and electronic data restoration expenses	✓	
First party coverage for computer fraud and funds transfer fraud – protection for fraudulent transfer of money or securities, or, with respect to computer fraud, other property	✓	
E-commerce extortion coverage – applies to computer viruses and denial of service attacks	✓	
Business interruption coverage – extends to denial of service attacks	✓	
Coverage for security breach remediation and notification expenses extends to: • Purchase of an identity fraud insurance policy • 365 days of credit monitoring services	✓	

	CyberRisk™	Other policy
Defence expense regulatory claim coverage – it is not limited to specific governmental agencies and includes claims by any state attorneys general in the United States	✓	
Communications and media coverage – applies to content in any electronic format including websites and electronic mail	✓	
Coverage extends to claims seeking – non-monetary relief and arbitration, mediation or similar alternative dispute resolution proceedings	✓	
Coverage for punitive or exemplary damages on a most favourable venue basis	✓	
Network and information security coverage extends to: • Electronic or non-electronic data and is not limited to e-commerce, website or other specified activities, or only to information "on premises" • Medical or health care information • Any private personal information that is protected under any local, provincial, state, federal or foreign law • Failure to provide notification required by ANY security breach notification law • Claims made by employees	✓	
Defence expense coverage for regulatory claims – for network and information security coverage and communications and media liability	✓	
Coverage for unfair business practice claims under network and information security or communication and media insuring agreements – if such practices directly result from a network and information security wrongful act or a communications and media wrongful act	✓	
Network and information security coverage is not narrowed by exclusions for: • Failure to maintain a computer network or system • Failure to maintain risk controls • Lack of performance in software • "Spyware," "cookies" or other invasive devices or methods used to collect private information • Trading losses	✓	

Contact Travelers or visit travelerscanada.ca today to learn more about Travelers Canada CyberRisk™.

TRAVELERS

travelerscanada.ca