CREECHURCH Underwriters
The Smarter Side of Risk

550-55 University Avenue | Toronto ON M5J 2H7
1701-2001 McGill College Avenue | Montreal QC H3A 1G1
1511-701 West Georgia Street | Vancouver BC V7Y 1C6

P 1-877-814-7778 | www.creechurch.com

CYBER*PLUS* PLATINUM

In today's world, privacy and data breaches are a fact of life that can happen to any business, large or small. Any organization that collects personal information on employees or customers; stores confidential business information on its customers; transacts business online or provides portable devices such as laptops or smart phones to its employees is susceptible to a privacy or network security breach ("cyber liability"). The exposures arising from disclosure (whether by negligence, security breaches or hacking) of information such as credit and debit cards, SINs, health records, customer lists, merger and acquisition insider information, intellectual property and trade secrets can be significant. Interruption of a network, introduction of a virus or theft of data could disable access to company websites, corrupt databases, or result in the theft of large volumes of confidential customer information. The fall out may include the commission of fraud with the exposed data or extortion to restore electronic access. Company employees or agents may inadvertently or purposefully defame competitors on company websites, blogs or the ever expanding social media realm.

Creechurch recognizes the unique needs of the Canadian environment and has developed the market leading Cyber*Plus* Platinum Insurance Policy. This comprehensive policy is laid out in an easily understood format and provides the liability and first party coverage necessary to address the growing cyber liability threats to all types of organizations.

COVERAGE OVERVIEW

A. LIABILITY

Privacy & Security Liability

coverage for third party damages and defence costs arising out of actual, or potential:

- Breach of any right to privacy of employees or third parties
- Theft, loss, unauthorized access to or disclosure of personal information or confidential third party corporate information
- Failure to provide timely disclosure or notification of a privacy breach
- Failure to protect against unauthorized access or use, theft or destruction of data, denial of service attacks and virus transmission involving the insured's computer system

Multimedia Liability

coverage for third party damages and defence costs arising out of display of electronic content on the insured's website (or on other's website's for which insured is responsible)

- Extends to many internet-related exposures including advertising injuries that are not covered under many of today's general liability policies including copyright infringement, piracy, libel and slander

B. FINES AND PENALTIES

- Civil fines/penalties imposed in a regulatory proceeding for a privacy breach
- Equitable relief funds for payment of consumer claims in a regulatory proceeding
- Fines or noncompliance assessments arising out of a breach of the rules, standards and agreements governing the Payment Card Industry

C. FIRST PARTY COVERAGES

Privacy Breach Response Expenses

coverage for expenses arising out of privacy and security breaches, including:

- Notification (voluntary or mandatory), including legal fees to determine actions necessary in event of privacy breach
- Computer security expert to demonstrate ability to prevent a future data breach
- Mitigation to reputation, including public relations consultancy, crisis management or legal advice, advertising and communications
- Identity theft protection, including changing, restoring and monitoring credit, identity or healthcare records; call centre services

.../2

CYBER*PLUS* PLATINUM

Forensic Expenses - costs to investigate source of failure of computer security to prevent a breach

Data Protection Loss - costs to restore insured's data and to determine scope, cause or extent of a security breach

Data Protection Loss- costs to restore insured's data and to determine scope, cause or extent of a security breach

Business Interruption - covers income loss and extra expenses incurred to minimize loss, from interruption of computer systems until earlier of: (1) end of the interruption, or (2) 60 days after business activities are restored

Cyber Extortion - covers extortion payment and related expenses arising out of a threat to breach, interrupt, prevent access to, transmit virus to, or perpetrate a theft of data from, the insured's network

Reward Expense - covers payments to an informant for information leading to arrest and conviction of person responsible for an extortion threat or security breach

Cyber Terrorism - covers income loss and extra expense arising from an electronic terrorism act, from interruption/failure of computer systems until earlier of: (1) end of the interruption, or (2) 60 days after business activities are restored

COVERAGE HIGHLIGHTS

- Canadian–recognition of key legislative, regulatory and environment differences
- Broad Claim trigger – including:
  - ⇒ formal administrative, regulatory or investigative proceedings
  - ⇒ "informal" regulatory proceedings for privacy breaches
  - ⇒ actual and potential privacy breaches
  - ⇒ information located outside insured's property and custody
  - ⇒ no requirement that there be a demand or action to trigger privacy response expense coverage
  - ⇒ coverage for electronic or hard document breaches
  - ⇒ PCI penalties coverage triggered by written demand or notice received by insured from debit/credit card processor or issuer for payment of penalty
  - ⇒ vicarious liability for breaches by third parties for whom the insured is liable
- Insured Persons - includes employee "insiders" and independent contractors
- Computer Systems - includes systems operated by a third party providing hosting, storage and processing services to the insured
- Punitive damages - covered to extent insurable under most favourable jurisdiction
- Affirmative cover for mental aguish claims resulting from a privacy or security breach
- Fines/Penalties - leading coverage for insurable fines/penalties resulting from a privacy or security breach imposed in a regulatory proceeding or for breach of PCI Industry Rules
- Notification Expenses:
  - ⇒ includes legal costs to determine actions necessary
  - ⇒ includes voluntary notification and notification where recommended as a best practice
- Third Party Corporate Information - protected for theft, loss, unauthorized access & disclosure
- Prior consent often not required - coverage recognizes insured's need to act quickly and/or incur expense without Creechurch's prior consent in certain situations, including:
  - ⇒ notification expenses and data restoration
  - ⇒ settlement where loss does not exceed 50% of retention
- Conduct Exclusions have late trigger - requires final, non-appealable adjudication in underlying proceeding
- Severability - full for exclusions and application for all insured persons
- No mandatory reporting of potential claims
- Past Subsidiary covered for past wrongful acts while it was a Subsidiary (coverage does not expire at end of policy period)

Please contact our Information Technology Underwriting Team for more information.