TRAVELERS

Expense Reimbursement Coverage

CYBERFIRST®

In today's data-driven world where sensitive information is stored and transferred both on paper and 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 because of lost or stolen computers, laptops, flash drives, smart phones or dumpster diving, the breaches can have serious ramifications. There are substantial financial costs involved in finding the cause of and remedying a breach, including the cost of notifying customers — now legally mandated by almost every state. The company can also suffer immense damage to its reputation and from the interruption to business.

CyberFirst offers ten optional first-party insuring agreements designed to help you protect your business.

The following claim scenarios are hypothetical. Refer to the terms and conditions of the applicable policy and the actual facts of the claim to determine coverage.

1 Security Breach Notification and Remediation Expenses Coverage

Coverage for expenses incurred by you directly attributable to an actual or alleged security breach to:

- determine the cause of the security breach and the persons whose identity information was accessed or acquired without their authorization;
- develop materials to notify the persons, and notification to those individuals whose identity information was accessed or acquired;
- provide credit or identity monitoring for two years or longer as required by a breach notification law
- provide identity fraud insurance to affected persons
- provide a call center to handle inquiries.

CLAIM SCENARIO: A skilled cyber criminal hacks into your company's internal processing system. Names, addresses, and credit card information for over 50,000 of your members are captured out of the system. Expenses will likely include hiring a breach response firm to find the cause of the breach, assisting with notice requirements and expenses, providing credit monitoring and a call center for impacted individuals, and obtaining an ID fraud policy for affected victims.

2 Crisis Management Service Expenses Coverage

Coverage for expenses associated with retaining public relations services to mitigate negative publicity directly attributable to a wrongful act under any of your ***CyberFirst*** coverage forms.

CLAIM SCENARIO: Your Chief Customer Service Officer has her laptop stolen. The laptop contains over 100,000 donor records, including their personal contact information. Expenses will likely include hiring a public relations firm to restore donor confidence or mitigate negative publicity generated from the incident.

3 Business Interruption and Additional Expenses Coverage

Coverage for loss of income, and additional expense incurred to restore operations directly attributable to a computer system disruption caused by a virus or other unauthorized computer attack.

CLAIM SCENARIO: Your organization's server is infected by a severe virus; and as a result, your donation website is not available for an extended period. This coverage will reimburse the net proceeds that would have been earned (or net losses that would have been avoided) directly attributable to computer system disruption.

4 Contingent business interruption coverage – IT provider

Coverage for the policyholder's business interruption loss and additional expenses directly attributable to a disruption caused by a virus or other unauthorized computer attack to an IT provider's computer system.

CLAIM SCENARIO: Your external IT provider's network is the victim of a distributed denial of service attack. As a result, you are unable to process customer transactions, resulting in a business interruption.

5 Contingent business interruption coverage – outsource provider

Coverage for the policyholder's business interruption loss and additional expenses directly attributable to a disruption caused by a virus or other unauthorized computer attack to an outsource provider's computer system.

CLAIM SCENARIO: Your outsource provider's network is the victim of a distributed denial of service attack. As a result, they are unable to deliver necessary parts, resulting in a business interruption to your business.

6 Extortion Expenses Coverage

Coverage for money you pay due to threats made regarding intent to sell or disclose information about your customers, initiate an intentional attack on your computer or communications network, destroy data, or other covered threats against you.

CLAIM SCENARIO: You receive a series of notes which threaten to hack into your customer database and disclose all of the contact information to the general public. This coverage can include money or securities paid to the extortionist.

7 Computer Program and Electronic Data Restoration Expenses Coverage

Coverage for expenses incurred to restore, replace or reproduce damaged or destroyed computer programs, software or other electronic data stored within your computer or communications network directly attributable to a computer violation.

CLAIM SCENARIO: A computer virus damages your operating system software and data. This coverage will reimburse costs for repair and restoration of your computer programs and electronic data.

8 Computer Fraud Coverage

Coverage for loss of money, securities or other property directly attributable to unauthorized and fraudulent entry of data or computer instructions.

CLAIM SCENARIO: An organized crime ring gains unauthorized access to your accounts payable in your computer system and alters the bank routing information on outgoing payments. The result: $1 million transferred to the crime ring's account. This coverage reimburses for the direct loss of money, securities or other property.

9 Funds Transfer Fraud

Coverage for loss of money or securities directly attributable to a fraudulent transfer instruction to a financial institution.

CLAIM SCENARIO: You receive an email that appears to be from your bank but is not. Your employee opens the email, which activates a computer virus called a Trojan horse that reads keystrokes. The perpetrator uses this means to obtain banking and password information and initiate a fraudulent electronic wire transfer from your bank account. This coverage reimburses funds that were fraudulently transferred.

10 Telecommunications Theft Coverage

Coverage for charges incurred by you that are directly attributable to the intentional, unauthorized and fraudulent access of your outgoing long distance telephone services.

CLAIM SCENARIO: A criminal gang gains access to your long distance telephone system, placing numerous calls to foreign countries. This coverage reimburses for the loss directly attributable to telecommunications theft.

Travelers *eRiskHub*®

All ***CyberFirst*** policyholders are granted access to Travelers ***eRiskHub***, a private Web-based portal containing information and technical resources that can assist in the prevention/mitigation of network, cyber and privacy events.

eRiskHub is a registered trademark of ***NetDiligence***®