



Expense reimbursement coverage

CYBERFIRST® FOR PUBLIC ENTITIES

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.

CyberFirst offers 12 optional first-party insuring agreements designed to help you protect your budget.

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 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 a call center to handle inquiries

CLAIM SCENARIO: A skilled cyber criminal hacks into your entity's internal processing system. Names, addresses and credit card information of your residents are captured from the system. Expenses will likely include hiring a breach response firm to find the cause of the breach, assisting with notice requirements and expenses, and providing credit monitoring and a call center for impacted individuals, as well as 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 finance officer has his laptop stolen. The laptop contains taxpayer records, including his personal contact information. Expenses will likely include hiring a public relations firm to restore confidence and mitigate negative publicity generated from the incident.

3 Business interruption and additional expenses coverage

Coverage for loss of income, and additional expenses 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 virus, and as a result, your online bill-pay 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 the computer system disruption.

4 Contingent business interruption coverage – IT provider

Coverage for the policyholder's business interruption loss, as well as additional expenses directly attributable to a computer system 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 utility payment transactions, resulting in a business interruption.

5 Contingent business interruption coverage – outsource provider

Coverage for the policyholder's business interruption loss, as well as additional expenses directly attributable to a computer system 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, you are unable to process utility payment transactions, resulting in a business interruption.

CyberFirst is comprised
of three modules.
Build the policy you need to
round out your protection.

Network
and information
security liability

Communications
and media liability

Expense
reimbursement
coverage



6 Extortion expenses coverage

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

CLAIM SCENARIO: You receive a series of notes that threaten to hack into your utility 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, which are attributable to a computer violation.

CLAIM SCENARIO: A computer virus damages your operating system software and data. This coverage will reimburse costs for 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 is that out-going payments are fraudulently directed to the crime ring's account. This coverage reimburses for the direct loss of money, securities or other property up to the limit purchased.

9 Funds transfer fraud coverage

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.

11 Social engineering fraud coverage

An optional endorsement that covers direct loss of money or securities directly caused by an employee being intentionally misled into sending money or diverting payment based on fraudulent information.

CLAIM SCENARIO: A social engineer, posing as a legitimate vendor, emails an employee who routinely wires money with an urgent request for payment. The request includes new wiring instructions to an off-shore bank where payment is sent. The account is then closed and all funds are lost.

12 Reputational harm coverage

Coverage for net profit lost by a policyholder due to damage to their reputation directly attributable to a security breach caused by a network and information security wrongful act and for which impacted persons were notified.

CLAIM SCENARIO: The municipality-owned convention center receives numerous cancellations in the wake of a well-publicized data breach as consumers are reluctant to do business with the events venue.

Travelers' eRisk Hub®

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

eRisk Hub is a registered trademark of **NetDiligence**®.



travelers.com

The Travelers Indemnity Company and its property casualty affiliates. One Tower Square, Hartford, CT 06183

This material does not amend, or otherwise affect, the provisions or coverages of any insurance policy or bond issued by Travelers. It is not a representation that coverage does or does not exist for any particular claim or loss under any such policy or bond. Coverage depends on the facts and circumstances involved in the claim or loss, all applicable policy or bond provisions, and any applicable law. Availability of coverage referenced in this document can depend on underwriting qualifications and state regulations.

© 2019 The Travelers Indemnity Company. All rights reserved. Travelers and the Travelers Umbrella logo are registered trademarks of The Travelers Indemnity Company in the U.S. and other countries. CP-8692 Rev. 6-19