

**THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.**

**CYBERONE COVERAGE**

**COMPUTER ATTACK AND NETWORK SECURITY LIABILITY ENDORSEMENT**

If the "Declaration Page" indicates that this endorsement has been purchased the property and liability sections of the policy to which it is attached are amended with the addition of Section 1 (Computer Attack) and Section 2 (Network Security Liability) as defined and limited by this endorsement.

The limit and deductible applicable to CyberOne Coverage are separate from the limits and deductibles that apply to the policy to which the endorsement attaches:

**SECTION 1 - COMPUTER ATTACK**

**SECTION 1 - COVERED CAUSE OF LOSS**

This Computer Attack coverage applies only if all of the following conditions are met:

1. There has been a "computer attack"; and
2. Such "computer attack" is first discovered by you during the policy period for which this endorsement is applicable; and
3. Such "computer attack" is reported to us as soon as practicable, but in no event more than 60 days after the date it is first discovered by you.

**SECTION 1 - COVERAGES PROVIDED**

If all three of the conditions listed above in SECTION 1 - COVERED CAUSE OF LOSS have been met, then we will provide you the following coverages for loss directly arising from such "computer attack".

**1. Data Restoration**

We will pay your necessary and reasonable "data restoration costs".

**2. Data Re-creation**

We will pay your necessary and reasonable "data re-creation costs".

**3. System Restoration**

We will pay your necessary and reasonable "system restoration costs".

**4. Loss of Business**

We will pay your actual "business income loss" and your necessary and reasonable "extra expenses".

**5. Public Relations**

If you suffer a covered "business income loss", we will pay for the services of a professional public relations firm to assist you in communicating your response to the "computer attack" to the media, the public and your customers, clients or members.

## **SECTION 1 – LIMITS**

The most we will pay under Computer Attack coverage is the Computer Attack Limit shown on the Declaration Page. If no limit is shown or is shown as Excluded on the Declaration Page, then the Computer Attack coverage will be considered to have a limit of \$0.

The most we will pay under Data Re-creation coverage for loss (including "business income loss" and "extra expense" related to data re-creation activities) arising from any one "computer attack" is the Data Re-creation Sublimit shown on the Declaration Page. This sublimit is part of, and not in addition to, the Computer Attack Limit. If no sublimit is shown or is shown as Excluded on the Declaration Page, then the Data Re-creation coverage will be considered to have a sublimit of \$0.

The most we will pay under Loss of Business coverage for loss arising from any one "computer attack" is the Loss of Business Sublimit shown on the Declaration Page. This sublimit is part of, and not in addition to, the Computer Attack Limit. If no sublimit is shown or is shown as Excluded on the Declaration Page, then the Loss of Business coverage will be considered to have a sublimit of \$0.

The most we will pay under Public Relations coverage for loss arising from any one "computer attack" is the Public Relations Sublimit shown on the Declaration Page. This sublimit is part of, and not in addition to, the Computer Attack Limit. If no sublimit is shown or is shown as Excluded on the Declaration Page, then the Public Relations coverage will be considered to have a sublimit of \$0.

The Computer Attack Limit is an annual aggregate limit. This amount is the most we will pay for the total of all loss covered under Section 1 arising out of all "computer attack" events which are first discovered by you during the present annual policy period. This limit applies regardless of the number of "computer attack" events occurring during that period.

A "computer attack" may be first discovered by you in one policy period but it may cause covered costs in one or more subsequent policy periods. If so, all covered costs arising from such "computer attack" will be subject to the Computer Attack Limit applicable to the policy period when the "computer attack" was first discovered by you.

## **SECTION 1 – DEDUCTIBLE**

The Computer Attack coverage is subject to the Computer Attack Deductible shown on the Declaration Page. You shall be responsible for the applicable deductible amount as respects loss arising from each "computer attack" covered under this endorsement.

## **SECTION 2 - NETWORK SECURITY LIABILITY**

### **SECTION 2 - COVERED CAUSE OF LOSS**

This Network Security Liability coverage applies only if all of the following conditions are met:

1. You first receive notice of a "network security liability suit" during the policy period for which this endorsement is applicable or any Extended Reporting Periods; and
2. Such "network security liability suit" is reported to us as soon as practicable, but in no event more than 60 days after the date it is first received by you.

### **SECTION 2 - COVERAGES PROVIDED**

If both of the conditions listed above in SECTION 2 - COVERED CAUSE OF LOSS have been met, then we will provide you the following coverages for loss directly arising from such "network security liability suit".

**1. Defense**

We will pay your necessary and reasonable "network security liability defense costs".

**2. Settlement Costs**

We will pay your necessary and reasonable "network security liability settlement costs".

**SECTION 2 – LIMITS**

Except for post-judgment interest, the most we will pay under Network Security Liability coverage is the Network Security Liability Limit shown on the Declaration Page. If no limit is shown or is shown as Excluded on the Declaration Page, then the Network Security Liability coverage will be considered to have a limit of \$0.

The Network Security Liability Limit is an annual aggregate limit. This amount is the most we will pay for the total of all loss covered under Section 2 (other than post-judgment interest) arising out of all "network security liability suits" of which you first receive notice during the present annual policy period or any Extended Reporting Periods. This limit applies regardless of the number of "network security liability suits" of which you first receive notice during that period.

You may first receive notice of a "network security liability suit" in one policy period but it may cause covered costs in one or more subsequent policy periods. If so, all covered costs arising from such "network security liability suit" (other than post-judgment interest) will be subject to the Network Security Liability Limit applicable to the policy period when notice of the "network security liability suit" was first received by you.

The Network Security Liability Limit for the Extended Reporting Periods (if applicable) shall be part of, and not in addition to, the Network Security Liability Limit for the immediately preceding policy period.

**SECTION 2 – DEDUCTIBLE**

The Network Security Liability coverage is subject to the Network Security Liability Deductible shown on the Declaration Page. You shall be responsible for the applicable deductible amount as respects loss arising from each "network security liability suit" covered under this endorsement.

**EXCLUSIONS, ADDITIONAL CONDITIONS AND DEFINITIONS APPLICABLE TO ALL SECTIONS**

**EXCLUSIONS**

The following additional exclusions apply to this coverage:

We will not pay for costs or loss arising from the following:

1. Loss to the internet, an internet service provider, or any computer or computer system that is not owned or leased by you and operated under your control.
2. Costs to research or correct any deficiency.
3. Any fines or penalties.
4. Any criminal investigations or proceedings.
5. Any threat, extortion or blackmail. This includes, but is not limited to, ransom payments and private security assistance.
6. Your intentional or willful complicity in a covered loss event or your reckless disregard for the security of your

computer system or data.

7. Any criminal, fraudulent or dishonest act, error or omission, or any intentional or knowing violation of the law by you.
8. Any "computer attack" occurring prior to the first inception of this CyberOne coverage endorsement or any coverage substantially similar to that described in this endorsement.
9. That part of any "network security liability suit" seeking any non-monetary relief.
10. Any "network security liability suit" arising from a propagation of malware, denial of service attack, or if applicable, loss, release or disclosure of business data that occurred prior to the first inception of this CyberOne coverage endorsement or any coverage substantially similar to that described in this endorsement.
11. The propagation or forwarding of malware, including viruses, worms, Trojans, spyware and keyloggers in connection with hardware or software created, produced or modified by you for sale, lease or license to third parties.

#### **ADDITIONAL CONDITIONS**

The following additional conditions apply to all coverages under this endorsement.

##### **A. Due Diligence**

You agree to use due diligence to prevent and mitigate costs covered under this endorsement. This includes, but is not limited to, complying with reasonable and industry-accepted protocols for:

1. Providing and maintaining appropriate computer and internet security; and
2. Maintaining and updating at appropriate intervals backups of computer data.

##### **B. Duties in the Event of a "Network Security Liability Suit"**

1. If a "network security liability suit" is brought against you, you must:
  - a. Immediately record the specifics of the "network security liability suit" and the date received; and
  - b. Provide us with written notice, as soon as practicable, but in no event more than 60 days after the date the "network security liability suit" is first received by you.
  - c. Immediately send us copies of any demands, notices, summonses or legal papers received in connection with the "network security liability suit";
  - d. Authorize us to obtain records and other information;
  - e. Cooperate with us in the investigation, settlement or defense of the "network security liability suit";
  - f. Assist us, upon our request, in the enforcement of any right against any person or organization which may be liable to you because of loss to which this insurance may also apply; and
  - g. Not take any action, or fail to take any required action, that prejudices your rights or our rights with respect to such "network security liability suit".

##### **C. Extended Reporting Periods**

1. You shall have the right to the Extended Reporting Periods described in this section, in the event that:

- a. You or we cancel this CyberOne coverage;
  - b. You or we refuse to renew this CyberOne coverage; or
  - c. We renew this CyberOne coverage on an other than a claims-made basis or with a retroactive date later than the date of the first inception of this CyberOne coverage endorsement or any coverage substantially similar to that described in this endorsement;
2. If an event as specified in Paragraph 1. has occurred, you shall have the right to the following:
- a. An Automatic Extended Reporting Period of 30 days after the effective date of cancellation or nonrenewal at no additional premium in which to give to us written notice of a "network security liability suit" of which you first receive notice during said Automatic Extended Reporting Period for any propagation of malware, denial of service attack, or if applicable, loss, release or disclosure of business data occurring before the end of the coverage period for this CyberOne coverage and which is otherwise covered by this CyberOne coverage; and
  - b. Upon payment of an additional premium of 100% of the full annual premium applicable to this CyberOne coverage, a Supplemental Extended Reporting Period of 1 year immediately following the effective date of cancellation or nonrenewal in which to give to us written notice of a "network security liability suit" of which you first receive notice during said Supplemental Extended Reporting Period for any propagation of malware, denial of service attack, or if applicable, loss, release or disclosure of business data occurring before the end of the coverage period for this CyberOne coverage and which is otherwise covered by this CyberOne coverage.

To obtain the Supplemental Extended Reporting Period, you must request it in writing and pay the additional premium due, within 30 days of the effective date of cancellation or nonrenewal. The additional premium for the Supplemental Extended Reporting Period shall be fully earned at the inception of the Supplemental Extended Reporting Period. If we do not receive the written request as required, you may not exercise this right at a later date.

This insurance, provided during the Supplemental Extended Reporting Period, is excess over any other valid and collectible insurance that begins or continues in effect after the Supplemental Extended Reporting Period becomes effective, whether the other insurance applies on a primary, excess, contingent, or any other basis.

#### **D. Network Security Liability Defense**

1. We shall have the right and the duty to assume the defense of any applicable "network security liability suit" against you. You shall give us such information and cooperation as we may reasonably require.
2. You shall not admit liability for or settle any "network security liability suit" or incur any defense costs without our prior written consent.
3. If you refuse to consent to any settlement recommended by us and acceptable to the claimant, we may then withdraw from your defense by tendering control of the defense to you. From that point forward, you shall, at your own expense, negotiate or defend such "network security liability suit" independently of us. Our liability shall not exceed the amount for which the claim or suit could have been settled if such recommendation was consented to, plus defense costs incurred by us, and defense costs incurred by you with our written consent, prior to the date of such refusal.
4. We shall not be obligated to pay any damages or defense costs, or to defend or continue to defend any "network security liability suit", after the Network Security Liability Limit has been exhausted.
5. We shall pay all interest on that amount of any judgment within the Network Security Liability Limit which

accrues:

- a. After entry of judgment; and
- b. Before we pay, offer to pay or deposit in court that part of the judgment within the Network Security Liability Limit or, in any case, before we pay or offer to pay the entire Network Security Liability Limit.

These interest payments shall be in addition to and not part of the Network Security Liability Limit.

#### **E. Other Data Coverage in This Policy**

Some elements of this CyberOne coverage may also be covered under the policy to which this endorsement is attached. If so, this CyberOne coverage will apply as excess, additional coverage. If loss payment has been made under the policy for the same event, the amount of such payment will count towards the deductible that applies to this CyberOne coverage.

#### **F. Services**

The following conditions apply as respects any services provided to you by any service firm provided or paid for in whole or in part under this endorsement:

1. The effectiveness of such services depends on your cooperation and assistance.
2. We do not warrant or guarantee that the services will end or eliminate all problems associated with the covered events.

#### **DEFINITIONS**

With respect to the provisions of this endorsement only, the following definitions are added:

1. "Business Income Loss" means the sum of the:
  - a. Net income (net profit or loss before income taxes) that would have been earned or incurred; and
  - b. Continuing normal and necessary operating expenses incurred, including employee payroll, actually lost by you during the "period of restoration".
2. "Computer Attack" means one of the following involving a computer or other electronic hardware that is owned or leased by you and operated under your control:
  - a. Unauthorized Access - meaning the gaining of access to your computer system by an unauthorized person or persons; or
  - b. Malware Attack - meaning damage to your computer system or data arising from malicious code, including viruses, worms, Trojans, spyware and keyloggers. This does not mean damage from shortcomings or mistakes in legitimate electronic code or damage from code installed on your computer system during the manufacturing process.
  - c. Denial of Service Attack - meaning a deliberate act to prevent third parties from gaining access to your computer system through the internet in a manner in which they are legally entitled.
3. "Data Re-creation Costs"
  - a. "Data re-creation costs" means the costs of an outside professional firm hired by you to research, re-create and replace data that has been lost or corrupted and for which there is no electronic source available or where the electronic source does not have the same or similar functionality to the data that has been

lost or corrupted.

- b. "Data re-creation costs" also means your actual "business income loss" and your necessary and reasonable "extra expenses" arising from the lack of the lost or corrupted data during the time required to research, re-create and replace such data.
- c. "Data re-creation costs" does not mean costs to research, re-create or replace:
  - 1) Software programs or operating systems that are not commercially available; or
  - 2) Data that is obsolete, unnecessary or useless to you.

4. "Data Restoration Costs"

- a. "Data restoration costs" means the costs of an outside professional firm hired by you to replace electronic data that has been lost or corrupted. In order to be considered "data restoration costs," such replacement must be from one or more electronic sources with the same or similar functionality to the data that has been lost or corrupted.
- b. "Data restoration costs" does not mean costs to research, restore or replace:
  - 1) Software programs or operating systems that are not commercially available; or
  - 2) Data that is obsolete, unnecessary or useless to you.

5. "Extra Expense" means the additional cost you incur to operate your business during the "period of restoration" over and above the cost that you normally would have incurred to operate your business during the same period had no "computer attack" occurred.

6. "Network Security Liability Defense Costs"

- a. "Network security liability defense costs" means reasonable and necessary expenses resulting solely from the investigation, defense and appeal of any "network security liability suit" against you. Such expenses may be incurred by us. Such expenses may include premiums for any appeal bond, attachment bond or similar bond. However, we have no obligation to apply for or furnish such bond.
- b. "Network security liability defense costs" does not mean your salaries or your loss of earnings.

7. "Network Security Liability Settlement Costs"

- a. "Network security liability settlement costs" means the following, when they arise from a "network security liability suit":
  - 1) Damages, judgments or settlements; and
  - 2) Defense costs added to that part of any judgment paid by us, when such defense costs are awarded by law or court order; and
  - 3) Pre-judgment interest on that part of any judgment paid by us.
- b. "Network security liability settlement costs" does not mean:
  - 1) Civil or criminal fines or penalties imposed by law;
  - 2) Punitive or exemplary damages;

- 3) The multiplied portion of multiplied damages;
- 4) Taxes; or
- 5) Matters which may be deemed uninsurable under the applicable law.

8. "Network Security Liability Suit"

- a. "Network security liability suit" means a civil proceeding against you in which damages are alleged. Such proceeding must be brought in the United States of America, Puerto Rico or Canada. Such proceeding must be based on an allegation that a negligent security failure or weakness with respect to a computer or other electronic hardware that is owned or leased by you and operated under your control allowed one or more of the following to happen:
  - 1) The unintended propagation or forwarding of malware, including viruses, worms, Trojans, spyware and keyloggers. Malware does not include shortcomings or mistakes in legitimate electronic code.
  - 2) The unintended abetting of a denial of service attack against one or more other systems.
- b. If the 3<sup>rd</sup> Party Business Information line under Network Security Liability Optional Coverage on the Declaration Page is marked as Included, then "network security liability suit" also means a civil proceeding against you in which damages are alleged which is brought in the United States of America, Puerto Rico or Canada and which is based on an allegation that a negligent security failure or weakness with respect to a computer or other electronic hardware that is owned or leased by you and operated under your control allowed the loss, release or disclosure of business data that is owned by or proprietary to a third party. This does not include personally identifying information or other information that is sensitive or personal to individuals. If the 3<sup>rd</sup> Party Business Information line under Network Security Liability Optional Coverage on the Declaration Page is marked as Excluded or is blank, then "network security liability suit" does not include such suits.
- c. "Network security liability suit" includes the following:
  - 1) An arbitration or alternative dispute resolution proceeding that you are required to submit to or which we agree you should submit to; or
  - 2) A written demand for money, when such demand could reasonably result in a civil proceeding as described in this definition.
- d. "Network security liability suit" does not mean any demand or action alleging or arising from property damage or bodily injury.
- e. "Network security liability suit" does not mean any demand or action brought by or on behalf of someone who is:
  - 1) Your director or officer;
  - 2) Your owner or part-owner; or
  - 3) A holder of your securities;in their capacity as such, whether directly, derivatively, or by class action.

9. "Period of Restoration" means the period of time that begins at the time that the "computer attack" is discovered by you and continues until the earlier of:

- a. The date that all data restoration, data re-creation and system restoration directly related to the



"computer attack" has been completed; or

- b. The date on which such data restoration, data re-creation and system restoration could have been completed with the exercise of due diligence and dispatch.

10. "System Restoration Costs"

- a. "System restoration costs" means the costs of an outside professional firm hired by you to do any of the following in order to restore your computer system to its pre- "computer attack" level of functionality:

- 1) Replace or reinstall computer software programs;
- 2) Remove any malicious code; and
- 3) Configure or correct the configuration of your computer system.

- b. "System restoration costs" does not mean:

- 1) Costs to increase the speed, capacity or utility of your computer system;
- 2) Labor of your employees;
- 3) Any costs in excess of the actual cash value of your computer system; or
- 4) Costs to repair or replace hardware.

**All other provisions of this policy apply.**

