

Cyber Suite Coverage Explanatory Memorandum

We have developed a new product solution, Cyber Suite Coverage, that responds to the threat of unauthorized intrusion into or interference with an insured's computer systems. This product includes coverages that address damage to data and systems from a computer attack and the liability that may arise from insufficient systems security. This suite of coverages and services also enables an insured entity to respond effectively when there has been a breach of personal information.

The Cyber Suite Coverage is comprised of the following coverage components:

First Party Coverages

- Data Compromise Response Expenses
- Computer Attack
- Cyber Extortion
- Identity Recovery

Third Party Coverages:

- Data Compromise Liability
- Network Security Liability
- Electronic Media Liability

The rates for this program have been developed in the absence of data specific to this coverage. No credible data exists today for the exposure covered by this new coverage. The Hartford Steam Boiler Inspection and Insurance Company (HSB) developed these charges primarily from publicly available data about events that would be covered by this program; various studies conducted by the U.S. Government Accountability Office, Ponemon Group, and Gartner; and expert elicitation.

Data Compromise Response Expenses Coverage (DC RE)

Data Compromise Response Expenses Coverage is a first party coverage and includes Named Malware coverage and the following additional coverage components:

- Forensic IT Review (Information Technology) - Coverage for the cost to hire outside computer experts to determine the nature and extent of the breach.
- Legal Review - Coverage for the cost to obtain professional legal advice
- Notification to Affected Individuals - Coverage for reimbursement of expenses associated with the notification of those whose personal information was compromised.
- Services to Affected Individuals - Coverage for the cost of providing services (Packet of informational materials, Toll-free help line, One year of credit monitoring and Identity restoration case management) to affected individuals for 12 months from the date of the notice.
- Public Relations - Coverage for the cost to implement public relations recommendations of a professional public relations firm. This may include advertising and special promotions designed to retain the relationship with affected individuals.
- Regulatory Fines and Penalties - Coverage for any fine or penalty imposed, to the extent such fine or penalty is legally insurable under the law of the applicable jurisdiction.
- PCI Fines and Penalties - Coverage for any Payment Card Industry (PCI) fine or penalty imposed under a contract to which you a party. PCI Fines and Penalties do not include any increased transaction costs.

Rate Development - DC RE

Frequency was developed from a recent U.S. Census Data and various public accounts. Severities were calculated using data drawn from the U.S. Government Accountability Office, Ponemon Group, and Gartner. This was supplemented by research conducted with agents, small commercial entities, and the National Center for Educational Statistics (which cites data from the U.S. Department of Education).

Cyber Suite Coverage Explanatory Memorandum

The following factors were used to develop the Data Compromise Response Expenses loss costs:

\$50,000 Limit

Tier	1	2	3	4	5
Frequency	0.1245%	0.1853%	0.2385%	0.4133%	0.6368%
Severity	\$14,300	\$17,000	\$17,600	\$19,100	\$19,880
Loss Cost	\$17.80	\$31.50	\$41.98	\$78.94	\$126.60

\$100,000 Limit

Tier	1	2	3	4	5
Frequency	0.1245%	0.1853%	0.2385%	0.4133%	0.6368%
Severity	\$23,000	\$25,984	\$27,080	\$29,120	\$34,880
Loss Cost	\$28.64	\$48.15	\$64.59	\$120.35	\$222.12

\$250,000 Limit

Tier	1	2	3	4	5
Frequency	0.1245%	0.1853%	0.2385%	0.4133%	0.6368%
Severity	\$35,000	\$50,900	\$54,920	\$55,880	\$74,720
Loss Cost	\$43.58	\$94.32	\$130.98	\$230.95	\$475.82

\$500,000 Limit

Tier	1-3
Frequency	0.2385%
Severity	\$79,710
Loss Cost	\$190.11

\$1,000,000 Limit

Tier	1-3
Frequency	0.2385%
Severity	\$114,980
Loss Cost	\$274.23

Computer Attack (CA) and Cyber Extortion (CE) Coverage

Computer Attack and Cyber Extortion is a first party coverage that is triggered by the insured's discovery that a computer attack has effected a computer system owned or leased by the insured and under the insured's control.

A computer attack may be:

- A hacking event or other instance of unauthorized person gaining access to the computer system.
- An attack against the system by a virus or other malware.
- A denial of service attack against the insured's system.

Discovery of the attack must occur during the policy period. Coverage does not apply to breaches that occur prior to the first inception of the coverage.

Computer Attack Coverage provides coverage for:

- Data Restoration Costs - Coverage for the cost of a professional firm hired by the insured to replace lost or corrupted data from electronic sources.
- Data Re-creation Costs - Coverage for the cost of a professional firm hired by the insured to research, recreate and replace lost or corrupted data from non-electronic sources.
- System Restoration Costs - Coverage for the cost of a professional firm hired by the insured to restore its computer system to its pre-attack level of functionality by replacing or reinstalling software, removing malicious code and correcting the configuration of the insured's computer system.

Cyber Suite Coverage Explanatory Memorandum

- **Loss of Business** - Coverage for business income lost by the insured and extra expenses incurred by the insured during the period of time when system data and recovery activities are taking place.
- **Public Relations** - Coverage for assistance from a professional public relations firm in communicating with outside parties concerning the Computer Attack and the insured's response.

Cyber Extortion (CE) Coverage - Coverage is provided for the cost of a professional firm hired by the insured to investigate and negotiate after the receipt of a cyber extortion threat - a credible threat or series of threats to launch a potential denial of service attack against an insured.

Rate Development - CA & CE

Frequency was derived from data gathered from the 2011 Computer Security Institute Computer Crime and Security Survey and from the HSB/Ponemon survey. Severities were calculated for three of the sub-coverages (data restoration, data re-creation and systems restoration) using data drawn from the HSB/Ponemon survey and from the 2003 Graziado Business Review which were then combined with dollar amounts that represented the costs of repairing various kinds of covered damages. These costs were obtained from a variety of IT repair resources, including surveys and published rates.

The following factors were used to develop the Computer Attack loss costs:

Annual Aggregate Limit	Frequency	Severity	Loss Costs
\$50,000	0.300%	\$14,900	\$44.70
\$100,000	0.300%	\$16,500	\$49.50
\$250,000	0.300%	\$60,600	\$181.80
\$500,000	0.300%	\$121,200	\$363.60
\$1,000,000	0.300%	\$206,000	\$618.00

The following factors were used to develop the Cyber Extortion loss costs:

Annual Aggregate Limit	Frequency	Severity	Loss Costs
\$10,000	0.300%	\$7,400	\$22.20
\$25,000	0.300%	\$11,200	\$36.60

Data Compromise Liability Coverage (DCL)

Data Compromise Liability Coverage is a third party coverage that supplements the program by providing coverage for defense and settlement costs in the event that "affected individuals" sue the insured.

Rate Development - DCL

Frequency was developed from a recent U.S. Census Data and various public accounts. Severities were calculated using data drawn from the U.S. Government Accountability Office, Ponemon Group, and Gartner. This was supplemented by research conducted with agents, small commercial entities, and the National Center for Educational Statistics (which cites data from the U.S. Department of Education).

A nationwide search of data breach related court cases returned no statistically relevant data. There are also breaches that result in settlements prior to resulting in a court action. There is no repository that identifies these often private settlements. Therefore the loss costs were derived using our best estimate to select frequency and severity.

Severity is mainly a function of the volume of data breached. The larger the number of records breached, the larger the number of affected individuals that may bring an action against the insured. Such actions against an insured can result in three potential outcomes: settlement, motion to dismiss, or a verdict.

Cyber Suite Coverage Explanatory Memorandum

We recognized that legal fees can vary greatly by geography, and we estimated an appropriate cost to achieve a motion to dismiss. This may represent the minimum costs involved to address a dispute. It is anticipated that the majority of actions will result in an out of court settlement.

The following factors were used to develop the Data Compromise Defense and Liability loss costs:

\$50,000 Limit

Tier	1	2	3	4	5
Frequency	0.0374%	0.0556%	0.0716%	0.1240%	0.1910%
Severity	\$23,000	\$27,000	\$28,000	\$30,000	\$32,000
Loss Cost	\$8.59	\$15.01	\$20.03	\$37.20	\$61.13

\$100,000 Limit

Tier	1	2	3	4	5
Frequency	0.0374%	0.0556%	0.0716%	0.1240%	0.1910%
Severity	\$35,000	\$40,000	\$44,000	\$48,000	\$55,000
Loss Cost	\$13.07	\$22.24	\$31.48	\$59.52	\$105.07

\$250,000 Limit

Tier	1	2	3	4	5
Frequency	0.0374%	0.0556%	0.0716%	0.1240%	0.1910%
Severity	\$56,000	\$77,000	\$85,000	\$87,000	\$112,000
Loss Cost	\$20.92	\$42.80	\$60.82	\$107.87	\$213.96

\$500,000 Limit

Tier	1-3
Frequency	0.0716%
Severity	\$168,000
Loss Cost	\$120.20

\$1,000,000 Limit

Tier	1-3
Frequency	0.0716%
Severity	\$230,000
Loss Cost	\$164.57

Network Security Liability Coverage (NSL)

This third party coverage is triggered by the insured's receipt of notice of a network security liability suit. The network security liability suit can be a civil action, an alternate dispute resolution or a written demand for money.

Network Security Liability Coverage provides coverage for:

- The breach of third party business information
- The unintended propagation or forwarding of malware
- The unintended abetting of a denial of service attack

There need not be a covered loss under the first party Computer Attack and Cyber Extortion Coverage in order for there to be a loss under the third party Network Security Liability Coverage.

Receipt of notice of the suit must occur during the policy period, and the suit must arise from an event that occurs after the first inception of the coverage.

Rate Development - NSL

Frequency for each of the kinds of disputes that are covered was based on how often these disputes arose in the public realm and were adjudicated. HSB began with an initial frequency for each of the coverages. For example, a dispute about the transmission of malware always begins with the insured itself suffering a malware attack; a dispute about the insured's participation in denial of service attack also always begins with the insured itself suffering a malware attack; and a dispute about a breach of third party business information always begins with such a breach. A frequency for each of these initial events was obtained from the Ponemon and Computer Security Institute surveys and from a 2012 survey conducted by the National Cyber Security Alliance and Symantec.

Cyber Suite Coverage Explanatory Memorandum

HSB interviewed several lawyers that focus their practices in the cyber area and asked them to quantify, for each kind of dispute, how much it costs to take the dispute to trial, etc. This expert elicitation process produced the severity estimates.

The following factors were used to develop the Network Security Liability loss costs:

Annual Aggregate Limit	Frequency	Severity	Loss Costs
\$50,000	0.171%	\$13,600	\$23.26
\$100,000	0.171%	\$16,500	\$28.22
\$250,000	0.171%	\$49,500	\$84.65
\$500,000	0.171%	\$84,200	\$143.98
\$1,000,000	0.171%	\$117,800	\$201.44

Electronic Media Liability (EML)

Electronic Media Liability is a third party coverage that provides coverage for defense and settlement costs in the event that a third party claimant sues the insured alleging that the insured's electronic communications resulted in defamation, violation of a person's right of privacy, interference with a person's right of publicity or infringement of copyright or trademark.

The following factors were used to develop the Electronic Media loss costs:

Annual Aggregate Limit	Frequency	Severity	Loss Costs
\$50,000	0.171%	\$13,100	\$22.40
\$100,000	0.171%	\$14,600	\$24.97
\$250,000	0.171%	\$21,800	\$37.28
\$500,000	0.171%	\$23,100	\$39.50
\$1,000,000	0.171%	\$34,000	\$58.14

Identity Recovery Coverage (IDR)

Identity Recovery coverage (IDR) is a combination of support service and expense reimbursement. IDR support services include case management that reduces the time burden on the insured identity theft victim and a branded, toll-free help line. This coverage also reimburses various out-of-pocket expenses due to a covered identity theft. These expenses include: legal fees for answer of civil judgments and defense of criminal charges, notary and filing fees, credit bureau reports, lost wages, child/elder care, etc.

Since this is our initial offering of this product, the proposed rates and rules reflect our research and are our best evaluation of the identity theft exposure. According to a recent study commissioned by the U.S Department of Justice Victims of Identity Theft-2014, 82.5% of total financial loss due to identity theft losses are \$1,000 or less. While we do not have significant experience with this coverage, we believe that the availability of case management restoration services will reduce this severity to approximately \$18. The same DOJ report suggest a frequency of 7.0%. Thus, our loss content is expected to be approximately \$1.23.

Loss related expenses (toll-free help-line and case management services) are expected to be \$3.50. Thus our total loss cost is \$4.73.

Coverage is provided up to an annual aggregate per insured of \$25,000, and no deductible applies.

Gross Premiums

We applied our expense and profit load of 35% to arrive at our gross premiums.