

Cyber Suite Coverage Rate and Rule Manual

1. Description of Coverage

The Cyber Suite coverage is comprised of the following First Party coverages: Data Compromise Response Expenses, Computer Attack, Cyber Extortion, Misdirected Payment Fraud, Computer Fraud, Telecommunications Fraud, and Identity Recovery, and the following Third-Party coverages: Privacy Incident Liability, Network Security Liability, and Electronic Media Liability.

2. Form

Use **Cyber Suite Coverage Form** Number 148503.

3. Eligibility

All insured entities are eligible. The following classes of business are ineligible for this program: Financial Institutions, Adult Business, Gambling or Gaming, Credit Card or Financial Transaction Processing, Hospitals, Credit Reporting Agencies, Collection Agents, Information/Data Brokers, Cannabis Facilities, Telecommunications Firms, Data Processors, and IT Outsourcing Companies.

4. Coverage Limits and Sublimits

Refer to the Rate Table and Sublimit Table for available limits and sublimits. Third Party coverages will be defense within the limits.

A single Cyber Suite annual aggregate limit applies to Data Compromise Response Expenses, Computer Attack, Privacy Incident Liability, Network Security Liability, and Electronic Media Liability. Identity Recovery is subject to a separate and independent \$25,000 limit per identity recovery insured.

The following coverages are sublimited under the Cyber Suite annual aggregate limit: Cyber Extortion, Misdirected Payment Fraud, Computer Fraud, Telecommunications Fraud, Future Loss Avoidance, Reputational Harm, Public Relations, and Reward Payments.

5. Deductible

Refer to the Rate Table for available deductibles. No deductible applies to Identity Recovery.

6. Premium Determination

Refer to the Rate Table. The premiums shown are annual gross premiums per policy. Premiums will be prorated for short or odd-term policies. These premiums are not subject to further modification by the application of any other factors not shown in these tables (e.g. package factors, company deviations, or IRPM factors).

Premiums will be assigned based on the limit and deductible selected, and by the following rating tier classes:

Tier 1 Classes

Industries that are unlikely to experience a cyber incident and, should they experience a cyber incident, it would have a minimal impact on their business operations due to low dependency on software, technology, or data, a lack of sensitive data being collected/stored, or a lack of high value transactions. These industries would generally be able to continue to conduct business as usual in the event of a cyber incident.

Tier 2 Classes

Industries that have a low likelihood of experiencing a cyber incident. These industries have minimal system dependency on software, technology, or data, collect/store minimal sensitive data, or have minimal high value transactions. Due to the level of system dependency, information collected/stored, or high value transactions, a cyber incident would have a low impact on their business operations.

Tier 3 Classes

Industries that have a moderate likelihood of experiencing a cyber incident. These industries have some system dependency on software, technology, or data, collect/store sensitive data, or process high value transactions. Due to the level of system dependency, information collected/stored, or high value transactions, a cyber incident would have a moderate impact on their business operations.

Tier 4 Classes

Industries that have a high likelihood of experiencing a cyber incident. These industries have substantial system dependency on software, technology, or data, collect/store highly sensitive data, or process significant high value transactions. Due to the substantial level of system dependency, information collected/stored, or high value transactions, a cyber incident would have a high impact on their business operations.

Tier 5 Classes

Industries that have a very high likelihood of experiencing a cyber incident. These industries have critical system dependency on software, technology, or data, collect/store highly sensitive data, or process significant high value transactions. Due to the level of system dependency, information collected/stored, or high value transactions, a cyber incident would have a significant impact on their business operations.

Rate Table

Annual Aggregate Limits	Deductible	Tier 1	Tier 2	Tier 3	Tier 4	Tier 5
\$50,000	\$1,000	\$384	\$430	\$480	\$708	\$1,769
\$100,000	\$1,000	\$595	\$666	\$744	\$1,097	\$2,742
\$250,000	\$2,500	\$1,126	\$1,259	\$1,407	\$2,073	\$5,183
\$500,000	\$10,000	\$1,925	\$2,152	\$2,406	\$3,545	\$8,863
\$1,000,000	\$10,000	\$2,931	\$3,278	\$3,664	\$5,399	\$13,498

Sublimit Table

Annual Aggregate Limits	Reputational Harm Cyber Extortion Misdirected Payment Fraud Computer Fraud Telecommunications Fraud	Public Relations		Reward Payments	Future Loss Avoidance
		DC RE	CA		
\$50,000	\$10,000	\$10,000	\$10,000	\$25,000	10% of eligible payment with respect to any one Computer Attack
\$100,000	\$10,000	\$10,000	\$10,000	\$25,000	
\$250,000	\$25,000	\$10,000	\$10,000	\$25,000	
\$500,000	\$25,000	\$10,000	\$10,000	\$25,000	
\$1,000,000	\$25,000	\$10,000	\$10,000	\$25,000	

Identity Recovery Sublimit Table

Annual Aggregate Limit	Lost Wages and Child or Elder Care	Mental Health Counseling	Miscellaneous Expense
\$25,000	\$5,000	\$1,000	\$1,000

7. Minimum Premiums

This coverage is not subject to a minimum premium.

8. Midterm Additions/Increases

This coverage may be added at the anniversary of the policy or may be added in-term at the insured's request. The rate will be prorated for in-term transactions or odd-term policies. Increased limits are available upon coverage inception or subsequent anniversary.

9. Supplemental Extended Reporting Period

A Supplemental Extended Reporting Period of one year immediately following the date of termination of coverage may be purchased for an additional 100% of the full annual third party premium applicable to this coverage.