Send new submissions to
submissions@koop.ai

KOOP

Cyber Liability

NEW

Protect commercial enterprises from system hacks that could lead to first-party or third-party damages

- Admitted product
- Limits of $1M, $2M, and $3M
- Bespoke coverage form
- Claims-Made with Full Prior Acts
- No Minimum Earned Premium (MEP)
- ERM-enabled coverage

Cyber Liability

Primer

Cyber Liability coverage supports enterprises in the event of a data breach or cyber attack. For technology companies that handle sensitive data and rely heavily on digital infrastructure, this coverage is vital.

What it covers:

- ✓ Data Breach Response
- ✓ Data Recovery
- ✓ Cyber Extortion
- ✓ Business Interruption
- ✓ Network Security Liability

Policy Limits

Limits can range widely, from $1 million to $10 million or more, depending on the company's risk exposure.

Deductibles

Deductibles vary based on the size of the company and the risk profile but can start anywhere from $5,000 to $25,000.

Why do you need Cyber Liability coverage:

Contractual Obligations

Clients and partners may require evidence of cyber liability coverage before engaging in business arrangements.

Regulatory Compliance

Companies are often required to adhere to strict data protection regulations, and non-compliance can lead to hefty fines.

Client Trust

Assures clients that the company is proactive about cybersecurity and prepared to handle incidents responsibly.

Increasing Cyber Threats

With the prevalence of cyber attacks, a technology company is at a higher risk for potential breaches and system disruptions.

Available in 50 U.S. states

A.M. Best **Rating A-**

Send new submissions to
submissions@koop.ai

KOOP

Cyber Liability

NEW

Base Policy

Security and Privacy Liability	Third-party liability for defense and damages if the insured is found responsible after a cyber event.
Breach Response Expenses	The cost of notifying individuals affected by a breach of the insured's data and monitoring those individuals' credit, as well as the cost of forensics to discover what exactly happened.
Regulatory Defense and Penalties	The insureds' costs defending themselves if the breach results in a regulatory proceeding, and also the cost of potential resulting fines or penalties.
Cyber Extortion and Ransom Payments	The forensics, interest, and negotiation expenses the insured incurs because of an extortion event. This includes the cost of paying ransom to hackers in order to regain control of systems or data after a ransomware attack.
PCI Fines and Penalties	Fines or penalties if the insured is found to be in breach of the security and risk management requirements of the PCI merchant agreement.
Business Interruption and Restoration	The cost of getting the insured's e-commerce activities up and running again after a cyber incident, so they can resume generating revenue. If the insured's e-commerce activities remain interrupted during a specified period of restoration, this coverage also pays for revenue lost during that time.

Optional Coverages

Computer Funds Transfer	Reimbursement if the insureds' money is stolen in a fraudulent transaction (for example, if the insured's email is hacked, and the scammer uses it to initiate a fraudulent bank transfer).
Hardware Replacement	The cost of replacing the insured's computer systems, if they are permanently damaged ("bricked") in a cyber attack.
Post-Breach Remediation	The cost of making improvements and eliminating vulnerabilities in the insured's computer systems after a data breach, to prevent similar incidents from happening again. This is not included in a standard policy.
Social Engineering	Reimbursement for money lost if a scammer reaches out to the insured and tricks them into sending money.
Telecommunications Fraud	Any costs from fraudulent use of the insured's telecommunications equipment, such as bogus charges to the company phone bill.
Service Fraud, incl. Cryptojacking	Any costs from fraudulent use of cloud-based services and unauthorized access or use of a computer to mine for virtual currency leading to increased electricity, natural gas, oil, or internet costs.
Enhanced Business Interruption and Restoration	Includes system failures in addition to cyber incidents.
Extended Reporting Period	Tail coverage for cyber incidents, which often have a delayed discovery period. Insureds can choose to have coverage available for past incidents even after the policy has expired, for up to 3 years.