

Cyber Risk

In our increasingly online and digital world, every company has a potential “cyber risk.” It is a term used frequently and a topic of the daily news cycle. Cyber risk represents two major perils: network security failure and privacy incident, which simply means an organization’s failure to protect its computer systems or private information or both. A network security failure or a privacy incident can be totally intertwined or mutually exclusive. If either of these incidents occur there can be various losses your organization can suffer.

Starr’s Cyber Risk Response policy addresses many of the common repercussions organizations face as a result of cyber risk perils. We provide protection for losses with a comprehensive policy form that is designed to pay for various expenses sustained by your organization from an actual or suspected network security failure or privacy incident.

In addition, the policy will also provide defense costs and pay for damages that arise from legal liability stemming from these types of incidents.

Target Risks

- Commercial enterprises including public, private and nonprofit entities

Coverages Available

- **Incident Response Expenses** – Pay the expenses sustained by your organization to:
 - contain a network security failure or privacy incident
 - retain legal counsel, forensic investigators, and public relations professionals to help determine your responsibilities
 - notify affected people and provide identity theft assistance
- **Security & Privacy Liability** – Pay to defend you in the event of:
 - class actions by customers whose personal information has been compromised
 - regulators bringing investigations for violating a law relating to these types of incidents
- **Business Interruption** – Reimburse the loss of income for interruption or suspension of business
- **Data Recovery** – Reimburse the costs to restore, recreate or re-collect lost electronic data
- **Cyber Extortion** – Reimburse payouts made in exchange for eliminating a threat or demand made against your organization’s computer system or private information

Additional Coverages Available

- **Media Content Liability** – Pay to defend in the case of liability arising from alleged trademark infringement, copyright infringement, defamation, false light, product disparagement and other types of content related issues
- **PCI-DSS Assessment Coverage** – Pay for loss arising from claims for non-compliance with PCI Data Security Standards
- **Contingent Business Partner** – Reimburse for loss of income after a material business interruption caused by a security failure of any entity that you depend on to conduct business other than a Third-Party Computer System Provider
- **System Failure Coverage** – Expands the cause of a material interruption to include through other unintentional failures
- **Cyber Crime** – Reimbursement for the loss of the organization’s funds sustained from a network security failure or fraudulent impersonation
- **Contingent Bodily Injury/Property Damage** – Provides contingent coverage in the event that a network security failure or privacy incident result in physical injury or property damage

Limits

- Up to \$25,000,000 - primary or excess limits
- Shared or separate limits available

Cyber Overview (continued)

Deductibles

- Minimum \$5,000

Highlights

- Adaptable coverage for a client's growing business, including manuscript endorsements
- Responds on a discovery basis
- No Retroactive Date
- Coverage for third-party computer services providers and information handlers
- Knowledge limited to executive officers
- Rogue employee carve-back
- Cyber Terrorism Coverage
- Contingent Business Income Loss
- Cyber Extortion includes threats and demands; also contemplates intangible property of value
- Coverage for regulations requiring protocols to protect computer systems
- Other Insurance Clause options – primary or excess to other insurance policies
- GDPR (General Data Protection Regulation)
- Wrongful Collection
- Non-Physical Damage Loss of Use (Bricking)
- Voluntary Shutdown
- Reputational Loss Coverage

Risk Management Services

Starr eRisk Hub® Highlights

- Free Breach Coach®, legal consultation with a pre-qualified attorney following an incident
- Incident Roadmap to assist in planning a network or data breach incident response
- Access to pre-qualified industry experts in pre-breach and post-breach disciplines
- Risk management tools, including policies and procedures, training, cyber-risk assessments, loss calculator, breach notification guides and research tools
- Access to news on major breach events, best practices articles, white papers, webinar training events, risk management events, and security and privacy blogs

Reach out to Starr for more information on how a Starr solution can work for you:

Contact our Cyber Risk team at cyber@starrcompanies.com or visit us at www.starrcompanies.com/insurance/cyberoverview

Coverages described herein are underwritten by Starr Indemnity & Liability Company or Starr Surplus Lines Insurance Company.

The coverages described in this document are only a brief description of available insurance coverage. It is intended for general information purposes and does not provide any guidance regarding coverage that may or may not be available under this policy as respects any claim. Any Policy issued by Starr Companies will contain limitations, exclusions and termination provisions. Not all coverages are available in all jurisdictions. For costs and complete details of specific policy coverage, please contact the insurance professional above.