TRAVELERS | Truckers INSURANCE ASSOCIATES

CyberRisk

HOW OUR COVERAGE RESPONDS FOR PRIVATE, NONPROFIT AND PUBLIC COMPANIES

LIABILITY INSURING AGREEMENTS

Insuring Agreement	Definition	Claim Scenario	Coverage Response
Privacy and Security	Coverage for claims arising from unauthorized access to data, failure to provide notification of a data breach where required by law, failure to destroy confidential information, failure to comply with a privacy policy, wrongful collection of private or confidential information, failure to prevent a security breach that results in the inability of authorized users to gain system access, the participation in a DDoS attack or the transmission of a computer virus.	A hacker obtains sensitive personal information from the insured's computer system. As a result, a number of customers bring a claim against the insured for allowing access to their personal information.	Damages and defense costs for covered lawsuits.
Media	Coverage for claims arising from copyright infringement, plagiarism, defamation, libel, slander and violation of an individual's right to privacy or publicity in electronic and printed content.	A third party brings a lawsuit against the insured alleging that the insured plagiarized the third party's online content and organizational branding and infringed upon its trademarks.	Damages and defense costs for covered lawsuits.
Regulatory	Coverage for administrative and regulatory proceedings, civil and investigative demands brought by domestic or foreign governmental entities or claims made as a result of privacy and security acts or media acts.	A hacker obtains sensitive personal information from the insured's computer system. As a result, attorneys general in multiple states bring regulatory action against the insured.	Costs for responding to regulatory claims stemming from the data breach, including any resulting fines or penalties.

BREACH RESPONSE INSURING AGREEMENTS

Insuring Agreement	Definition	Claim Scenario	Coverage Response
Privacy Breach Notification	Coverage for costs to notify and provide services to individuals or entities who have been affected by a data breach. Examples include call center services, notification, credit monitoring and the cost to purchase identity fraud insurance.	A fraudster hacks into the insured's internal processing system. Names, addresses and Social Security numbers for more than 50,000 of the insured's customers are captured from the system, requiring notification to all the customers.	Costs to deliver notice to impacted customers, and to provide credit monitoring, a call center and an ID fraud policy for impacted individuals.
Computer and Legal Experts	Coverage for costs associated with analyzing, containing or stopping privacy or security breaches; determining whose confidential information was lost, stolen, accessed or disclosed; and providing legal services to respond to such breaches.	An insured suspects that a fraudster hacked into their internal processing system when law enforcement notifies them of identity theft impacting a number of the insured's customers.	Costs to engage a forensics provider to contain the breach and determine its scope, and legal costs to determine the insured's notification obligations under relevant privacy laws and provide other services to assist the insured in responding to and managing the breach.
Betterment	Coverage for costs to improve a computer system after a security breach, when the improvements are recommended to eliminate vulnerabilities that could lead to a similar breach.	The insured's computer system is compromised by ransomware. Forensic providers contain the virus and determine that the source of the infiltration is a vulnerability in the insured's computer system. Upon recommendation from the forensic provider, the insured purchases new software to improve their system security.	Costs to purchase new software to address the system vulnerability.
Cyber Extortion	Coverage for ransom and related costs associated with responding to threats made to attack a system or to access or disclose confidential information.	The insured's system is infected with a virus that encrypts the insured's data. A ransom payment is demanded to unlock the system.	Costs to manage and mitigate the incident and, if necessary, payment of the ransom demand.
Data Restoration	Coverage for costs to restore or recover electronic data, computer programs or software lost from system damage due to computer virus, denial-of-service attack or unauthorized access.	A computer virus corrupts the insured's software and data.	Costs for recovery and restoration of the insured's electronic data and computer programs.
Public Relations	Coverage for public relations services to mitigate negative publicity resulting from an actual or suspected privacy breach, security breach or media act.	The insured's chief financial officer has a laptop stolen. The laptop contains more than 100,000 customer records, including Social Security numbers.	Costs for hiring a public relations firm to mitigate negative publicity generated from the incident.

CYBERCRIME INSURING AGREEMENTS

Insuring Agreement	Definition	Claim Scenario	Coverage Response
Computer Fraud	Coverage for loss of money, securities or other property due to unauthorized system access.	An organized crime ring gains unauthorized access to the insured's accounts payable in their computer system and alters the bank routing information on outgoing payments, resulting in a $1 million transfer to the crime ring's account.	Reimbursement of the insured's funds.
Funds Transfer Fraud	Coverage for loss of money or securities due to fraudulent transfer instructions to a financial institution.	A fraudster obtains the insured's information and uses the information to impersonate the insured to their financial institution. The fraudster requests a $1 million wire transfer from the insured's bank account.	Reimbursement of the insured's funds.
Social Engineering Fraud	Coverage for loss of money or securities due to a person impersonating another and fraudulently providing instructions to transfer funds.	An employee in the insured's accounts payable department receives an email purportedly from an established vendor changing the vendor's banking instructions. The employee relies upon the fraudulent email instruction and wires $100,000 from the insured's bank account to the fraudster. The insured discovers the fraud when the real vendor contacts the insured requesting payment.	Reimbursement of the insured's funds.
Telecom Fraud	Coverage for amounts charged by a telephone service provider resulting from an unauthorized person accessing or using an insured's telephone system.	An unknown third party gains unauthorized access to the insured's telephone system and uses the system to incur $50,000 in international charges. The insured discovers the loss when they receive their monthly statement from their telephone provider containing the fraudulent charges.	Reimbursement of the fraudulent charges the insured is required to pay to their telephone provider.

BUSINESS LOSS INSURING AGREEMENTS

Insuring Agreement	Definition	Claim Scenario	Coverage Response
Business Interruption	Coverage for loss of income and expenses to restore operations as a result of a computer system disruption caused by a virus or computer attack, including the voluntary shutdown of systems to minimize the business impact of the event.	An insured's computer system is infected by a virus, and as a result, the insured's internal computer network is not available for an extended period of time.	Payment to the insured for their lost income as a result of the disruption and expenses incurred to restore operations.
System Failure	Coverage for loss of income and expenses to restore operations as a result of an accidental, unintentional and unplanned interruption of an insured's computer system.	An organization's computer system is rendered inoperable through employee negligence, and as a result, the insured's business operations are shut down for an extended period.	Payment to the insured for their lost income as a result of the disruption and expenses incurred to restore operations.
Dependent Business Interruption	Multiple coverage options for loss of income and expenses to restore operations as a result of an interruption to the computer system of a third party that the insured relies upon to run their business.	A cloud service provider's system is infiltrated by malware and rendered inoperable. As a result, the insured is unable to access their data and the business operations are shut down for an extended period.	Payment to the insured for their lost income as a result of the disruption and expenses incurred to restore operations.
Reputation Harm	Coverage for lost business income that occurs as a result of damage to a business's reputation when an actual or potential cyber event becomes public.	The insured's system is compromised by malware that permits an unknown third party to gain access to 100,000 customer records containing personally identifiable information. Following the insured's investigation, and notification to affected individuals, the local media runs an article about the event, damaging the insured's business reputation.	Payment to the insured for their lost income resulting from disclosure of the event.

Travelers CyberRisk coverage is offered as a stand-alone policy or as a cohesive part of the Wrap+® *and* Executive Choice+® management liability suite of coverages. CyberRisk provides a combination of coverage options to help protect organizations from emerging cyber threats and enables customers to access innovative pre-breach and post-breach risk management services.

TRAVELERS

travelers.com