TRAVELERS

CyberRisk

CLAIM SCENARIOS

A CyberRisk policy provides coverage to help protect against data breaches and other fast-evolving cyber exposures and can respond in multiple ways such as security breach remediation and notification expense, network and information security liability, regulatory defense expenses, crisis management event expenses, and computer program and electronic data restoration expenses.

Claim Scenarios

Hacker event

A hacker obtained sensitive personal information from the insured's computer system. As a result, a number of customers filed a claim against the insured for allowing access to their personal information. In this situation the Network and Information Security Liability insuring agreement could pay damages and defense costs for covered lawsuits. On average, these lawsuits could cost U.S. businesses more than $1.3 million, according to the NetDiligence 2015 Cyber Claims Study.

Stolen laptop

The insured's chief customer service officer had his laptop stolen. The computer contained more than 100,000 donor records, including donors' personal contact information. The Crisis Management Event Expenses insuring agreement could pay to hire a public relations firm to restore donor confidence or mitigate negative publicity generated from the incident. This represents just one area of post-breach costs, which on average can total $1.7 million for a U.S. business, according to the Ponemon Institute 2016 Cost of Data Breach Study.

Data breach

A charity with offices nationwide suffered a major data breach involving thousands of donors. As a result, attorneys general in multiple states brought regulatory action against the insured. The Regulatory Defense Expenses insuring agreement could pay for responding to regulatory claims stemming from the data breach, including any resulting fines or penalties. On average, this could cost $430,000 in legal defense costs, according to the NetDiligence 2015 Cyber Claims Study.

Fraudulent activity

A credit card company received more than 100 reports of fraudulent credit card activity connected to one of the insured's retail stores. The credit card company requested that the insured confirm that its system is secure and fill out a form to be returned to the company. Potentially 16,000 people living in five states were affected.

Security breach

A company believed that one of its employees, who worked in data processing, was responsible for a computer security breach at the organization. The company put the employee on leave and thought it had cut off her access to the computer system. The employee was terminated later that month. Soon after, the insured's technology staff discovered a potential breach. Someone had been accessing the system from a computer that did not belong to the insured. That same computer had been used by the former employee when she worked for the insured. The insured notified police and the FBI.

Rogue employee

A rogue employee accessed a company's data system and attempted to extort money in exchange for restoring project files. When the company refused to pay, the employee threatened to destroy the files, which would have been catastrophic due to lack of an adequate backup system. After hiring a forensic IT expert, the company was able to identify the employee and restore the files. There was significant business interruption. The company also had to hire a crisis PR coach to explain missing a major project deadline. These post breach costs can average $1.7 million, according to the Ponemon Institute 2016 Cost of Data Breach Study.

Cloud data breach

A construction company stored its customers' information in a third-party cloud computing environment which suffered a major data breach. As the data owner, the company managed the resulting impact to its business and customers. As a result Attorneys General in several states began a regulatory investigation to determine whether the company responded appropriately to the breach in accordance with various state laws. The Security Breach Remediation and Notification Expense insuring agreement could pay costs of approximately $200 per record for U.S. businesses, according to the Ponemon Institute 2016 Cost of Data Breach Study.

Lost smartphone

An employee lost his personal smartphone, which he used to access an unsecured database containing protected health information for over 15k clients. This resulted in costs for legal services and a forensic investigation. In addition to data breach notification and remediation costs, thecompany lost its largest client. Other clients are considering legal action against them for failing to prevent unauthorized accessed to electronic data containing confidential information. The company would need to pay notification costs, which average $590,000, according to according to the Ponemon Institute 2016 Cost of Data Breach Study.

Point of sale system breach

A credit card company identified 20 million credit cards that had been used legitimately at the insured's retail locations were later compromised. The credit card company alleged that a breach occurred within the insured's point of sale system and required the retailer to undergo a forensic audit of its system and related infrastructure by a certified forensic examiner. A number of class action lawsuits were filed as a result of the incident. For a US business, post-breach expenses can cost an average of $1.7 million, according to the Ponemon Institute 2016 Cost of Data Breach Study.

Why Travelers

- We've provided effective insurance solutions for more than 150 years and address the needs of a wide range of industries.
- We consistently receive high marks from independent ratings agencies for our financial strength and claims paying ability.
- With offices nationwide, we posses national strength and local presence.
- Our dedicated underwrites and claim professionals offer extensive industry and product knowledge.

TRAVELERS

travelersbond.com