Cyber Liability and Data Security +

Claim Examples

COVERAGE PART A

- **Data Breach Liability:** Alice owns a restaurant whose point of sale machines had been illegally skimmed with a small, hidden electronic device for eight months, affecting nearly 1,000 cards. Over those eight months, some cardholders became identity theft victims, and paid for their own credit monitoring; others had debit cards skimmed and were not able to recover stolen funds from their bank accounts because too much time had expired without them noticing the fraudulent activity. Victims banded together and sued the store for costs incurred, including paying for credit monitoring, recovering lost funds and expenses incurred in clearing their identity.
- **Security Breach Liability:** Diane's real estate agency is sued by an e-commerce organization for its participation in a denial of service attack against the e-commerce firm. Diane's agency had antivirus and firewall protection on its computers; however, the firm had not made updates to them in the past couple years. It turns out their computers became infected with malware, which, when activated, participated in an attack against the e-commerce firm's servers, overloading them with requests and shutting down their system for a day. The e-commerce firm sued the agency, among others for lost revenue and costs to repair their server as a result of the neglect of standards of care by those unknowingly participating in the attack. Diane's agency paid over $50,000 in defense and settled for $30,000 in loss.
- **Defense of Regulatory Proceedings:** Joe owns an appliance sales organization. Joe makes the decision to store client names, addresses, phone numbers and spending habits to help cross-sell their other products. The organization does not have proper security in place to protect the information. A hacker gains access to the personal information and sells it on the Internet. The state where the merchant is located accuses them of privacy law violations and sets up hearings to decide if fines will be asessed. Joe expends $10,000 to defend the company and is ultimately fined $30,000.
- **Payment Card Industry (PCI) Fines & Penalties:** A small family restaurant in Utah was informed by their payment card-processing bank of a potential data breach of their point-of-sale system. A forensics investigation found they unintentionally stored credit card numbers. However, the payment card processor demanded indemnification for fines assessed by the credit card companies who alleged a data breach. The payment card processor withdrew $10,000 from the restaurant's bank account and sued them for the balance of $80,000.

COVERAGE PART B

- **Data Breach Expense:** A retail drug store chain is hit with a data breach exposing the credit and debit card numbers and expiration dates on a large number of their customers. State law requires the chain to report the breach and notify customers. The chain spends over $400,000 to hire a firm to conduct forensics to determine all those affected, re-secure its network, send out notification letters across multiple states and set up credit monitoring for the customers. In addition, $75,000 is spent on hiring a public relations firm to manage the publicity surrounding the event.
- **Cyber Extortion Threat Expense:** Jerry, the president of an insurance agency, arrives at work to find he and his employees are locked out of the computer system. A hacker notifies him that they have 24 hours to pay $10,000 or all files on the server will be deleted. As the deadline nears, Jerry realizes that he cannot thwart this attack and he is forced to pay the amount demanded.

COVERAGE PART C

- **Website Liability:** A coffee shop with a cinematic theme posts links on their Web site to movie coming attractions and uses images from movies in ads on their Web site. However, the coffee shop never received permission to post these images. Several movie studios threaten lawsuits based on violations of intellectual property. At first, the coffee shop fights but then relents, agreeing to take down the postings after spending $10,000 in defense costs.
- **Website Liability:** Mike owns a boutique hotel along the Florida coast. The hotel has a Web site that includes a section for customer feedback. Mike monitors posts daily and is shocked to find a one star review from a well-known hotel reviewer who stated that his room and the property in general was dirty and had poor customer service. Mike posted a reply on the blog that he remembered the reviewer, and he was the one who was unkempt, rude and confrontational with staff. The reviewer sued for $1,000,000 for libel and intentional infliction of emotional distress.

COVERAGE PART D

- **Identity Theft:** Carl is a small business owner of a local pizzeria looking to expand his operation. When Carl inquired about a loan to open up a new location, the bank turned him down for poor credit. Apparently his identity was stolen, and the thief had opened up additional lines of credit and was purchasing big ticket items such as a car and boat. They all went unpaid and collection attempts went to a fake address set up by the thief. Carl's operation is now headed toward bankruptcy as he cannot dedicate time to his business while he tries to clear his credit record nor can he access credit to keep the business going.