ABA Insurance Services

# CYBER INSURANCE

## The following examples demonstrate how a cyber claim can damage a small business or nonprofit.

| CLAIM | SCENARIO |
|---|---|
| **Crime-Funds Transfer** | The owner of a small manufacturer noticed three payments totaling $204,620 had been wired from the company's bank account. The transactions were reported to the bank as unauthorized and the bank shut down the account but was unable to recover any of the money. Investigators determined that someone had gained access to the owner's username and password for the manufacturer's online banking software. |
| **Crime-Ransomware** | A florist was hit with a ransomware virus which locked their server and delivered an extortion demand for the equivalent of $1,000 in bitcoin. Working with their insurance carrier, the decision was made to pay the ransomware as there were no backup files from which to restore the data. The payment of $1,000 was under the policy deductible but the carrier helped acquire the bitcoin and settle the transaction. The carrier also initiated a forensic review to ensure no private data was exposed. Total cost of the review was $15,000. |
| **Data Breach Response Expenses** | The HR manager at a nonprofit association inadvertently disposed of a box of employee files while moving offices. The nonprofit later learned the entire box–five years' worth of employment records, including social security numbers and dates of birth–was pulled from the garbage by an unknown person. The incident cost the nonprofit over $12,000 in forensic costs, notification costs, and identity theft protection costs. |
| **PCI Violations** | The owner of three buffet style restaurants experienced a breach on their point of sale system involving over 1,000 customer credit card records. A subsequent audit performed by Visa found the restaurants were not in compliance with the security standards in their PCI agreement. The company was fined $5,000 per month by Visa until the violations were corrected. |
| **Reputational Harm** | Due to adverse publicity after a breach, a physician's office lost almost one hundred patients and $140,000 in profits. The policy reimbursed the practice for lost profit and extra expense for negative media coverage tied to the incident. |
| **Multimedia Liability** | An employee of an insurance agency sent an internal email to his colleagues accusing a customer of habitually lying. Another employee forwarded the email to the customer. A defamation lawsuit was brought against the agency. The matter settled for nearly $25,000. |
| **Privacy Liability** | The finance manager at an auto dealership opened an email attachment which downloaded malware onto their network. The malware enabled criminals to access customer finance records, which they used to perpetrate identity theft on hundreds of the dealer's customers over a period of several months. Eventually, law enforcement traced the source of these identity theft cases to the dealership. A class action lawsuit was brought against the dealership for negligence, breach of fiduciary duty and failure to notify impacted individuals that their privacy was breached as required by state law. Total damages awarded exceeded $1,000,000. |
| **Privacy Liability** | A physical therapy practice was hit with a DDoS (distributed denial of service) attack in which hackers used the practice's network to send out tens of thousands of emails to a nearby physician's office. The physician's network was so overwhelmed with traffic, it became inoperable. The physicians brought suit against the physical therapy practice for negligence and sought to recover $20,000 in lost business revenue. |