# Cyber Claim Examples

## Ransomware / Cyber Extortion

A company provides customers with hosting and connectivity solutions, including Internet access, hosted environments for internal and external facing websites, hosted application services, etc. Access is restricted to authorized users through assigned user identification with user-controlled passwords.

Situation: The company receives a threat from an unknown third party that will cause an interruption of the company's network and unauthorized access to the data stored on the company's servers. After investigating the threat, it's determined that the threat is credible and the company makes an extortion payment to the person or group making the threat.

Challenge: The cyber extortion threat results in the following expenses for the company: $25,000 cyber extortion expenses

Resolution: The total expenses incurred by the insurer were $25,000.

## Medical Records Hacked

When an insured hospital was notified by the United States Secret Service of a potential HIPAA breach that may have compromised data for 40,000 patients, our experienced team of dedicated cyber claims specialists quickly engaged a breach coach and a forensic investigator. As a result, the insured had knowledgeable partners to provide advice, handle notifications, create a call center, offer patients access to identity-monitoring products, and ensure the incident was properly reported to the state regulatory agencies.

BIZLock®
BUSINESS CYBERCRIME PROTECTION

# Cyber Claim Examples

## Malware Data Breach

A regional retail computer system was compromised when a third party sent a malware program via email to a number of employees. The invasive software allowed the third party to access the system and capture the names, addresses and credit card numbers for more than 500,000 customers.

## Stolen Laptop

An employee's company laptop containing private customer information is stolen from his home. As a result, customers sue the company for damages resulting from alleged failure to protect their private financial information.


## eNetwork Interruption

When an insured with hundreds of outlets experienced a 48-hour systems failure at the start of a busy holiday weekend due to a hack, the insured could not process sales and payments quickly and its operations were disrupted. The response team added expertise, assisted the retailer in retaining a forensic accountant, and verified the lost sales calculation for the holiday weekend. The insured was also reimbursed for approximately $200,000 of lost sales incurred after the waiting period applicable to the network interruption caused by a malicious attack.

*"Our agency was targeted and hit by a cyber-attack a few weeks ago. BIZLock's response was immediate, comprehensive and heartwarming."*
*- Karen N., Owner, Insurance Agency*

## Rogue Employee

An employee stole a donor's credit card information from a non-profit that resulted in a forensics investigation, a lawsuit and a PCI fine. The per record insured cost for that incident was $50,000.

## Data Theft From Server

When a server and hard drive maintained by a company acquired by an insured were stolen, sensitive data for nearly 45,000 individuals was compromised. The insured was provided $1 million to cover notification, public relations, and other incident-related services.

# Cyber Claim Examples

## Payment Card Industry (PCI) Related Fines and Penalties

A large movie theater operation had its transaction processing systems at a specific movie theater location hacked. Thieves collected card data from one machine over the course of one year before the Secret Service notified the movie theater owners. A forensic investigation ensued. Mastercard issued PCI related contractual fines and penalties in excess of $250,000 to the payment processor, who in-turn contractually passed the obligation to the movie theater owners. The insurance aggregate limit was reached at $100,000.

## Pharmacy Procedural Error

A woman purchased a used computer from a pharmacy. The computer still contained the prescription records, including names, addresses, social security numbers, and medication lists of pharmacy customers. The cost of notifying affected parties per state law totaled nearly $110,000. Two lawsuits were filed: one alleged damages in excess of $200,000 from a party who claimed she lost her job as a result of the disclosure; the second alleged the plaintiff's identity was stolen, and the costs of correction and emotional distress exceeded $100,000.

## Media Liability Exposure

Two employees at a Pizza chain posted derogatory comments and a video online. The video captured their employee uniforms and work location.

*"We were hacked and the hackers gained access to sensitive records. We called BIZLock and their Incident Response On-Demand was timely, effective and certainly comforting. We were very satisfied. We encourage every small business to purchase cyber insurance. It is sad how easy it is to suffer from a breach, which makes having cyber insurance a simple decision."* - Dawn C., Michigan

BIZLock
BUSINESS CYBERCRIME PROTECTION