CYBER SECURITY CLAIMS SCENARIOS

Cyber Security coverage is designed to help businesses respond to a range of cyber incidents, including breaches of personally identifying or personally sensitive information, threats of unauthorized intrusion into or interference with computer systems, damage to data and systems from a computer attack and cyber-related litigation.

Claims Scenarios

Paid Loss after Deductible total may include multiple coverages

Data Compromise Response Expenses
A burglar broke into an accountant's office and stole a computer with the tax records of clients. The insured's clients were in four states and he needed assistance meeting the various state law notification requirements. Legal counsel helped to notify affected individuals, who were offered a toll-free hotline and credit monitoring services.
Paid Loss after Deductible: $28,000

PCI Assessments
A retailer experienced a data breach, which exposed all of their customers' credit card numbers. Upon review by a Payment Card Industry (PCI) forensic investigator, it was determined that the retailer was not compliant with PCI security standards. As a result, the credit card company levied fines and penalties against the retailer for noncompliance and required that they pay for a PCI investigation. Coverage was provided for the fines and penalties, as well as the PCI assessment.
Paid Loss after Deductible: $44,541

Computer Attack & Data Compromise Response Expenses
An employee of an investment company installed peer-to-peer file sharing software on a company computer. When configuring the service, the employee unintentionally shared personal identifying information of clients and employees and identity thieves were able to access it. After consultation with an attorney, the insured learned that he was obligated to notify affected individuals of the breach. Additionally, it was determined that the insured would need to hire an outside firm to help restore the computer system to its pre-attack functionality.
Paid Loss after Deductible: $50,000

Cyber Extortion
While trying to balance the books, a business owner received a strange pop-up on his laptop. A ransomware virus locked the system until the extortion demand was paid. After consulting with the insurance company, the insured decided to pay the $600 to unlock the system.
Paid Loss after Deductible: $2,400

Future Loss Avoidance
A small business owner clicked on an email attachment that looked legitimate. However, the attachment contained malware (commonly referred to as a computer virus) and within a short period of time, the malware spread throughout the owner's computer system causing damage to the company's network. As a result, an outside firm was called in to restore the computer system to its pre-attack functionality. Upon completing the restoration, the firm discovered that the insured was using an outdated operating system. The firm advised the insured to upgrade to a more current operating system that has regular patch updates. The insured did just that and insurance covered $1,000 of the total cost, since the coverage allows for up to 10% of the remediation cost.
Paid Loss after Deductible: $10,000 for system restoration and $1,000 towards future loss avoidance coverage

Reward Payments
A burglar broke into an accountant's office and stole a computer with client tax records. After consulting with the insurance company, the accountant offered a reward for assisting in finding the burglar. A few weeks later, the burglar boasted about the score in a public forum and a third party reported the heist to police. The report led to the arrest and conviction of the perpetrator and coverage reimbursed the accountant for the reward payment he had offered to bring the criminal to justice.
Paid Loss after Deductible: $15,000

Continued on next page

Learn more at secura.net/cyber

SECURA INSURANCE COMPANIES

Cyber Security Claims Scenarios

Computer Attack
A small business owner experienced a computer attack that corrupted data and caused the company's laptops to stop functioning properly. The insured hired a system restoration firm to remove the malware and reinstall software however the firm determined it would be more cost effective to simply replace the insured's three laptops. Coverage paid for the initial data and system restoration work, as well as the new laptops after it was determined that it would reduce the amount of the loss.
Paid Loss after Deductible: $11,259

Data Compromise Liability
An unknown actor stole approximately 20 deal jackets containing the Personal Identifying Information of customers from a dealership. The insured provided breach notifications and credit monitoring services to affected individuals. Two customers subsequently made legal demands as a result of this breach.
Paid Loss after Deductible: $20,013

Network Security Liability
A business experienced a cyber-attack that involved compromise of its servers. After hacking into the system, criminals used the contacts from the business system to launch a ransomware attack against every email address in the insured system's contacts. Several of the contacts filed lawsuits claiming that they failed to properly secure the insured's system. Coverage was provided for the costs of hiring lawyers and to settle cases.
Paid Loss after Deductible: $14,000

Electronic Media Liability
A business posted a picture of a local celebrity on their website. The insured noticed increased business attributed to this change. However, a letter was received from the celebrity's lawyer demanding that the picture be taken down. The lawyer also argued that their client's reputation may have been harmed by the association to this insured's product. The business owner hired an attorney to respond to the demand letter.
Paid Loss after Deductible: $7,000

Privacy Liability
A small online retailer had their privacy policy listed on their website. Even though the small business never had a security incident or data breach, one of their savvy customers, who was also a lawyer, sued the retailer claiming that their treatment of his personal information violated the retailers own privacy policy. The coverage paid for defense and settlement of the lawsuit.
Paid Loss after Deductible: $32,360

Identity Recovery
A business owner reported being sued due to unauthorized accounts that had been opened in his name. An unauthorized person used the insured's personal information to rent several items and open lines of credit. An identity recovery case manager consulted with the insured and placed fraud alerts. The insured hired an attorney to help resolve the issues.
Paid Loss after Deductible: $5,652

Misdirected Payment Fraud
An employee in the finance department received an email that looked like it was from the company's CFO directing that employee to send a wire for an overdue vendor invoice. Later that day after the employee sent the wire, he bumped into the CFO in the hallway and mentioned he sent the payment. The CFO said he never sent any such request. The employee checked the email and noticed that the CFO's name was spelled slightly incorrectly. The company had been duped by a fraudster that made an outside email look like it came from the CFO. The coverage reimbursed the amount of the wire.
Paid loss after deductible: $9,500

Computer Fraud
A hacker found his way into a company's computer system and changed the banking instructions on several employee's payroll deduction accounts, mapping the payroll deductions to his bank account. Within a few weeks after several employees complained they did not get their pay, the company investigated and realized they had been hacked. The coverage reimbursed the amount of the diverted funds.
Paid loss after deductible: $17,500

Telecommunications Fraud
A small business owner received an exorbitant bill from their telephone service provider. It was later determined that a hacker infiltrated the insured's telecommunications system to automatically make outgoing phone calls to expensive 900 numbers which the hacker also controlled. Coverage was provided to reimburse the insured for the amount of the fraudulent phone calls.
Paid Loss after Deductible: $21,963

Reputational Harm
A small business owner experienced a data breach and provided the necessary notification to affected individuals. The breach was also reported in local media outlets. Over the next three weeks, the owner noticed a decrease in business income as word spread of the breach. Coverage was provided for the loss of business income for the 30 days following the data breach notification.
Paid Loss after Deductible: $18,360

Learn more at secura.net/cyber

SECURA INSURANCE COMPANIES