ProWriters
Professional & Management Liability Insurance

Cyber Insurance—What It Is & Why You Need It

The increasing reliance on technology and digital data heightens the risk of cyber attacks and data breaches.

Cyber criminals can access sensitive information, leading to identity theft, financial fraud, or ransom demands.

Such breaches can disrupt business operations, causing significant losses in productivity, revenue, and reputation, with financial impacts often hard to recover from.

Cyber Insurance provides coverage against losses related to cyber attacks, data breaches, and other computer-related crimes.

Cyber Insurance typically covers both first-party and third-party liabilities. First-party liabilities are the direct costs the insured business incurs as a result of an incident. Third-party liabilities are the costs others incur.

Depending on your policy, the expenses it can cover include:

- IT Forensics
- Data Recovery and Restoration
- Extortion Demands (Ransoms)
- Systems Repair
- Notification of affected individuals
- Credit Monitoring for affected individuals
- Lost Revenue
- Crisis Management (including PR)
- Legal Fees, Settlements, and Judgments

ProWriters
Professional & Management Liability Insurance

4 Cyber Insurance Claim Examples

Cyber criminals target companies of all sizes, from small startups to large multinational corporations. Additionally, they can launch attacks from anywhere in the world, making it possible for them to target companies regardless of geographical location.

Cyber attacks take many forms. Here are four of the most common—and costliest.

Ransomware Attacks

What is it?
In a ransomware attack, hackers gain unauthorized access to a computer system or network and encrypt their victim's files or data. Once they've encrypted the files, the hackers demand a ransom payment, usually in cryptocurrency, in exchange for the decryption key.

Claim Example:
A ransomware attack on Doctors' Management Services affected the protected health information of some 206,695 people. The breach went undetected for more than a year. The medical management company settled with the U.S. Department of Health and Human Services' Office for Civil Rights for $100,000.

Funds Transfer Fraud

What is it?
Fund transfer fraud (wire transfer fraud) occurs when a hacker gains access to banking information, typically by stealing usernames and passwords from a network, and uses it to move funds from a targeted bank account. Usually, by the time the victim becomes aware of the unauthorized transfer, the funds are already gone.

Claim Example:
In Cottage Grove, Oregon, the city's accounting specialist sent an email about a sewer project to an incorrect address. Days later, a fraudster took advantage of the slip-up, sending a request for "updated payment information." The city transferred more than $1.2 million to a fraudulent account. By the time the fraud came to light, the fraudster had moved the money to many different accounts.

ProWriters
Professional & Management Liability Insurance

Invoice Fraud and Manipulation

What is it?
Invoice fraud occurs when bad actors create false invoices and convince their targets to pay them. Invoice manipulation involves modifying existing, actual invoices to redirect payments to their bank accounts (for example, simply by changing the bank routing number). Fraudsters sometimes can send invoices from email addresses that resemble legitimate ones—or sometimes even use stolen login credentials to send from a victim's authentic email account. Since these fake or altered invoices appear legitimate, no one's the wiser until vendors report they've gone unpaid.

Claim Example:
A Manhattan company's procurement manager created and sent his company false invoices, sometimes in the names of employees of the company's real vendors. He incorporated more than a dozen false companies and opened bank accounts in names differing only slightly from actual vendors' names. Using his position at the company, he authorized payment of the 40 invoices he'd created, defrauding his company of about $4.4 million.

Social Engineering

What is it?
Social engineering is "human hacking." It exploits human psychology and tricks individuals into divulging sensitive information or performing actions that compromise security. Social engineering attacks include phishing emails, phone calls, or even physical interactions. Attackers can pose as a trusted individual or organization, create a sense of urgency, or appeal to emotions to deceive their target and achieve their objective.

Claim Example:
Scammers emailed the accounts payable coordinator at Upsher-Smith Laboratories in Maple Grove, Minnesota, pretending to be the CEO. They also provided a lawyer's name. Over three weeks, the employee, following the emailed instructions, initiated nine wire transfers that wound up costing the company more than $50 million.