What Is Cyber Liability?

INSURANCE OFFICE OF AMERICA

Cyber liability coverage is designed to provide protection for exposures related to the use of the internet. Policies may include any or all of the following coverages:

Third-Party Liability Coverages

- Network Security Liability
- Privacy Liability
- Media Liability
- Professional Liability/Errors & Omissions

Regulatory Coverages

- Privacy Regulatory Actions & Investigations (Including Fines and Penalties).
- PCI (Payment Card Industry) Fines, Penalties and Assessments.

First-Party Coverages

- System Damage
- Network Interruption
- Consequential Reputational Harm
- Notification Costs
- Third-party notification costs
- Computer Crime with Social Engineering
- Identity Theft
- Cyberthreats & Extortion
- Telephone Hacking
- Phishing Scams

What a Cyber Breach Can Cost You

- 100% experience cost to investigate, repair or replace systems
- 74% report loss of customers
- 59% face possible litigation
- 33% face possible regulatory fines
- 32% experience loss of share value
- 18% report employee layoffs after a breach
- 18% report "devastating" blow to brand and reputation
- **Nearly 50% of all claims result from employee/internal sources (NOT HACKERS).**

TYPES OF CYBER LOSSES

Unintended Disclosure

Sensitive information posted publicly on a website, mishandled or sent to the wrong party via email, fax, or mail.

Hacking or Malware

Electronic entry by an outside party via malware and spyware.

Payment Card Fraud

Fraud involving debit and credit cards that is not accomplished via hacking. For example, skimming devices at point-of-service terminals.

Insider

Someone with legitimate access, such as an employee or contractor, intentionally breaches information.

Physical Loss

Lost, discarded, or stolen nonelectronic records, such as paper documents.

Portable Device

Lost, discarded, or stolen laptop, smartphone, flash drive, CD, etc.

Stationary Device

Lost, discarded, or stolen stationary electronic device, such as a computer hard drive.

INSURANCE OFFICE OF AMERICA

GLOSSARY

NETWORK SECURITY LIABILITY
Covers defense costs and damages for which you are held liable for failure to protect your network and/or the transmission of a virus to others.

PRIVACY LIABILITY
Covers defense costs and damages for which you are held liable for disclosure of or failing to protect non-public information.

MEDIA LIABILITY
Covers defense costs and damages for which you are held liable for infringement of intellectual property, allegations of defamation, libel and/or slander.

REGULATORY DEFENSE FINES AND PENALTIES
This provides defense costs and damages for which are you held liable for an alleged violation of applicable state, federal or international data protection laws. Fines and penalties coverage may be included as well.

BREACH RESPONSE EXPENSES
Covers the costs related to the breach or disclosure of nonpublic information stored on your computer systems and often if stored on your behalf. Your paper records are usually covered as well. Costs may include forensics, legal advice, costs to notify those affected by the breach, setting up a call center, credit monitoring costs, etc.

NETWORK EXTORTION
In the event your computer systems are under an extortion threat from a hacker, this coverage will provide response costs (and usually pay ransom payments to limit or avoid potential damage).

NETWORK INTERRUPTION
Covers loss of revenue during an actual system outage that occurs as a result of a hacking or virus attack.

DATA RESTORATION
Covers the cost to restore or repair data lost during a hacker or virus attack.

CONSEQUENTIAL REPUTATIONAL HARM
Covers loss of revenue for the period directly following the business interruption outage, where revenue is still affected due to lost customers or contracts.

COMPUTER CRIME
Covers the cost of an unauthorized third-party funds transfer from insured's account.

SOCIAL ENGINEERING
Covers loss resulting from an insured being induced/tricked into voluntarily parting with funds (i.e., wiring funds due to fraudulent instructions received by a hacker disguised as an internal executive).

IDENTITY THEFT
Covers the theft of insured's electronic corporate identity, where someone fraudulently is communicating or entering into contracts as if they were the insured.

TELEPHONE HACKING
Covers costs associated with a hack of the insured's phone system.

PHISHING SCAMS
Covers costs associated with responding to fraudulent electronic communications/websites designed to impersonate the insured (e.g., press release, etc).