Cyber Liability insurance options for AOA member practice owners

UNDERSTANDING YOUR COVERAGE OPTIONS

AOA-endorsed Cyber Liability insurance

The AOA Insurance Program, administered by Lockton Affinity, has partnered with Beazley, one of the leading experts in cyber insurance, to offer a Cyber Liability insurance policy that is available in two forms:

$515/year*

$500,000 coverage limit
Base coverage to protect your practice.

$715/year*

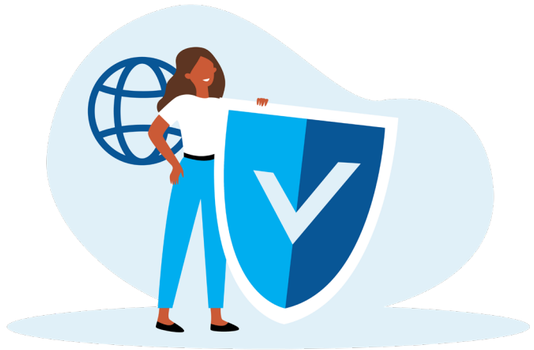
$1,000,000 coverage limit
Base coverage, plus enhancements like Payment Card Liability, Telephone Fraud, Funds Transfer Fraud and more, for added protection.

*Before applicable taxes and fees.

To help AOA members better understand these policy options and the common cyber risks optometrists face, Lockton Affinity has compiled a clear coverage guide, including an example cyber attack response scenario and a glossary of cyber-related terms.

Explore these resources below or contact Lockton Affinity's dedicated team of licensed insurance representatives for personalized support.

Info@AOAInsuranceAlliance.com | (888) 343-1998



UNDERSTANDING CYBER ATTACKS

Cyber attack response scenario

Ransomware attack
A cybercriminal sends your office staff a malicious email, though it looks to be an invoice from a regular vendor. An employee opens the email and downloads the invoice, unknowingly giving the criminal access to your practice's network.

The cybercriminal installs malware and gains access from their system to yours. They search for valuable resources, such as patient and employee information, banking details and backups for business-critical resources and systems. Because of the amount of valuable patient data in your system, including Social Security numbers and payment information, they quickly deploy ransomware, encrypting your files and data.

They demand a ransom payment in cryptocurrency in exchange for your stolen data. How do you proceed?

Forensic analysis and legal expert needs
You determine the breach is more than you feel comfortable handling. You decide to hire forensic analysis and legal experts.

Forensic analysists help determine exactly what happened, how it happened and provide suggestions to implement so it doesn't happen again, such as routine cyber audits, monitoring and other consulting services.

Legal experts help ensure your organization takes the right steps after the incident. They review your contracts and communications and advise on legal obligations. Should a civil suit or regulatory action arise from the cyber event, they'll be available to assist in mounting a defense.

These services don't come cheap. How will you pay for your forensic analysis and legal expert needs?

Patient notification and public relations support
The cyber incident raises many questions, and not just internally. Patients, vendors and even the public have questions about the event. Some of your employees are diverted to manning the phones, but you're also legally required to notify your patients. It quickly becomes overwhelming, so you decide to hire a local public relations firm.

They help communicate with your patients in the most effective way and work to repair patient relationships and improve your practice's reputation.

These are ongoing services that can take months. Can your practice handle the expenses out of pocket?

With Cyber Liability insurance from Lockton Affinity's AOA Insurance Program, just one phone call gives you access to Beazely's robust network of cyber response professionals whose primary job is to resolve cyber incidents swiftly and effectively.

Concerned that a cyber incident could impact your practice? **Apply now**

Know which policy form you'd like? Apply now

CYBER LIABILITY COVERAGE AND LIMIT OPTIONS

	Base coverage **$515/year***	Base coverage with enhancements **$715/year***
BREACH RESPONSE Coverage for investigating, containing and mitigating the impact of a cyber incident.		
Notified individuals	25,000	50,000
Legal, forensic and public relations/crisis management	$500,000	$1,000,000
Aggregate limit of liability	$500,000	$1,000,000
Additional breach response limit	$100,000	$1,000,000
FIRST-PARTY LOSS Coverage for damage or loss to your practice caused by a covered cyber incident.		
Business interruption loss (from security breach)	$500,000	$1,000,000
Business interruption loss (from system failure)	$500,000	$1,000,000
Dependent business loss (from dependent security breach)	$100,000	$250,000
Dependent business loss (from dependent system failure)	$100,000	$250,000
Cyber extortion loss	$500,000	$1,000,000
Data recovery	$500,000	$1,000,000
THIRD-PARTY LIABILITY Coverage for damage or loss to third parties, including patients, vendors and more, caused by a covered cyber incident.		
Data and network liability	$500,000	$1,000,000
Regulatory defense and penalties	Not included	$250,000
Payment card liabilities	Not included	$250,000
Media liability	Not included	$1,000,000
ADDITIONAL COVERAGES Coverage for eCrime, criminal reward and more.		
Fraudulent instruction	Not included	$100,000
Funds transfer fraud	Not included	$100,000
Telephone fraud	Not included	$100,000
Criminal reward	$50,000	$50,000
Cryptojacking	Not included	$10,000 sublimit
Reputation loss	Not included	$10,000 sublimit
Computer hardware replacement	Not included	$10,000 sublimit
DEDUCTIBLES		
Breach response (each incident, loss or claim)	$2,500 and $2,500 for legal	$2,500 and $2,500 for legal
Forensic and public relations/crisis management	$2,500	$2,500

**Before applicable taxes and fees.*

UNDERSTANDING KEY CYBER TERMS

Glossary of terms

Types of cyber attacks

Cryptojacking

When a threat embeds itself within a computer and uses its resources to mine cryptocurrency at the expense of your device and the overall health of your network.

Cyber breach

A cyber breach, or security breach, is a type of cyber incident that involves the bypassing or overcoming of your company's cybersecurity protections. A breach means your private data or your patients' private data may have been exposed to unauthorized parties.

Funds transfer fraud

When a cybercriminal inserts themselves into communications facilitating a transaction involving large sums of money, such as mergers and acquisitions, real estate transactions, legal settlements, retirement disbursements and more. This scam is dangerous because of the sums of money involved and the considerable difficulty getting the funds back, especially when they are quickly wired overseas.

Malware

Malware, short for malicious software, is a piece of software intentionally designed to cause harm to a computer, a network or a user. This attack can cause computers and networks to run slowly or break. It can also be used to create privacy and security vulnerabilities that can be exploited by hackers. Pharming code is one example of malware. Ransomware is another.

Phishing

A common type of online fraud through emails that are often transactional, promising something in return for your response and providing a convincing reason for you to respond, such as a contest prize or a security check. Requests can ask for login credentials, passwords, credit card numbers, security codes and more. The danger of phishing is that the requests are often quite similar to legitimate requests from people and organizations you regularly do business with.

Ransomware

Ransomware works by installing malicious code on a computer or network when you download an infected email attachment, click a malicious link or visit a fraudulent or compromised website. The software is programed to lock up the files on your device and display a screen with instructions for paying a large ransom with the promise of returning your files. Paying the ransom offers no guarantee your files will be returned. Past attacks have ended with data being publicly exposed.

Social engineering

Social engineering involves trickery, deception or psychological manipulation to facilitate online attacks, scams or fraud. Cybercriminals often use social engineering as a first step to convince business owners and employees to divulge sensitive information such as passwords or security procedures that can then be used to hack a computer or network.

Telephone fraud

When a phone is used to deceive another person into providing personal information, money or access to their accounts through deceptive tactics. This often involves impersonating a real company or person to trick the victim.

Coverage terms

Breach response

Coverage for costs associated with a data breach, such as notifying affected parties, credit monitoring and hiring legal advisors, forensic experts, public relations professionals and more.

Business interruption loss

In the event of a cyber attack, your practice may experience loss of income and expenses to restore operations. This may include the voluntary shutdown of systems to minimize the business impact of the event.

Computer hardware replacement

Coverage for costs to replace your computer systems that are permanently impacted by malware or other cyber incidents.

Criminal reward

Payment of a reward for information that leads to the arrest and conviction of someone who commits an illegal cyber act related to your coverage.

Cyber extortion

This coverage can offer reimbursement for ransom payments and associated costs (where such payment is legally permissible).

Data and network liability

Coverage against losses for the failure to protect a customer's personally identifiable information (SSN, credit card numbers, medical information, passwords, etc.) via a cyber incident.

Data recovery

Coverage for costs to restore or recover data, computer programs or software lost from system damage due to covered events such as malware, ransomware, computer viruses, denial-of-service attacks or unauthorized access.

Dependent business loss

Income loss and extra expenses your practice experiences during the interruption and restoration of operations caused by a dependent security breach or dependent system failure. This may occur if a credit card processer or a health insurance company used by patients experiences a cyber attack and their services are unavailable.

Dependent security breach

A failure to prevent a breach of computer systems operated by a dependent business.

Dependent system failure

An unintentional and unplanned interruption of computer systems operated by a dependent business.

Ecrime

Criminal activities that involve the use of computers or networks. These may include social engineering, ransomware and fraudulent schemes involving paying a invoice or bill.

Fraudulent instruction

When an employee is tricked by an impersonating entity and provides information that leads to a breach.

Media liability

Liability related to items such as copyright infringement, libel, slander occurring via digital communications or on the insured's website.

Notified individuals

In the event of a cyber incident, your practice may be legally required to inform patients of a breach of their data. These patients are known as notified individuals.

Payment card liabilities

Vendors who offer credit, debit and cash card transactions must adhere to a widely accepted set of standards to safeguard transactions and protect cardholders against misuse of their personal information. As a result of a cyber incident, you may face fines or penalties for breach of contract with a card brand or payment processor.

Regulatory defense and penalties

Your practice may face fines and penalties, administrative and regulatory proceedings or civil and investigative demands brought by domestic or foreign government entities as a result of alleged wrongful privacy, security or media acts. This coverage helps your practice pay for associated expenses.

Reputation loss

Coverage to help alleviate the damage to your practice's reputation, brand and goodwill that may occur if word of a cyber incident goes public.

System failure

Helps cover the expenses to restore operations as a result of an accidental, unintentional and unplanned interruption of a computer system.

General insurance terms

First-party loss

Coverage for damage or loss to your practice caused by a covered cyber incident. This may include costs associated with business interruption, data recovery, cyber extortion and more.

Limit of liability

The maximum amount the insurer will pay for a single covered loss.

Policy aggregate

While a policy limit defines the maximum amount payable for a single claim, a policy also has an aggregate limit, which is the maximum amount the insurer will pay out for all claims under a policy during the policy period.

Sublimit

The maximum amount an insurer will pay for a specific type of loss or claim.

Third-party liability

Coverage for damage or loss to third parties, including patients, vendors and more, caused by a covered cyber incident.

Concerned about your practice's cyber risks?

Get protection from Lockton Affinity and Beazley today.

Just as you provide expert care for your patients, you need experts to handle cyber attacks. Ensure you have the support you need in the event of a cyber attack.

Apply now!