at bay

Cyber Insurance Designed to Help Prevent Loss

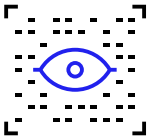
At-Bay helps protect against cyber attacks and minimize disruption

Cyber attacks are a serious threat to anyone that uses technology to power their business. Ransomware claims cost small to medium sized businesses $370,000 on average in 2023.[1]

Cyber insurance can help protect you from significant financial loss and help you quickly recover from an incident. When you choose At-Bay for your cyber insurance needs, you get:

Detailed Security Report at time of quote

At-Bay measures the strength of your security before you purchase a cyber policy.[2]



Security solutions via At-Bay Stance™

At-Bay Stance Exposure Management[3] provides mission-critical products and services that reduce cyber risk–all as part of the insurance policy.

In-house claims & Incident response teams[4]

At-Bay helps you recover quickly with top industry talent from teams that have handled thousands of claims and cyber events.

At-Bay policyholders are up to

5X less likely than the industry average to experience a ransomware attack.[5]

[1] *At-Bay 2024 InsurSec Report*.
[2] A unique web domain is required to receive a full Security Report and Active Risk Monitoring.
[3] At-Bay Stance Exposure Management offerings include Stance Exposure Manager and Stance Advisory Services, which are available to policyholders via the Embedded Security Fee and corresponding Endorsement. Please refer to the policy form for additional information. Note: The Embedded Security Endorsement refers to "At-Bay Stance Advisory Services" as "At-Bay Stance Managed Security."
[4] At-Bay's Response and Recovery team is offered to policyholders as an incident response panel vendor by At-Bay Security, LLC, a wholly owned subsidiary of At-Bay, Inc., providing cybersecurity services including MDR and incident response.
[5] Frequency Based on Primary and Excess Cyber and Tech Errors & Omissions losses reported and exposure earned through 9/30/2022, evaluated as of 10/1/2022, and 2020-2021 industry analysis.

Why Every Modern Business Needs Cyber Insurance

Does my business need cyber insurance?	Cyber insurance helps protect and recover your business from financial loss and liability in the event of a cyber attack. Having a comprehensive cyber policy is especially important if you: • Sell products or services online • Use email, computer software, or other technology to conduct your business • Store or process sensitive data or customer information
What does At-Bay's cyber policy cover?	A cyber policy from At-Bay can help minimize the disruption from a cyber attack and cover the financial costs related to resolving and recovering from an incident, including: • Ransomware • Financial fraud and cyber crime • Lost income from business interruption • Breach response and data recovery • Liability claims from network security or information privacy events
My business is small and we don't have a lot of data Why should I buy Cyber insurance?	Despite their size, small businesses are frequent targets for cyber attacks due to their lack of resources and expertise to combat evolving threats. Cyber insurance is crucial for small businesses, not only to provide comprehensive coverage in the event of a cyber attack but also to offer security services and access to security products. These resources can help protect your business and prevent an incident that could decimate your bottom line.
If I outsource my data to a cloud or third-party service provider, do I still need coverage?	Yes, you need your own Cyber insurance. Once a client or partner entrusts their data to you, you may be legally responsible for that data. Your responsibility to protect client and partner data doesn't transfer when you store or process it with a third party. You are ultimately accountable, and may be held liable, for damages to your client or partner, regardless of whether it occurs on your own computer system.
I may already have Cyber coverage with my package or business owner policy (BOP). Why do I need a standalone policy?	Some carriers allow you to add Cyber coverage to a package policy or BOP. This coverage is often a substandard alternative to a sophisticated Cyber standalone policy. Cyber add-ons often lack expert-backed resources and critical first-party coverages that mitigate the financial, operational, and reputational damages a cyber event can inflict on an organization.

True stories of At-Bay customers

Construction Company Email Compromised

An attacker accessed an employee email account and sent fraudulent wire instructions to a client. The loss was approximately $20,000; however, the client's bank was able to recover the funds. At-Bay investigated the incident and paid nearly $28,000 to cover the costs of a breach coach, forensics, legal notifications, and credit monitoring for all affected individuals.

Food Retailer Suffers Wire Fraud

An employee received an email that a vendor's bank information changed. The employee transferred funds to the new account, only to later learn the instructions were fraudulent. At-Bay investigated the incident and reimbursed the food retailer approximately $60,000 for its loss.

Summary of Cyber coverages

Learn what's included in At-Bay's insuring agreements

First-Party Coverage:

- **Event Response & Recovery:** Covers the cost to hire forensic computer experts to determine the source and scope of a Network Security Event; the cost of restoration and recreation of data that has been lost, corrupted, or destroyed; and the overall cost for the insured to restore systems to their functionality prior to the cyber event.
- **Event Response & Management:** Covers costs when the insured has a legal obligation to notify individuals who are affected by an Information Privacy Event, including expert determination of the type of data affected, legal communications, cost of a breach hotline, and identity theft or credit monitoring for affected individuals.
- **Direct Business Interruption:** Covers the insured's lost income and extra expenses incurred following an interruption or outage of computer systems due to a cyber event.
- **Contingent Business Interruption:** Covers lost income and extra expenses incurred if the insured's business relies on a third-party technology or non-technology vendor whose systems are interrupted or shutdown due to a cyber event.
- **Contingent & Direct System Failure Coverage:** Covers lost income and extra expenses incurred by the insured as a result of an unplanned system outage to the insured's computer systems or the computer systems of a third-party technology or non-technology vendor.
- **Cyber Extortion:** Covers the cost and expenses incurred to mitigate the severity of the extortion loss and the payment of funds, cryptocurrencies, or assets requested by the malicious third party that is threatening the insured's systems and/or data.
- **Social Engineering & Computer Fraud:** Covers the theft of funds or other assets that the insured suffers as a result of social engineering or computer fraud.
- **Reputational Harm Coverage:** Covers income loss incurred by the insured due to an adverse publication stating they experienced a cyber event.

Third-Party Coverage:

- **Information Privacy Liability:** Covers defense costs and damages for claims made by a third party due to an actual or alleged violation of privacy regulations or a failure to protect personal information.
- **Network Security Liability:** Covers defense costs and damages for claims made by a third party due to an actual or alleged network security failure or malware attack.
- **Regulatory Liability:** Covers defense costs, damages, and regulatory penalties if a government agency or regulatory authority brings a claim for the actual or alleged violation of privacy regulations. Also covers regulatory investigations into potential violations.
- **Payment Card Liability:** Covers actual or alleged noncompliance with the Payment Card Industry Data Security Standards (PCI-DSS) including defense costs, reimbursements, fines and penalties, chargebacks, etc.
- **Media Liability:** Covers defense costs and damages for claims made by a third party due to actual or alleged defamation, invasion of privacy, or intellectual property infringement arising from published media content.