Cyber 101

What you need, why you need it, and how At-Bay's coverage responds

Frequently Asked Questions

My business is small and we don't have a lot of data. Why should I buy Cyber insurance?

Most cyber attacks do not target businesses due to their size. Malware takes many forms, and blanket attacks are often unleashed to reach a high volume of businesses, regardless of their size or industry. In fact, small businesses represented nearly half of all cyber attacks in 2019, according to a Verizon data breach report.

If I outsource my data to a cloud or another 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 are 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. Direct indemnification for compromised data may be your responsibility to handle, though your Cyber policy may pay for these costs on your behalf and pursue your vendor for those damages.

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 are typically not as broad or as up-to-date with cyber threat vectors as a standalone policy. They also fall short in providing the same level of pre-breach and post-breach resources.

Where coverage has been afforded in the past, non Cyber-first carriers are taking great measures to include exclusionary language in form updates, clarifying their intentions to not cover these threats. Cyber add-ons often lack expert-backed resources and critical first-party coverages that mitigate the financial, operational, and reputational damages a data breach can inflict on an organization.

Summary of Cyber Coverages

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

First-Party Coverages

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 adverse 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 loss of revenue and associated expenses due to an interruption or outage of their system caused by a breach or network security event.

Contingent Business Interruption: Covers lost business income and subrogation on the insured's behalf if the insured's business relies on a third-party technology provider whose systems are interrupted or shutdown due to a cyber event.

Contingent & Direct System Failure Coverage: Covers lost revenue or extra expenses incurred by the insured as a result of a non-breach-related incident, such as unplanned human error, programming error, or technology infrastructure failure to their systems or the systems of their third-party provider.

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 computer fraud loss that the insured suffers as a result of a malicious actor duping them and/or impersonating an employee or client.

Reputational Harm Coverage: Covers business income loss incurred by the insured due to an adverse publication stating they had an information privacy event or a network security event, whether or not this is "fake news."

Third-Party Coverages

Information Privacy Liability: In the event the insured is sued for damages due to a violation of privacy regulations or failure to protect personal information, the policy would respond to those damages and defense costs.

Network Security Liability: In the event the insured is sued for damages due to failed network security or failure to protect against a network attack, the policy would respond to those damages and defense costs.

Regulatory Liability: If a government agency or regulatory authority finds that the insured has violated a privacy regulation, the policy will pay for the civil fines and penalties. Coverage also responds to regulatory assessments or investigations if there is a potential violation.

PCI DSS Liability: If there is actual or alleged noncompliance with the Payment Card Industry Data Security Standards by the insured, the policy will respond to defense and investigative costs, fines and penalties, fraud recoveries, chargebacks, etc.

Media Liability: If the insured is sued for damages by a third party due to the release or display of media content resulting in defamation, slander, trade libel, infringement of trademark/copyright, etc., the policy would respond to those damages and defense costs.

At-Bay writes Cyber and Technology E&O Insurance as an MGA through HSB Specialty Insurance Company, rated A++ by A.M. Best and part of Munich Re.