JLK GROUP
INSURANCE AND FINANCIAL SOLUTIONS

Independent Insurance Agency
www.jlkinsurancegroup.com

Why Cyber Insurance Is Essential To Your Small Business Risk Management Portfolio

It might feel like cybersecurity risk is only for the big companies; after all, they're the ones making headlines. But according to the Cybersecurity and Infrastructure Security Agency (CISA), there's a ransomware attack every 11 seconds — and 43% of cyberattacks target small businesses.

Commercial auto, property and liability insurance are the staples of every business risk portfolio — most owners wouldn't consider doing business without them. A hack can be just as devasting as a fire. Yet only 17% of small business owners reported having cyber liability insurance (according to a November 2021 study by Advisorsmith).

The expense to restore corrupted computer files, replenish lost income due to business interruption, and pay ransom demands is enough to throw profits into a downward spiral. Add in the cost of notifying clients about the breach, credit monitoring, inevitable lawsuits, federal and state fines, and a tarnished public reputation — and you've got a recipe for bankruptcy.

Reboot your risk management portfolio and discover how cyber insurance can protect business income and help you recover after a cyberattack.

Even a minor data breach can ruin your business

If a breach exposes personal data, you could be required to offer free credit monitoring services for one year (or two years if the data is covered by the Health Insurance Portability and Accountability Act). Credit monitoring services can cost $10 to $30 a month per individual, and that adds up.

> ***For example, if you're found liable for the breach of 2,000 accounts, the cost to comply with credit monitoring services starts at $240,000. Since cybersecurity and data protection laws exist in nearly every state, credit monitoring isn't something you can ignore. If you have international clients or vendors, your risk just got risker. Most countries have cybersecurity legislation, which means more penalties and the added complication of international lawsuits.***

Even if you manage to escape a lawsuit, the out-of-pocket cost for credit monitoring services and government fines could devastate your business.

What does cyber liability insurance cover?

Some insurance companies distinguish between cyber liability and data breach insurance, but often it's just a difference in terminology. Cyber liability insurance covers things like:

- Lost income caused by a cyberattack (fines, ransom payments, downtime)
- Customer notification of a data breach (legally required in most states)
- Reputational damage and public relations (support from experts who understand the process)
- Legal defense costs (when clients or vendors sue you for exposing their data)
- Civil damages and settlement awards (as a result of the lawsuits)
- Costs to repair damage to computer systems and networks (reimburses the cost for tech expertise)
- Free credit monitoring for affected customers (most states require it)
- Charges to recover encrypted data (tech assistance to reclaim lost data)
- Cyber extortion and ransom demands (covers ransom paid for the code to unlock your data)
- Ransom negotiations (help from experts who have done it before)
- State and federal fines and penalties (fees vary based on the state you're in)
- Computer fraud (coverage kicks in when a computer is used for information theft, denial of service schemes or hacking)
- Loss of transferred funds (money transferred to an impostor)
- Loss of revenue and business interruption due to a cyberattack (when your website, network or computer records are inoperable and you temporarily close to repair them)

- Dependent business interruption system failures (if other networks or vendor networks go down and you lose business because of it)
- System failures of outsourced providers (if your vendor or partner providers are compromised)
- Betterments (replaces damaged systems with upgraded systems)

Cyber liability options in detail

Once you understand your options, it's easier to make informed decisions. Take a deeper dive into the cyber liability pool with the information below.

Cyber liability coverage:	**What it's for:**
Forensic investigations	Costs related to computer forensic analysis. Forensics can reconstruct how a data breach occurred, identify the stolen data and assist with restoration. (Data reconstruction might be a separate endorsement, so check with your agent.)
Litigation (defense) expenses	Defense costs related to the data breach. Check the limits and the wording on this one. Legal bills could exhaust your coverage before your claim completes (unless you've named separate defense limits on the policy). Excess or umbrella insurance could help, too.
Regulatory defense expenses or fines	Expenses associated with state or federal laws. You might have to defend yourself in civil court and pay fines or penalties for noncompliance with existing data protection policies (like the Consumer Data and Privacy Security Act).
Cyber event response coaching	Proactive consultation. Depending on the policy, you might get free, proactive advice from a data response coach (usually a lawyer) on compliance and security to prevent a breach. Check with your agent about this valuable coverage.
Crisis management or reputational damage	Public relations and customer notification. You'll incur costs to notify customers about the breach. You'll also have to pay for free credit monitoring services and release statements about how you're handling the incident and the steps you're taking to prevent a future breach. You'll probably need a company to do these things for you. (Some policies have a complimentary service, while others reimburse your expenses.)

Business interruption and losses	Lost business due to a security breach. If a malignant hacker takes down your website or ordering system, your clients (and vendors) won't be able to do business with you. Depending on the hack, you could lose weeks of revenue while restoring your systems.
Cyber extortion or ransom demand	Negotiations. If a nefarious hacker locks you out of your network and your data is encrypted, you'll need help negotiating the demands. (Think about losing the use of your email, client resource manager, website, e-commerce, proprietary data, ordering systems, fleet tracking or GPS.)
Betterments	Upgrade after an attack. A betterments endorsement can help offset the cost of replacing hardware or software after a covered data breach. After the attack, you'll probably need the upgrades to correct any vulnerabilities. You might even be required to make the upgrades as part of your claim settlement.
Post-breach first party	Helps when your system is breached. It can help with data restoration, client notification and forensic analysis (for proof of the attack and how it happened).
Post-breach third party	Helps when your client's system is breached and they sue you for it. It can help with legal defense costs or forensic analysis to prove (hopefully!) you weren't the weak link that caused the breach. It's an asset to freelancers and businesses working inside their clients' systems.
Extended reporting period (ERP)	Extends the dates of coverage for reported claims. An ERP allows you to extend the dates that your insurance coverage will respond to a claim reported. It can be useful if you think you might have a claim reported against you after your policy has ended.
Claims-made basis	Claims are covered only if the claim is reported within the dates of the policy. A claims-made policy covers claims reported during the policy period or within the ERP. Check the declarations page of your policy for coverage dates and any extensions.
Per-occurrence basis	Claims are covered based on the date of the event. Per occurrence covers incidents that occur during the active policy dates, even if reported years later. It's unusual for a cyber policy to be on a per-occurrence basis.

Defense within limits	Legal defense costs and retainer fees are applied to the policy limits and reduce the overall funds available for coverage. If you have $750,000 in cyber liability coverage and spend $650,000 on legal costs, you'll only have $100,000 left for future expenses (like settlement fees, credit monitoring, fines or data recovery). Ask about separating defense costs from the rest of your cyber policy or look into commercial umbrella coverage.

The cost of a cyber policy

Cyber liability insurance is priced based on your business risk exposure. Companies that process payment information or store personally identifiable information are at the higher end of the price spectrum. Cyber insurance is highly customized, so you can design coverage to suit your needs and budget. Depending on the deductible and your business risk rating, you could get $1 million in coverage for less than $2,000 per year. (Not too bad when you weigh it against the cost of mandated credit monitoring services.)

Your agent can help with the moving parts

Cyber liability insurance responds to many interrelated moving parts, and the policies themselves can get just as complicated. That's where your agent comes in. They'll help you insure the gaps by zeroing in on your risk exposure areas and matching you with the best policy for your risk level. Give your agent a call — they're happy to explain the details (no tech experience required)!

JLK Group

(443) 303-0393
info@jlkinsurancegroup.com

JLK Group
7524 Main St.
Ste. 202
Sykesville, MD 21784
www.jlkinsurancegroup.com

Agency Locations

Annapolis Office - 1125 West St., Ste 208, Annapolis, MD 21401

Sykesville Office - 7524 Main St., Ste. 202, Sykesville, MD 21784

Professional Liability. Office Package/General Liability and Property. Worker's Compensation. Home. Auto. Life. Health. Disability. Surety.