# CYBER LIABILITY INSURANCE PROTECTION

WA GROUP
100% Employee Owned

WINONA ROCHESTER SAINT PAUL LA CRESCENT WALiveBig.com

Cybercrime is on the rise, and small business owners face the highest risk. Now, more than ever, companies must step up to the plate to protect themselves from data breaches. After the Coronavirus onset, business owners have had to adapt to virtual operations, work-from-home employees, and online processes.

However, many companies fail to recognize that they're leaving themselves vulnerable to a myriad of cyber threats. Only a minority of business owners have a cybersecurity strategy, employee readiness training, or an insurance policy in place.

## Impact of COVID-19 on Cyber Security

According to a recent study, internet crime has increased by 600% since the onset of the pandemic. The average cost of these attacks is tremendous and can leave small business owners in dire circumstances. Most cybercrime takes place in the US, and 43% of attacks target small businesses. Over half of these companies are forced to close their doors just six months following an incident.

The statistics reveal how severe the impacts of COVID-19 have been. But what is at the root of this surge in cybercrime? Several factors are contributing to increased attacks, such as:

- Employee negligence
- Third-party mistakes
- System errors
- Hacking attempts
- Lack of readiness

Most small business owners aren't adequately prepared for a data breach and haven't invested in a cybersecurity plan.

## Cyber Threats on the Rise

The health crisis has further complicated matters as hackers take advantage of new opportunities to pursue malicious activities. A rise in work-from-home conditions has led to more frequent attacks, including:

- Malware – Viruses, spyware, and adware that damages system data
- Phishing – Targeted emails that trick individuals into releasing confidential information
- Ransomware – Holds data hostage until companies pay attackers
- Cryptojacking – Unauthorized use of a PC to mine cryptocurrency

Nearly all, 98% of cyber breaches involve social engineering tactics. Using this approach, hackers attempt to manipulate individuals into providing sensitive data psychologically.

The need for counteracting these threats has never been greater. Luckily, companies can proactively mitigate the risks of digital data. A comprehensive Cyber Liability Insurance policy combined with a clearly defined response plan can prepare your business for potential attacks.

## Cyber Insurance Overview

Cyber Liability Insurance can protect your business from the financial impacts of cybersecurity breaches, data loss, and your reputation. Typically, your policy will help cover the following expenses in the event of a cyber attack.

- Legal defense fees
- Notifying customers of data breaches
- Restoring consumer data
- Recovering lost or damaged files
- Repairing computer systems
- Credit monitoring

Your Cyber Insurance may include different types of first and third-party liability protection. Depending on your company's unique exposures and data protection concerns, your insurance agent can help you design a policy specifically for these risks.

## First-Party Coverage

First-party Cyber Liability Insurance covers directly-related business expenses that incur as a result of an attack. For example, your first-party coverage can help pay to restore your data or notify clients about losses.

### Electronic Data Loss

Following a cyberattack, you'll likely need to repair, restore, or replace software, data, and other electronic systems that were damaged. In most cases, your policy can cover the cost of hiring data reconstruction professionals. This coverage is designed to bring your organization back to “pre-loss” conditions, not improve upon or upgrade IT systems.

### Cyber Extortion

Cybercriminals often threaten to damage data or prevent a victim's access to it until a ransom is paid. Your insurance coverage can help pay for the expenses of paying for this extortion and other necessary actions to protect data.

### Notification Expenses

In most states, the law requires business owners to notify customers of data breaches and provide credit monitoring. These costs can be substantial, especially for companies that have to set up a call center first.

### Income Loss

During a cyber attack, you may incur additional expenses to avoid system failure. Your Cyber Insurance policy could help pay for the income losses you suffered if the income loss is determined to be direct result of a cyber attack.

## Third-Party Coverage

Third-party coverage can cover costs incurred when affected parties file a claim

against your organization. For example, another company or a customer could sue for negligence if they suffered a loss due to a system breach.

### Network Security and Privacy Liability

If a business partner, vendor, or customer sues you for negligence if you cannot protect their data from a cyberattack, Privacy Liability could help cover the costs. Your policy may cover other types of negligent acts resulting from a data breach.

### Errors and Omissions

If you're unable to deliver services to customers during a cyber attack, your Errors and Omissions coverage may help pay for legal and indemnification expenses resulting from negligence or breach of contract claims.

### Network Business Interruption

Many businesses rely on a network provider to complete daily transactions and processes. If your network partner shuts down due to a cyberattack and can no longer operate, your company could suffer severe revenue losses. When your third-party provider experiences a system or security failure, coverage can help compensate you for your resulting losses.

### Media Liability

This type of third-party liability coverage can protect you from expenses related to unintentional electronic copyright infringement, defamation, and invasion of privacy lawsuits.

## Cyber Insurance Policy Enhancements

Aside from the standard first-party and third-party coverage options, there are endorsements and enhancements that you may consider. The coverage options below can offer particular value to business owners, susceptible to security breaches. (Availability of these endorsements are dependent upon class of business, and insurance carrier.)

### Bricking

Some cyberattacks cause permanent damage to hardware, making it unusable. Bricking coverage can help pay for the cost of replacing computer systems, servers, and damaged hardware that your company needs to perform its everyday activities.

### Reputational Harm

Following an attack, your brand could experience reputational damage and profit losses as a result. For example, if a data breach occurred and went public, you could lose hundreds of loyal customers. Reputational Harm coverage can offer income loss compensation for a predetermined timeframe.

### Social Engineering

Hackers and cyber criminals prey on the element of human error, giving the attacker financial gain. Social Engineering coverages pays for losses that occurred due to a cyber criminal tricking an employee of an

organization into transferring funds to the fraudster. Since the funds are parted with willingly, it is specifically excluded under the Crime policy.

## What's Not Covered Under Cyber Insurance

Business owners should be aware that Cyber Liability Insurance has limitations like most other coverages. Typical exclusions include the following.

- Future profit loss
- Upgrade expenses
- Loss of intellectual property value
- Intentional acts of fraud

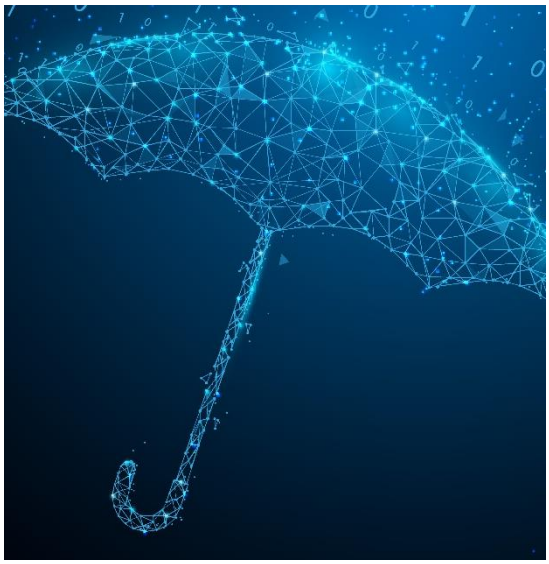
It's highly recommended that you speak with your insurance agent about which incidents are covered or not.

## Who Benefits From Cyber Insurance?

For some companies, operating without coverage could be a dangerous game of roulette and merely a matter of time before becoming the next victim of a cybercriminal. Nearly every business that meets any of the criteria below can benefit from Cyber Liability Insurance.

- Companies with computers, servers, or mobile devices
- Businesses that accept digital payments and credit cards
- Firms that store confidential information
- Medical practitioners with electronic patient records
- Financial institutions with digital data

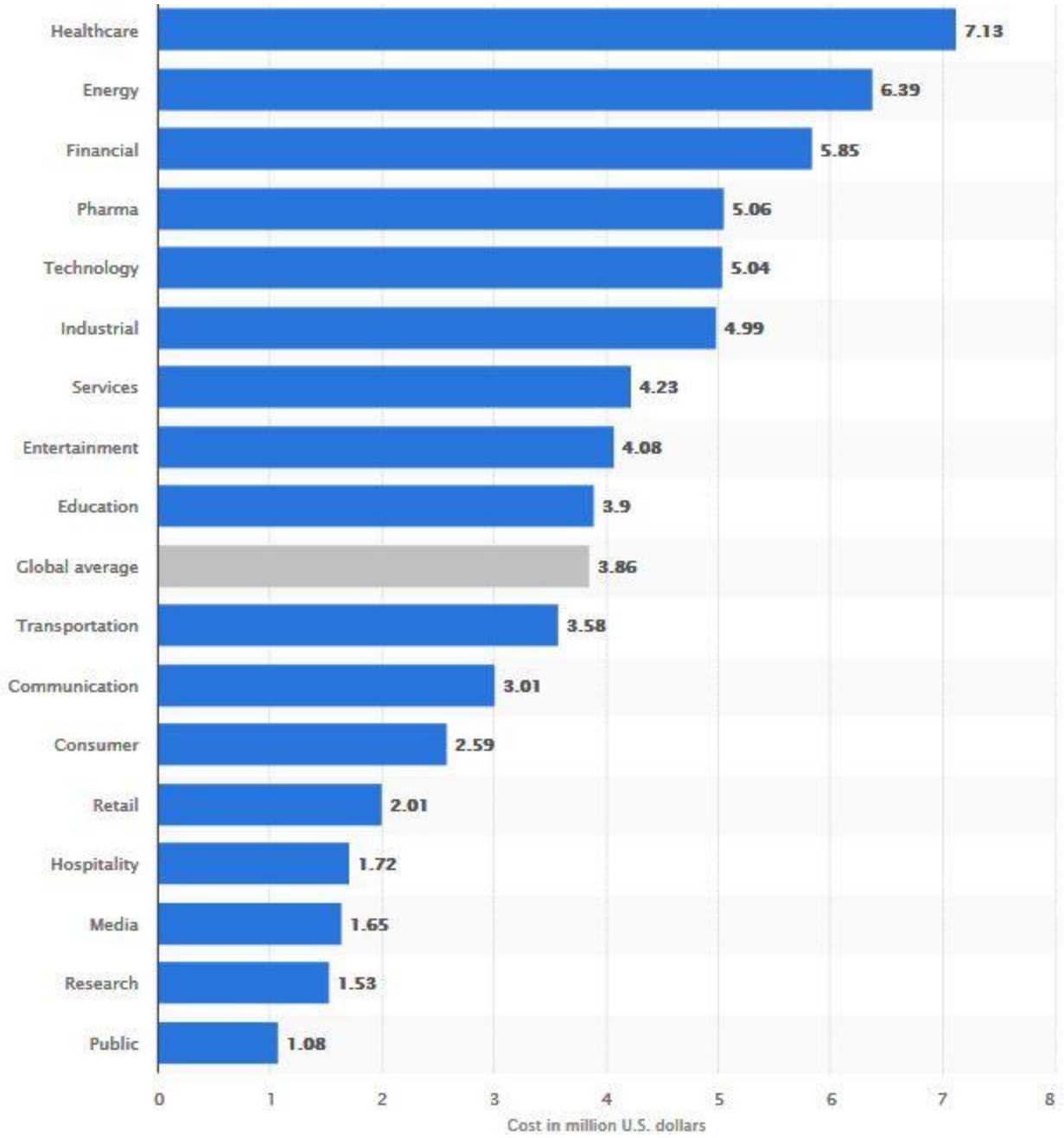
Regardless of your company's size, Cyber Insurance offers your business protection from detrimental claims that could damage your revenues and your brand's reputation.



## Average Cost of Cyber Security Breaches

Cybersecurity breaches can cause financial ruin to companies, particularly owners of small businesses. On average, cyberattacks cost businesses $200,000, regardless of size. While large corporations can handle the blow, most SMEs cannot, and nearly half of all incidences target smaller companies.

Some industries are more likely to experience expensive data breaches than others. Below are the average incurred expenses from cyber attacks in different industries around the globe.




[Global Data Breach Costs]

Industries at the highest risk of experiencing security breaches tend to have valuable electronic data. Recently, scammers have become savvier in their delivery techniques, attacking through fake invoices, point-of-sale systems, and other cleverly-disguised tactics.

Many hackers go after small businesses because they perceive them as easier targets. Smaller companies are more likely to use personal computers, weak passwords, and overlook security issues or updates that make their systems easier to access.

## Tips for Enhancing Cyber Security

You can protect your business from potential cybersecurity issues by establishing a strategy with best practices. Below are tips you can implement immediately to keep your company's data safe from breaches.

## Cyber Security Response Plan

You'll need a plan of action to follow in the event of a cybersecurity incident. Once you have a strategy in place, it's essential to ensure that employees understand it fully. Along with implementing a response plan, organizations should regularly do tabletop exercises with the entire organization to ensure there’s no gaps in the plan, and everyone knows their role when a cyber event occurs. Ideally, a cybersecurity response plan should include the following:

### 1. Hardware and Software Protection

Ensure that the latest updates are installed on all systems, devices, and software. Out-of-date web browsers and operating systems make it easier for attackers to access your data.

### 2. Essential Data Backups

Complete frequent backups of business files and information that your company needs for its daily functions. Automatic backups can move copies of critical documents to a cloud or offsite location where you can access them in an emergency.

### 3. Secure WiFi Connection

Encrypted WiFi password protection provides additional security, so hackers can't steal your data via your internet connection.

### 4. Firewall Protection

Securing your internet connections with a firewall helps block outside attempts to access information on your server. Employees working from home should also have firewalls, and antivirus software enabled.

### 5. Employee Education and Training

Train and inform employees of best practices that can minimize their risks. Companies of all sizes should ensure employees acknowledge internet protocol guidelines, written cybersecurity policies, and carrier breach response plans.

### 6. Controlled Device Access

All employees should have their usernames and passwords to access company computers and electronic records. This step helps prevent unauthorized individuals from stealing or editing private information.

### 7. Strong Passwords

Use strong passwords that are unique and change them quarterly throughout the year. For additional security, consider hiding sensitive data behind two-step or multi-factor authentication.

When it comes to protecting your organization's electronic data and vital records, you want to ensure that your entire team is on board. Written copies of privacy

policies and periodic reviews of best practices can help employees respond to threats more appropriately.

**8. Multi-Factor Authentication (MFA)**

MFA is an electronic authentication method in which a computer user is granted access to a website or application only after successfully presenting two or more pieces of evidence to an authentication mechanism. An example of MFA is having a code texted to a cell phone that needs to be entered into the website or application the user is attempted to gain access too.

## Cyber Liability Claims Examples

Below are a few hypothetical scenarios to explain how Cyber Insurance can save the day.

### Example 1

One of a store's employees is checking the inbox when they open an attachment that appears to be from one of the retail partners. Unknowingly, the phishing scam gave a cybercriminal access to customer records. The individual uses ransomware to bring online sales to a halt until they receive a hefty payment. Cyber Liability Insurance could help pay for the expenses to resume business as usual.

### Example 2

A physician's cloud storage provider is hacked, compromising patient privacy. As required by law, the small business owner must inform all affected individuals and provide credit monitoring. A Cyber Insurance policy can help pay for the costs of notifying clients of data breaches, hiring a forensic analyst to determine what information was compromised, and other regulatory responsibilities.

### Example 3

An online attack leaves a company's electronic booking process unavailable, and customers aren't happy. Fortunately, the Network Business Interruption coverage helps pay for the losses and the recovery of the digital property. Without the policy, the company couldn't have covered the extra expenses of getting their website back online.

## How WA Group Can Help

Cyber Liability Insurance policies require careful consideration of a business's unique risk profile. Because of the severity of the threats involved, coverage protection details can become exceedingly complicated.

Small and mid-sized business owners can benefit from working with experienced agents familiar with the financial impacts of

data breaches and cybersecurity losses. The WA Group is the only 100% employee-owned, Employee Stock Ownership Plan (ESOP) company in Minnesota with an executive risk expert.

We're dedicated to helping your business avoid and prepare for potential cybersecurity breaches. Find out more about **Cyber Liability Insurance** from our executive risk expert at the **WA Group** at **(507) 452-3366**. We look forward to answering your inquiries.