SolCyber

What Does Cyber Insurance Cover?

A Comprehensive Guide for SMEs

SolCyber

$4.24 million. That's the cost of an average data breach in the US. And in a world where hackers move faster than ever before and cybersecurity threats are increasingly more advanced, data breaches are bound to happen.

No matter how well-protected you are, the risk of being affected by cybercrime is still present. And as a small to medium-sized enterprise (SME), you need to make sure you are covered in the event of a breach. For many SMEs, procuring cyber insurance is a relatively easy and cost-effective option to offset the financial damage that can occur due to a security compromise.

What does cyber insurance cover though?

In this article, we'll take the clearest and most comprehensive path to discuss the benefits of cyber insurance, as well as what cyber insurance covers. Read on to find out more.

Why Cyber Insurance for SMEs?

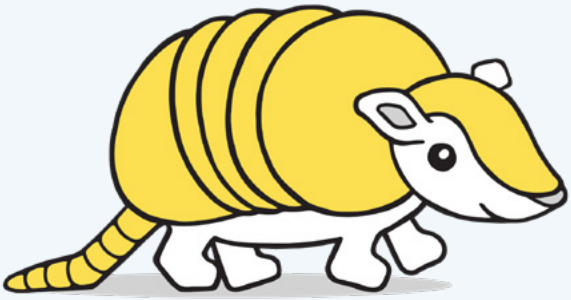
Smaller businesses may feel like they're less likely to be attacked by cybercriminals. After all, there are bigger fish in the sea, right?

Wrong.

Cybercrime is at an all-time high. In mid-2022, cybercrime rates have already increased by more than 15% as compared to 2021. And some studies forecast cybercrime will continue to grow -- to the point where the world will lose more than **$10 trillion** to it.

The worst part of it all?

No business, large or small, is safe from cyberattacks.



In 2021, nearly half (41%) of SMEs had been affected by cyberattacks. Despite that, only a small percentage of SMEs have cyber risk insurance, with some reports showing numbers as low as 7%. However, we recommend seriously considering cyber risk insurance for the following reasons.

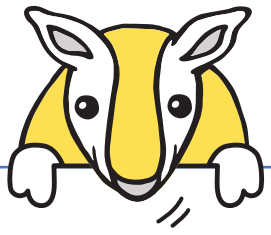
It helps you offset the financial impact caused by a data breach
Depending on the policy you get, cyber risk insurance can cover various expenses related to the initial recovery, investigation, as well as privacy compliance costs. This includes hiring a privacy attorney to consult on the regulatory implications, computer forensics team to identify how the cybercriminal entered the network and what data was exfiltrated and a PR company to help with damage control. Cyber insurance can help you access resources that can help you get your business back on track after a cyberattack. They can also help cover the cost of credit monitoring and identity theft restoration services, which may be required depending on the type of information that's been affected.

Improves the balance sheet of a company. Cyber risk insurance improves the financial position of a company by transferring the financial risk off of the balance sheet and on to an insurance product, ensuring the company's financial position post-attack is strong and the company is capable of remaining operational. Additionally, it's an excellent risk mitigation tool, which can help in a variety of situations, particularly when you are seeking investors.

It helps you strengthen your cyber resilience. By investing in cyber insurance, you are also investing in your company's ability to protect itself from cyberattacks and bounce back after a data breach. Cyber insurance can help you access the resources you need to get your business up and running again as soon as possible. One of the most valuable features of a cyber risk policy is the panel of service providers who work with policyholders pre and post breach to avoid and mitigate an attack.

Different types of cyber insurance coverage will help you in different situations, so it's crucial not only to get cyber insurance as soon as possible but also to get the right type of coverage.

A cyber risk policy provides very robust coverage to policyholders and is bifurcated between first-party expenses and third-party liability types of losses.



Cyber Insurance: First-Party Coverage

Given everything mentioned so far, you'll want to ensure your business is both protected from cybercriminals and capable of navigating the aftermath of a potential cyberattack.

First-party coverage cyber insurance is designed to do just that -- help you recover from a data breach and get your business back on track. In essence, the "first-party" element of this type of insurance coverage refers to who, more exactly, is affected by the cyberattack

In other words, first-party coverage will pay expenses incurred to your business to recover when there is a breach to your company's network. Outside of the world of cybercrime, first-party coverage would respond similarly to commercial property insurance, for example, where the policyholder is the one that suffers the loss -- and the one that will be covered if something happens with the property.

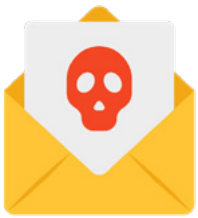
What Does First-Party Cyber Insurance Cover?

First-party coverage is comprehensive, meaning it can cover a wide variety of expenses related to data breaches and cybercrime. These include:

Cyber extortion (such as ransomware payments)

Ransomware is one of the most common types of cybercrime, and it can have devastating consequences for businesses. With ransomware, cybercriminals will encrypt your data and demand a ransom payment to decrypt it.

Depending on the policy, first-party coverage would pay the ransom payment, up to the limit, and assign a consultant to negotiate with the cybercriminal to reduce the ransom request, secure access to your data, and ensure it's usable. It will also cover costs associated with digital asset damages and recovery related to the ransomware attack.



Lost revenue associated with the cyberattack (including business interruptions)

First-party insurance will also cover lost revenue associated with the cyberattack and which is directly correlated to business operations. For instance, if you've suffered a business interruption as a result of a cyberattack, your first party coverage may include reimbursement for lost business income incurred for the time your company was not operational due to the attack. It would also pay those extra expenses incurred to get your network back up and running.

Costs related to investigation, recovery, and remediation

Mitigating the immediate impact of a compromise is absolutely crucial to ensure a business functions properly. First-party cyber insurance coverage is likely to cover the costs related to a security incident investigation, recovery, and remediation. Few SMEs have the capabilities of conducting these response actions in-house so they'll likely bring in a third-party. Having those costs already covered can help organizations move quicker after a security compromise. In most cases, the insurance carrier has a panel of expert service providers who focus on nothing but these recovery responses 24/7/365, putting you in very capable and practiced hands.

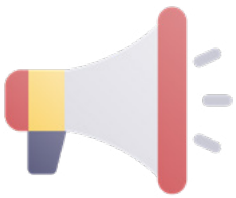
Post-incident response (such as risk and vulnerability assessment)

Having a quick and apt response to cyberattacks is one thing but making sure you know the cause so you can protect your business from similar attacks is equally as important.

This is where the post-incident response comes in. Identifying how a compromise occurred, fixing exploited vulnerabilities, and conducting a comprehensive risk assessment will help reduce your risk of a repeat compromise and help you focus on running your business. Your first-party cyber insurance policy can help you with costs associated with this. 67% of companies who have suffered a data breach suffer another one within 12 months.

Fines related to compliance and regulations

This type of cost is relevant if there's an investigation and you're found to be non-compliant or negligent. For instance, if you have (unknowingly, perhaps) breached one of the GDPR laws and someone in the EU reports it, you might have to pay a fine (which can get very hefty.) In this situation, your liability insurance might cover this fine.



Post-breach services, such as communication, PR, and credit monitoring

Data breaches are a public matter, and you will need to be very careful about how you communicate what happened. In some cases, it's often best practice to hire a professional PR firm to help you manage the fallout. These costs are often covered by your cyber risk insurance policy.

To give you a bit more context, here are some of the more common scenarios in which first-party cyber insurance coverage can be claimed:

- Your data has been breached and it is now held hostage. The cybercriminals will only release it based on a ransom.
- Your business has been forced to shut down operations following a cyberattack, and you are now losing revenue. You need to hire a team to help you mitigate the damage and get your business up and running again.
- A cybercriminal (or a team of them) destroys all of your data and you need to recover it or restore it via back-up servers.
- Hackers launch a Denial-of-Service attack on your business, bringing your site down.
- Someone (maybe within your company) accidentally destroys or exposes a database.
- Hackers plant malware or a virus within your network.
- A power surge or a storm affects your databases.

In short, first-party cyber insurance can cover pretty much any scenario in which your business is affected by a cyberattack to your company's network or even in the case of a security incident as a result of an accident or negligence.

Cyber Insurance: Third-Party Coverage

Also known as "liability coverage", this type of cyber insurance is meant to help businesses that are held liable for damages following a breach. This coverage pays for the financial harm that comes to third parties as a result of your company's failure, error, or omission in protecting the privacy of others and the security of the network.

For example, if your business is responsible for a data breach that affects your customers, they might sue you for the damages. This is where third-party cyber insurance coverage comes in: it can help you cover the legal fees and damages of the lawsuit.

Likewise, employees or business partners might also be entitled to sue you if their data is leaked through your company. Liability coverage can help you in these situations too.

What Does Liability Cyber Insurance Cover?

As the name suggests, liability cyber insurance is all about making sure that you are covered if your customers, employees, or business partners sue you in the event of a cyberattack.

Although this type of insurance might not cover as many use cases as first-party insurance, it is absolutely crucial if your business is storing or processing customer data, which is likely the case for almost any company. With GDPR (the General Data Protection Regulation in the EU), CCPA (California Consumer Privacy Act), and other regulations prioritizing protecting customer data, it is more than likely that you would be liable in the event of a data breach.

Third party liability cyber risk insurance will cover costs associated with this kind of liability, such as:

Legal fees

If your business is sued for a data breach, third-party cyber insurance can cover your legal fees, which can be quite expensive.

Defense in a regulatory investigation or proceeding

Depending on how a proceeding or investigation progresses, you may need to obtain a legal defense representative. This cost is covered under third-party liability cyber insurance.

Settlement fees

Likewise, if your business loses a data breach-based lawsuit, the settlement fees can be covered by your cyber insurance policy.

Do SMEs Need Cyber Insurance?

In short, yes, SMEs absolutely need cyber risk insurance. Here are three very important reasons why you should consider cyber insurance as an SME:

1. You have a small budget

This might be counterintuitive, but small businesses actually have a higher chance of being successfully targeted by cybercriminals. The reason is simple: they usually don't have the budget to invest in robust cybersecurity solutions and can often succumb to automated attacks because they lack foundational cybersecurity protections.

Additionally, even if you do have a small budget for cybersecurity, the costs of data breaches can turn your entire business upside down, and they can have an even more powerful effect on you, as an SME, than the effect they'd have on a large company.

2. Recovery will require additional parties

Because you're running a smaller enterprise, you may not have fully-fledged cybersecurity, risk, and PR teams hired in-house. Or they may specialize in areas outside of cybersecurity and data breaches. This means that, in the event of a cyberattack, you'll have to seek out these services externally. In this case, the costs of hiring agencies and companies to deal with the aftermath of a cyberattack can be offset by your cyber insurance policy.

3. You have a small(er) digital footprint

The cost of a cyber insurance policy can vary depending on your digital footprint - the number of devices, employees, locations, servers, etc. SMEs are likely to have smaller digital footprints, meaning they're likely to pay less for a policy.

In a world where a seemingly innocent cat video can be a cybersecurity risk, you need to protect your organization. If your business:

- Stores data on owned, physical servers, or in the cloud
- Handles a large database of customers and sensitive information
- Has valuable assets or nets a high revenue
- Has an internet presence
- Uses Wi-Fi connectivity
- Has a BYOD policy
- Has remote employees
- Uses email
- Has customer portals to the network to transact business

How to Get the Best Cyber Insurance Coverage

Understandably, the world of cyber insurance can be quite confusing, but SMEs can get help via key partners. A modern managed security provider can help make sure you get the best cyber insurance coverage there is.

Modern managed security providers like SolCyber can:

- Help provide proof to insurers that the right security controls are in place, which will increase the likelihood (and speed) of approval
- Help your organization get approval because they already have partnerships with A+ AM Best insurance companies and brokers (as SolCyber does with its SolCyber Insurance+ Program)
- Help you get better cybersecurity and discounted premiums (as much as 30%) on your cyber insurance

Want to learn more? Contact SolCyber at **hello@solcyber.com** for a confidential discussion.

TAKE OUR 3-MINUTE CYBER INSURANCE RISK QUIZ AND FIND OUT YOUR RISK SCORE!