

What is Cybercrime Insurance?

Cyber Insurance is specifically designed to cover a business's liability arising out of the events of cyber attacks or data breaching, which primarily involves the stealing of sensitive information, such as credit card numbers, health records, driver's licenses, or customer's account number.

The insurance plan covers a wide range of cyber frauds, such as hacking, e-mail spoofing, virus dissemination, web jacking, unauthorized online transactions, cyber bullying, cyber stalking, hurting business e-reputation, phishing, e-extortion, data diddling activities, and so on. Any cost arising from defending a cyber claim will be covered under the insurance plan to assist the business owner in coping with the unintentional loss or leakage of personal information.

Why Do Businesses Need Cyber Crime Insurance?

With the marked-up internet penetration, every business, no matter how small or big, is exposed to more than one kind of cyber fraud. Cybercriminals have developed sophisticated tactics (such as phreaking and social engineering fraud) to steal data, money or any other information of the company. This gives us the reason why data breaching and many other forms of cybercrimes have acquired commonplace in cyberspaces.

Cybercrimes can damage your business more than just damaging your computer system. It can go to the extent of damaging your business's reputation and putting your customer's data at a higher risk. With a Cybercrime Insurance plan, you can take smart precautions to cover against any loss arising out of cyber frauds.

Key Types of Cybercrime Insurance

The classification of cybercrime insurance can be done in two different forms. They are as follows:

1. For First-Party:

In this type of coverage, all the people directly involved in the event are covered. Typically, it covers a range of cybercrime issues, such as extortion, online theft, hacking, data destruction, etc.

2. For Third-Party:

The incident of cybercrime caused to clients or customers is covered under this form. Generally, the plan covers data breaches, data theft, errors, defamation, etc.

What are the Salient Features of the Cybercrime Insurance Policy?

Some of the key features of cybercrime insurance are enumerated below:

Shields All Devices:

In an era where plugging-in and synchronization across multiple devices have been taken a significant place, it becomes important to have cyber protection across all the devices you use.

As cybercrime insurance provides all-device coverage, you need not worry about having insurance separately for each one. Under a single plan, you can get a multitude of your devices covered.

What's the Typical Sum Insured?

In cybercrime insurance policy the options of the sum insured ranges from around Rs. 1 lakh to Rs. 1 crore. The amount of sum insured largely depends upon how much time an individual or organization spends online.

Eclectic Blend of Multiple Coverages!

Cybercrime insurance covers almost all losses that might arise due to any fraudulent online activities. A typical cybercrime insurance policy will provide wider coverage from phishing and data breaches to damaging e-reputation and theft of money.

Do You Want to Protect Your Family Too?

Cybercrimes can create turmoil among your family members and can affect them mentally as well as emotionally. In order to let your family browse without any worry, the cybercrime policy also provides add-on coverage of family cover.

Thus, you can now secure your family members in case damage or loss is arising out of cybercrime. The add-on typically covers the policyholder, his/her spouse, and two children (no age limit) so that complete digital security can be provided to the entire family.

How Limits of Policy are Determined?

On a general basis, the limit of cybercrime insurance policy depends upon the risk factor. Lesser risks mean lower limits, and higher risks mean higher limits. In the case of higher limits, a more comprehensive analysis of risk and assessment of underwriting is done to determine the limits.

Moreover, each clause of cybercrime policy has some sub-limits. For instance, a specific level of percentage is pre-determined for the cases of phishing or e-mail spoofing, which cannot be exceeded.

Who All Are Eligible to Take the Policy?

When talking about the eligibility criteria of cybercrime insurance, anyone who is above 18 years of age, can purchase the policy. Besides, it can be purchased by an individual or a corporation.

What Are the Benefits of Choosing a Cybercrime Insurance Policy?

360-Degree Protection!

Cybercrime insurance provides multifaceted protection to the insured person or organization in the following ways:

- **Prevents Hackers from Getting Hands on Your Information**

The policy protects the insured person or organization from any kind of fraudulent or unauthorized access by a hacker, which is primarily done to hack personal or confidential data.

- **Protects Your Identity**

Many cybercriminals tend to attack identity-oriented platforms, such as social media, which can result in identity theft.

For instance, one can steal your personal data and use your Social Security Number (SSN) to create a replica of your social media account. The information can be used without your consent to make a fraudulent purchase or to carry out other unauthorized tasks.

- **Scared of Digital Abuse? – The Policy Will Take Care of It Too!**

These days digital platforms are being used more as a medium to commit digital abuse. Besides hurting the sentiments of an individual or a company, digital abuse can lead to disastrous consequences.

To overcome this problem, a cybercrime insurance policy provides significant protection against threatening and harassment on online platforms. Any harm, loss, or damage caused by digital abuse will be covered under the policy.

- **Helps You Tackle with Malicious Programs**

Disseminating a virus is one of the most common methods adopted by cybercriminals to damage the system. Some of these malicious programs are superficially designed to go beyond just hacking the information. They can damage computer programs, delete important files, format hard drives, crash applications, and erode a computer's memory.



The cybercrime policy provides coverage to the damage caused by such malicious programs that can seep their ways through text message links, emails, downloaded files, etc.

- **Provides Protection Against Unauthorized Transactions**

The policy also protects you from unauthorized transactions, that is, wrongful payments done from your banking profile or e-wallets. Cybercriminals do this by intruding into your profile illegally.

- **Other Important Protections**

- - **Protection against phishing**, i.e., illegal attempt to capture your information, such as ID, passwords, usernames, credit card or debit card details, etc.
 - **Protection against the unintended publication** of content on digital platforms out of cyber-attack.
 - **Protection against the disclosure of your personal information** from a third-party computer system.

Be It a Third-Party OR First-Party – Cover Them All!

One of the greatest advantages of cybercrime insurance is that it provides liability coverage to both first and third parties. This simply means that everyone from individuals and employees to businesses and customers can achieve numerous benefits.

Expensive Legal Costs? – Save Them!

In order to file a case against any cyber-attack or fraudulent activity, a significant amount of money is required to win the lawsuit. From court proceedings and court hearings to the damage already done by the cyber-criminal, the cost may break your bank and cause immense mental and emotional pressure.

The cybercrime insurance policy assists you in covering firmly the costs of all legal proceedings, in case of any damage or loss caused due to the actions of cyber-criminal. Any costs arising in legal proceedings, such as defense costs, prosecution costs, transportation costs, documentation costs, etc. are all covered by the policy.

Premium Rates That Don't Bind You!

One can choose the premium rates from a few lakhs to some crores depending upon the risk factor and the type of industry. In case you wish to cover around Rs. 5 crores, your premium amount will range between Rs 5-10 lakhs. In case your industry is more vulnerable, you can double the coverage and so the premium rates will also double.

Thus, there is no hard-and-fast rule that you need to pay a fixed amount. After analyzing your industry type and risk exposures, you can leverage the flexibility by choosing premium options that suit you.

What Does a Cybercrime Insurance Policy Cover?

Email Spoofing:

Email spoofing is the manipulation or forgery of email headers to make the recipients believe that the email is from the original source. Thus, financial expenses and prosecution costs arising out of email spoofing will be covered under the policy.

Damage to E-Reputation:

A single troll can tarnish your name as an individual or an organization. The cybercrime insurance policy creates a shield against the threats or attempts of damage to your e-reputation.

Phishing:

Phishing can be defined as unauthorized access to various types of personal information, such as usernames, passwords, bank card details, etc. Any financial loss due to the leakage of sensitive information and the prosecution costs arising against the cybercriminal for phishing attacks will be covered.

Unofficial Online Transactions:

The policy also covers the loss or damage caused due to unauthorized online transactions from your bank account, e-wallet, or credit/debit card. In this way, you can easily save your hard-earned money at a nominal cost.

Identity Theft:

Identity theft is primarily defined as the process of using, deleting, or modifying personal data stored on either online platforms or computers. Any prosecution costs arising out of filing a case against the cybercriminal, transportation costs to the court, and documentation costs will be covered under the policy in case of identity theft.

Cyber Bullying & Stalking:

Any cost arising out of the damage or loss caused due to digital abuse, threatening, and harassment will be covered under the policy. Moreover, the costs arising out of legal proceedings, in case the insured person files a case, will also be covered.

e-Extortion:

The policy also provides protection against blackmailers, malware attacks, and ransomware attacks. The cost of restoration, transportation to the court, prosecution, and documentation will be covered.

Business Interruption Costs:



In case there is a business interruption after the event of a cyber-attack, such as loss of income, etc., the respective cost of business interruption will be covered under the policy.

Forensic Coverage:

In case there is a need for forensic investigation after a cyber attack, the costs associated with the operation will be also be covered by the policy.

Restorative Work Coverage:

In case of data loss, the costs associated with the restoration process will be covered under the policy. Everything from repairing to replacing the damaged computers will be taken care of by the plan to bring things back in order.

Litigation Coverage:

The costs of obligatory meetings due to lawsuits, court judgments, fines, and penalties will be covered by the policy.

Social Media Liability Coverage:

Any cost arising due to social media attacks, such as the financial loss due to identity theft, prosecution cost, documentation, and transportation cost will be covered.

Liability for Privacy and Data Breach:

In case there is an unsanctioned disclosure of private or confidential information, the cybercrime insurance policy covers the liabilities arising out of such breaches. All the legal expenses can be claimed by the insured person or company.

What's Not Covered Under the Cybercrime Insurance Policy?

Under the cybercrime insurance policy, the following things are not covered:

Physical OR Bodily Injury:

Any physical or bodily injury arising out of a cyber attack.

Pre-Existing Loss:

Any loss or damage occurring before the beginning of the policy.

Offline Operations: Any fraudulent activity done through offline mediums will not be covered.

Property Damage:

Any kind of property damage caused due to a cyber attack.

Unsolicited Communication: Any kind of telephonic conversation, fraud, or spam.

Cryptocurrency Loss: Any kind of fraud witnessed in online trading, such as loss of cryptocurrency, shall not be covered.

Dishonest Conduct: Any kind of dishonest, unfair, or improper conduct of the policyholder to get a claim.

Technical Failures:

Any loss of data due to mechanical failures, media malfunction, electrical disturbances, or network disturbances will not be covered.

What's the Claim Process for Cybercrime Insurance?

1. Submitting Claim Form:

The policyholder must fill up the claim form and submit it within 90 days of the incident of cyber-attack.

2. Gathering & Submission of Required Evidences:

All the required pieces of evidence of loss asked by the insurance company must be submitted as soon as possible.

3. Investigation:

Once the claim form and required evidence reach the insurance company, an investigator will look into the case.

4. Verification:

If the investigator finds that all the pieces of evidence are indicating towards the incident, he/she then sends a green signal to the claim.

5. Claim Settlement:

After verification is done, the company pays the compensatory amount to the policyholder. In case the claim is rejected, the claimant is informed about the same.

Documents Required for the Claim Process

- Duly filled claim form
- Forensic or investigation reports
- Details of the loss or damage, such as date, place of incident, etc.
- Evidence of the loss or damage, such as witnesses, screenshots, etc.