**Cyber attacks** are very common in today’s corporate world. Consequently, they are becoming an increasing concern for organizations. With **cyber incidents** of different intensity and nature happening everyday all over the world, businesses are turning to cyber insurance as a way to protect themselves from harmful effects of **data breaches**. In this article, we will discuss what is cyber insurance, how does cyber insurance work, what are the types of cyber insurance, and why cyber insurance is necessary for your organization?

# What is Cyber Insurance?

Cyber insurance is a policy that allows organizations to stay protected from the adverse outcomes of a cyberattack or **security breach**. By having a cyber insurance policy, there is minimal disruption in business after a cyber incident actually occurs, along with potential covering of financial cost of elements involved in the attack.

However, cyber insurance cannot **protect your business** against everything. Your organization needs to ensure that it fully understands what **cyber insurance covers** and what it doesn’t cover when signing up to a coverage plan. While **insurance companies** can help businesses in times of a cyber-attack, the **cyber security** of a company is ultimately its own responsibility. It isn’t something that is entirely shifted to the insurance company.

# How Does Cyber Insurance Work?

Cybersecurity insurance policies are offered by most of the suppliers that also sell related **business insurance**, such as business liability and commercial property. Most of these policies cover first-party coverage which includes losses impacting a company directly. They also include third-party coverage, applying to losses that are suffered by a third-party as a result of a **network security** breach or incident.

First **party coverages** include the cost of **insurance work** such as investigating the cyber crime, recovering lost data and restoring information lost during the incident. It also covers the recovery of income lost as a result of the business shutting down, managing reputation, notification costs, and extortion payment by cyber criminals.

Organizations are obligated to keep the Personally Identifiable Information (PII) and Personal Health Information (PHI) of their customers protected. If this information is exposed in the event of a data breach, they may face liability. Third party **cyber risk** coverage includes the cost of legal defense against claims of GDPR breach, crisis communications, digital forensics team, and setting up **credit monitoring** and call center for parties affected by the breach.

# Types of Cyber Insurance

The types of cyber insurance packages can take many different categories and forms, depending upon the criteria. For instance, it can by classified on the basis of locality, coverage, or risk. However, the following are generally the key types of cyber insurance available for individuals and businesses.

**First Party Cyber Insurance**

In this case, insurance packages are designed to pay for the damages, costs, and inconvenience caused to the owner due to the security breach. Some of these are as follows:

***Fraud and Theft***

This policy covers payment for the costs arising out of data loss due to fraud or theft. It may also cover **risk management** of crimes resulting from dishonesty or fund transfers.

***Forensic Work***

This policy covers the cost of conducting forensic investigations. It pays for all legal and technical services required to meet the standardsof the presiding court.

***Business Interruption***

This type of cybersecurity insurance policy covers the costs of **business interruption** after an incident. This is identified by the policy holder being unable to carry out routine business due to the cyber attack.

***Blackmail and Extortion***

Many cybercrimes involve blackmailing and extortion by the criminals to destroy the **intellectual property** of a company if it fails to pay a ransom amount. The policy holder many pay the amount to save themselves from reputational damage, or at times to help assist in collecting evidence against the perpetrator.

***Loss of Data***

A first party insurance coverage policy may cover the costs of data loss and restoration required to bring the operations back to normal. These costs may include repairing and replacing damaged **computer systems** and other organizational assets such as **electronic data**.

**Third Party Cyber Insurance**

Difference packages in third-party coverage are as follows:

***Litigation Coverage***

It covers costs incurred on meeting obligations arising out of lawsuits, court judgements, fines, and penalties imposed as a result of an incident.

***Regulatory Coverage***

This type of insurance helps in covering costs for all technical and forensic services that are carried out while responding to a government order or request. It may cover costs incurred after an incident where the government wants to know the causes of the incident and prevent it from happening in future. It may also pay if the policy holder is fined after an inquiry.

***Notifications and Communications***

It covers costs related to communicating with stakeholders about the incident and how you are dealing with it. These stakeholders may be your clients, employees or third parties.

***Emergency and Crisis Management***

This type of insurance deals with emergency or unexpected events requiring extraordinary responses, such as putting warning signs to the public after a **security breach**.

***Credit Monitoring and Review***

If a policy owner has to work on **credit monitoring** and review along with anti-fraud procedures, this policy will compensate them.

***Media Issues***

This package covers expenses regarding media overtures after an incident. It may also cover your costs in case of copyright infringement that may cause insurance costs to be met for avoiding any further **general liability**.

***Customer Privacy***

This type of insurance policy covers the costs that may arise as a result of breach of customer confidential information, such as [bank account](http://www.cardzgroup.com/ContactSmartCard.html) details of customers.

# Why is Cyber Insurance Necessary?

If your business deals with sensitive customer data like names, bank details, or addresses, you need to protect this data as it can be compromised during a **cyber attack**. You will also need to protect yourself against financial losses that may be incurred as a result of heavy fines if your customer’s PII is leaked, stolen, or lost.

If your company is subjected to a breach, a cybersecurity insurance can help you as a lifeline, while legal fees, potential fines and claims keep adding up. However, it is also important to ensure that you follow all security best practices necessary to protect your business, since having an insurance policy alone cannot prevent a data breach or cyber attack. Before you make a claim, it is expected that you have all these proactive measures in place.