WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Cyber Insurance

Anu. P

B.com., LLB (Hons), School of Excellence in Law, The Tamilnadu Ambedkar Law University, Chennai

ABSTRACT

Cybercrime is becoming common in the developing internet-based world. Cyber risks are faced by the business more often. The growth of ransomeware attacks made way for the expansion of Cyber insurance policies. Cyber insurance companies are acting as compliance managers. It indemnifies the loss or damage incurred due to the cyberattacks. This article provides a clear view of cyber insurance in various aspects like (i) what is cyber insurance, (ii) what does it cover, (iii) what does it not cover, (iv) initiatives taken by government of india for cyber security, (v) eligibility criteria to opt for cyber insurance, (vi) history of cyber insurance, (vii) Position of india, (viii) Information Technology Act, 2000, (viii) importance of cyber insurance, (ix) future of cyber insurance, (x) case laws on cyber insurance, (xi) how to claim for cyber insurance. This makes it clear how insurance companies play their role in compensating the loss or damage of the enterprises whose business relies on the internet or who maintains an electronic record.

Keywords: Cybercrime, Cyber insurance, ransomware, indemnifies, internet-based.

Introduction

Cyber insurance is a policy framework to indemnify the loss or damage suffered by the business or even individuals from cyberattacks. Cyber insurance is otherwise known as cybersecurity insurance or cyber liability insurance.

Cyber insurance generally covers the business's liability for data breach involving sensitive customer information.

Cyber insurance will protect the insured person from the first party, third party and additional costs.

Insurance regulatory and development authority of India (IRDAI)[1] set up a committee which recommended cyber insurance.

These insurances are becoming necessary in the upcoming era as most of the industries or companies depend on internet-based technology for conducting their work.

What does it cover?

Cyber insurance covers the area of cyberattacks such as[2] :-

- **Identity theft** : It refers to the theft or unauthorized access to personal data, or deleting or altering of such data. The legal expenses incurred by the parties for such an act will be compensated or indemnified.
- **Cyber stalking** : It is the behavior of harassing or threatening the other person. It is a continuous process consisting of a series of actions each of which may be entirely legal in itself. The insurance covers the cost of prosecution.
- **Malware attack** : These attacks are the common cyber attacks and refer to various malicious programs. This occurs by way of sending text messages, emails or causing harm to computer, server or computer networks. It can take many forms.The affected party can claim insurance at the cost of restoring the computer, server or computer network after a malware attack.
- **Phishing** : A cyber attack which steals the personal data or causes financial loss or revealing of personal information through a website unknowing of the fact that will cause loss to them. The financial loss or prosecution expenses will be indemnified.

[1] The Insurance Regulatory and Development Authority of India (IRDAI) is a statutory body under the jurisdiction of the Ministry of Finance , Government of India and is tasked with regulating and licensing the insurance and reinsurance industries in India. It was constituted by the Insurance Regulatory and Development Authority Act, 1999,an Act of Parliament passed by the Government of India.

[2]https://www.paisabazaar.com/commercial-insurance/cyber-security-insurance/

- **Email spoofing** : An act by the cybercriminal with an intent of getting the personal information or business information or stealing money by way of sending an email by impersonating a person who is known to that target person. The financial loss incurred or prosecution fees,if a case is filed against a third party, will be compensated.
- **Media liability claims** : it refers to intellectual property infringement. Defense cost, Prosecution cost, and transportation cost to the cost will be indemnified by the cyber insurance.
- **Cyber extortion** : The hackers execute these attacks through a link containing malicious software. When the victim clicks the link, the hacker can get access to the victim's storage or data and demand money or payment in order to get it back.The amount of loss and prosecution cost will be compensated.
- **Privacy and data breach by third parties** : Act of getting information without one's knowledge. Legal fees incurred by the victim due to the damage will be compensated.

In order to be compensated, the loss must have been caused by the aforesaid attacks. The loss or damage should be of insurable nature. Cyber insurance will protect the insured person from the first party, third party and additional costs.

What does it not cover?

Cyber insurance does not provide coverage to infringement of intellectual property rights, physical harm, loss which is caused through electronic or mechanical failure or through activities which are illegal, loss of currency which are not regulated by the Reserve Bank of India like cryptocurrency.

Cyber insurance is excluded from general liability insurance.

Indian government initiatives for cyber security

The Government of India is taking enormous steps in order to create awareness for cyberattacks. The RBI (reserve bank of India) has made it mandatory to take cyber insurance coverage for financial institutions as cybercrimes are increasing. Few initiations of indian government :-

1. The Indian Computer Emergency Response Team (CERT-In)[3]
2. Cyber Surakshit Bharat
3. National Critical Information Infrastructure Protection Center (NCIIPC)
4. Appointment of Chief Information Security Officers
5. Personal Data Protection Bill
6. Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Center)
7. National Cyber Security strategy, 2020
8. Appointing Chief information security officer (CISO)
9. Drills and trainings
10. Website audit

Eligibility to opt for a cyber insurance

The citizens of a country who are above the age of 18, and corporations or businesses can buy cybersecurity insurance.

History of cyber insurance

The history of cyber insurance trace back to 1997, when Steven Haase helped AIG(American International Group) write the first internet or cyber security liability policy. The United States framed policy for cyber insurance in 1990s which provided limited scope. In 2000s, it incorporated numerous aspects of cyberspace issues.

[3]https://unacademy.com/content/upsc/study-material/science-and-technology/initiatives-taken-by-indian-government-for-cyber-security/

Position of India

There is no specified legal framework for cybercrime attacks in India till 2000. Indian penal code(IPC) doesn't provide coverage for computer related crimes. Then the information technology bill was passed in May 2000. It addresses the abuse of computers, servers or networks or issues of cyberspace and electronic commerce. India is one among the countries facing huge cybercrime attacks.

Information technology Act, 2000

An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.[4]

Importance of cyber insurance

As the use of technology increases, most of the activities are carried over through online mode to make our work and life simple. The greater the increase in technology, the more will be the number of users of such technology. Many organisation are conducting their business online. The banking business also has numerous customers transacting online. Therefore, the risk of getting exploited will be high. The financial information can be gathered by way of cyberattacks and personal information through various platforms like social media etc. If the electronic data of a business is stolen, it will cause huge losses to the business including loss of customers and revenue.

The victim affected through this will be rescued from the loss incurred to some extent by giving them financial help with exchange for consideration. Thus helping them to regain their position.

Further, cyber insurance helps the customer to get notified about the data breach, restore the data and personal identities of the victim, and repair the damaged parts of the computer network. Having a cyber insurance policy will be like sheltering. Cyber insurance is an expense for good cause as it helps to protect the valuable assets of data stored online.

Future of cyber insurance

We live in the world of technology. It has shown a drastic change over the past years. The growth of technology is inevitable which will result in a reduction of manpower in the upcoming year, making all data and information stored online or in a cloud that can be hacked through hackers. Here comes the role of cyber insurance that safeguards the victims who suffer loss due to cyber threats. Cyberattacks in the field of automobiles are expected to increase in future. Cyber insurance will play a very crucial role in the future more than any other insurance policy. The global market for cyber insurance is expected to grow to a great extent.

Cases related to cyber insurance

In **Travelers Prop. Cas. Co. of Am. v. Fed. Recovery Servs., Inc.,**[5] the US District Court for the District of Utah held that under technology errors and omissions liability coverage, the insurer, Travelers, had no duty to defend the insured, Federal Recovery Services (FRS), against allegations that FRS acted with knowledge, willfulness and malice. 103 F. Supp. 3d 1297 (D. Utah 2015). The facts are as follows:

- FRS provided data storage and processing to a fitness company called Global Fitness Holdings. at 1299.
- Global Fitness Holdings alleged that FRS refused to transfer its data pursuant to a contract “until Global Fitness satisfied several vague demands for significant compensation.” at 1300.
- The relevant Technology Errors and Omissions Liability form covered loss caused by “any error, omission or negligent act.” at 1302.
- The court held that Global Fitness did not allege errors, omissions or negligence, but rather “knowledge, willfulness, and malice,” and therefore Travelers had no duty to defend FRS under the policy.

The US District Court for the District of Arizona analyzed a cyber-insurance policy in **P.F. Chang’s China Bistro, Inc. v. Fed. Ins.**[6] The policy at issue covered “direct loss, legal liability, and consequential loss resulting from cyber security breaches.” In 2014, P.F. Chang’s was hacked and thousands of its customers’ credit card data was posted online. Id. at *1-2. Federal Insurance Co. disclaimed coverage for fees and assessments that P.F. Chang’s had agreed to reimburse its credit/debit card processor as a result of the breach, and P.F. Chang’s brought suit. Id. at *2. The court found that two exclusions

[4] The gazette of India. New Delhi, 9/5/2000-Jyaistha 19, 1922

[5] 156 F. Supp. 3d 1330 (D. Utah 2016)

[6] No. CV-15-01322-PHX-SMM (D. Ariz. May. 26, 2016)

for loss assumed by contract, as well as a similar restriction in the definition of "Loss," barred coverage for P.F. Chang's contractually assumed liability. Id. at *7-8. In analyzing coverage, "the Court turned to cases analyzing commercial general liability insurance policies for guidance, because cybersecurity insurance policies are relatively new to the market but the fundamental principles are the same." Id. at *8.

The National Bank of Blacksburg v. Everest National Insurance Company.[7] At issue in the case was whether the cyberattacks should be covered under the bank's C&E Crime Rider with its higher coverage limit, or the bank's debit card rider, which had a much lower limit. The bank argued that Everest improperly denied coverage under the policy's two exclusions for losses related to the use of credit or debit cards and ATMs. On January 23, 2019, the parties settled as a result of mediation proceedings.

Kavin Mitnic, the first hacker aged 17 in 1981 who deviated the subscribers' calls as he wanted. In 1983, he accessed the Pentagon computer. In 1990, he hacked or cracked or poked into the computer systems of world top techno-telecommunication computers like Motorola, Sun micro systems. He got arrested by the FBI and later released.

Gary, an Englishman, was arrested on the charge of hacking 90 US military computer systems located in the UK.

Levin, first Russian hacker to steal money from citibank in 1995 and robbed US Dollar 10 million.

How to claim for cyber insurance?

A FIR (First information report) must be filed at the police station or cyber department.

The insurance company must be notified about the cyber fraud or crime.

The claim has to be submitted within 90 days from the date on which the cyber fraud or crime has taken place.

Forensic evidence, if any, must be submitted and other proofs and evidence must be submitted to the insurance company.

The insurance company will appoint a person who is authorized with the power to investigate the matter of loss or damage.

The investigator will find out whether the claim is insurable or not.

After the investigation is complete, the claimant will be compensated if the investigation is satisfactory and the claim is insurable.

The claimant will be notified in case of rejection.

If the claimant is not satisfied with the insured amount, he can go for mediation.

Conclusion

Since cyberattacks happen over many years, the government is taking various steps to eradicate the problems faced in cyberspace. Cyber insurance is one step ahead of all plans. It helps in demolishing the efforts made by the hackers to attack the target computer or business or individuals. In order to be secure, everyone must be careful in giving their personal and financial details online like text messages, email or through social media or even through calls. Do not click a link or go into any website which is recommended by another website or by someone who is unknown to you. All systems and mobile should be encrypted properly.

[7] No. 7:18-cv-310 (W.D. Va), 2018