Legal Research Development
An International Refereed e-Journal
ISSN: 2456-3870, Journal home page: http://www.lrdjournal.com
Vol. 07, Issue-I, Sep. 2022

CYBERCRIME INSURANCE IS A PROTECTION TOOL OF THE SOCIETY: AN ANALYTICAL STUDY

Ramdas Gautam [a,*] **Dr. Vinod Kanker**[b**]

[a] *Ph.D., Scholar, Govt. M.L.B. College of Excellence, Gwalior, Jiwaji University, Gwalior, Madhya Pradesh (India).*

[b] *Associate Professor, Govt. M.L.B. College of Excellence, Gwalior, Jiwaji University, Gwalior, Madhya Pradesh (India).*

KEYWORDS

Cyber-crime, Cyber-attack, Cyber Crime is a Social Problem, Cyber insurance, Cyber Crime rate, Cyber Crime Insurance, Insurance is Protection Tool, Identity theft, Phishing, Malware, Spam, Cyber Stalking, Theft.

ABSTRACT

Despite the increasing awareness of cybercrime, there are many people who are still not sure what it is. Cybercrime is a criminal activity that is committed using computers or the internet. It can include anything from hacking and identity theft to fraud and child pornography. With the rise of technology, cybercrime has become one of the most common forms of crime. According to a report by Norton, a cyber-security company, there were 4.1 billion records breached in the first six months of 2019 alone. And the rate of cybercrime is only increasing. The same report stated that the average cost of a data breach globally was $3.86 million in 2018, which is up 6% from the previous year. During the duration of the Pandemic of Covid-19 most, most of the cyber-crimes increased by around five hundred times is stated by Chief of Defence Staff (CDS) General Bipin Rawat in a discussion with the Hindu Newspaper reporter in Nov. 2021. With the growing rate of cybercrime, many businesses are starting to purchase cybercrime insurance. Cybercrime insurance is a protection tool that businesses can use to financially protect themselves in the event of a data breach or other type of cyber-attack. In this research paper, we will explore the need for cybercrime insurance and how it can help businesses recover from a cyber-attack. We will also look at some of the challenges that businesses face when it comes to purchasing such insurance.

Introduction

Cybercrime insurance is a policy that offers protection against losses due to cybercrime. This type of insurance is designed to help organizations recover from a wide range of attacks, including data breaches, malware, ransom ware, and more as like unauthorized access to or exposure of private, sensitive, or otherwise protected data constitutes a data breach. This could be trade secrets, intellectual property, or personal data (such as details about one's health or financial accounts). Cybercrime insurance can help cover the cost of data recovery, litigation, and other expenses that can result from a cyber-attack. It can also help organizations keep their operations running in the event of an attack. In some cases, cybercrime insurance can even provide financial assistance for victims of identity theft. Organizations should carefully consider their needs when shopping for cybercrime insurance. Some policies may only cover certain types of attacks, while others may have limits on the amount of coverage they provide. It's important to work with an experienced broker to find the right policy for your organization.

What is the Cyber-crime?

The term computer crime and cybercrime may be used synonymously as in the definition that follows: "Computer crime, or cybercrime, refers to any crime that involves a computer and a network, where the computers may or may not have played an instrumental part in the commission of a crime". It has been also defined as an 'illegal activity using a computer, and includes computer-related extortion, fraud and forgery and unauthorized access to or interference with data'.[1]

What is the cyber insurance?

Cyber insurance we can denote as a "Digital protection in India". Digital insurance is a protection contract to safeguard policyholders from cybercrimes and is fundamentally designated towards people instead of associations and companies. An individual digital insurance contract incorporates security against burglary of assets, wholesale fraud cover, web-based entertainment cover, digital tormenting, malware cover, phishing cover, unapproved online transactions, media obligation claims cover, digital blackmail cover, and information break cover. In the present scenario Digital insurance is presented in India, both as an independent item and an extra inclusion to customary contracts, for example, protective covers for the property. It can incorporate inclusion for first-party liabilities such as liabilities borne as an immediate consequence of the occurrence and as well as outsider liabilities.

What types of cybercrime are there?

There are many types of cybercrime, but some of the most common include:

Identity theft: This occurs when someone uses your personal information, such as your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes.

Phishing: This is a type of online scam where criminals send emails or texts pretending to be from a legitimate company in an attempt to trick you into giving them your personal information.

Malware: This is software that is specifically designed to damage or disable computers and computer systems. It can be used to steal personal information, destroy data, or allow criminals to take control of a victim's computer.

Spam: This is unsolicited email or text messages that are sent in bulk. They can be used to promote products or services, spread malware, or phish for personal information.

Cyber Stalking: Cyber stalkers often use somebody else's and company's identities. They create fake email IDs and other important documents. After that use it like the original. After that, the Cyber stalkers commit the crime with the help of fake IDs and documents.

Theft of Business data

Some cyber stalkers many times stole the data of individuals and companies. In the other words, we can say that Information burglary alludes to the demonstration of illicitly getting computerized data from an association for monetary benefit or with the plan to attack the

Corresponding author

***E-mail:** ramdasgautam208@gmail.com (Ramdas Gautam). https://orcid.org/0000-0001-8032-183X

****E-mail:** kankarvk1963@gmail.com (Dr. Vinod Kankar). https://orcid.org/0000-0002-6359-4155

DOI: https://doi.org/10.53724/lrd/v7n1.12

Received 15th August 2022; Accepted 25th August 2022

Available online 30th Sep. 2022

business activities. Foes or even vindictive workers can take corporate information from got record servers, data set servers, cloud applications, or even from individual gadgets. There is a tremendous market for taking individual information, for example, telephone numbers, Master Card data, work email locations, and significantly more, which keeps noxious insiders and programmers spurred.

How does cybercrime insurance work?

- Cybercrime insurance is designed to protect businesses and individuals from the financial losses that can result from cybercrime. This type of insurance covers a wide range of risks, including data breaches, cyber extortion, and cyber fraud.
- Policyholders can purchase cybercrime insurance policies with different levels of coverage, depending on their needs. For example, some policies may provide reimbursement for lost or stolen data, while others may cover the cost of legal fees and damages resulting from a lawsuit.
- In order to file a claim, policyholders must first prove that they have suffered a financial loss as a result of cybercrime. They will then need to submit documentation to the insurance company, such as police reports or evidence of hackers accessing their systems. The insurer will then investigate the claim and determine whether or not to pay out the benefits.

Why needs cybercrime insurance?

In some circumstances, we need to protect ourselves from cybercrime such as:

1. Cybercrime insurance is a protection tool for the society against the financial losses that could result from cybercrime.
2. It is important for businesses to have insurance in place to protect themselves from the cost of recovering from a cybercrime, as well as the legal fees associated with defending themselves if they are accused of being responsible for the attack.
3. Cybercrime insurance can also help cover the cost of notifying customers or employees that their personal information may have been compromised in a data breach.
4. While no one wants to think about being the victim of a Cyber-attack, it is important to be prepared in case it happens. Cybercrime insurance is one way to help mitigate the financial risks associated with these attacks.
5. It helps protect businesses and organizations from the financial losses that can result from a data breach or other type of cyber-attack.
6. It can also help cover the costs of legal defense, investigation, and recovery.
7. In addition, it can provide peace of mind to business owners and employees knowing that they have some protection against the potentially devastating consequences of a cyber-attack.

What type of loss covered by the cyber insurance policies[2] which is first noticed during the Period of Insurance and which are reported to the Insurer in accordance with this Policy's Terms & Conditions?

- Privacy and Data Breach by Third Party
- Personal Social Media Data Breach Cover
- Personal Cyber Stalking without permission
- Personal I.T. (Information Technology) Theft Loss Cover
- Personal Malware Cover
- Personal Data Phishing Cover
- Personal E-mail Spoofing & E-mail hacked
- Personal Media Liability Claims Cover
- Personal Cyber Extortion Cover
- Identity Theft & Personal Data Cover

Legal provisions related to Cyber Crime in India

- **Sec. 65 of the I.T. (Information Technology) Act, 2000**

Under the section 65 of Information technology Act, 2000 denotes about 'Tampering with computer source documents'. If the anyone breaches the terms and conditions intentionally of section 65 of IT act 2000 then award the punishment of shall be punishable with imprisonment up to 03 years, or with fine which may extend up to 02 lakh rupees, or with both.[3] Whoever knowingly or deliberately conceals, destroys or alters or deliberately or knowingly motives every other to conceal, destroy, or alter any pc supply code used for a computer, laptop programme, pc device or laptop network, when the laptop supply code is required to be stored or maintained via regulation for the time being in force, shall be punishable with imprisonment up to 03 years, or with exceptional which can also prolong up to 02 lakh rupees, or with both.

- **Section 65 of the I.T. (Information Technology) Act, 2000**

If everyone commits a crime associated with the pc and goal dishonestly for the motive of committing any crime with the assistance of laptop/computer skill then shall be convicted under sec. 66 of the I.T. (Information Technology) Act, 2000. Punishment shall be awarded imprisonment for a term which may extend to 03 years or with a fine which may extend to 05 lakh rupees or with both.

- **Section 66A of the I.T. (Information Technology) Act, 2000**

"Cyber Stalking" is not defined under the I.T. (Information Technology) Act, 2000. Then in other words we can say that "Cyber Stalking" is outside the jurisdiction of I.T. (Information Technology) Act, 2000. But section 66A makes the relevant provision to catching cyber stalkers.[4]

- **Section 57 of the I.T. (Information Technology) Act, 2000**

Section 57 of the I.T. (Information Technology) Act, 2000 provides a provision of appeal. Under In this section, any person aggrieved by an order made by the Controller or an adjudicating officer under the Act may prefer an appeal to the Tribunal.

However, no appeal shall lie to the Tribunal from an order made by an adjudicating officer with the consent of the parties. Every appeal shall be filed within a duration of 45 days from the date of the order of competent authority.[5]

Any complaint filed with the Court will be dealt with by the Court as expeditiously as soon as possible and he will endeavor to finally dispose of it within 06 months from receipt of the complaint.[6]

Role Judiciary to stop cyber crime

Judiciary performs a vital function and additionally helps in resolving the conflicts amongst the events in cybercrime. Many times the judiciary delivered landmark judgments related to Cyber Crime. Some judgment details are given below.....

Kumar v/s Whiteley[7]

In this case, the defendant obtained unauthorized access to a joint bank server, deleted new record files, changed passwords, and denied access to authorized users. The accused was sentenced to 01 Year's rigorous imprisonment with fine 5000 rupees.

Sanjay Kumar v/s State of Haryana[8]

In this case, the complainant manipulated interest entries in computerized bank accounts and falsified electronic records to defraud the complaining bank and cause the bank unjustified losses. The Applicant was convicted of an offense punishable under Sections 65 & 66 of the Information Technology Act, read with Sec. 420, 467, 468, & 471 of the Indian Penal Code, 1860, and was sentenced to rigorous imprisonment. However, the petitioner appealed and the order was dismissed by the appellate court & which upheld the trial court judgment.

Syed Asifuddin and Ors. v/s State of Andhra Pradesh and Anr[9]

This was the first case related to the Information Technology Act under section 65. In this case, the court ruled that mobile phones meet the definition of a computer under the Information Technology Act and a unique electronic serial number such as a SID (system identification code) is programmed into each mobile phone and MIN (Mobile Identification Number) is a computer source code retained and named by law within the meaning of the Information Technology Act..

Are there any drawbacks to cybercrime insurance?

There are a few potential drawbacks to cybercrime insurance. For one, it can be expensive, and may not be worth the cost for some businesses. Additionally, it's possible that insurance companies will become more selective in what they cover and who they insure if cybercrime becomes more prevalent. This could lead to higher premiums and fewer options for coverage. Finally, insurance can't protect against all risks, and businesses still need to take proactive measures to prevent and mitigate attacks.

Conclusion

This research was conducted to analyses the role of cybercrime insurance as a protection tool for the society. It was found that cybercrime insurance does act as a protection tool for the society against online risks and helps organizations in recovering from financial losses due to cybercrime. The study also found that there are certain challenges associated with the adoption of cybercrime insurance, such as lack of awareness and understanding about the benefits of this type of insurance. Despite these challenges, it is clear that cybercrime insurance can play a key role in protecting societies against the financial impact of cybercrime.

Suggestions

There are some suggestions for the stop cyber-crimes details given below:

1. Cyber insurance should be mandatory for all electronic devices.
2. Cyber Insurance cost should be included in the product cost.
3. Government should make a special police cell to catch the Cyber attackers only.
4. Need to modify the cyber security because there is a much delayed process to catch offenders.
5. Many times cyber security is unable to find out real cyber offenders that's why need to enhance cyber technology
6. The Parliament needs to make new rules, regulations, and Laws also according to the new era related to cyber insurance.
7. Cyber insurance should be economic for the common man.
8. Remove the loopholes for the organization's cyber-attack.

Endnotes

[1] Dr. J.P. Mishra: An Introduction to Cyber Law: Central Law Publication Allahabad, Second Edition 2014, page no. 177

[2] Personal Cyber Risks Policy-Claims Made Policy Wording: What are we covering insured for?: Last seen 20/07/2022, https://www.irdai.gov.in/ADMINCMS/cms/UploadedFiles/NonLifeProducts/2020-21/IRDAN132RP0001V01202021.pdf

[3] Section 65: the Information Technology Act, 2000

[4] Section 66A: the Information Technology Act, 2000

[5] Section 57 of the Information Technology Act, 2000

[6] Section 84: the Information Technology Act, 2000

[7] 2009

[8] CRR No. 65 of 2013 (O&M)

[9] 2006 (1) ALD Cri 96, 2005 Cr.L.J. 4314

****