Role of Cyber Insurance in India to Protect Cyber Theft: A Socio-Legal 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	ABSTRACT
Role of Cyber Insurance, Need of cyber Insurance, cyber threats, Types of Cyber insurance, Merits and Demerits of Cyber Insurance, Socio-Legal study, Awarness of cyber insurance, awareness of cyber crimes.	Cyber insurance can help protect your business from potential cyber threats. With the right cyber insurance, you can protect yourself and your data from potential damage. Here are some tips to help you choose the right cyber insurance policy- Check the cyber risk associated with your business. Make sure that the cyber risks your business faces are realistic and not exaggerated. Look at the cyber insurance policies available. There are many cyber insurance policies available, so make sure to compare prices and policies to find the best deal for your business. Choose the right cyber insurance policy for your business. Make sure to choose a policy that covers all of your cyber needs, including data loss, cyber theft, and third-party cyber-attacks. Get a policy that covers your business's entire staff. A policy that covers your entire staff can help protect your data and business from potential cyber threats. Get a policy that has generous coverage. A policy that has generous coverage will protect your business from potential cyber threats, even if they are not specifically covered in the policy. Get a policy that is easy to use. A policy that is easy to use will help you understand the policy and make sure you are getting security.

Introduction

Over the last few years, the number of cyber-attacks is growing rapidly and has become a threat to the security of information resources and the cyberspace. The cost of cybercrime has been estimated to be around US $1 trillion per annum. In India, the estimated cost of cybercrime is Rs 11,400 crore. [1] The recent WannaCry ransomware attack has been a wake-up call for Indian businesses.

Cyber insurance is gradually emerging as a powerful tool to minimize the financial losses arising out of data breaches and other malicious cyber-attacks. The insurance sector in India has started acknowledging the potential of cyber insurance and is taking steps to develop the product and make it more accessible to customers. The Indian government is also playing an active role in promoting the use of cyber insurance as a means of reducing the economic impact of cybercrime. Despite these efforts, the uptake of cyber insurance in India has been relatively low.

On the Awareness and the Attitude of Indian Enterprises, the paragraph needs to be at least four sentences. I have already written the following: Role of Cyber Insurance in India to Protect Cyber Theft: A Critical Study on the Awareness and the Attitude of Indian Enterprises, the paragraph needs to be at least four sentences. I have already written the following: Role of Cyber Insurance in India to Protect Cyber Theft: A Critical Study on the Awareness and the Attitude of Indian Enterprises, the paragraph needs to be at least four sentences. I have already written the following: Role of Cyber Insurance in India to Protect Cyber Theft: A Critical Study on the Awareness and the Attitude of Indian Enterprises, the paragraph needs to be at least four sentences.

(a) The current situation: With an increase in internet users and digitalization, cyber-attacks have also increased manifold. India currently ranks 3rd in the world in terms of the number of internet users. By 2021, the number of internet users is projected to reach 650 million.

(b) How cyber insurance can help: Cyber insurance can help protect individuals and businesses in the event of a cyber-attack or data breach.

Types of Cyber Insurance

1. **First-Party Coverage**:[2]
This protects your company against financial losses in case of a data breach. These include expenses to notify customers, public relations, and credit monitoring. First-party coverage also includes business interruption and extra expenses incurred if your business is forced to close its doors due to a cyberattack.

2. Third-Party Coverage:[3]
This protects your company against financial losses related to third parties, which include your customers, vendors, and others with whom your company has a contractual relationship. These include expenses such as litigation, settlements, and judgments.

3. Crime Coverage:
This protects your company against financial losses related to crimes involving your computer systems, including theft of data, funds transfer fraud, and cyber extortion.

4. Media Coverage:
This protects your company against financial losses related to media content, including defamation, invasion of privacy, and copyright infringement.

5. Network Security and Privacy Coverage:
This protects your company against financial losses related to network security and privacy, including data breaches, cyber extortion, and cyber terrorism.

6. Cyberterrorism Coverage:
This protects your company against financial losses related to cyberterrorism, including data breaches, cyber extortion, and denial of service attacks.

7. Professional Liability Coverage:
This protects your company against financial losses related to professional liability, including errors and omissions, negligence, and

breach of contract.

Why need of Cyber Insurance

There are a number of reasons why you might need cyber insurance. For example, if you run a business and store customers' personal data, you could be held liable if that data is compromised in a cyber attack. Cyber insurance can help cover the costs of investigating and responding to a data breach, as well as any legal fees and damages you may be ordered to pay.

Cyber insurance can also help cover the costs of restoring lost data, recovering from system downtime, and repairing damaged hardware or software. If your business relies heavily on technology, cyber insurance can help protect against the financial losses that can result from a major cyber incident.

Present condition of Cyber Insurance in India

There is no specific law governing cyber insurance in India. The Insurance Regulatory and Development Authority of India (IRDAI) has not issued any regulations specifically for cyber insurance. However, the IRDAI has released guidelines for the insurance industry on cybersecurity in October 2017.[4] These guidelines are not mandatory, but they provide valuable guidance for insurers on how to underwrite and manage cyber risks.

The cyber insurance market in India is still in its infancy. According to a report by Marsh, the total size of the cyber insurance market in India was only US$79 million in 2016. This is expected to grow to US$1.78 billion by 2020, at a compound annual growth rate (CAGR) of 60%.

How can get the Cyber Insurance

There are a few ways to get cyber insurance. You can purchase it through an insurance broker, through a specialized cyber insurance provider, or through some traditional insurance carriers. You can also get it through a few online marketplaces.

What are the minimum qualification for Cyber Insurance?

There is no minimum qualification for cyber insurance, but most insurers will require companies to have certain cyber security measures in place before they will provide coverage. These measures may include things like data encryption, firewalls, and intrusion detection systems.

What are the demerits of Cyber Insurance?

There are a few potential drawbacks of cyber insurance, including:

1. **It may not cover all types of cyber risks:** Cyber insurance policies can vary widely in terms of what they cover. Some policies may exclude certain types of risks, such as those related to terrorism or war.

2. **It may have high deductibles:** Cyber insurance policies typically have high deductibles, which means that the policyholder will have to pay a significant amount out of pocket before the insurance coverage kicks in.

3. **It may not cover all losses:** Even if a cyber insurance policy covers a particular type of risk, it may not cover all potential losses. For example, a policy may have a limit on the amount of coverage for data breaches.

4. **It may be expensive:** Cyber insurance can be expensive, particularly for small businesses. The cost of a policy will depend on factors such as the size of the business, the type of coverage, and the deductible.

Survey work

In order to Socio-Legal study what people understand by cyber insurance and whether people are benefited or harmed by it, an attempt has been made to know what effect it has on the people of the society through questions and answers related to it. Regarding which online survey has been done through Google Form, the result of which is as follows-

We have fill up the questionair of 100 people to know that what the impact of Cyber Insurance on the socity is. It is beneficial of expensive.

Q.No. 01: What is the nature of your family?

Ans. 01: In response to the above question, 15.0 percent of the respondents said that the nature of their family is "in Below the Poverty line". And 54.0 percent of the respondents said that the nature of their family is "middle class". And 22.0 percent of the respondents said that the nature of their family was "upper class". And 9.0 percent of the

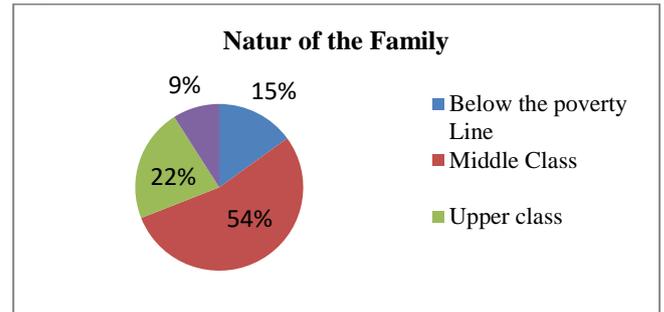respondents said that the nature of their family is "other".

Fig.: 01

Q.No. 02: What is your family like?

Ans. 02: In response to the above question, 52.0 percent of the respondents said that the nature of their family is "Joint Family". And 32.0 percent of the respondents said that the nature of their family is "Nuclear Family". And 16.0 percent of the respondents said that the nature of their family was "other".
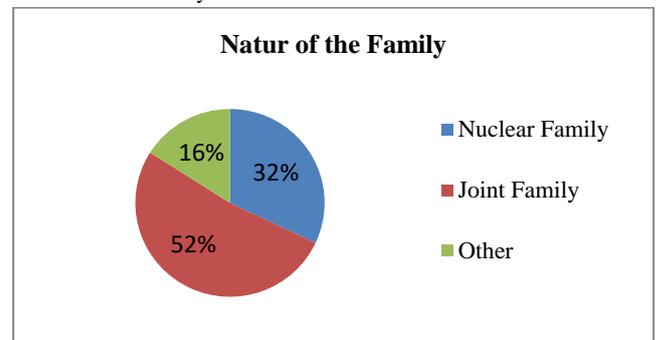

Fig.: 02

Q.No. 03: Do you know about the Cyber-Crime?

Ans. 03: In response to the above question, 72.0 percent of the respondents said that they know about Cybercrime and replied with "Yes". And 18.0 percent of the respondents said that they don't know about Cybercrime and replied with "No". And 10.0 percent of the respondents said that they know about Cybercrime a little bit and replied with "Little bit".
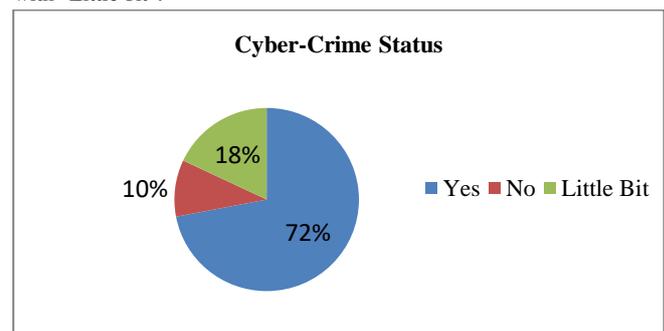

Fig.: 03

Q.No. 04: Do you know how cybercrime happens?

Ans. 04: In response to the above question, 6.0 percent of the respondents said that Cybercrime happens by the laptop and replied with "By Laptops". And 7.0 percent of the respondents said that Cybercrime happens by Mobile phone and replied with "By Mobile devices". And 7.0 percent of the respondents said that cybercrime happens by Phone Calls and replied with "By Phone Calls". And 40.0 percent of the respondents said that cybercrime happens through Social Media Platforms and replied with "By Social Media Platforms". And 5.0 percent of the respondents said that cybercrime happens through stolen data and other ways and replied with "By Stolen data and other ways". And 30.0 percent of the respondents said that cybercrime happens through All the above ways and replied with "All the above". And 5.0 percent of the respondents said that cybercrime happens through none of

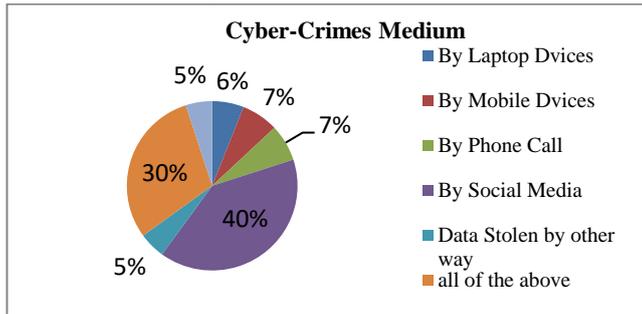the above ways and replied with "None of the above".

Cyber-Crimes Medium

- By Laptop Dvices
- By Mobile Dvices
- By Phone Call
- By Social Media
- Data Stolen by other way
- all of the above

Fig.: 04

Q.No. 05: Do you know about the Any Social Platform? If yes then….

Ans. 05: In response to the above question, 20.0 percent of the respondents said that they know about WhatsApp and replied with "Yes". 22.0 percent of the respondents said that they know about Facebook and replied with "Yes". 10.0 percent of the respondents said that they know about Instagram and replied with "Yes". 5.0 percent of the respondents said that they know about Telegram and replied with "Yes". 5.0 percent of the respondents said that they know about other platforms and replied with "Other Platform". 35.0 percent of the respondents said that they know about all of the above Platforms and replied with "all of the above". 3.0 percent of the respondents said that they don't know about all of the above Platforms and replied with "None of the above".
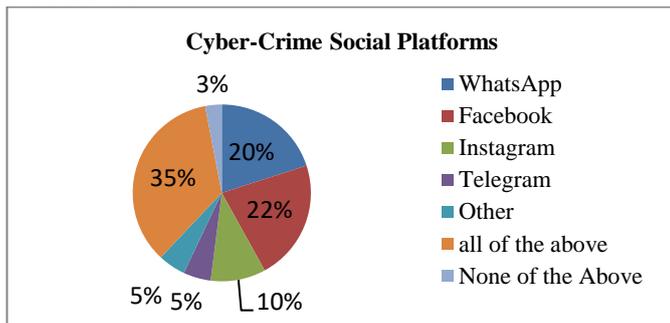
Cyber-Crime Social Platforms

- WhatsApp
- Facebook
- Instagram
- Telegram
- Other
- all of the above
- None of the Above

Fig.: 05

Q. No. 06: How come to know about the Cyber Crimes?

Ans. 06: In response to the above question, 06.0 percent of the respondents said that they Came to know about Cyber crimes by Government employees and replied with "Govt. employees". 10.0 percent of the respondents said that they Came to know about Cyber crimes by NGO's and replied with "NGO's". 11.0 percent of the respondents said that they Came to know about Cyber crimes through the Internet and replied with "Internet". 12.0 percent of the respondents said that they Came to know about Cyber crimes through the awareness program and replied with "the awareness program". 41.0 percent of the respondents said that they Came to know about Cyber crimes through Social Media and replied with "Social Media". 15.0 percent of the respondents said that they Came to know about Cyber crimes through All of the above means and replied with "All of the above". 5.0 percent of the respondents said that they did not come to know about Cyber crimes through none of the above means and replied with "None of the above".
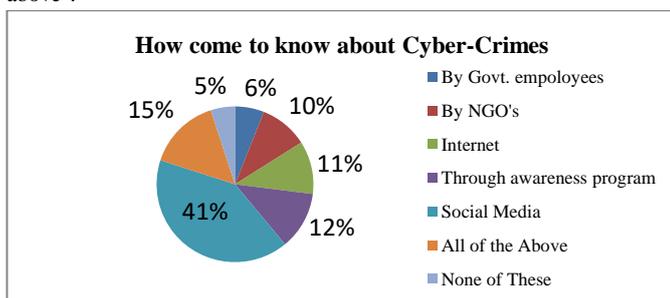
How come to know about Cyber-Crimes

- By Govt. empoloyees
- By NGO's
- Internet
- Through awareness program
- Social Media
- All of the Above
- None of These

Fig.: 06

Q. No. 07: Cybercrime has ever happened to you?

Ans. 07: In response to the above question, 23.0 percent of the respondents said that Cybercrime happened to them and replied with "Yes". 62.0 percent of the respondents said that Cybercrime did not happen to them and replied with "No". 15.0 percent of the respondents said that I don't know what Cybercrime happened to them and replied with "I don't know".
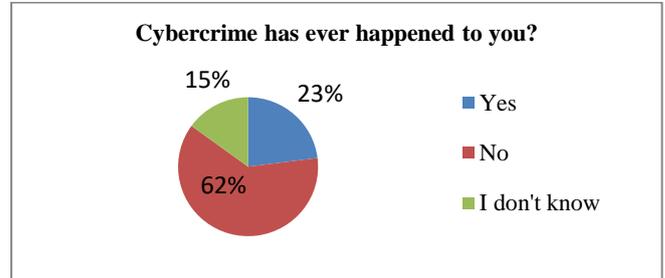
Cybercrime has ever happened to you?

- Yes
- No
- I don't know

Fig.: 07

Q. No. 08: Cybercrime has ever happened to any member of your family?

Ans. 08: In response to the above question, 36.0 percent of the respondents said that Cybercrime happened to one of their family members and replied with "Yes". 50.0 percent of the respondents said that Cybercrime did not happen to one of their family members and replied with "No". 14.0 percent of the respondents said that I don't know whether Cybercrime happened or not to their family members and replied with "I don't know".
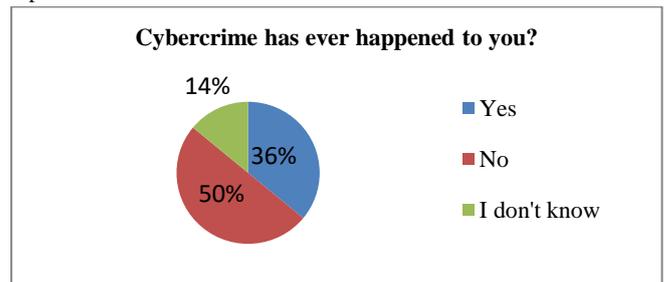
Cybercrime has ever happened to you?

- Yes
- No
- I don't know

Fig.: 08

Q. No. 09: Can you tell me please how can be stopped cybercrime?

Ans. 09: In response to the above question, 10.0 percent of the respondents said that Cybercrime can be stopped if you use a strong password and they replied with "Use a Strong Security Password". 5.0 percent of the respondents said that Cybercrime can be stopped if you use internet security tools and they replied with "use internet security tools". 15.0 percent of the respondents said that Cybercrime can be stopped if you are aware of cyber fraud and they replied with "awareness of cyber fraud". 33.0 percent of the respondents said that Cybercrime can be stopped if you Manage Social media settings and they replied with "Manage Social media settings". 37.0 percent of the respondents said that Cybercrime can be stopped if they Manage All of the above methods and replied with "All of the above". 5.0 percent of the respondents said that Cybercrime can not be stopped with the help of all of the above methods and replied with "None of the above".
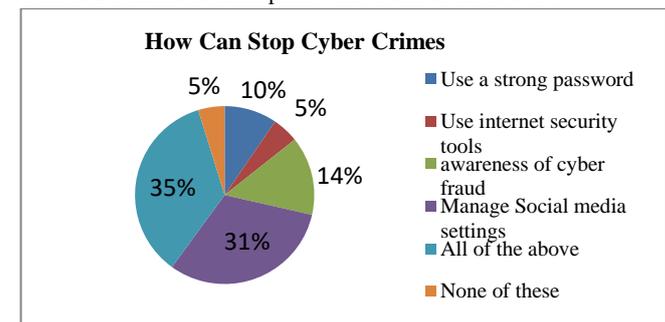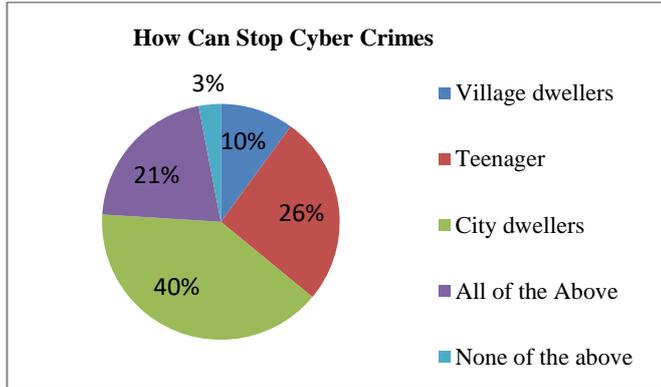
How Can Stop Cyber Crimes

- Use a strong password
- Use internet security tools
- awareness of cyber fraud
- Manage Social media settings
- All of the above
- None of these

Fig.: 09

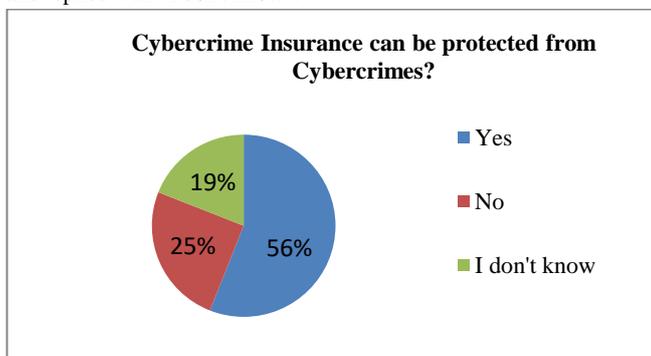**Q. No. 10:** Who are the most cybercrime victims?

Ans. 10: In response to the above question, 10.0 percent of the respondents said that the victims of cybercrime are village dwellers and they replied with "Village dwellers". 26.0 percent of the respondents said that the victims of cybercrime are teenagers and they replied with "Teenager". 40.0 percent of the respondents said that the victims of cybercrime are City dwellers and they replied with "City dwellers". 21.0 percent of the respondents said that the victims of cybercrime are All of the above and they replied with "All of the above". 3.0 percent of the respondents said that the victims of cybercrime are none of the above and they replied with "None of the above".

How Can Stop Cyber Crimes

- Village dwellers
- Teenager
- City dwellers
- All of the Above
- None of the above

Fig.: 10

Q. No. 11: Do you think that Cyber crime Insurance can be protect from the cyber crime?

Ans. 11: In response to the above question, 56.0 percent of the respondents said that Cybercrime Insurance can be protected from cybercrime and replied with "Yes". 25.0 percent of the respondents said that Cybercrime Insurance can not be protected from cybercrime and replied with "No". 19.0 percent of the respondents said that I don't know whether Cybercrime Insurance can be protected or not from cybercrime and replied with "I don't know".

Cybercrime Insurance can be protected from Cybercrimes?

- Yes
- No
- I don't know

Fig.: 11

Coclusion

Cyber insurance provides protection against financial losses that can result from a data breach or other cyber-attack. It can help cover the costs of responding to an attack, such as notifying affected customers and providing credit monitoring services. It can also help cover the costs of lawsuits that may result from an attack. After the socio-legal study, 56% of people say that if you take cyber insurance for the protection of cyber crimes and fishing then you can not be protected but you can full fill damages and losses. Often people get trapped by cyber thieves due to greed. After that, they have to get loss. There are many ways to trap people with electronic gezzets. If people are aware of cyber crimes then we can remove cyber crimes from society. We know that knowledge and awareness are the cure for cyber crimes

Suggestion:

If you want to avoid cybercrimes then you have to adopt Security methods such as securing your online accounts with strong passwords, use to security keys, avoid third-party apps and unauthorized apps. You must be knowing that there is no single silver bullet that can stop all cyber threats. However, there are a number of steps that organizations can take to reduce their risk of being attacked. The best way to stop cyber threats is to be proactive and take steps to protect your computer and your information. Some tips to help you protect yourself from cyber threats include:

1. Security controls and practices should be strong
2. Security awareness training camps should be organized by the governments at the grounds level.
3. Need to modify Monitoring network systems for suspicious activities.
4. Keep your operating system and software up to date by authorized companies.
5. Use good quality anti-virus and anti-malware software.
6. Carefully open emails and attachments after scanning the antivirus.
7. Be cautious about what you download whether it is secure or not.
8. Don't open and click on links received by emails or Text messages from people you don't know.

Endnotes:

[1] Steve Morgan- Editor-in-Chief: Cybercrime Costs. PHOTO: Cybercrime Magazine, Cybercrime To Cost The World $10.5 Trillion Annually By 2025, Published on 13th Nov. 2020, Last Seen on 30th April 2022, https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

[2] Cyber Insurance: https://cyberinsureone.com/types/ (Last seen 20th April 2022)

[3] Third-party cyber liability insurance: published on 29th April 2022,https://www.insureon.com/insurance-glossary/cyber-liability-third-party (Last seen 01st May 2022)

[4] IRDA: Guidelines on Information and Cyber Security for Insurers, Letter date: 07/04/2017, https://www.irdai.gov.in/ADMINCMS/cms/Uploadedfiles/07.04.2017-Guidelines%20on%20Information%20and%20Cyber%20Security%20for%20insurers .pdf (Last Seen 05th April 2022)