International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

An Analytical Study of Cybercrime and Its Impact on Social Awareness

Dr Sheeja Varkey

Assistant Professor, St Thomas College, Ruabandha Bhilai

Abstract

The rapid digital transformation of society has significantly increased dependence on computers, mobile devices, and internet-based services, leading to a parallel rise in cybercrime. Cybercrime encompasses a wide range of illegal activities conducted through digital platforms, where computers or networks act as either the target or the instrument of crime. With advancements in information and communication technology, cyber threats have become more sophisticated, organised, and transnational in nature.

In India, cybercrime has witnessed substantial growth due to expanding internet access, digital banking, e-commerce, and social media usage. Common cyber offences include online financial fraud, identity theft, phishing, hacking, cyber stalking, data breaches, ransomware attacks, cyber terrorism, and the distribution of malicious software. Unlike traditional crimes, cybercrime is characterised by anonymity, global reach, technical complexity, and rapid evolution, which make detection and prosecution challenging.

The legal framework governing cybercrime in India is primarily based on the Information Technology Act, 2000, which provides provisions for electronic governance, cybersecurity, and penalties for digital offences. However, the dynamic nature of cyber threats demands continuous updating of laws, improved digital forensics, stronger institutional mechanisms, and enhanced public awareness.

Addressing cybercrime requires a multi-dimensional strategy involving government agencies, private organisations, law enforcement bodies, and citizens. Strengthening cybersecurity infrastructure, promoting digital literacy, and encouraging responsible online behaviour are essential steps toward building a secure and resilient digital ecosystem in India.

Keywords: Cybercrime, Cybersecurity, Digital India, Online Fraud, IT Act, Data Protection, Cyber Awareness.

Introduction

The rapid advancement of information and communication technologies has transformed the way individuals, businesses, and governments operate. While digital innovation has brought efficiency, connectivity, and economic growth, it has also created new opportunities for criminal activities in cyberspace. Cybercrime refers to unlawful acts carried out using computers, digital devices, or networks, where technology serves either as the tool, the target, or both. These offences range from malware attacks and hacking to financial fraud, identity theft, phishing, cyber stalking, and data breaches.

Cybercriminals often exploit system vulnerabilities to gain unauthorised access, steal confidential information, disrupt services, or cause financial and reputational damage. For instance, malicious software (malware) can infiltrate systems to delete, encrypt, or manipulate data for extortion or monetary gain. In

addition to direct attacks, cyber-enabled crimes such as online fraud, digital payment scams, and data theft have become increasingly prevalent with the growth of e-commerce and digital banking.

Given the growing dependence on digital platforms, assessing the level of awareness and preparedness among individuals and organisations has become essential. While certain sections of society demonstrate adequate knowledge of cybersecurity practices—such as strong password management, two-factor authentication, and safe browsing habits—many remain vulnerable due to limited awareness, insufficient training, or lack of access to protective resources. Identifying these gaps is crucial for designing effective awareness programs and strengthening preventive strategies.

This study seeks to examine the various dimensions of cybercrime, evaluate public awareness levels, and analyse the broader societal impact of digital threats. It also aims to explore the role of legal and institutional frameworks, particularly the Information Technology Act, 2000, in addressing cyber offences and promoting cybersecurity in India.

By providing a comprehensive understanding of cybercrime trends, awareness levels, and preventive measures, this research intends to offer practical recommendations for enhancing cybersecurity resilience. Strengthening collaboration among government agencies, private institutions, law enforcement bodies, and citizens is essential to building a secure digital ecosystem and ensuring safer cyberspace for present and future generations.

Types of Cybercrimes

Cybercrime encompasses a wide range of unlawful activities carried out through computers, digital devices, and internet platforms. It can broadly be classified into three major categories: cybercrimes against individuals, cybercrimes against property, and cybercrimes against government.

- Cybercrimes against individuals include offenses such as online harassment, cyberstalking, identity theft, defamation, and the dissemination of offensive or discriminatory content based on sexual, racial, or religious grounds. These crimes primarily affect a person's privacy, dignity, and mental well-being.
- Cybercrimes against property involve unauthorised access, data theft, hacking, computer vandalism, and the transmission of malicious software such as viruses and ransomware. These activities cause financial loss and damage to digital assets.
- Cybercrimes against government include cyber terrorism and attacks on government systems or critical infrastructure. Such offences may threaten national security by enabling information breaches, electronic threats, or disruption of public services.

Who are the Cyber Criminals?

Cybercriminals can generally be classified into four major groups based on their motives, skills, and level of organisation.

- **Young Offenders (Age 9–16):** A segment of cyber offenders consists of children and teenagers who engage in hacking or other online activities either knowingly or unknowingly. Some view hacking as a challenge or a matter of pride, often without fully understanding the legal consequences of their actions.
- **Organized Hacktivists:** Hacktivists are groups of hackers who operate collectively to promote political, religious, or social causes. Their activities may include website defacement, data leaks, or denial-of-service attacks intended to spread messages or disrupt targeted entities.

- **Disgruntled Employees:** Employees who feel dissatisfied or unfairly treated may misuse their authorised access to organisational systems. Such individuals can cause significant harm by stealing sensitive data, disrupting operations, or sabotaging internal systems.
- **Professional Hackers:** Professional hackers possess advanced technical expertise and may operate either legally or illegally. While ethical hackers are employed to strengthen cybersecurity systems, malicious hackers may be hired by rival organisations or criminal networks to steal confidential information, conduct corporate espionage, or exploit system vulnerabilities for financial gain.

LITERATURE REVIEW

Recent studies highlight that the rapid expansion of digital technologies, online banking, e-commerce, social media platforms, and remote working environments has significantly increased exposure to cyber threats worldwide.

- **Sharma and Gupta (2020):** The authors examined the rise of cybercrime during the COVID-19 pandemic and observed a substantial increase in phishing attacks, online fraud, and ransomware incidents due to increased internet usage and remote work practices. The study emphasised that a lack of digital literacy and poor cybersecurity practices contributed to higher victimisation rates.
- **Kumar and Bansal (2021):** This study focused on cybersecurity awareness among college students in India. The findings revealed moderate awareness regarding basic cyber hygiene practices such as password protection and safe browsing; however, limited knowledge was observed regarding advanced threats like social engineering and ransomware. The authors recommended integrating cybersecurity education into academic curricula.
- **Rahman et al. (2022):** The researchers analysed global cybercrime trends and highlighted the growing role of organised cybercriminal networks. The study noted that cybercrime has evolved from individual hacking activities to sophisticated, profit-driven operations involving cryptocurrency transactions, dark web marketplaces, and cross-border cyberattacks.
- **Patel and Sinha (2023):** This research examined the effectiveness of cyber laws and regulatory frameworks in India. The study emphasised the importance of strengthening enforcement mechanisms under the Information Technology Act, 2000 and improving coordination between law enforcement agencies and cybersecurity institutions. It concluded that legal reforms must keep pace with rapidly evolving digital threats.
- **Global Cybersecurity Reports (2023–2024):** Recent international reports indicate a sharp increase in AI-enabled cyberattacks, identity theft, financial fraud, and data breaches. The studies stress the importance of public awareness campaigns, organisational cybersecurity investment, and international cooperation to combat transnational cybercrime.

Steps to Prevent Cyber Crimes

Preventing cybercrime requires awareness, caution, and responsible online behaviour. The following preventive measures can significantly reduce the risk of becoming a victim:

- Personal information should be kept confidential. Sharing sensitive details on public platforms is equivalent to revealing one's identity to strangers and may lead to misuse.
- Avoid sending personal photographs or sensitive content while chatting online, especially to strangers, as such materials can be exploited or misused.

- Never disclose banking details, OTPs (One-Time Passwords), passwords, or personal document information, as this may result in financial fraud or identity theft.
- Refrain from visiting suspicious websites or downloading applications from unverified sources.
- Use secure and trusted applications, regularly update software, and enable strong security settings to ensure safer digital transactions.

Impact of the Study on Cybercrime and Societal Awareness

The study titled *"A Study on Cybercrime: Its Impact and Awareness towards Society"* is expected to generate significant academic, social, and policy-level implications. The potential impacts are outlined below:

1. **Enhanced Understanding of Cybercrime:** The study contributes to a comprehensive understanding of various forms of cybercrime and their far-reaching consequences on individuals, organisations, and society at large.
2. **Increased Public Awareness:** By highlighting the prevalence, patterns, and severity of cyber threats, the research promotes greater awareness among citizens, businesses, and policymakers regarding the necessity of adopting effective cybersecurity measures.
3. **Policy Development and Legal Strengthening:** The findings may support policymakers in strengthening legal frameworks such as the Information Technology Act, 2000 and formulating improved regulatory strategies to combat emerging cyber threats.
4. **Positive Behavioural Change:** Greater awareness can encourage individuals and organisations to adopt safer online practices, including responsible data sharing, strong password management, and secure digital transactions.
5. **Empowerment of Stakeholders:** The study equips individuals, corporate entities, and government agencies with relevant knowledge to proactively safeguard digital assets and reduce vulnerability to cyberattacks.
6. **Economic Safeguarding:** By examining the financial impact of cybercrime, the research underscores the importance of investing in cybersecurity infrastructure and technologies to minimize economic losses.
7. **Addressing Psychological Impact:** Understanding the emotional and psychological consequences of cybercrime—such as stress, fear, and anxiety—may encourage the development of support systems and victim assistance programs.
8. **Strengthening Trust in Digital Platforms:** Improved awareness and preventive measures can help restore public confidence in digital systems, promoting safer online engagement.
9. **Promotion of Education and Training:** The study highlights the importance of cybersecurity education and digital literacy initiatives, encouraging the integration of cybersecurity awareness into academic and professional training programs.
10. **Encouraging International Cooperation:** Since cybercrime transcends geographical boundaries, the study may foster global collaboration in prevention, investigation, and enforcement strategies.

Overall, the study has multidimensional implications, influencing policy formulation, individual behaviour, economic stability, and international cooperation, thereby contributing to the creation of a more secure and resilient digital society.

Research Methodology

This study adopts a systematic approach to assess the level of awareness regarding cybercrime and cybersecurity among respondents. The methodology applied for the study is described below:

1. Objectives of the Study

The study is guided by the following objectives:

1. To examine the relationship between the educational level of respondents and their awareness of cybercrime and cybersecurity.
2. To determine the frequency with which respondents have experienced cybercrime incidents.
3. To analyse the pattern and extent of regular internet usage among respondents.
4. To assess the level of awareness regarding online safety practices while using personal computers and internet services.
5. To identify and evaluate the different cyber-related situations encountered by respondents.

2. Nature and Sources of Data

The study is based on both primary and secondary sources of data.

Primary Data: Primary data were collected through a structured questionnaire administered to respondents. The survey method enabled the collection of first-hand information regarding awareness levels, experiences, and perceptions related to cybercrime.

Secondary Data: Secondary data were obtained from published journals, research articles, newspapers, official reports, and credible internet sources to support and strengthen the conceptual framework of the study.

3. Sample Size

The study was conducted using a sample size of 52 respondents.

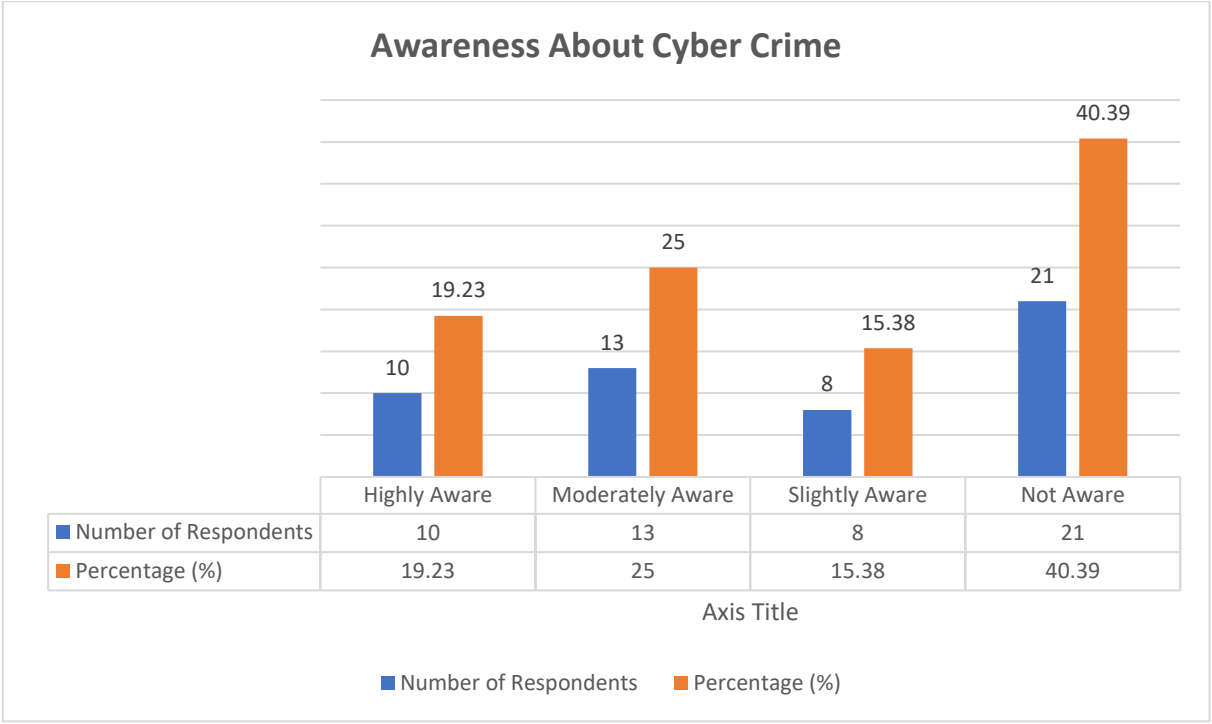
4. Sampling Method and Research Design

The research adopts a **descriptive research design**, which focuses on describing and analysing the existing level of awareness and experiences related to cybercrime. Data were collected primarily through a survey method, supported by observation where necessary. The descriptive approach helps in understanding patterns, behaviours, and attributes of respondents concerning cybersecurity awareness.

Results and Interpretation

Table 1: Demonstrate the awareness about cybercrime by the respondents.

Level of Awareness	Number of Respondents	Percentage (%)
Highly Aware	10	19.23
Moderately Aware	13	25
Slightly Aware	8	15.38
Not Aware	21	40.39

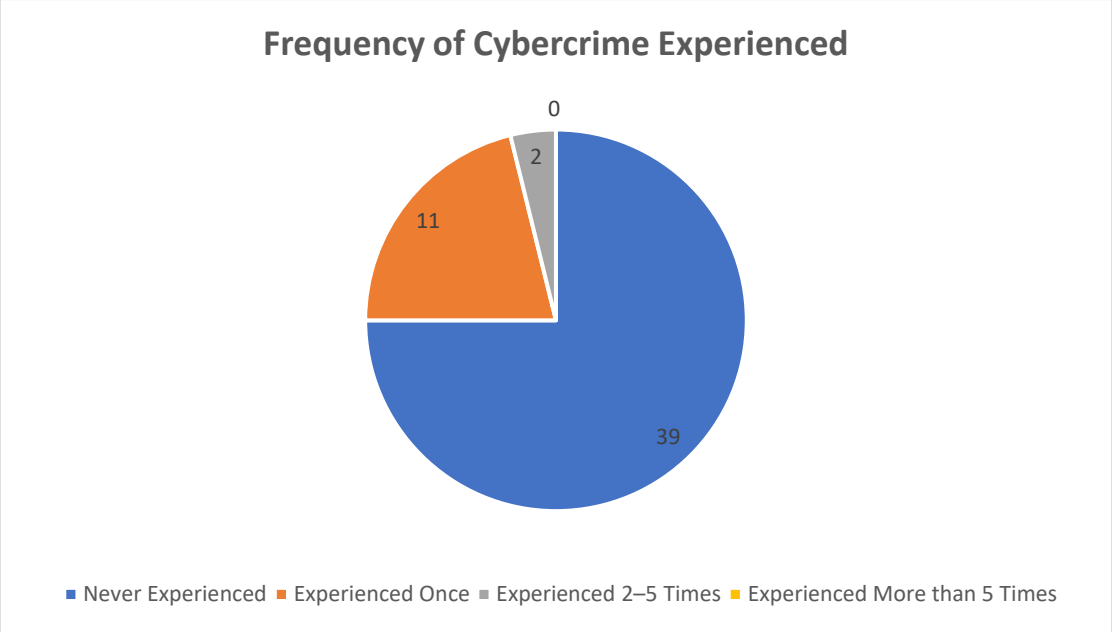


Analysis: The analysis of respondents' awareness levels shows that a significant proportion lacks adequate knowledge about the subject. Among the respondents, 40.39% reported that they are not aware, which represents the highest percentage. Additionally, 25% indicated that they are moderately aware. About 19.23% stated that they are highly aware, while 15.38% reported being slightly aware.

Overall, although 44.23% of respondents demonstrate moderate to high awareness, a larger proportion has limited or no awareness. These findings highlight the need for effective awareness programs and strategic initiatives to improve knowledge and understanding among the target population.

Table 2. The following table presents the frequency with which respondents have experienced cybercrime incidents:

Frequency of Victimisation	Number of Respondents	Percentage (%)
Never Experienced	39	75
Experienced Once	11	21.15
Experienced 2–5 Times	2	3.84
Experienced More than 5 Times	0	00



Analysis: From the above table, it is clearly observed that a majority of the respondents have not experienced cybercrime. Nearly 75% (39 respondents) reported that they have never been victims of cybercrime. This indicates that most of the participants in the study have not faced direct cybercrime incidents.

However, 21.15% (11 respondents) stated that they have experienced cybercrime once, showing that a noticeable portion of the population has encountered at least one incident.

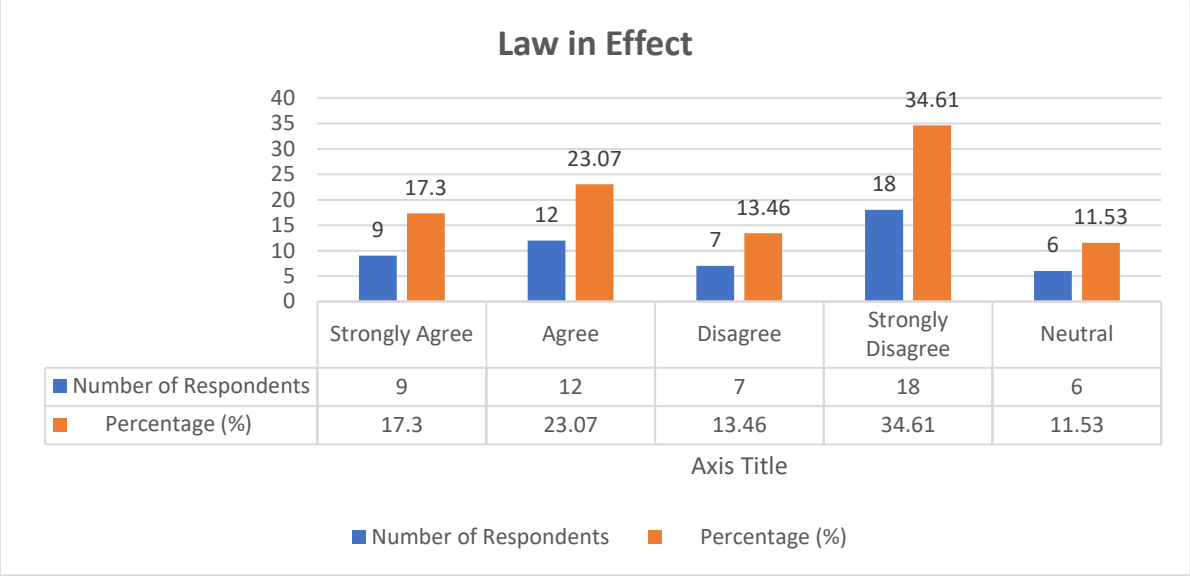
A small percentage, 3.84% (2 respondents), reported experiencing cybercrime 2–5 times, which suggests repeated victimisation among a few respondents. No respondents reported being victims more than 5 times, indicating that frequent or chronic victimisation is not evident in this sample.

Overall, the data shows that while the majority of respondents remain unaffected, approximately 25% of the respondents have experienced cybercrime at least once, highlighting that cybercrime is still a significant issue affecting a considerable segment of society. This emphasises the need for increased awareness and preventive measures to reduce cybercrime incidents.

Respondents' Opinion on the Effectiveness of Existing Cyber Laws

Table 3 illustrates respondents' perceptions regarding whether existing laws are effective in controlling cybercriminal activities:

Level of Agreement	Number of Respondents	Percentage (%)
Strongly Agree	9	17.30
Agree	12	23.07
Disagree	7	13.46
Strongly Disagree	18	34.61
Neutral	6	11.53



Analysis: From the above table, 17.30% of respondents strongly agree, and 23.07% of respondents agree with the statement. In contrast, 13.46% of respondents disagree, and 34.61% of respondents strongly disagree with the statement. Additionally, 11.53% of respondents remain neutral in their opinion.

The findings show that the highest proportion of respondents strongly disagree with the statement, followed by those who agree. When combined, 48.07% of respondents either disagree or strongly disagree, which is higher than the 40.37% who agree or strongly agree. This indicates that the overall opinion of respondents leans toward disagreement with the statement under study.

Conclusion

In the current digital era, where technology is continuously evolving, awareness of both the benefits and risks of cyberspace is crucial. Cybercrime has emerged as one of the fastest-growing forms of criminal activity worldwide, encompassing hacking, malware, phishing, identity theft, financial fraud, and other online offences. Protecting personal and sensitive information is paramount; individuals must refrain from sharing private data with strangers, unverified sources, or unauthorised entities.

In India, the Information Technology Act, 2000, provides the legal framework to combat cybercrime and promote cybersecurity. However, awareness among citizens remains uneven. While some individuals and organisations demonstrate strong knowledge of cybersecurity practices, others remain vulnerable due to limited awareness, training, or resources. This highlights the urgent need for comprehensive education programs and preventive initiatives to empower users to safeguard themselves effectively.

The study underscores the importance of collaborative efforts between governments, law enforcement agencies, private organisations, and civil society groups. Such collaboration should focus on strengthening legal frameworks, allocating resources for cybersecurity infrastructure, promoting international cooperation, and conducting targeted awareness campaigns.

Ultimately, addressing cybercrime requires a multifaceted approach combining technological solutions, legal measures, and societal awareness. By fostering a culture of vigilance, investing in cybersecurity education, and encouraging responsible digital behaviour, societies can create a safer, more resilient digital environment that protects individuals, organisations, and nations against the ever-growing threat of cybercrime.

References

1. Bossler, A. M., & Holt, T. J. (2020). *Cybercrime: Critical issues and emerging trends.* Routledge.
2. Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., & Savage, S. (2021). Measuring the cost of cybercrime. *Journal of Cybersecurity, 7(1), taaa007.*
3. McQuade, S. C. (2021). *Understanding and managing cybercrime* (2nd ed.). Pearson.
4. Wall, D. S. (2022). *The Routledge international handbook of internet crime* (2nd ed.). Routledge.
5. Kshetri, N. (2023). *Cybercrime and digital forensics: An introduction* (2nd ed.). Springer.
6. Smith, R. G., & Kumar, S. (2023). Cybersecurity awareness and behaviors among internet users: A cross national study. *Computers & Security, 119, 102832*
7. Europol (2024). *Internet Organized Crime Threat Assessment (IOCTA 2024).* European Union Agency for Law Enforcement Cooperation.
8. Interpol (2024). *Global Cybercrime Report 2024.* International Criminal Police Organization.
9. Chapple, M., & Kiltinen, J. (2025). Cybersecurity and society: Impacts, policies, and prevention. *Journal of Digital Security, 15(2), 45–67.*

Websites / Online Resources

1. Kaspersky. (2024). *Cybersecurity threat resource center*. Retrieved from https://www.kaspersky.com/resource-center/threat
2. AAG-IT. (2024). *The latest cybercrime statistics*. Retrieved from https://aag-it.com/the-latest-cyber-crime-statistics/
3. PurpleSec. (2024). *Cybersecurity statistics and trends*. Retrieved from https://purplesec.us/resources/cyber-security-statistics/
4. Norton. (2024). *Emerging threats and cybersecurity statistics*. Retrieved from https://us.norton.com/blog/emerging-threats/cybersecurity-statistics
5. Statista. (2024). *Global cybercrime statistics and trends*. Retrieved from https://www.statista.com/topics/3115/cyber-crime/