JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

An Analysis on Cybercrime Incident Awareness and Reporting

Ananiya Anantharaman
Mulund College of Commerce
Mulund west, Mumbai, Maharashtra
ananiyaapril06@gmail.com

Dr. Vishal Borude
Assistant Professor, Mulund College of Commerce
Mulund west, Mumbai, Maharashtra
vishal.borude@mccmulund.ac.in

ABSTRACT:
This article presents the results of a comprehensive survey investigating citizens' awareness of cybercrimes in India. The study gauges the extent to which individuals recognize prevalent cybercrimes, their familiarity with official helpline numbers, and assesses their ability to handle cybercrime situations independently. Furthermore, the survey explores respondents' capacity to identify scammers' tactics and examines the proportion of victims who reported incidents to cyber cells or local police stations. By analyzing response patterns and graphical data, the report highlights key trends in cybercrime awareness, self-efficacy, and official reporting behavior within the surveyed population.

Keywords: Cybercrime Awareness, Cybercrime Reporting, Public Awareness, Cybercrime Helpline

INTRODUCTION:

Cybercrime in India has been flourishing at an alarming rate, particularly since the onset of the COVID-19 pandemic. As citizens were confined to their homes during lockdowns, digital dependency became not a choice but a necessity. Online platforms for shopping (Flipkart, Amazon), education, banking, healthcare, and essential services became indispensable. This enforced digitization of society, while enabling continuity, simultaneously created a massive vulnerable population with inadequate cybersecurity awareness. Cybercriminals have capitalized on this unprecedented opportunity, exploiting the gap between rapid technological adoption and cybersecurity literacy. The result: cybercrime in India has reached its peak, affecting individuals across all demographic segments and socioeconomic backgrounds. Cybercrime is criminal activity conducted using computers and the Internet[1][5].This definition encompasses a wide spectrum of illicit activities:
Monetary Offenses like Stealing millions of rupees from online bank accounts through unauthorized access and fund transfers, Credit card fraud, digital wallet theft, and online financial scams, Unauthorized access to financial accounts and digital payment systems and **Non-Monetary Offenses** like, Downloading illegal music files and distributing copyrighted content without authorization, Creating and distributing viruses, malware, and ransomware to compromise computer systems, Posting confidential business information on the Internet, leading to corporate reconnaissance, Hacking into systems and extracting sensitive data for unauthorized purposes.

In contemporary times, as Artificial Intelligence becomes increasingly prevalent across every field and industry, the risks of information being leaked or stolen by adversaries have multiplied exponentially. AI-powered systems process vast amounts of personal, financial, and confidential data, making them attractive targets for cybercriminals.

The information gathered through cyberattacks is being leveraged by adversaries for:
Monetary gains: Selling stolen personal data on dark web marketplaces, conducting identity theft, perpetrating large-scale financial fraud, and extorting victims for ransom
Taking revenge: A prevalent phenomenon, particularly between competing companies, where data breaches are weaponized for competitive disadvantage or retaliation
Corporate espionage[4]: Stealing trade secrets, intellectual property, and strategic business information to benefit rival organizations. The convergence of AI sophistication and cybercriminal intent has created a dangerous ecosystem where the scale and speed of attacks far exceed what traditional cybersecurity measures can address.

Despite extensive efforts to combat cybercrime, a striking contradiction has emerged. Multiple government agencies, cybersecurity organizations, and media outlets continuously broadcast advertisements and awareness campaigns to educate citizens about cyber threats. Educational institutions and workplaces have incorporated cybersecurity training into their programs. Television, radio, social media, and public forums are saturated with cybercrime awareness messaging.

Yet despite this widespread awareness, a paradoxical pattern persists: many individuals who fall victim to cybercrimes do not report the incidents to cyber cells or police stations. This awareness-reporting gap reveals a fundamental disconnect:

Citizens know what cybercrime is, Citizens recognize that they are at risk, Citizens may have even experienced cybercrime themselves, Yet citizens refrain from reporting to authorities.
This phenomenon raises critical questions about where the awareness-action gap originates and what systemic or behavioral factors prevent reporting.

To understand this critical gap between awareness and action, a comprehensive survey was conducted among 200+ Indian citizens across diverse age groups, educational backgrounds, and professional categories. The survey assessed awareness levels, examined personal encounters with cybercrimes, analyzed how respondents handled these incidents independently, explored the reasons they did not report incidents to authorities, and investigated what factors would motivate or prevent them from doing so.

LITERATURE REVIEW:

A Dutch study of 97,186 victims shows cybercrimes like identity theft, consumer fraud, and hacking have the lowest police reporting rates (4-30%) compared to traditional crimes, with unique victim traits influencing decisions across subtypes and reporting targets (police vs. banks). Low reporting obscures surging prevalence (e.g., 3.5% consumer fraud in Netherlands), despite multiple options, due to barriers like perceived inefficacy. A separate 2019 Saudi survey of 1,230 nationals aged 18+ used an online questionnaire on skills, activities, cybercrime awareness, and cases to highlight gaps needing training. Exponential cyber risks drive global policies for resilience via certifications, sharing, audits, and anti-malware measures, with incident reporting mandated by EU NIS, NIST, and ENISA for recovery and prevention. Despite adoption, no prior evaluations exist; this realist synthesis tests if reporting serves as a "fire alarm" for CSIRT action and "policy learning" tool, using Italy's case

with interviews. The Italian context traces policy evolution, offering recommendations to avoid bureaucracy and enable adaptive strategies against cyber threats[6][7][8].

METHODOLOGY:

The research was conducted through a survey consisting of 5 to 6 targeted questions designed to assess public awareness of cybercrimes, experiences of cybercrime incidents, and scenarios where individuals may be unaware they have become victims. Additionally, the survey aimed to identify reasons why some individuals refrain from reporting such incidents. While many respondents have reported cybercrimes, only a limited proportion have experienced satisfactory solutions to their issues.

This survey-based methodology provides a foundation for a deeper analysis of the collected responses. The survey was administered using Google Forms and shared initially among family and friends, with further distribution through various social groups and networks to maximize reach.

The methodology serves as a critical basis for conducting subsequent, thorough analysis of the data gathered, enabling a comprehensive understanding of public perception and response to cybercrime.

ANALYSIS:

This analysis section interprets the survey findings on cybercrime awareness, victim experiences, and reporting behaviors to uncover key patterns and insights. It builds directly on the results by examining response trends, statistical relationships, and qualitative themes from the 5-6 questions distributed via Google Forms.

Fig. 1: presents the **gender-wise distribution** of more than 200 respondents who participated in the **"Incident Handling and Cybercrime Reporting"** survey. The sample is nearly balanced, with **males** constituting **48.9%** of respondents and **females 51.1%**, indicating an almost equal representation of both genders.
This near **50–50** split shows that female participation is slightly higher than male participation.

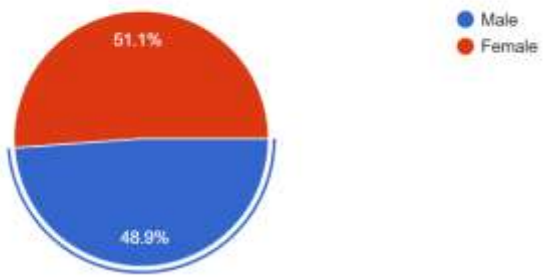

Fig.1 Gender-Wise Distribution in the Survey of 200+ people.

Fig. 2: presents a pie chart of **more than 200 respondents**, representing **100%** of the **survey sample**. The distribution shows that **98.2%** answered **"Yes", 1%** answered **"No"** and **1%** selected **"Maybe"** when asked about awareness of cybercrimes. This indicates that an overwhelming majority of participants are **aware of cybercrimes occurring around them**, and many are likely to **have encountered** such incidents either **directly or indirectly**.

Fig.2 Awareness of Cybercrimes

Fig. 3:

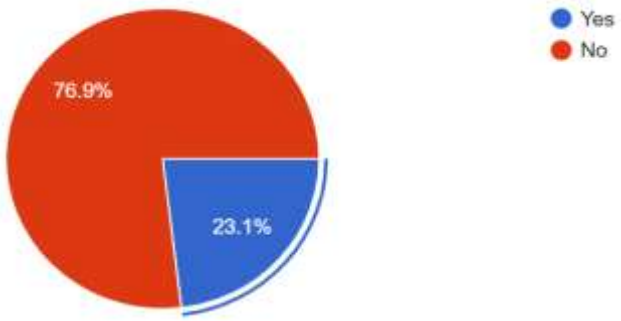

Fig.3 Cybercrime incidents encountered

Figure shows that **76.9% (170 out of 221)** survey respondents have not directly or indirectly encountered cybercrime incidents, while **23.1% (51 respondents)** reported experiencing such incidents. Considering India's estimated population of **approximately 1.46 billion in 2025**, this survey sample represents a very small fraction of the total population. Specifically, the **221 respondents correspond to roughly 0.000015% of India's population**. Despite the limited sample size, these percentages highlight the prevalence of cybercrime awareness and victimization within the surveyed group.

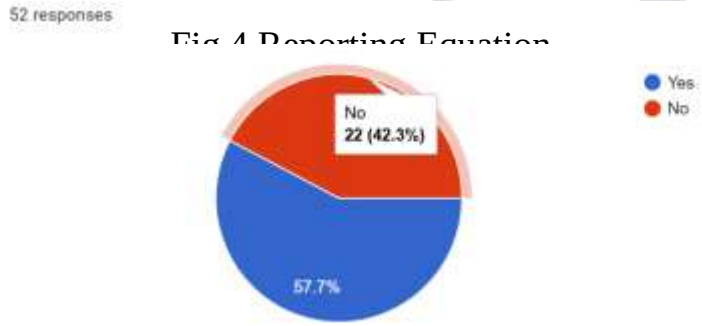

Fig.4 Reporting Equation

Fig. 4: Illustrates the reporting behavior of respondents who have experienced cybercrime incidents. Among **52** such respondents, **30 individuals (57.7%)** reported the incident to the relevant authorities, while **22 individuals (42.3%) chose not to report it.**

This distribution suggests that, although a slight majority of victims are willing to approach formal channels, a substantial proportion still refrains from reporting.

These unreported cases indicate possible barriers such as **lack of awareness, fear, or mistrust in the system**, which can contribute to underestimation of cybercrime in official records.

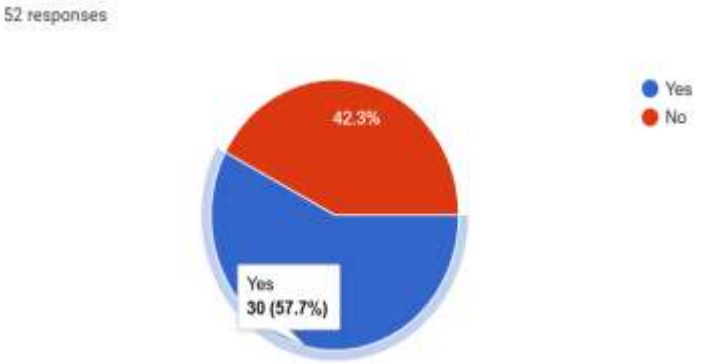

Fig.5: The figure presents a pie chart summarizing how **40 respondents** assessed the outcome of the cybercrime incidents they reported to authorities. The **largest segment (37.5%)** indicates that the cases were not resolved, while **25%** of respondents stated that their incidents were **completely resolved** and **15%** reported that they were only **partially resolved**.

The remaining, smaller portions of the chart correspond to responses such as **"Not reported," "I haven't confronted any such incident,"** and **comments** noting that authorities either did not register the complaint properly or only lodged it without effective follow-up. Overall, the chart suggests that although a portion of victims receive full or partial resolution, a significant share either experience no resolution or do not progress to a proper formal reporting stage.

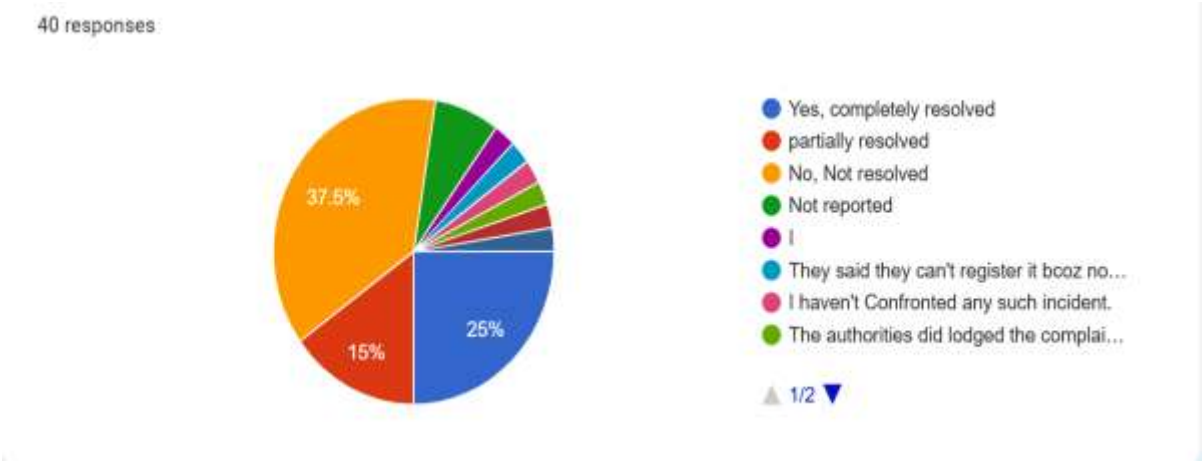

Fig.5 "Perceived Outcomes of Cybercrime Reports to Authorities"

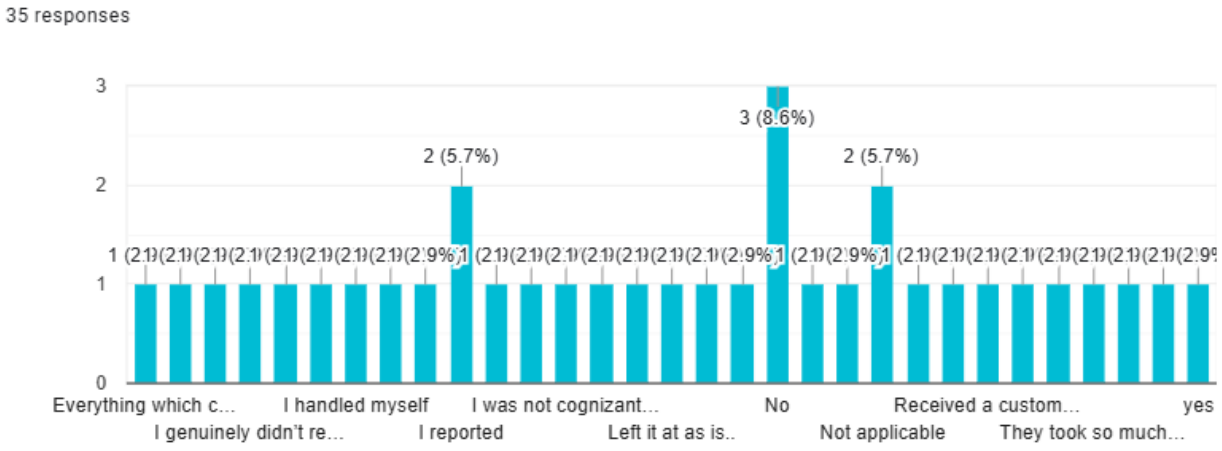

Fig.6 Categories of responses over complete, partial and no resolution provided.

Fig.6: This chart presents a range of responses that reveal how individuals experienced the resolution process of cybercrime incidents. Many respondents stated that they had reported the incident but did not receive a proper solution, while others may not have followed up after the initial report. This indicates that reporting alone does not always lead to closure, and victims often disengage when the process feels slow or ineffective.

A closer look at the responses also highlights several important patterns. Some individuals mentioned that it was **too late to file the complaint**, suggesting delays in recognizing or acting on the incident. Others explained that they chose not to report because there was **no monetary loss**, which reflects a perception that only financial harm justifies formal reporting. These insights point to gaps in awareness and motivation, where victims weigh the effort of reporting against the perceived seriousness of the incident.

From the chart, we can identify the following findings:

- **A small group reported their cases as completely resolved or partially resolved, showing that resolution is possible but not consistent.**
- **A larger portion indicated that incidents were not resolved or not reported, highlighting systemic weaknesses in follow-up and support.**

- **Some respondents mentioned reporting to helplines (such as 1930), but the outcomes remained unclear, suggesting a lack of transparency in the process.**
- **Several responses indicated no incident faced or marked the question as not applicable, showing that not all participants had direct experience with cybercrime.**

In my opinion, even when individuals report incidents correctly, the authorities often take too long to resolve them. This delay causes frustration and leads victims to lose patience, ultimately discouraging them from pursuing further action. The findings suggest that **timeliness, accessibility, and clear communication** are critical factors in building trust and ensuring that victims feel supported. Without these, many may choose not to report future incidents, which undermines both awareness and enforcement efforts.

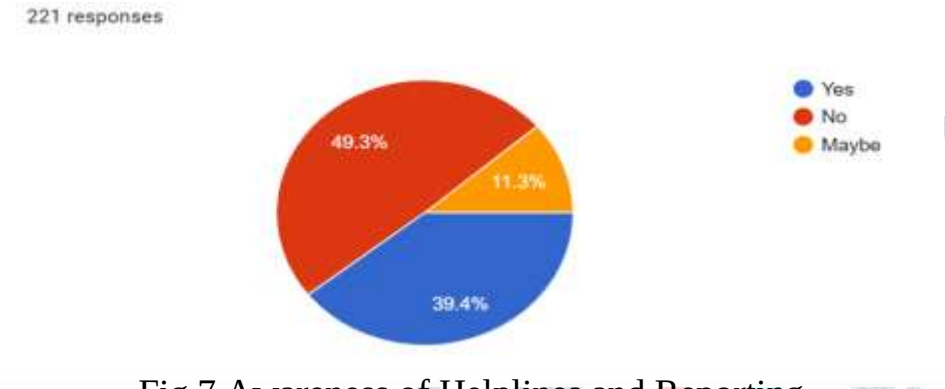

Fig.7 Awareness of Helplines and Reporting Channels

Fig.7: From the **221 respondents**, nearly half **(49.3%)** indicated that they are not aware of any helpline numbers for reporting cybercrime. A smaller portion, **11.3%**, mentioned that they might know, while **39.4%** confidently stated that they are aware of the helpline numbers.

An additional observation is that several responses included **"nil,"** which suggests uncertainty, either the individuals do not know the numbers or they are unsure whether the numbers they recall are correct. Some respondents also mentioned that, in the event of an incident, they would simply search online for the helpline and then act accordingly.

In my view, relying on a quick internet search during a sudden incident is not the best approach. In such stressful moments, panic can set in, and even a few seconds of hesitation may prevent timely action. It is far more effective to be mentally prepared in advance and to know the correct reporting channels. As citizens, we have the right to report cybercrime, and it is equally the responsibility of the authorities to ensure proper resolution. Strengthening awareness of helpline numbers and making them easily accessible can help reduce confusion and improve response during emergencies.

DISCUSSION:

The survey shows that most people understand what cybercrime is and know it happens around them, but far fewer actually face incidents or report them to the authorities. Even when victims do report, many feel their cases are not properly resolved, which reduces trust in cyber cells and police and makes them less likely to report again.

Knowledge of official channels such as the 1930 helpline and the National Cybercrime Reporting Portal is still limited, and many people say they would just "search online" during an incident, which might not work well in

a stressful situation. Some victims avoid reporting because they think the loss is too small, believe it is too late, or assume nothing effective will be done.

Overall, the study finds a clear gap between awareness and action: people know about cybercrime but are not fully prepared or motivated to use formal reporting systems. Improving communication about helplines, speeding up case handling, and explaining that non-financial harm also matters could help more citizens report incidents and feel supported.

CONCLUSION:

This study shows a critical gap between awareness of cybercrime and actual action taken by individuals. While most respondents are familiar with the risks, this awareness rarely translates into reporting incidents to cyber cells, police, or official helplines. Many people either have not faced cybercrime directly, or when they do, they choose not to report it. Even among those who report, a considerable number experience delays, unclear processes, or incomplete resolutions, which weakens trust in the system.The data also highlights that nearly half of the respondents are not aware of helpline numbers, while others are unsure or rely on searching online during emergencies. This uncertainty, combined with the belief that only major financial losses deserve reporting, contributes to underreporting. Such attitudes allow cybercriminals to continue unchecked and reduce the effectiveness of protective systems.

From my perspective, this study emphasizes the urgent need to simplify and speed up reporting procedures, make helpline information widely accessible, and encourage citizens to report all forms of cybercrime. Cybersecurity is not just about protecting individuals, it is a shared responsibility between the public and authorities. If reporting becomes easier and responses more reliable, people will feel empowered to act, and trust in the system can be rebuilt.

REFERENCES:

1. A Study on Awareness of Cyber Crime and Security Anupreet Kaur Mokha, Assistant Professor,SGTB Khalsa College, University of Delhi
2. A Study On Cybercrime Its Impact And Awareness Towards Society, NAMRATA K (Assistant Professor) CHETHAN V K(Assistant Professor) City College, Jayanagar City College, Jayanagar
3. A Qualitative Research on the Impact and Challenges of Cybercrimes V Krishna Viraja and Pradnya Purandare Symbiosis Centre for Information and Technology, Symbiosis International (Deemed University), Pune, Maharashtra, India
4. Analysis on Cyber Crimes and Preventive Measures Asha Thomas St. Albert's College (Autonomous), International Journal for Research in Applied Science & Engineering Technology (IJRASET) ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538 Volume 11 Issue V May 2023
5. Journal of Technology Innovations and Energy, ISSN: 2957-8809, https://doi.org/10.56556/jtie.v1i2.11, www.jescae.com, The Basic Concept of Cyber Crime, Osman Goni, Md. Haidar Ali, Showrov, Md. Mahbub Alam, Md. Abu Shameem
6. Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking,European Journal of Criminology 2019, Vol. 16(4) 486–508 © The Author(s) 2018 Article reuse guidelines: sagepub.com/journals-permissions DOI: 10.1177/1477370818773610 journals.sagepub.com/home/euc.
7. Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia Abdulaziz Alzubaidi, Department of Computer Science, Umm Alqura University, AlQunfudah, 28821, Saudi Arabia.
8. Evaluating incident reporting in cybersecurity. From threat detection to policy learning Simone Busetti, Francesco Maria Scanni University of Teramo, Via R. Balzarini 1, 64100 Teramo, Italy.