International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 06 | June - 2023 SJIF Rating: 8.176 ISSN: 2582-3930

CYBER CRIMES: TRENDING SOCIAL DISASTERS

Daxeshkumar Joshi

Research Scholar, Computer Science and Information Technology, Mahatma Gandhi University

---

ABSTRACT - Cybercriminals have taken advantage of the proliferation of online platforms where users are able to gather & disseminate information, leading to a raise in the online crime count. As a direct response to this, scholars & practitioners started attempting to comprehend this digital playground & the manner in which individuals who were socially & digitally entrenched could be influenced. This study's primary objective is to offer some insight into the problem of cybercrime in contemporary culture. The research design for this study is a combination of the exploratory research design & the descriptive research design. Per this investigation's findings, one can conclude that law enforcement agencies are exerting their maximum efforts to prevent cybercrime by monitoring communications activities that take place over the internet.

***Key Words*:** Cybercrime, Cybersecurity, Cyber Attack

1. INTRODUCTION

The introduction of continually new technology is one of the unique features of the modern world. People are extremely excited about new technology because they make life easier. However, new technologies will also bring up new criminal chances, which will eventually result in cybercrimes. The 4th Global Cybersecurity Index 2020[1] ranks India 10th in cyber security. India's cybercrime rate has quadrupled. Cybercrimes in India include phishing, fraud, hacking, & cyberstalking. Most cybercrimes in India involve phishing, along with credit/debit card & also online financial fraud. Also, cyber mishaps, in which fraudsters lure victims into clicking on harmful links & downloading malicious software to steal their personal information, are common in India.

CYBERCRIMES

When discussing cybercrimes, it is impossible to avoid mentioning hacking, which is the primary concern of businesses. In order to steal personal information from individuals & extort money from them, hackers make use of a wide array of dangerous software, such as Ransomware, Trojan, & Spyware. With over 560 million people connected to the internet, India is now the second-largest global online market. Also, in 2021, it reported an astounding number of 52,974 cases of cybercrime across the country (Aggarwal et al., 2022). Criminals in India are adopting increasingly sophisticated tactics to target their victims, which is contributing to the growing problem of cybercrime in the country. This problem is exacerbated by a number of variables, including low levels of public knowledge about the dangers of cybercrime & a shortage of qualified experts working in cyber security. Cyber-attacks have recently been carried out against a number of well-known companies, including Tata Power, CDSL, & AIIMS (Delhi) all of which are considered to be nationally important assets within their respective industries (Graves & Acquisti, 2023). The most important types of cybercrimes are as follows (Ibrahim et al., 2020):

PHYSICAL ATTACKS: Accessing an IoT device can lead to physical attacks. An IoT device-accessing firm employee can launch this assault.

ENCRYPTION ATTACKS: Hackers decipher your encryption keys. Cyber-assailants can install their algorithms & then take control of your system after unlocking the encryption keys.

DDOS (DISTRIBUTED DENIAL OF SERVICE) ATTACK: Services including websites may not have their data taken in this kind of attack. Multiple botnets are used to attack a service by sending it thousands of requests per second until it crashes and becomes unreachable.

FIRMWARE HIJACKING: Updated IoT devices are vulnerable to firmware attacks. Device hijackers can install malware. All firmware on computers is hackable.

BOTNET ATTACKS: When an IoT device is converted into remotely controlled bots that may be deployed as a member of the botnet, a botnet assault can be carried out. Botnets are able to connect to a network & send sensitive & confidential data. The Mirai botnet & also the PBot malware are two different botnet attacks.

MAN-IN-THE-MIDDLE ATTACK: This attack is carried out when a hacker inserts himself between two systems' communications by eavesdropping on a discussion between two people. The Man in the Middle assault has seven distinct varieties. Cybercrime takes many forms, some of which are: IP, along with DNS, as well as HTTPS spoofing & also SSL along with email hijacking as well as Wi-Fi eavesdropping & also cookie stealing, and so on.

BRUTE FORCE PASSWORD ATTACK: The hacker employs password hashing or password cracking software to try every possible combination of attacks on the server during the attack. Types of assaults using brute force: a) Basic brute force assaults b) Dictionary assaults c) Hybrid attacks using brute force d) Counterattacks using brute force e) Fake identification

PHISHING: Phishing is only one of the many online scams that aim to trick individuals into handing up their money.

[1] 'Global Cybersecurity Index' (Byju's) accessed 15 June 2023

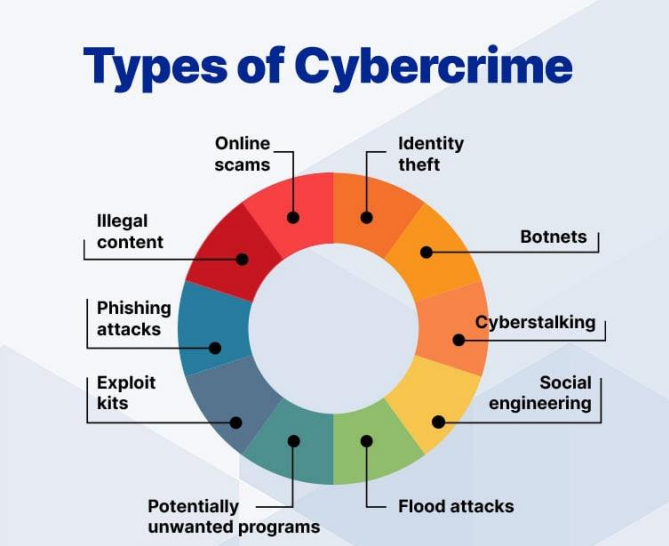

Figure 1: Types of cybercrimes (Yadav et al., 2021)

This study examines recent cybercrime research in relation to numerous security concepts, including confidentiality, integrity, & availability. The previous literature that is associated with this topic is discussed in greater depth in the following sections.

2. LITERATURE REVIEW

AUTHORS & YEAR	METHODOLOGY	FINDINGS
(Gupta et al., 2021)	Many nations, policymakers, & intelligence organizations are fighting cybercrime. Online processing's biggest challenge is protecting our daily data from digital misrepresentation & criminality.	This article analyses many cybercrimes & discusses efficient preventive & detection approaches to understand & protect our digital assets.
(Ho et al., 2022)	Examined how computer scientists, along with cybercrime researchers, & cybersecurity practitioners use SCP concepts to prevent & manage cyber-enabled crime.	SCP research on cybercrimes & discuss research gaps & future directions.
(Nguyen, 2023)	Discussed cybercrime effects in this work. Cybercrime involves individuals stealing data, documents, & financial information to harm organizations.	Comprehensive cybercrime information & tactics. Finally, I will study Internet-related financial crimes, cyber pornography, spoofing, bombing, & viral attacks.

Table 1: Literature Review

According to the literature survey listed above, cybercrimes on the Internet are an evolving concept whose varieties & impacts are changing daily. Thus, this paper briefly discusses cybercrimes & cyberattacks that can damage cybersecurity in general, encompassing numerous security principles.

3. METHODOLOGY

Both an exploratory research approach & a descriptive research strategy were utilised in the investigation. Researchers utilise exploratory methods to look for patterns in the occurrence of cybercrime. The evaluation of additional data that does not fit into any explanatory or exploratory research has been done using descriptive research. Since doing so best serves the intended aim, it is best to describe them. In order to effectively conduct market research and comprehend respondents' expectations of the government and knowledge of cybercrime, a sample of 325 respondents was selected. Both the study's geographical focus and its sample size are all of India. The basic data used in the analysis was collected from clients using a standardised questionnaire. Three hundred twenty-five people around the country filled out questionnaires for the study. These respondents, who are aware of cybercrimes & work in IT corporations & other government bodies, were taken into account for this study. The government website, papers, periodicals, & journals, among other places, were the primary sources of secondary data for the study, which mostly focused on the years 2020 to 2023.

4. RESULTS & DISCUSSIONS

According to a questionnaire analysis, one-fifth of respondents said that staff is one of the weakest points in the organization's defence systems against data theft, system compromise, or DDoS. Only 22% of CEOs were convinced they could identify these problems within 48 hours. Only 29% of the companies mentioned asking experts for help, according to the poll. According to 55% of respondents, laws pertaining to cybercrime need to be strengthened. 34% of people think that the laws & rules are unclear. 40% of the respondents think their proactive monitoring of cybercrime strategies is successful. The majority of respondents—44%—have effective data protection policies. However, according to 72% of respondents, their IT security teams lack the necessary experts to handle occurrences of cybercrime. Nearly 90% of the respondents agreed that social media posed a significant risk in terms of cybercrime.

This is fuelled by the reality that social media will play a significant role in their business's technological footprint & that they must be ready to manage the dangers connected with this channel. Less than 50% of respondents said they planned to increase their spending on items. According to a McAfee analysis , cybercrime is predicted to cost India 0.21 per cent of its GDP annually, & the number of occurrences is rising.

[2] https://www.mcafee.com/el-gr/consumer-corporate/newsroom/press-releases/press release. html?news_ id= 6859bd8c-9304-4147-bdab-32b35457e629&virus_k=98318

YEAR	CYBER CRIMES IN INDIA
2017	21796
2018	27248
2019	44735
2020	50035
2021	52974
2022	57976
Mean	39358
Std. deviation	13994.48
Coefficient of Variation	0.35557
Compound Annual Growth Rate	0.12546

Table 2: Descriptive statistics of Cyber Crimes in India from 2017 to 2022 [3]

The descriptive data for cybercrimes in India from 2017 to 2022 are shown in Table 2 above. In India, there were 39358 cybercrimes per year on average over the previous five years. According to the 13994.48 standard deviation value & 0.35557 coefficient of variation value, there is variation in the frequency of cybercrimes in India. With a compound annual growth rate of 0.12456 during the last five years, India has seen a 12.546 per cent increase in the number of cybercrimes committed there. The figure below illustrates the graphical representation of the above data.

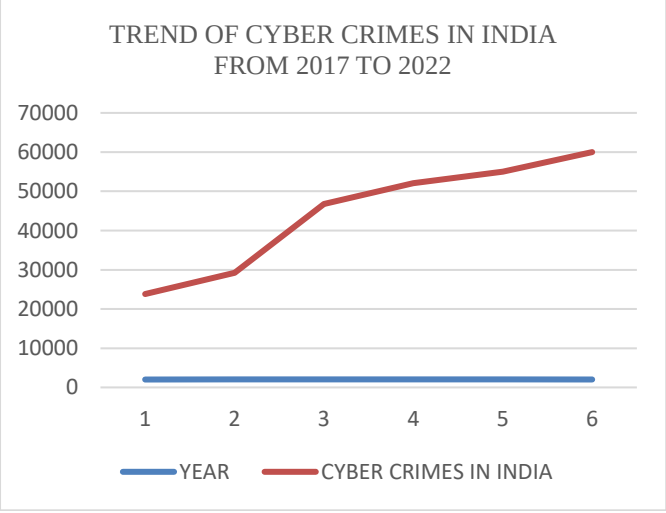

Figure 2: Trend of Cyber Crimes in India from 2017 to 2021

[3] https://ncrb.gov.in/en

A worrisome 33% of respondents to the poll indicated that businesses had trouble conclusively wrapping up their investigations into cybercrime incidents. Organizations may implement a cybersecurity defence paradigm, consisting of the following stages, to battle the dangers developing in this intricate cyber ecosystem.

PREVENT: proactive risk assessment of an organization's potential future risks

DETECT: Possible hacks are identified using cyber threat intelligence

RESPOND: delivering a dependable & consistent reaction to the situations

INVESTIGATE: examining the situation & determining the underlying reason

ADAPT: incorporating evaluation or inquiry results into the current information security practices

The two pieces of legislation in India that outline penalties for cybercrimes are the Information Technology Act of 2000[4] & the Indian Penal Code of 1860[5]. To give electronic transactions & businesses legal status, the Information Technology Act of 2000 was passed. Additionally, it sets out penalties for offences like data theft, cyberterrorism, & hacking. Section 43[6] , Section 66[7] , Section 66B[8] , Section 66C[9] , Section 66D[10] , Section 66E[11] , Section 66F[12] , & Section 67[13,14] , are a few of the act's sections that specifically include cybercrimes. There are penalties for offences including fraud, along with forgery, as well as identity theft, & more under the Indian Penal Code of 1860. Section 292[15] , Section 354C[16] , Section 354D[17] , Section 379[18] , Section 420[19] , Section 463[20] , Section 465[21] , & Section 468[22] are a few of the provisions of this code that deal with cybercrimes & their punishments (Vijayanand, 2022).

5. CONCLUSION

The technological landscape has been rapidly evolving, with recent shifts being particularly abrupt & unforeseen. Cloud, big data, mobile, & social media are just a few of the game-changing technologies that developed during this time. These innovations provided new capabilities &

[4] Information Technology Act 2000
[5] Indian Penal Code 1860
[6] Information Technology Act 2000, s 43
[7] Information Technology Act 2000, s 43
[8] Information Technology Act 2000, s 66B
[9] Information Technology Act 2000, s 66C
[10] Information Technology Act 2000, s 66C
[11] Information Technology Act 2000, s 66E
[12] Information Technology Act 2000, s 66E
[13] Information Technology Act 2000, s 67
[14] Ibid
[15] Indian Penal Code 1860, s 292
[16] Indian Penal Code 1860, s 354C
[17] Indian Penal Code 1860, s 354D
[18] Indian Penal Code 1860, s 379
[19] Indian Penal Code 1860, s 420
[20] Indian Penal Code 1860, s 463
[21] Indian Penal Code 1860, s 465
[22] Indian Penal Code 1860, s 468

benefits for businesses, but they also brought with them new threats. These technologies have the potential to breach the secure perimeter of businesses & expose confidential data if they are widely adopted. The risks connected with such technologies could perhaps increase in a geometric progression as they continue to change at an accelerated rate. As awareness among the companies has grown over the past ten years, so too have the cybersecurity controls that have been implemented. The emphasis is now on seeing assaults in real time & responding to them appropriately, rather than concentrating on "prevention" after the events.

ACKNOWLEDGEMENT

I would like to express our sincere gratitude to all the individuals and organizations that have contributed to the publication of this research paper.

First and foremost, I would like to thank my mentor, professors, for their invaluable guidance and support throughout the research process. Their expertise and insights were instrumental in shaping the direction and focus of my research. I am also grateful to Dr. Dinesh Baishya and officials of the Department of Computer Science and Information Technology at Mahatma Gandhi University for providing me with the resources and support I needed to complete this paper.

I would also like to thank my colleagues at Intelligence Team - my work place for their feedback and support throughout the research process. In particular, I would like to thank Mrs. F D Joshi, Advocate, for her valuable insights and suggestions.

Finally, I would like to thank all the participants in this study for their time and willingness to share their experiences. Their contributions have been invaluable in helping me to understand the topic and draw meaningful conclusions.

I would also like to express my appreciation to the IJSREM for considering my work and providing the opportunity to publish my findings.

REFERENCES

1. Ho, H., Ko, R., & Mazerolle, L. (2022). Situational Crime Prevention (SCP) techniques to prevent & control cybercrimes: A focused systematic review. Computers & Security, 115, 102611.
2. Gupta, D., Jha, S. K., & Surajmal, S. M. M. (2021, September). Internet Crimes-It's Analysis & Prevention Approaches. In 2021 9th international conference on reliability, Infocom technologies & optimization (trends & future directions)(ICRITO) (pp. 1-4). IEEE.
3. Nguyen, T. N. (2023). A review of cyber crime. Journal of Social Review & Development, 2(1), 01-03.
4. Graves, J. T., & Acquisti, A. (2023). An empirical analysis of sentencing of "Access to Information" computer crimes. Journal of Empirical Legal Studies.
5. Aggarwal, N., Sehgal, M., & Arya, A. (2022, November). An empirical analysis of Cyber Crimes, their prevention measures, & laws in India. In 2022 Seventh International Conference on Parallel, Distributed & Grid Computing (PDGC) (pp. 570-575). IEEE.
6. Vijayanand, K. (2022). Cybercrime, Cyber Protection, & Cyber Laws in India. Jus Corpus LJ, 3, 1190.
7. Yadav, H., Gautam, S., Rana, A., Bhardwaj, J., & Tyagi, N. (2021). Various Types of Cybercrime & Its Affected Area. In Emerging Technologies in Data Mining & Information Security: Proceedings of IEMIS 2020, Volume 3 (pp. 305-315). Springer Singapore.
8. Ibrahim, S., Nnamani, D. I., & Soyele, O. E. (2020). An analysis of various types of cybercrime & ways to prevent them. Int. J. Educ. Soc. Sci. Res, 3(02), 274-279.

BIOGRAPHY

An author is a professional investigator and uniformed official, engaged with one of the Government Disciplines. As a Research Scholar of PhD, he is researching on legal procedures and Indian laws to control cybercrimes. He possesses specialized qualifications in Cyber Crime Investigation & Computer Forensics, Detective (P) as well as Intelligence Management in addition to degrees of BCA, MBA & MCA. His focused aim of research emphasizes on mitigating cybercrimes in the society.