# Awareness Amongst Indian Citizens About Cybersecurity and Cyberattacks: in Mumbai

Shubham Surve[1], Clinton Santhis[2], Aaditya Thakur[3], Nafisa Ansari[4]
[1,2,3]*Department of Computer Science, Chikitsak Samuha's Patkar Varde College*

***Abstract* — In today's rapid digitalization era data is increasingly stored digitally. This data can vary from individual to large organizations. Cyber criminals aim to steal this data for ransoms, data manipulation, and phishing or for political gains through illegally obtaining confidential information. This kind of theft is known as the cyberattack, where the victim can be both an individual and large organization. Lack of awareness of the cyber hygiene amongst the citizens and poor security management of the organizations are the core reasons for increasing cyberattacks. This study explores the awareness of the cyberattacks and cybersecurity amongst Indian citizens, focusing on their concerns regarding their feeling of vulnerability to data loss, data breaches and preventive measures against cyberattacks. This research combines survey responses of individuals from diverse fields examining their familiarity with the common cybercrimes like doxxing, phishing, unauthorized access and ransomware. This paper further highlights the necessity of cybersecurity and cyber hygiene practices in educational discourse, suggesting initiatives like corporate training, government led campaigns to increase cyber literacy. By addressing these gaps, this research paper aims to promote a culture of encouraging tough digital practices to mitigate risk of cyberattacks to individuals and organizations in India.**

***Index Terms* — Awareness, Cyberattack, Cyberhygiene Cybersecurity, Digital literacy.**

## I. INTRODUCTION

In today's digitalized world large amount of data is being stored digitally on a large scale from individual to corporate level. Many organizations have their own databases or use cloud storage to store client's data. But there's a high risk of losing this data to cybercriminals. These Criminals aim to steal this information through *Phishing, Malware and unauthorized access of your accounts for personal financial gain or for political reasons.* India being the largest populated country in the world has also faced these types of cyberattacks for a long time.

These cyberattacks are increasing with both strength and sophistication. *India recorded 79 million cyberattacks in 2023, ranks 3rd globally.* The major reasons behind these attacks are limited digital literacy, lack of cyber awareness and poor security management.

This paper focuses on examining the familiarity and awareness amongst Indian citizens. Further this study proposes some effective implication to increase cyber awareness and cyber literacy to mitigate risk and to build safer digital ecosystem for organizations and individuals. The contents in paper are organized as follows: Section 1 contains the introduction of the paper. Section 2 deals with the information about the types of cyberattacks and the organizations responsible for these crimes. Section 3 reports the overview of cybersecurity in India. Section 4 contains the insights about the understanding of the people about cybersecurity through survey responses. Section 5 proposes the implicating measures to enhance cyber awareness and cyber hygiene. At last section 6 concludes the paper.

## II. CYBERATTACKS AND THEIR PERPETRATORS

### 2.1 CYBERATTACKS

*A cyberattack is any intentional effort to steal, expose, alter, disable, or destroy data, applications, or other assets through unauthorized access to a network, computer system or digital device.* Large organizations and individuals can be targeted for these attacks. Following are the some of the prominent types of cyberattacks:

- Malware Attack

This is one of the most common types of cyberattacks. "Malware" refers to malicious software viruses

including, ransomware, spyware and Trojans. Malware breaches a network when the user downloads an email attachment or clicks on a dangerous link or when an infected pen drive is used.

- Doxing

It is an act of publicly providing the personal identifiable information of an individual or organization without their consent via internet. Cybercriminals use doxing to target people for harassment, blackmail or for extortion of money.

- Phishing Attack

Attackers gain access of confidential information and account credentials through sending fake emails to the victims, impersonating self as to be a trusted contact of the victim. Unaware of this victim opens the mail and clicks on malicious links or downloads harmful attachments from mail.

- Ransomware Attack

It is a type of malware that encrypts victim's data until some amount of ransom is paid. These attacks are carried out through Trojan files attaching to the mails for tricking user into downloading these files. Attackers commonly use difficult to trace digital currencies such as crypto currencies, Bitcoin, paysafecard making difficult for authorities to trace them.

- Denial of Service Attack

It is also known as DDoS(Distributed Denial of Service) attack when attackers use multiple systems for attack. It is a significant threat to companies, here attackers exhausts resources and bandwidth of servers, websites or networks by flooding them with traffic.

- Data Breach

The unauthorized exposure, disclosure or loss of personal information can be known as data leak or data breach. Many criminals use this data to sell on dark web which elevates the identity theft of the people and organizations. Sometimes political repression, political activism becomes the motivation for these breaches.

- Insider Threat

In these cases, there isn't any third party responsible for the attack; it could be individual from the organization that knows everything about the organization and has access of all data. Greed or carelessness could be the reasons behind this attack.

- Emerging Threats

These are the new cyber threats that exploit technologies like quantum computing, artificial intelligence (AI) to commit cybercrimes. These technologies will give rise to the crimes like deepfake scams, AI- enable cyberattacks, supply chain attacks, IoT device attacks, etc.

The ongoing sophistication and development of cyberthreats across the globe highlights the increasing complexity in the digital world. Ransomware, phishing, doxing are just few of the many examples of the tools that cybercriminals employ. With new types of threats increasing learn regularly, it is necessary to learn more about the organizations coordinating these attacks. Next part will focus on the goals and strategies of the organizations responsible for such acts.

## 2.2 ORGANIZATIONS RESPONSIBLE FOR CYBERATTACKS

- Hacktivist Groups

Hacktivist groups promote environmental, political and social causes through cyberattacks. Ideological expression and protest are the motives behind their attacks. Large scale DDoS attacks, website defacement, data leaks, intend to draw attention to their message are the key operations of these groups.

Examples: *Multiple DDoS attacks carried out on gaming netwoks in 2014 by Lizard Squad, Infamous Anonymous Group known for conducting multiple attacks against institutions, corporations and organizations accused of corruption.*

- State Sponsored Entities

These cyberattack groups are backed by the national governments to fulfill their political, economical and military objectives through spreading misinformation, disrupting critical infrastructure, radicalization and intellectual property theft. These groups have highly skilled professionals working with advanced technologies and resources.

Examples: *2014 Sony Pictures Hack carried out by hacker group "Guardians of Peace" demanding*

*withdrawal of its then-upcoming political satire film "The Interview".*

- Terrorist Groups

These groups increasingly turn to cyberspace for circulating propaganda, recruitment and financial transactions. These groups have also started disrupting communication system, energy grids and financial institutions.

Examples: *ISIS leveraged social media for recruitment and radicalization across globe, Increase in infrastructure threat as terrorist groups explore methods like malware or hacking.*

- Corporate Espionage Groups

These groups focus on stealing intellectual property, business strategies and trading secrets to gain a competitive edge. These attacks may be arranged by rival corporations or state backed groups to dominate in industries.

Examples: *Confidential data of Google and Adobe allegedly obtained by Chinese entities in 2009.*
With increasing competition between enterprises and corporate, many of them committed cyberattacks on their competitors to affect their revenue and to boost their own sales. *According to the survey report of the Cloudflare, 40% of all DDoS attack on their cutomerss during Q4 of 2024 were committed by the competitors and remaining were state sponsored, self DDoS or committed by a disgruntled user.*

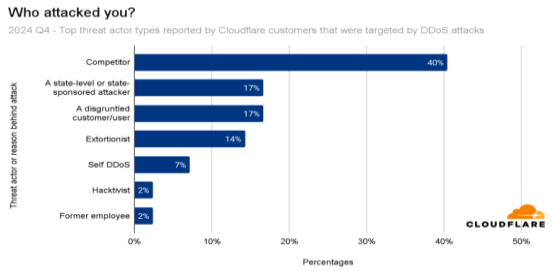



*Fig. 2.2.1 Cloudflare Top Threat Actors: 2024 Q4*

These organizations are significant reasons behind the rising tide of cyberthreats globally. There are many numbers of individuals and entities are still actively conducting these attacks where dark web serves as a hub for these cybercrimes. Their diversity in motives displays evolving and complex nature of cybersecurity challenges.

## III. OVERVIEW OF CYBERSECURITY IN INDIA

India is undergoing digital revolution, but with this exponential growth the vulnerability to the cyberthreats has also increased in multiple sectors like education, medical, e-commerce and governance. Over the last few years, there's a significant rise can be seen in cyber breach and cybercrime in India affecting large organizations and national security. According to CERT-In 2023 report, *CERT-In handled total 15,92,917 cyber incidents like Website Intrusion, Malicious code, Phishing, DDoS attacks, Website Defacement etc., in India.*

| Security Incidents | 2023 |
|---|---|
| Phishing | 869 |
| Unauthorized Network Scanning /Probing | 447720 |
| Vulnerable Services | 941592 |
| Virus/ Malicious Code | 184131 |
| Website Defacements | 10665 |
| Website Intrusion & Malware Propagation | 1045 |
| Others | 6895 |
| Total | **1592917** |

*Fig.3. 1 Security Incidents Handled By CERT-In in 2023*

CloudSEK's ThreatLandscape Report 2024 stated that *India has emerged as the second most targeted nation for cyberattacks globally, with 95 entities falling victim to data theft in 2024.*

India is facing multiple cyberattacks over a decade and this number is increasing at an alarming rate challenging security strategies of the authorities and organizations. These increasing cybercrimes are highlighting the critical gaps in cybersecurity awareness and readiness in India.

### 3.1 DIGITAL LITERACY RATE

India's digital literacy remains the significant obstacle in creating secure cyber space in the country. Oxfam reported in India Inequality Report 2022: Digital Divide that, only 38% of households in country are

digitally literate; where only 31% of the rural population uses internet as compared to 67% of urban population.

This data indicates that a large population of the country lacks in the basic skills required to safe their presence in the digital space. Due to this individuals and businessmen often overlook simple but important cyber practices as regularly updating software, using strong passwords and recognizing phishing attempts, making vulnerable and easy prey for the criminals.

### 3.2 AN EXPANDING DIGITAL ECOSYSTEM

India had over 886 million active internet users with 488 million users in rural areas by the end of 2024, holding second largest online population globally. However, this large number of user base attracts the criminals to take advantage of the poor security measures and lack of awareness, results in the increase in the cyberthreats like phishing scams, ransomware, doxxing, and spyware assaults by taking advantage of people's poor knowledge of online safety.

### 3.3 AWARENESS AMONGST THE CITIZENS

Despite of increasing cyberthreats, awareness remains low amongst people about cybersecurity. Surveys shows that fewer than *28% of individuals* identify security warnings. In addition, practices like password reuse is widespread, with *63% of internet* users rely on identical credentials across multiple platforms risking the chances of data breach. The absence of structured cybersecurity education in workplaces, colleges and schools inflame the problem. Without any training and knowledge individual fails to identify the warning indicators before attacks leaving themselves exposed to the threat.

### 3.4 GROWING RISKS TO CYBERSECURITY

India ranked second in the world for cyber incidents in 2024, notable cyberattacks as *The Wannacry ransomware event, BSNL data breach, Angel One data breach, Cosmos Bank cyber heist and the AIIMS ransomware assault* underlines the urgency for improving defenses. These attacks have not only caused the financial damage but also compromised the private data of the multiple individuals. The government and enterprises should focus on proactive response for these threats to prevent further damage in future.

Rapid advancement in technology has fueled growth of cyber attacks making it more sophisticated and harder to tackle. India's journey towards digital empowerment is filled with challenges, especially maintaining its rapidly increasing digital ecosystem. Addressing these challenges will help the authorities to build a resilient digital framework that will safeguard the information and data securely. The next section dives into insights gathered from generalize survey to shedding light on current state of cybersecurity knowledge among citizens.

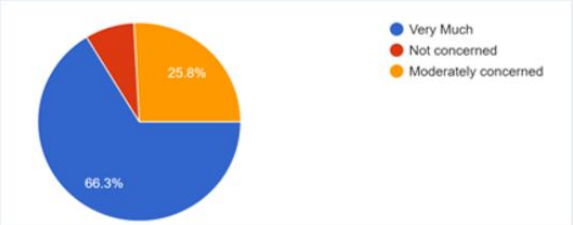
## IV. INSIGHTS OF CYBERSECURITY AWARENESS IN INDIA FROM SURVEY

Understanding amongst citizen plays a vital role in tackling and avoiding cyberthreats in the country. India being one of the largest populated countries in the world, it is necessary to understand the familiarity and awareness amongst the citizens about the topic. To get the overview of this understanding, we have conducted a survey through Google forms targeting individuals from Mumbai of age between 16 to 24 years. This survey focused on understanding familiarity of the Mumbai's youth with the terms like cyber hygiene and cyberattacks to evaluate their knowledge of cybersecurity threats, practices and opinion on India's digital safety preparedness ensuring a representation of the younger generation.

### 4.1 SURVEY RESULTS

- Concerns about data vulnerability
  - 63.3% respondents are very concerned about their data vulnerability.
  - 25.8% of respondents are moderately concerned about their data vulnerability.
  - 7.9% are not concerned about their data vulnerability

*Fig. 4.1.*




*data vulnerability stats*

- Awareness About Government Initiatives

- 51.1% of respondents are aware of government initiatives.
- 48.9% of respondents are not aware of any initiatives.

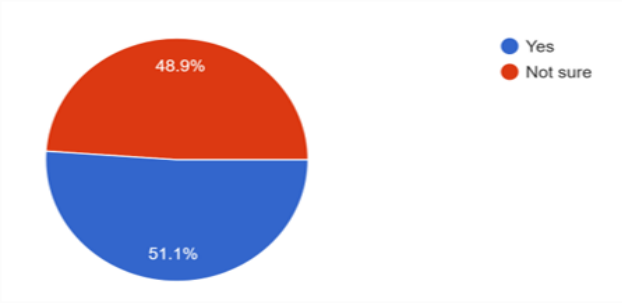



*Fig.4.1.2 Awareness of Government Initiatives*

- Participation in Training Programs or any Workshops
- 46.1% respondents have not attended any training programs or workshops.
- 36% have attended any training or program.
- Remaining 18% are not sure about they attended or not

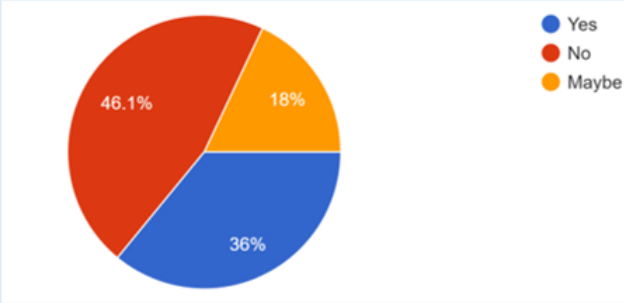



*Fig. 4.1.3 Participation in Workshops or Training*

- Trust On Preparedness Of Organizations
- 40.9% are not sure to respond.
- 38.6% of respondents believe that our organizations are poorly prepared.
- 20.5% think that our organizations are well prepared to tackle cyberattacks.

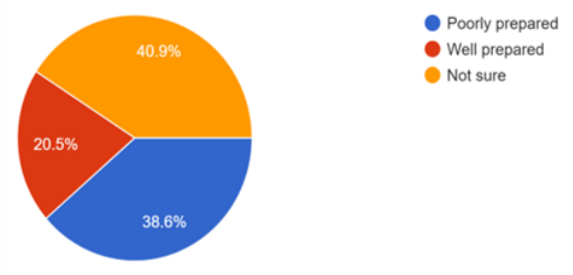



*Fig. 4.1.4 Trust on security of organizations*

- Experience of Cyberattack
- ~56% of respondents haven't experienced a cyberattack by themselves or any of the people they know.
- ~43.8% respondents have experienced cyberattacks by themselves or another person they know.

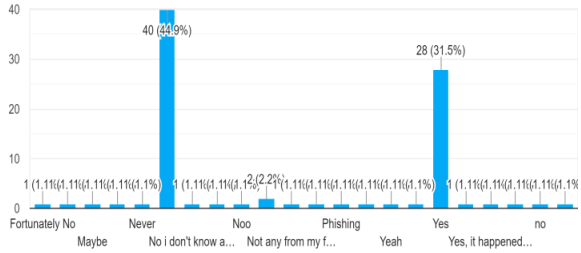



*Fig. 4.1.5 Cyberattack Experience*

- Reasons For Increasing Cyberattacks in India
- Majority of respondents believe that lack of awareness and knowledge amongst workers is the major reason for cyberattack.
- Some of them believe that lack of accountability, poor security management and lack of advancement in software usage and tech are reasons for the uprising of cyberattacks.
- Remaining ~10% of respondents don't have any idea about the reasons.

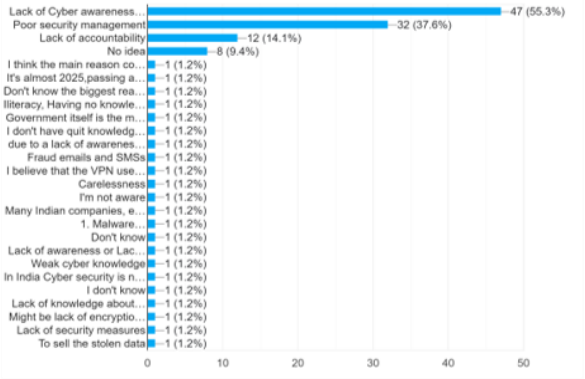



*Fig. 4.1.6 Reasons for Increasing Cyberattacks*

- Need Of Cybersecurity in Educational Discourse
- Nearly 95% of respondents believe that the every education institutions should provide awareness amongst students regardless of their fields.
- ~5% respondents answered that the workshops should be centered around only IT fields.


*Fig. 4.1.7 Need of cybersecurity in educational discourse*

4.2 Summary of Survey

The findings highlight the lack of awareness in the respondents about any of the government initiatives like *Cyber Surakshit Bharat, Personal Data Protection Bill, National Cybersecurity Policy 2013, Cyber Crime Coordination Centre, The Information Technology Act, 2000.* Also it shows the less number of participation in cybersecurity campaigns and workshops. Majority of the respondents are concerned about their data but also show their lack of trust on the security of the organizations and the authorities, reflecting the failure of the authorities and enterprises to provide and ensure security of their data. The lack of surety to respond also shows the lack of information about the topic. However, a majority of the respondents believe that the lack of awareness amongst citizens is the key reason behind this issue and it is necessary to mitigate this problem to tackle the future attacks.

## V. EFFECTIVE MEASURES FOR CYBERSECURITY ENHANCEMENT

In today's digitalized world, securing data has become a primary concern for everyone from individuals to large organizations. To secure this data basic awareness is required among citizens to identify these threats. In terms of India, even after having a rapid expansion in the digital landscape, the majority of the population fails in basic cyber threat identification, lack of simple cyber practices resulting in growth of cyberattacks. By looking at the possible use of advanced technologies for cyberattacks it is essential for the authorities and enterprises to take a forward step to mitigate this risk by enhancing cyber knowledge across the country. In this section, we have proposed some of the measures for the government and large organizations to enhance cybersecurity of India.

### 5.1 RAISING AWARENESS

The first step towards this initiative should start with making people aware about cyber threats and their consequences through government led campaigns and programs to put a strong impact on the people. After creating urgency about this topic; the next step should be educating everyone for performing basic cyber practices and identifying cyber threats through workshops and campaigns.

To improve the security of the enterprises, corporations should educate and aware their workers by conducting training programs in their offices throughout the year for each worker to identify bigger threats quickly.

### 5.2 PROMOTING DIGITAL LITERACY AND CYBER HYGIENE

The major challenge for the authority is to reach out to every side of the country. It will be hard for them because of India's large population of multiple ethnicities distributed in rural and urban areas across the various professions. It will take lots of time to educate each and everyone. To overcome this problem, the government should promote digital literacy and cyber hygiene with the help of multiple media elements like Television, Social Media and News Articles.

- Television

Large number of households use television across India for entertainment, news, etc,. Even the rural areas also have a large number of access to the television. Television would be a great medium for the government to educate people about maintaining cyber hygiene by airing a show that focuses on teaching some basic cyber practices like setting strong practices, using multi-factor authentication, and avoiding spam messages. This will help to reach adults and senior citizens at once across the country in their own regional languages.

- Social Media

India has nearly *462 million active social media users.* As we just saw in the survey , most of the respondents were unaware about any of the government initiatives taken for cybersecurity. This highlights how our

authorities lack in reaching their campaigns and initiatives to the people. Social media would be the most beneficial option for promoting these campaigns on various platforms like Instagram, Youtube, Whatsapp. It will help authorities to encourage the people to voluntarily participate in their campaigns.

- Newspaper

Newspapers can be used to publish articles on cyberattack incidents across the globe, to inform people about new trends and technology and their usage, to tell them the importance of cyber practices through some professionals. These articles can be published once or twice in a week.

### 5.2 TOPICS RELATED TO CYBERATTACK AND CYBERSECURITY IN EDUCATIONAL DISCOURSE

Young generations are the future of the country and it is essential for them to be prepared to tackle cyberattacks in future, and this can be achieved by introducing topics like cyber hygiene, cybersecurity, cyberattacks in educational discourse regardless of the fields. This initiative can be divided into three sections.

- Section 1: This section focuses on the students studying in secondary and higher secondary standards. In this section the syllabus will focus on introducing the basics of cybersecurity where they first learn about how the data is digitally stored and how essential it is to keep it safe. Further they will briefly learn about the cyber laws of India like *The National Cyber Security Policy, 2013, The Personal Data Protection Bill, 2019, Information Technology Act, 2000.*

- Section 2: This section focuses on theoretical based learning. This section is structured for the undergraduate and postgraduate students who aren't part of the IT fields. In this section the syllabus gives the insights on how the cyberattacks are executed in various ways targeting every kind of person. Further they will study how to identify the cyberthreat, cyber hygiene and multiple cyber practices which an individual must follow. Then information about the legal procedure to take while experiencing a cyberattack.

- Section 3: This is the most important section amongst all of them. This section focuses on undergraduate and postgraduate students in the IT fields. It is structured for half theoretical and half application based learning. Syllabus contains the overview on how cybercriminals unauthorizedly access the data, data security, knowledge about the use of AI in cyberattacks and different ways to identify and tackle the cyberthreats.

  The application in this syllabus is conducting multiple workshops and campaigns with the help of universities or higher authorities for senior citizens and adults to educate them about data safety and teaching some basic cyber practices to avoid data breach and unauthorized access to any individuals.

### 5.3 FOCUS ON STRENGTHENING CYBERSECURITY

Governments and organizations have the responsibilities of the security of the data of multiple citizens and to keep this data safe it is necessary to have strong cybersecurity. Increasing sophistication in cyberthreats demands strong tackle from the authorities.

To enhance this defence, the government should invest in advanced technologies like machine learning and AI to detect and counteract threats in real time. Prioritizing important public sector systems like healthcare, power grids, banks to prevent larger threats. Creating user-friendly system to report cybercrimes, including toll free helpline for immediate assistance. Collaborating with tech organizations to increase resources and expertise. Cooperating on the international stage by engaging in information sharing and threat intelligence.

To create a safer digital space for the country it is essential for India to focus on education, governance, technology and collaboration. By embedding these measures within the nation, the country can enable sustainable digital growth.

## VI. LIMITATIONS & CONCLUSION

### 6.1 Limitations

This research paper aims to explore and showcase the level of awareness amongst the Indian citizens regarding to cybersecurity and cyberattacks, it is

important to mention certain limitation that can affect generalizability of its findings. The most important limitation lies in geographic limitation of the study. The survey data collection is conducted exclusively within the Mumbai metropolitan region. As a result, the conclusion drawn from this survey represents the knowledge and understanding of individuals residing in Mumbai.

Mumbai is a digitally connected and highly urbanized city; it offers better access to technological infrastructure, internet and cybersecurity awareness initiatives compared to many other regions in India. This larger accessibility can increase the awareness and responsiveness to cyber threats, compared to the people in semi urban or rural individuals.

Therefore, the survey results don't fully represent the demographically diverse and varied population. Factors like income disparity, access to digital resources, education levels and state specific initiatives on cybersecurity can influence the awareness levels in different part of the country.

6.2 Conclusion

In an increasingly digitized world, cybersecurity has particularly become the topic of attention for many nations worldwide. In India, where digital development has exploded, the challenges for addressing cyberthreats are numerous due to low awareness, limited digital literacy, and poor cybersecurity infrastructure. The findings of this study highlights the gaps in public understanding of cybersecurity resulting in exponential growth of cyberthreats in the country. Private and public sectors must concentrate on the efforts to mitigate these risks. This paper tries to propose some initiatives for both sectors to adopt so we can work toward a safer digital environment.

As India embrace digital transformation, the focus must shift towards building a cybersecurity culture where individual is equipped with the knowledge to secure his digital presence and focus in advanced technologies like AI driven threat detection for secure data handling. India's future digital landscape pivots between security and innovation.

REFERENCE


[1] Pushkar Sudhir Baviskar, Manikant Roy "Wanna cry ransomware: A case study in Indian perspective".

[2] CERT-In Annual Report 2023.

[3] Kurt Baker "12 Most Common Types of Cyberattacks", CROWDSTRIKE, May 13, 2024 https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/common-cyberattacks/

[4] PTI, "India Recorded 79 Million Cyber Attacks In 2023, Ranks 3rd Globally", NDTV, Apr 30, 2024 https://www.ndtv.com/india-news/india-recorded-79-million-cyber-attacks-in-2023-ranks-3rd-globally-report-5558748

[5] PTI, "Significant percentage of Indian companies hit by ransomware attacks in 2023", Hindustan Times, May 14, 2024 https://www.hindustantimes.com/technology/significant-percentage-of-indian-companies-hit-by-ransomware-attacks-in-2023-sophos-101715676050970.html

[6] Simon Kemp, "Digital 2024: India", DataReportal, 21 Feb 2024 https://datareportal.com/reports/digital-2024-india#:~:text=There%20were%20751.5%20million%20internet%20users%20in%20India%20in%20January,January%202023%20and%20January%202024.

[7] Gaurav Sahay, "Legal Challenges of Cybersecurity Risks", CXOtoday.com, Oct 08, 2024https://cxotoday.com/specials/legal-challenges-of-cybersecurity-risks/

[8] Anu Thomas, "Zomato hacked: Security breach results in 17 million user data stolen", TheEconomicTimes, May 19, 2017 https://economictimes.indiatimes.com/small-biz/security-tech/security/zomato-hacked-security-breach-results-in-17-million-user-data-stolen/articleshow/58729251.cms?from=mdr

[9] AICTE, "Cyber hygiene / Cyber Security / Prevention of Cyber Crimes"https://www.aicte-india.org/CyberSecurity

[10] Cyber Law - Trends and Developments in India - Pavan Duggal

[11] Significant percentage of Indian companies hit by ransomware attacks in 2023 - Hindustan Times

https://www.hindustantimes.com/technology/significant-percentage-of-indian-companies-hit-by-ransomware-attacks-in-2023-sophos-101715676050970.html

[12] Information technology act 2000 India - https://www.meity.gov.in/content/cyber-laws

[13] Key Government's Initiatives to Enhance Cybersecurity Awareness. https://pib.gov.in/PressReleasePage.aspx?PRID=2037115

[14] Recod-breaking 5.6 Tbps DDoS attack and global DDoS trends for 2024 Q4 – Cloudflare https://blog.cloudflare.com/ddos-threat-report-for-2024-q4/#:~:text=In%202024%2C%20Cloudflare's%20autonomous%20DDoS,4%2C870%20DDoS%20attacks%20every%20hour.