10.48047/jocaaa.2024.33.08.82

Cybercrime and India's Economy: Assessing the Current Landscape

Dr. Sandeep
Assistant Professor,
School of School of Engineering and Technology
Om Sterling Global University,Hisar-125001
Email: - sanghanghas1991@gmail.com

Abstract

Indian economy is world fifth largest economy according to projections by the International Monetary Fund (IMF). Government o India launched Digital India initiative to the country's digitalization system on July 1st, 2015, a project worth Rs.1,13,000 crores. According to analysts, this initiative could increase GDP by up to $1 trillion by 2025.The rapid advancement of digital technology has brought about significant changes like revolutionizing the way people communicate, conduct business, and access information. . However, this transformation has also given birth to new forms of criminal activity. Criminal activities done by using computer and internet are commonly known as cybercrime. Cybercrime puts India's ambitious digital transformation projects in danger. Fear of cybercrime may prevent the companies to adopt the digital technology. It halting development and obstructing the potential benefits of a digital economy. The purpose of this paper is to provide a comprehensive analysis of impact cybercrime on Indian economy. It examines the nature and types of cybercrimes prevalent in the country, the legal framework governing cybercrime, and the difficulties and associated strategies. The findings emphasize the importance of strong cybercrime legislation, stronger law enforcement powers, and a development of a safe and efficient framework for dealing with cybercrime. This paper aims to contribute to a better understanding of cybercrime trends in India by examining the present cybercrime landscape.

Keywords: cybercrime, ransomware, data breach, phishing, deepfake.

1. Introduction

Indian economy is one of the fastest developing economies in the world, with a very young population that accounts for (65%) of total population. Government o India launched Digital India initiative to the country's digitalization system on July 1st, 2015, a project worth Rs.1,13,000 crores[1]. According to analysts, this initiative could increase GDP by up to $1 trillion by 2025.The rapid advancement of digital technology has brought about significant changes like revolutionizing the way people communicate, conduct business, and access information. However, this transformation has also given birth to new forms of criminal activity. Criminal activities done by using computer and internet are commonly known as cyber crime. Cybercrime is an umbrella term used to refer to all illegal activities which are done over the internet such as identity theft, or invasion of privacy, trafficking in child pornography, Cyber terrorism,Cyber stalking, Data breaches etc.[2] Cybercrime puts India's ambitious digital transformation projects in danger. Cybercrime also impacts data security and infringes privacy, with major social consequences. It can have a substantial impact on macroeconomic aspects

10.48047/jocaaa.2024.33.08.82

such as GDP growth, worker productivity, job creation, business growth and revenue leakages for the government.

Cybercrime is an increasing threat to businesses and individuals worldwide, including India. The Indian government predicted that cybercrime cost the country's economy $1.4 trillion, in 2022.By 2025, this amount is predicted to increase to $2.5 trillion. According to a survey, the number of cyber attacks in India increased dramatically in the Q1 of 2023[3].According to Indusface's State of Application Security Report, over 500 million cyber attacks were blocked in India in Q1of 2023, out of a billion attacks globally[4].According to acyber security firm CheckPoint Research, weekly attacks scaled by 18% in India during the first quarter of 2023, compared to a 7% growth internationally, with an average of 1,248 attacks per week.

In January 2023, the Indian Computer Emergency Response Team published its yearly report on cy bercrime in India[5]. According to this report Indian economy suffered significantly by cybercrime in 2022. According to the report the number of cybercrime incidents in India scaled up by 35% in 2022. Phishing was the most common type of cybercrime, which represented 52% of all incidents. Other common types of cybercrime included ransom are attacks, data breaches and malware attacks. According to the report, cybercrime will cost the Indian economy $1.2 billion by 2022. This figure comprises thereputational damage, costs of lost production,
and the cost of reacting to cyber attacks.

As per World Bank projection, cyber-attacks could have caused losses of around $5.2 trillion to the world between the years 2019-2023[6].

As one of the world's largest digital economies, India has suffered significant financial losses as a result of cyber-attacks. Individuals, corporations, and financial institutions are all targeted in these incidents, which leads to direct financial losses and lowering customer trust[7]. Cyberattacks also obstruct commercial activities, which has a serious negative impact on Indian firms.They choke crucial infrastructure, limit productivity, and disrupt supply networks, limiting economic growth and progress. Furthermore, cybercrime threatens India's ambitious digital transformation ambitions.

In addition to immediate financial damages, cybercrime can harm firms' reputations as well as decrease productivity. Cybercrime can even result in loss of employment in certain cases. Cybercrime also increase the financial burden on companies because they invest a certain amount on cyber security. Companies should invest 10% of their information technology assets on cyber security[8].

2. Cybercrimes

The term cybercrime was given by Sussman and Heuston in 1995.It is difficult for many individuals to define "cybercrime" exactly, even if the phrase has been widely used. Cybercrime has many diverse aspects and takes place in a wide range of settings and situations, just like traditional crime. Cybercrime definitions today have changed as a result of experience. They vary based on the perception of both victim and observer/protector, and are partially a result of the geographic growth of crimes involving computers[40].

Thus, cybercrime can be seen as a broad word that includes computer-assisted crime, which is crime in which technology and computers play a supporting role, like sending harassing messages via a computer. However, the term "cybercrime" also refers to crimes that are specifically centered on computers and would not be possible without them[41]. It is an offence that can be done only through using a computer, computer network, and other form of information communication technology[18]. It include spread of malwares (like viruses, worms, Trojan horses), hacking, Denial of services etc.

10.48047/jocaaa.2024.33.08.82

2.1. Types of cybercrime that affect the Indian Economy

2.1.1Phishing -

It is a sort of cybercrime in which criminals send emails or text messages that appear to be from offi cial sources such as banks or government institutions. This email or text message many times contain links that, when clicked, take a person to counterfeit websites that look like the real websites. Once a person enters their private information on the counterfeit websites, the criminals can steal it. Phishing is an attack in which the perpetrator uses social engineering techniques to steal someone's identity. Traditionally, phishing involves sending a fake email, impersonating an online bank, auction, or payment website, and directing people to a fake website that is meticulously crafted to appear as the login for the real website.42

According to CERT-IN, it is a major threat to the Indian economy. The Indian Computer Emergency Response Team (CERT-In) stated a 35 per cent increase in scams in 2022. It also estimated that phishing attacks had cost the Indian economy over $1 billion in 2022. Section 66D of IT act 2000 deal with phising (By using phishing emails that connect to a fake bank or organisation website, fraudsters act as banks or financial institutions and defraud unsuspecting people; this also constitutes a violation under Section 66D).28

2.1.2. Ransomware

Ist is a type of malicious software that encrypts systems and demands a ransom payment in order to decrypt them. Ransomware attacks have grown in frequently in recent years and have had a substantial impact on the Indian economy. CERT-In stated that ransomware attacks had increased by 35% in 2022. According to CERT-IN, ransomware attacks had cost the Indian economy over $1 billion in 2022[43].

Figure 1 explores the ransomeware attack on various sector of Indian economy.

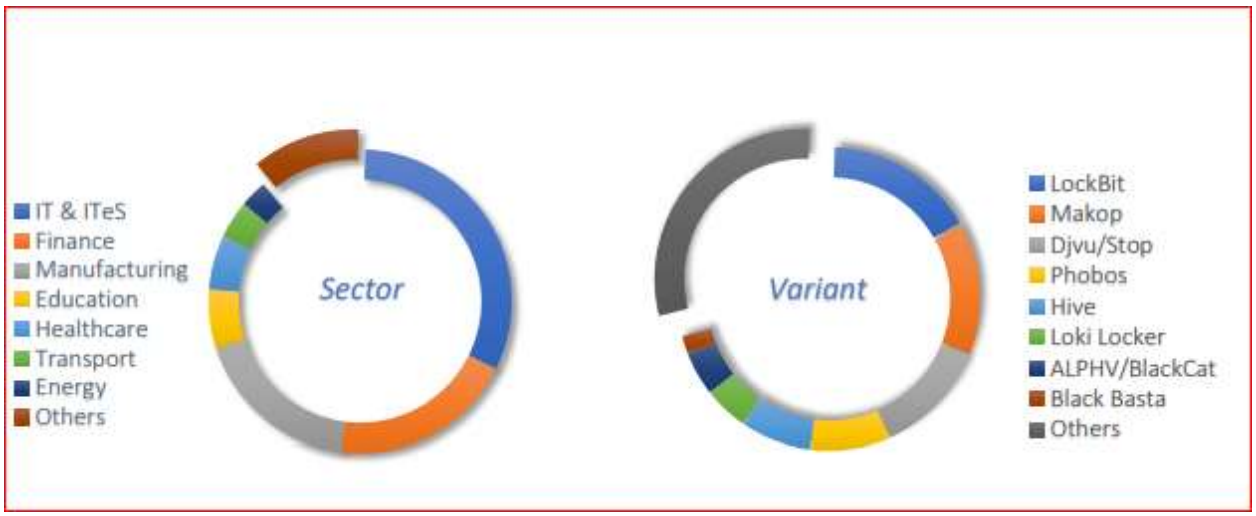

Figure. 1Ransomware attacks on various sectors of Indian Economy

10.48047/jocaaa.2024.33.08.82

Reproduced from:https://www.cert-in.org.in/PDF/RANSOMWARE_Report_2022.pdf

Overall, Ransomware incidents reported in 2022 are up 53% year on year. IT and ITeS were the most hit sectors, followed by finance and manufacturing. Early in February 2024, RansomHub appeared as a straightforward data leak website (DLS)[27].
In the Indian context, Lockbit was the most commonly encountered form, followed by Makopand DJVU/ Stopransomware[9].
Akira, a new found Ransomware operation, has been reported to be active in cyberspace[10]. This indicates that ransomware poses a growing threat to India's digital infrastructure and economy. Other sources have provided estimates of the potential economic impact of cybercrime in India, including ransomware attacks. For example, a report by the Indian government's Ministry of Electronics and Information Technology (MeitY) estimated that cybercrime could cost India up to 0.8% of its GDP in 2025. This translates to a potential loss of over Rs 1.2 lakh crore[44].

2.1.3. Denial-of-service (DoS)

DoS attacks are a sort of cybercrime in which attackers flood a website or server with traffic, rendering it inaccessible to genuine visitors[52]. DOS attacks have the potential to have a huge impact on the Indian economy by disrupting companies, government services, and key infrastructure.(DoS) attacks aim to prevent authorized users from gaining access to a particular network resource[53].

The impact of DOS assaults on the Indian economy is classified into two categories:

1. Direct costs: These are the direct expenses paid by businesses and individuals as a result of a DDoS attack. These expenses may include neglected productivity, data restoration, and the cost of employing consultants to assist with the investigation and remediation of the threat.
2. Indirect costs: These are the expenses made as a result of a denial-of-service attack. These expenses include loss of revenue, reputational damage,Intellectual challenge and loss of customer[54].

According to report of Ponemon Institute the average cost of direct a DOS attack for a big organization is $2.4 million. As per report of the University of California, Berkeley found that the average loss of revenue for a company that is the victim of indirect DOS attack is $1.2 million.

2.1.4.Data breaches

A data breach occurs when sensitive, protected or confidential data is copied, communicated, viewed, stolen, altered, or used by someone who is not authorized to do so.These are also a major threat to the Indian economy. In India, over 600 data breaches were recorded, harming the personal information of millions of people in 2022.Phishing attacks were the most frequent attack type in India approximately 22%followed by compromised or stolen credentials (16%), Social engineering was the costliest root cause of breaches at INR 191 million, followed by malicious insider threats, which amounted to approximately INR 188 million[24].The average cost of a data breach in India reached an all-time high of Rs 19.5 crore in the first half of 2024, according to an IBM securtiy the Ponemon Institute[45,46], report. The direct expenses of data breaches in India are indeed projected to exceed $4 billion in 2024. This significant figure underscores the growing threat of cyberattacks and the substantial financial impact they can have on businesses and individuals. This represents a significant increase from previous years, highlighting the growing financial impact of data breaches on Indian

10.48047/jocaaa.2024.33.08.82

organizations. The year 2024 is a significant year for data breaches in India, with several high-profile incidents impacting millions of individuals and firms[55]. The average cost of data breach in India hits $2018 million as per RBI report[56].

Following are some statistics on data breaches in India in 2023-2024:

- The number of data breaches cases reported in India is projected to be over 700.
- Over 100 million people's personal information is projected to be exposed in data breaches in India.
- The direct expenses of data breaches in India are projected to exceed $4 billion in 2023.
- The indirect expenses of data breaches in India are projected to be over $2. billion[56].

2.1.4.1 Major Data Breaches

- **Star Health Insurance:** Millions of personal records, including medical details, were leaked online[47,48].
- **Angel One:** Personal information of around 7.9 million customers was exposed, including bank account numbers[49].
- **Hathway:** A data breach impacted approximately 4 million users, exposing sensitive KYC detail[50].
- **Aadhaar Data Breach:** A massive breach exposed 750 million individuals' personal data, including Aadhaar information[51].

2.1.5. Salami Attack

A salami attack is a small attack that grows into a larger one[38]. Malicious persons regularly use the salami attack strategy to commit financial crimes online. It have potential impcat on Indian Economy like financial losses, loss of trust in digital systems, disruption to critical infrastructure, investment in cyber security, job losses and sector-specific impacts etc.Criminalsusethesalamiapproachtotakeresourcesormoneygradually[37].Thisattackoccurswhensever alweakerattackscombinetocreateamorepowerfulattack.Section66ofITact2000 dealwith this attack.

2.1.6.Deepfakes

These are digital media such as audio, video, and photographs that have been edited and manipulated with Artificial Intelligence. It's simply hyper-realistic digital illusion. Deepfakes are designed to cause harm to both people and institutions. Deepfakes,ablendof"deeplearning"and"fake,"areincrediblylifelikerecordingsthathavebeendigitallyed itedtoshowindividualsspeakinganddoingthingsthatneverhappened[38].

Accordingtoreporttitled"TheStateofDeepfakes in India" by the CyberPeace Foundation. The financial cost to Indian enterprises due to deepfake is anticipated to be over $10 billion by 2023. Accordingtoarecentanalysis,deepfake-enabledandAI-driventechniquesareexpectedtobecomemorecommonin2025,withindustrieslikehealthcareandbanking

10.48047/jocaaa.2024.33.08.82

beingthemostvulnerable[57].
SeqriteandtheDataSecurityCouncilofIndia(DSCI)releasedtheIndiaCyberThreatReport2025,whichhighlightedthegrowingsophisticationofcybercriminalsand theirstrategies.[39]Section66ofITact2000deal withdeepfake[58].

3. The Economic Effects of Cybercrime in India

3.1. Financial losses: Businesses and individuals could face financial losses as a consequence of cybercrime. This could be as an outcome of money being stolen, data being destroyed, or operations being hampered[11].Globally, the average cost of cybercrime is around 2.5 percent of GDP[19].Cybercrimesthattarget developing economies are typically focused in well-developed industrial sectors, such banking and financial services and outsourcing in India[20, 21]. According to a report (titled "Cybercrime in India: Trends and Impact", was published in 2022) by the Indian Computer Emergency Response Team (CERT-In)the financial impact of cybercrime on the Indian economy is estimated to be around $1 trillion by 2023.

According to the Cost of Data Breach Study 2023 by IBM Security and Ponemon Institute the average cost of a data breach in India in 2023 was INR 179million[22].The report further found that India takes significantly more time than the global average of 217 days to detect and address a data breach, at 287 days on average. Companies in India with heavy use of security AI and automation helped cut data breach cost by INR 95 millions.[23] According to a forecast by the Indian Cyber Crime Coordination Centre (I4C), cyber thefts are expected to cost Indians more than 1.2 lakh crore in the coming year[26]. The online financial scams that could potentially siphon off 0.7% of the India's GDP[59].

3.2. Productivity losses

Cybercrime can also cause companies and individuals to decrease productivity. This could be because of the time spent dealing with cyber hacking attempts, losing access to data, or disrupting operations.By 2023, it is expected that cybercrime would have cost the Indian economy $50 billion in productivity losses. This is a significant rise from the projected loss of $20 billion in 2018.Cybercrime is estimated to cost the Indian economy $100 billion annually in productivity losses.This amounts to one percent of India's GDP.Data breaches, Malware attacks, Malware attacks, Business email compromise (BEC) attacks are the most typical forms of cybercrime which lead to productivity losses in India.

3.3. Reputational damage

Cybercrime can also harm a company's or an individual's reputation. This might make engaging customers or investors difficult, and it can result in market share loss. There are many ways for

10.48047/jocaaa.2024.33.08.82

reputational damage, identity theft is one of them.It is difficult to estimate the monetary impact of damage to reputation imposed on by cyberattacks.A cyberattack's reputational damage may have a long-term effect on the Indian economy.For example, WannaCry ransomware (2017) attack affected over 200,000 computers in India.The attack led to significant disruption, monetary losses, and a tarnished image for India as a secure location to do business.

3.4. Intellectual Property Theft

Intellectual property (IP) theft is defined as the unauthorized use, exploitation, or outright theft of creative works, trade secrets, ideas, and confidential information. Intellectual property theft can have a major impact on the Indian economy such as financial losses to companies, reputational damage, loss of jobs, reduced investment, a loss of competitiveness etc. Malicious person can use phishing attacks, malware, and other techniques to steal IP from businesses.
According to the report of the United States Trade Representative (USTR) estimated that the worldwide cost of piracy and counterfeiting was $2.5 trillion in 2023.This report estimated that the Indian economy loses $10 billion to $30 billion per year due to counterfeiting.

3.5. Supply Chain Disruptions

Cyberattacks on enterprises can have an adverse impact on supply chains. A cyber-attack on a key supplier or partner can disrupt the entire supply chain, making delays in manufacturing, shipment, and fulfillment. This disruption can result in lower customer satisfaction, lost company opportunities, and increased expenses for restoring normal operations[12].

3.6 Business Resilience

Cyberattacks underscore the significance of effective business continuity and disaster recovery planning.Businesses need to invest in incident response protocols, secure data backups, and proactive measures to protect their critical infrastructure. Cyberattacks will continue to disrupt business operations and have a higher overall impact if these protections are not followed[25].

3. Cyber attack prevention

Figure 2 represent the steps taken to prevent from cyber attack to organizations.

10.48047/jocaaa.2024.33.08.82

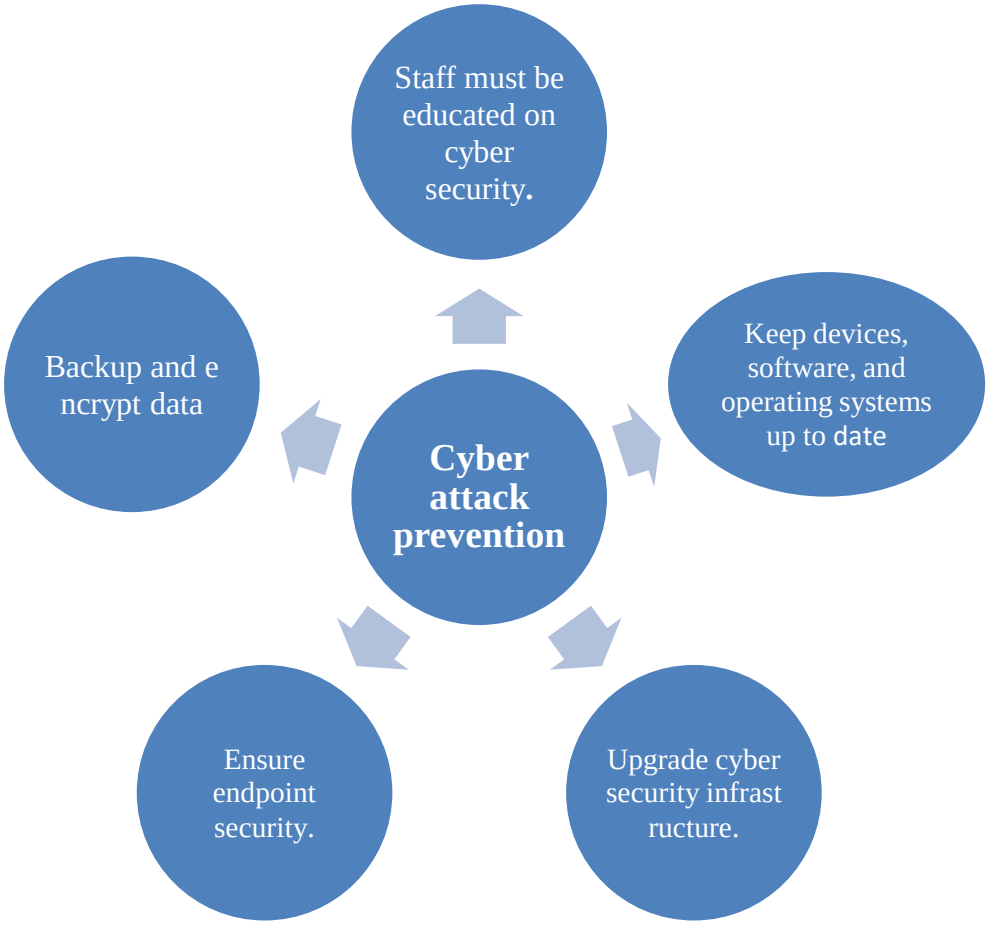

Figure2: - Cyber attack prevention

5. Initiatives by Indian Government

Day by day nature of cybercrime changed and become more sophisticated. Cybercriminals are using latest technologies such as AI to harm the businesses. Government of India has already taken a lot of steps to tackle the cybercrime, but due to complex in nature and rapid change in technology create challenge for government to address it. Recently Government presented The Digital Personal Data Protection Bill, 2023 in parliament[17]. The Bill will apply to the processing of digital personal data within India, whether obtained online or offline and digitized. A user will be able to 'request' information on data processing, as well as request correction and deletion of personal data, grievance redressal, and the designation of another person to exercise rights in exceptional cases.
Government of India takes the following initiatives to address the growing risk of cyber crime:-

5.1. National Cyber Security Strategy 2020:-With stricter audits, it aims to promote cyber awareness and cyber security Empaneled cyber auditors will examine firms' security features in greater depth than is permitted by law[60].

10.48047/jocaaa.2024.33.08.82

5.2. National Critical Information Infrastructure Protection Centre (NCIIPC): The NCIIPC, established under sec. 70A the Information Technology Act of 2000, serves as the nodal agency for vital information infrastructure safeguards and resilience[60,61].

5.3. Indian Cyber Crime Coordination Centre (I4C): I4C was setup in 2022. To ensure a comprehensive response to cybercrime, the Indian Government established the Indian Cyber-Crime Coordination Centre (I4C) [13].

5.4. Computer Emergency Response Team - India (CERT-In): It operational since 2004.It is the national nodal agency for responding to computer security incidents as and when they occur[14].

5.5. NATIONAL CYBERCRIME REPORTING PORTAL [NCRP]: (NCRP) was dedicated to the nation on 20th January 2020.The portal allows reporting of all types of Cybercrime[15]. Website: https://cybercrime.gov.in/.

5.6. National Cyber Security Policy -2013:- it was launched with the vision to build a secure and resilient cyberspace for citizens, businesses and Government[16].

5.7. Information Technology Act, 2000 (IT Act): Various sections of this act which deal with different types of cyber crime which negatively impacted Indian economy[28].

Section 66. Computer related offences. Any individual who deceitfully or dishonestly commits any of the crimes listed in section 43 faces a maximum sentence of three years in prison, a maximum fine of five lakh rupees, or both[29].

5.7.1. Section 66C. Punishment for identity theft. Anyone who uses another person's password, electronic signature, or other unique dentifying feature dishonestly or fraudulently faces upto three years imprison of any kind and affine of upto one lakh rupees[31].

5.7.2. Section 66E: punishment for violation of privacy. Anyone who willfully or knowingly takes a picture of someone else's private area and publishes it or sends it without that person's consent, in violation of that person's privacy, faces up to three years in prison, a fine of up to two lakh rupees, or neither[32.]

5.7.3. Section 66F. Punishment for cyber terrorism. Intentionally or deliberately breaches a computer resource without permission or beyond what is permitted, and through such actions, gains access to information, data, or computer databases that are prohibited for reasons of state security or international relations; or any restricted information, data, or computer databases, with reasonable suspicion that they may be used to harmor likely to harm India's sovereignty and integrity, the security of the State, friendly relations with other countries, public order, decency or morality, or inconnection with contempt of court, defamation, incitement to an offense, or to the benefit of any foreign country or group of individuals[33].

5.7.4. Section 67. Punishment for publishing or transmitting obscene material in electronic form. If someone publishes, transmits, or causes to be published or transmitted in electronic form any material that is lewd, appeals to the prurient interest, or has the effect of tending to deprave and corrupt people who are likely, considering all relevant circumstances, to read, see, or hear the matter contained or embodied in it, they will be punished on a first conviction with imprisonment of any kind for a term that may extend to three years and a fine that may extend to five lakh rupees. If they are convicted a second or subsequent conviction, they will be punished with imprisonment of any kind for a term that may extend to five years and a fine that may reach ten lakh rupees.[34]

5.7.3 Section 67C. Preservation and retention of information by intermediaries. Information preservation and retention through intermediaries(1) The intermediary is responsible for maintaining and keeping the information for the time frame, format, and manner that the

10.48047/jocaaa.2024.33.08.82

Central Government specifies[35].
(2) Any intermediary who knowingly or purposefully violates the terms of sub-section(1)facesapenaltyofupto25lakhrupees. [35]

6. Major Challenges in Cyber Security

Lack of technical staff: States are making modest attempts to recruit technical personnel to investigate cybercrime. According to the Information Technology (IT) Act of 2000, offences reported under the Act must be investigated by police officers not lower than the rank of inspector. In real, the district has a restricted number of police inspectors, and most field investigations are done by deputy inspectors.
No legal rules: there are any specific investigative procedures for cybercrime. Although electronic evidence differs considerably from traditional criminal evidence, it is vital to develop standardized and consistent methods for handling electronic evidence.
Shortage of Infrastructure (cyber labs):-Although most government cyber laboratories are well-equipped to analyse hard drives and mobile phones, many still employ "electronic evidence examiners" to provide expert opinions on digital data[25].

7. Conclusion

Cybercrime has a significant economic impact in India. It creates substantial challenges in terms of business interruptions, financial losses, data security, dangers to digital transformation, breaches of privacy as well as legal and judicial challenges. These effects have broad implications for corporations and society as a whole. Financial losses caused by cybercrime, such as online financial fraud, data breaches, and ransomware attacks, have a direct impact on individuals and businesses, decreasing trust in online transactions and hampering economic progress. Business disruptions due to cyber-attacks result in reputational damage, lost productivity, and supply chain disruptions. So, we can say that it hampers e-commerce, weaken innovation and competition, and present structural risks to critical infrastructure.

References

1.https://pib.gov.in/newsite/printRelease.aspx?relid=122837
2. Sandeep,Dr IJRTS Journal of Research | 2347-6117 | Volume 24 | Issue 01 | Version 1.4 | Jan-Jun 2023 https://ijrtspublications.org/issue-details.php?pid=254
3.https://economictimes.indiatimes.com/tech/technology/sharp-increase-in-cyberattacks-in-india-inq12023report/articleshow/100096450.cms?utm_source=contentofinterest&utm_medium=text&utm _campaign=cppst
4.https://economictimes.indiatimes.com/tech/technology/sharp-increase-in-cyberattacks-in-india-inq12023report/articleshow/100096450.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
5. https://www.cert-in.org.in/

10.48047/jocaaa.2024.33.08.82

6. https://pib.gov.in/PressReleasePage.aspx?PRID=1939176
7. https://www.legalserviceindia.com/legal/article-11766-the-impact-of-cybercrime-on-the-indian-economy-and-society.html
8. https://government.economictimes.indiatimes.com/news/secure-india/indias-dream-of-usd-5-trillion-economy-threatened-by-cybercrime-risks-are-the-systems-in-place-to-tackle-it/98464431
9. https://www.cert-in.org.in/PDF/RANSOMWARE_Report_2022.pdf
10.https://www.cert-in.org.in/
11.https://www.worldbank.org/en/programs/cybersecurity-trust-fund/overview
12. https://www.legalserviceindia.com/legal/article-11766-the-impact-of-cybercrime-on-the-indian-economy-and-society.html
13. https://i4c.mha.gov.in/ncrp.aspx
14. https://www.cert-in.org.in/
15. https://i4c.mha.gov.in/ncrp.aspx
16. https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf
17. https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023#:~:text= The% 20Bill %20will% 20apply%20to,goods%20or%20services%20in%20India.
18.Dr. Mike McGuire (University of Surrey) and Samantha Dowling (Home Office Science), Cyber crime: A review of the evidence.
19. https://government.economictimes.indiatimes.com/news/secure-india/indias-dream-of-usd-5-trillion-economy-threatened-by-cybercrime-risks-are-the-systems-in-place-to-tackle-it/98464431
20.Kshetri, N. (2010). The global cybercrime industry: Economic, institutional and strategic perspectives. New York, Berlin and Heidelberg: Springer.
21. Kshetri, N. (2010). Diffusion and effects of cybercrime in developing economies. Third World Quarterly, 31(7), 1057–1079.
22, 23,24.https://in.newsroom.ibm.com/IBM-Report-Average-cost-of-a-data-breach-in-India-touched-INR-179-million-in-2023
24. https://ustr.gov/sites/default/files/2023-04/2023%20Special%20301%20Report.pdf
25. https://lexpeeps.in/the-impact-of-cybercrime-on-the-indian-economy-and-society/
26. https://www.thehindu.com/sci-tech/technology/cyber-fraud-losses-could-amount-to-07-of-gdp-mha-study-projects/article68788093.ece
27.https://www.livemint.com/mint-lounge/business-of-life/ransomware-surge-india-digital-security-11730013128459.html
28.https://www.indiacode.nic.in/show-data?actid=AC_CEN_45_76_00001_200021_ 15178073240 77 & orderno=77
29. https://www.indiacode.nic.in/show-data?abv= null & statehandle=null&actid=AC_ CEN_ 45_76_ 00001 _200021_ 1517807324077 &orderno=76&orgactid=AC _CEN_45_76_ 00001_200021_1517807324077
30. https://www.indiacode.nic.in/show-data?abv=null&statehandle= null&actid=AC_CEN_ 45_76_ 00001_200021_1517807324077&orderno=79&orgactid=AC_CEN_45_76_00001_200021_151780 7324077
31. https://www.indiacode.nic.in/show-data?abv= null &statehandle= null &actid= AC_CEN_ 45_76_ 00001_ 200021_1517807324077 & orderno=80&orgactid= AC_CEN_45 _76_ 00001_ 200021_1517807324077

10.48047/jocaaa.2024.33.08.82

32. https://www.indiacode.nic.in/show-data?abv = null & statehandle= null & actid= AC_ CEN_ 45_ 76_ 00001 _ 200021_ 1517807324077 & order no= 81 & or gactid=AC _CEN_ 45_ 76_ 00001_ 200021_1517807324077
33.https://www.indiacode.nic.in/show-data? Abv = null & statehandle = null & actid = AC_ CEN_ 45_76_00001_200021_1517807324077&orderno=82&orgactid=AC_CEN_45_76_00001_200021_ 1517807324077
34. https://www.indiacode.nic.in/show-data?Abv = null & statehandle= null & actid= AC_ CEN_ 45_76_00001_200021_1517807324077&orderno=83&orgactid=AC_CEN_45_76_00001_200021_ 1517807324077
35. https://www.indiacode.nic.in/show-data? abv= null & statehandle = null & actid= AC_ CEN_ 45_ 76_ 00001_ 200021_ 1517807324077 & or derno= 86 & orgactid=AC _ CEN_45 _76 _00001_ 200021_1517807324077
36.https://www.meity.gov.in/writereaddata/files/itbill2000.pdf
37.B., Tapasya. (2022). The Aspects of Probing into the Online Fraud of'Salami Slicing Attack'. *Part 1 Indian J. Integrated Rsch. L.*, *2*, 1.
38.Westerlund, Mika. "The emergence of deepfake technology: A review." *Technology innovation management review* 9.11 (2019).
39.https://economictimes.indiatimes.com/tech/artificial-intelligence/ai-driven-deepfake-enabled-cyberattacks-to-rise-in-2025-healthcarefinance-sectors-at-risk-report/articleshow/115976846.cms?from=mdr
40. Gordon, S. and Ford, R., 2006. On the definition and classification of cybercrime. Journal in computer virology, 2, pp.13-20.
41.Bossler, A.M. and Berenblum, T., 2019. Introduction: new directions in cybercrime research. Journal of Crime and Justice, 42(5), pp.495-499.
42. Khonji, Mahmoud, Youssef Iraqi, and Andrew Jones. "Phishing detection: a literature survey." IEEE Communications Surveys & Tutorials 15, no. 4 (2013): 2091-2121.
43.https://www.cert-in.org.in/PDF/RANSOMWARE_Report_2022.pdf
44. https://www.thehindu.com/sci-tech/technology/cyber-fraud-losses-could-amount-to-07-of-gdp-mha-study-projects/article68788093.ece
45.https://in.newsroom.ibm.com/2024-07-31-IBM-Report-Escalating-Data-Breach-Disruption-Pushes-Average-Cost-of-a-Data-Breach-in-India-to-All-Time-High-of-INR-195-Million-in-2024
46.https://economictimes.indiatimes.com/tech/technology/data-breach-average-cost-touches-all-time-high-in-fy24-ibm-report/articleshow/112160790.cms?from=mdr
47.https://www.indiatoday.in/technology/features/story/star-health-insurance-hack-led-to-personal-data-of-31-million-customers-being-compromised-story-in-5-points-2615354-2024-10-11
48.https://www.business-standard.com/finance/personal-finance/31-mn-star-health-customers-personal-data-leaked-what-you-need-to-know-124101000462_1.html
49. https://economictimes.indiatimes.com/tech/technology/personal-data-of-almost-8-million-angel-one-customers-leaked-online/articleshow/111612380.cms?from=mdr
50. https://maktoobmedia.com/india/security-breach-at-indian-internet-service-isp-provider-hathway-hacker-exposes-kyc-data-4-million-users/
51.https://www.indiatoday.in/technology/news/story/data-of-750-million-telecom-users-in-india-being-sold-on-dark-web-cyber-experts-claim-2495752-2024-01-31
52. Wood, Anthony D., and John A. Stankovic. "Denial of service in sensor networks." Computer 35, no. 10 (2002): 54-62.

10.48047/jocaaa.2024.33.08.82

53.Zargar, Saman Taghavi, James Joshi, and David Tipper. "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks." IEEE communications surveys & tutorials 15, no. 4 (2013): 2046-2069.
54. Mahjabin, Tasnuva, Yang Xiao, Guang Sun, and Wangdong Jiang. "A survey of distributed denial-of-service attack, prevention, and mitigation techniques." International Journal of Distributed Sensor Networks 13, no. 12 (2017): 1550147717741463.
55. https://www.indiatoday.in/india/story/2024-a-year-of-data-leaks-espionage-and-ddos-attacks-ransomware-data-breach-2654230-2024-12-23
56. https://www.business-standard.com/finance/news/average-cost-of-data-breaches-in-india-hits-2-18-million-rbi-report-124072900610_1.html
57 .https://economictimes.indiatimes.com/tech/artificial-intelligence/ai-driven-deepfake-enabled-cyberattacks-to-rise-in-2025-healthcarefinance-sectors-at-risk-report / article show / 115976846. cms? from=mdr
58. https://www.indiacode.nic.in/show-data?actid=AC_CEN_45_76_00001_200021_1517807324077&orderno=81
59. https://www.thehindu.com/sci-tech/technology/cyber-fraud-losses-could-amount-to-07-of-gdp-mha-study-projects/article68788093.ece
60. https://www.dsci.in/files/content/knowledge-centre/2023/National-Cyber-Security-Strategy-2020-DSCI-submission.pdf
61. https://nciipc.gov.in/
62. https://www.india.gov.in/website-national-critical-information-infrastructure-protection-centre