Growth of Cyber-crimes in Society 4.0

Vinita Sharma
Amity University
Noida
Vinitasharma75@gmail.com

Tanu Manocha
IMM
New Delhi
emailtotanu@gmail.com

Seema Garg
Amity University
Noida
seemagarg1@gmail.com

Saatwik Sharma
Thapar University
Patiala
Saatwiksharma2002@gmail.com

Anshita Garg
Delhi Technological University
Delhi
anshitagarg362@gmail.com

Ritu Sharma
Torrens University
Australia
ritu.sharma@torrens.edu.au

2023 3rd International Conference on Innovative Practices in Technology and Management (ICIPTM) | 979-8-3503-3623-8/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICIPTM57143.2023.10118185

***Abstract* - In the fast-paced Information and communication technology, cyber-crimes are also evolving and growing very fast thereby increasing damage of the organizations and individuals universally. This paper is an attempt to get an overview of the different trends of cyber-crimes, to spread awareness about the cyber-crimes among people to increase security of the people of Delhi and NCR from cyber-crimes.**

Since Internet has become a basic need of life in metro cities today for almost every individual, increased dependence on Internet has led to the rise of cyber-crime and one of the best ways of protection from cybercrimes is its awareness. The paper intends to understand the level and intensity of awareness about various cyber-crimes present in the era of Society 4.0 in capital of India. The paper also identifies the importance of being acquainted with the effects of cyber-crime and awareness of the methods of prevention.

Keywords - cyber-crime, analysis, cyber security, society 4.0

I. INTRODUCTION

The science and technology based outlined Society 5.0 is the ideal future society for humans. There is a need of society 5.0 as it ensures no humans is left behind, as it emphasizes on well–being and happiness of humans.
It is a human-centered strategy that interacts heavily with cyberspace and physical location which seeks to balance economic growth with social problem-solving.[2]

The current society which is prevailing is society 4.0 and is called as informational society and prior to Society 4.0 we have different versions of society i.e. Society 3.0, Society 2.0 and Society 1.0 which is termed as Industrial Society, Farming Society, and hunting society respectively.[4][13][15]

Society 4.0 is an important part of the Social Innovation. After development of various types of previous societies, Society 4.0 started with the innovative and supporting technologies of Wi Fi, computers, satellite, internet, smart phones. The data generated is stored in a cyberspace called as cloud and this can be accessed through internet to retrieve and analyze the data. [6][7]

II. LITERATURE REVIEW

A. Cyber-crimes in Society 4.0

Every coin has two sides. Although Society 4.0 has filled our lives with lots of comfort in terms of exchange, maintenance of data and communication worldwide through information and communication technologies, it has given a fear of data theft too.[10][11]

Symantec report published in January 2019 showed that "Globally India is the third least honest country on the Internet". [21][25] Among Indian cities, most cyber-crimes take place in Bangalore followed by Mumbai and New Delhi. Among Indian cities, most cybercrime takes place in Bangalore. According to statistics, 76% of Indians have fallen victim to cybercrime in some way. Out of 76%, 60% of them have been victimized due to the various computer viruses and the Malware. 45% of cyber-crimes in India were never resolved.[9]

In 2018, India experienced a financial nightmare on October 19 [8][12]. Following an alleged malware-related intrusion in an ATM network not operated by the State Bank of India (SBI), 6 lakh debit cards out of the whole lot of various private and PSU banks

979-8-3503-3623-8/23/$31.00 ©2023 IEEE

were suspended. They came under India's biggest financial data breach. [13]

Cybercrime has become a bitter reality of the world whereas very little is known about it universally. Cyber-crime has affected the organizations in all arenas [1]. There is no particular or singular, world-wide acknowledged definition for cybercrime, according to [3]. Nonetheless, there are several counterarguments to it in the literature. The European Commission defined it as "criminal activities being carried out via electronic communications networks and information systems or against such networks and systems." Chen in 2019 noted that the concept includes both crimes against computers and those that were made possible by them.

According to a report by Times of India dated November 2019 discloses that Cyber-crime cases in Delhi & NCR are increasing almost exponentially in the last 5 years. Cases on objectionable posts on social media were increasing very fast till 2018 but have started decreasing. There is a significant decrease in the number of arrested cyber criminals within the difference of one single year by 2019.

B. Types of cyber-crimes

In 2013, Mike McGuire and Samantha Dowling proposed that the two categories of computer-enabled and computer-dependent cybercrimes would make it simple to understand these offenses [13].

The following list may include the top cybercrimes in India:

Virus/Worms Attacks- which includes Worms, Trojan Horses and Denial of Service

1. Hacking
2. Identity Theft
3. Cyberstalking
4. Credit/debit card theft over a phone call/e mail /sms
5. Fraud bank transactions
6. Data Piracy
7. Pornography/child Cyberbullying Cyber terrorism.
8. SQL Injection
9. Logic Bomb
10. Phishing
11. Spoofing
12. Email bombing or Spamming
13. Web Jacking
14. Data diddling
15. Salami Slicing Attack

C. Cyber-security - A prerequisite for Society 4.0

In order to protect against current cyber-attacks and threats, India is currently undergoing a phase of growth for its cyber security. The PWC study for 2019 states that there are numerous areas that necessitate a special strategy, therefore India's cyber security demands are not unique and distinct from those of the rest of the globe. They have chosen seven cyber security trends for the Indian market in 2019 after taking the country's business environment and its requirements for adopting cyber security tools and solutions into consideration. [20][22][23]

D. Significance of awareness of cyber-crimes

Awareness about cyber-crime is essential for the youth [14][27]. According to Curtis and Colwell the risk in cyber space can be reduced and controlled by educating young people about the cyber- crime and spread awareness [5][26]. More awareness and knowledge will help the people to decrease the cyber–crimes. This knowledge and awareness can be done by providing various training programme, resources for compliance, protection of personal information and to develop policies, rules and regulations [2][25].

According to Choi in 2008, university programmes are "effective in teaching learning, knowledge and more values concerning cybercrime since these programmes could influence students' future behaviour in regards to safety and security with regard to hacking. The literature evaluation suggests that expertise, gender, and age all have a big impact on cybercrime [4][24].

III. RESEARCH METHODOLOGY

After completion of the literature review, the data was collected from the both Secondary as well as primary data, which was used to examine the level of awareness of the residents of Delhi and NCR for cyber-crimes and means of cyber security. Convenience sampling is used for collection of data. For primary data most common source i.e. questionnaire was developed and randomly distributed among the groups of different age groups who were the residents of Delhi and NCR. The questionnaire has demographic based, cyber-crimes based and cyber-laws-based questions. The current study is based on 134 responses.

IV. ANALYSIS

Analysis of data gave a clear picture of the level of awareness of respondents for cyber-crimes and its prevention. To find out the relation in association of age, gender and educational qualifications and awareness of cybercrimes on respondents' inferential statistics has been used. Based on the literature following hypothesis were developed. A brief

description of questions and analyzed results from the questionnaire are as below:

I Age

H 01: There is no significant association of Age and Awareness of the respondents

H A1: There is significant association of Age and Awareness of the respondents

Collected firsthand information i.e. Primary data through questionnaire method was screened and tested for different variables considered for study. Checking was done for any missing or irrelevant values and engaged responses and during screening and checking it was found that there was no missing value in rows. In the data it was also found that there were no outliers. During variable screening was done and it was found that there was no missing value in Columns. The descriptive analysis was done. The questionnaire was distributed among 134 participants. The chart clearly indicates that maximum respondents in the range of 18-21 years of age is 65% whereas 31% of the respondents were between 22-25 range of age and 4% of respondents were found to have age more than 25 years.

To test the second Hypothesis, about the association between the age and Awareness of the respondents ONE WAY ANOVA was used.

TABLE I : ONE WAY ANOVA ON AGE

	Sum of Sq	df	Mean Sq	F	Sig.
Between Groups	1.308	3	.436	1.166	.328
Within Groups	28.790	77	.374		
Total	30.099	80			

Table 1 indicates that the significant value is 0.328, which is greater than the level of significance (p value = 0.05). Thus, there is not much evidence to reject the null hypothesis if the tabulated value is more than the p value. As a result, the null hypothesis is accepted, and it can be concluded that there is no significant and meaningful relationship between the respondents' ages and levels of awareness.

II Gender

Gender plays an important role while doing such kind of analysis. To find the association of gender and awareness the following is the hypothesis is framed

H 02: There is no significant association of Gender and Awareness of the respondents

H A2: There is significant association of Gender and Awareness of the respondents

It was observed that out of 134 respondents 36% were females and 68% were males.

TABLE II – GROUP STATISTICS OF GENDER

	Gender	N	Mean	Std. Deviation	Std. Error Mean
Awareness	1	72	2.19	.642	.076
	2	45	2.18	.614	.092

As the table III exhibits that the Significant value is 0.668 which is greater than 0.05, which clearly indicates that the result is insignificant and Null Hypothesis is accepted. Thus, there is no relationship between the gender and Awareness among the respondents.

III Qualification

Qualification of respondents is an important aspect which must be tested for weightage in awareness. Majority of the respondents of the questionnaire were post graduate i.e. 63% and 21% were graduates. That indicates that maximum respondents were highly educated people living in the capital of the country.

To test the association of qualification and awareness the following hypothesis is framed -

H 03: There is no significant association of Educational Qualification and Awareness of the respondents.

H A3: There is significant association of Educational Qualification and Awareness of the respondents.

To test the Hypothesis, to find the association between the Educational Qualification and Awareness of the respondents ONE WAY ANOVA was used.

TABLE III - INDEPENDENT SAMPLES TEST FOR AGE AND AWARENESS VARIANCE RATIO

		Test for Equality of Variances		t-test Equality of Means						
		F	Sig.	t	Degree of freedom	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
Awareness	Equal variances assumed	.185	.668	.139	115	.890	.017	.120	-.221	.254
	Equal variances not assumed			.140	96.734	.889	.017	.119	-.219	.252

TABLE IV: ASSOCIATION OF EDUCATIONAL QUALIFICATION AND THE AWARENESS OF THE RESPONDENTS USING ANOVA

	Sum of Sq	df	Mean Square	F	Sig.
Between Groups	0.112	3	.037	.189	.904
Within Groups	22.498	114	.197		
Total	22.610	117			

According to table IV, the significant value is 0.904, which is more than the level of significance of 0.05 (p value). Hence, in accordance with convention theory, the null hypothesis is accepted which shows that there is no significant relationship between respondents' educational backgrounds and their awareness of cybercrime.

V. PERCEPTION OF AWARENESS OF RESPONDENTS

A. Awareness of the respondents with various types of cyber-attacks

In the questionnaire, a list of 18 different types of cyber-attacks was provided to the respondents for the purpose to know about the maximum well known cyber-crime among the respondents.

The maximum known cyber-crime came out to be hacking.

The next best known cyber-attack is Credit/Debit Card Fraud, followed by fraud Bank transactions and then virus/worms attacks.

B. Awareness of cyber laws in India

Maximum respondents accepted that they are unaware of the any kind of anti-cyber-crime law or scheme in India. (45.4%). 35.3% respondents were aware of IT Act of India, 2000, 33.6% respondents

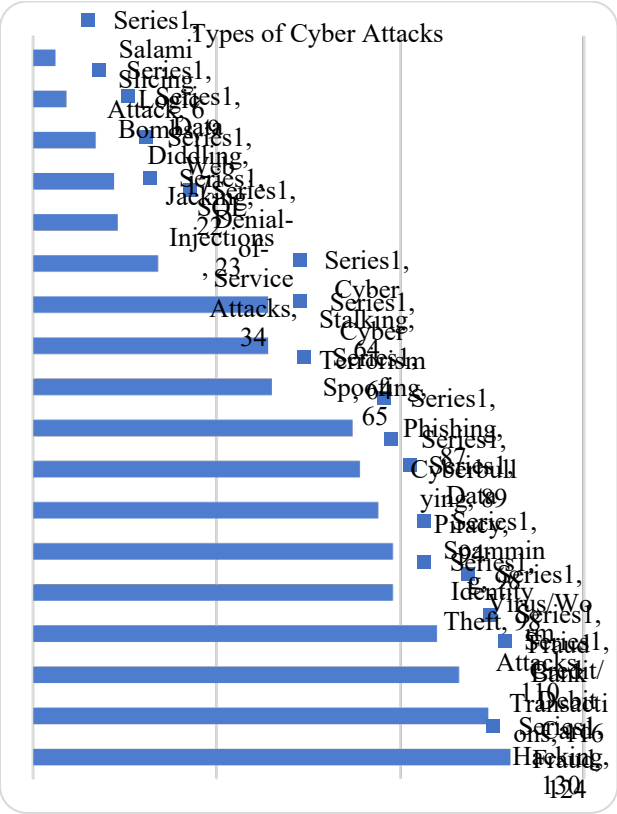

Figure 1 – Best known Cyber-attacks

were aware of 'Cyber- crime Unit of Delhi Police'. Few respondents were also aware of the cyber security portals but the percentage of awareness was very low.

I. CONCLUSION

With the development of new emerging technologies which are leading to the evolution of a new society which is a combination of both digital as well as the physical environment, enhances the communication ability and also developing human-machine based interacting system and also involves the huge volume of data sets.

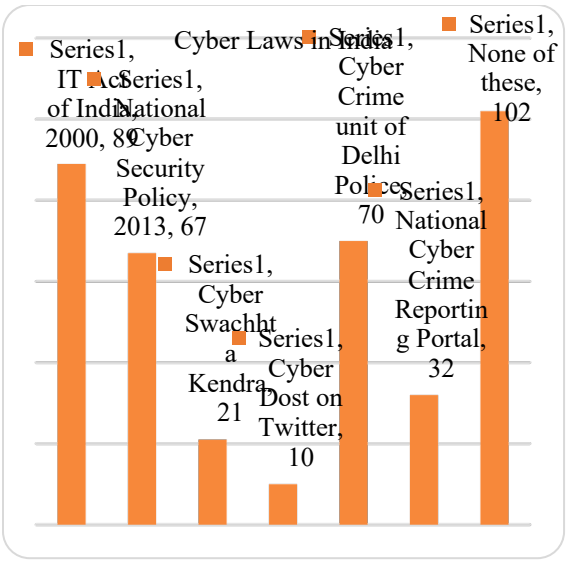

Figure 2 – Awareness of Cyber Laws

Cyber-crimes are increasing each and every day in newer forms. Therefore, in the era of Society 4.0, where working with computers, use of smart phones and Internet, exchanging data through social media has become a lifestyle of Delhi and NCR, awareness of cyber-crimes is one of the measures of being cyber-safe.

With more innovative practices, Industry 4.0 which constitutes both information technology and operational technology has bought new challenges and the major concern is about new challenges and the major concern is about the cyber security, in which government has also initiated with great efforts against these kinds of cyber security attacks.

This research work can be concluded with the statement that people of Delhi feel that they are well aware of cyber-crime, but they are required to have more knowledge of cyber-crimes as well as cyber laws. Actually, people know about those cyber-crimes which are more common in media. At the same time, cyber laws in India and Delhi are very less known to them.

More awareness of cyber-crimes will lead to use more measures to be taken for the cyber-security. And that will be one of the most prominent prevention measures for the Society from cyber-attacks.

II. REFERENCES

[1] Bendovschi, A. (2015). Cyber-attacks–trends, patterns and security countermeasures. Procedia Economics and Finance, 28, pp.24-31.

[2] Chawki M, (2005). “A critical look at the regulation of cybercrime”, ICFAI Journal of Cyberlaw, Vol. 3(1), pp. 1-55.

[3] Chen, Y., & Zahedi, F. M. (2016). Individuals Internet Security Perceptions And Behaviors: Poly contextual Contrasts Between the United States And China.publication MIS Quarterly, 40(1).

[4] Choi KS. (2008) “Structural equation modeling assessment of key causal factors in computer crime victimization” (Doctoral dissertation, Indiana University of Pennsylvania).

[5] Curtis PA, Colwell L, 2000. Cyber Crime: The Next Challenge An Overview of the Challenges Faced by Law Enforcement While Investigating Computer Crimes in the Year 2000 and Beyond. School of Law Enforcement Supervision, USA. 2000 Nov 12.

[6] Wall DS, 2008. “Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime”, International Review of Law, Computers & Technology. Vol. 22, No. (1-2), pp. 45- 63.

[7] Dubbudu R, 2016. Most number of Cyber Crimes reported in Maharashtra & Uttar Pradesh. Article published on Sep 2, 2016. https://factly.in/cyber-crimes-in-India-which-state-tops- the-chart/

[8] ET, 2018, Economics Times,19 Oct2018, Worst-nightmare, https://test.economictimes.indiatimes.com/topic/worst-nightmare

[9] European Commission. Towards a general policy on the fight against cyber crime. http://eur-ex.europa.eu/LexUriServ/LexUriServ.do?uri= COM:2007:0267:FIN:EN.pdf

[10] Fukuda, K. (2020). Science, technology and innovation ecosystem transformation toward society 5.0. International Journal of Production Economics, 220, 107460.

[11] Jotwani. D, 2019. The Growing Issue of Cyber Crime in the Technological Age. Bwcio. Business world http://bwcio.businessworld.in/article/The-Growing-Issue-of-Cyber-Crime-in-the-Technological-Age-/08-07-2019-172939/

[12] Kafle,V.(2019).Towards Society 5.0.My Republica https://myrepublica.nagariknetwork.com/news/toward-society-5-0/

[13] Karali, Y., Panda, S., & Panda, C. S. (2015). Cyber Crime: An Analytical Study of Cyber Crime Cases at the Most Vulnerable States and Cities in India. International Journal of Engineering and Management Research (IJEMR), 5(2), 43-48.

[14] Levin A, Foster M, West B, Nicholson MJ, Hernandez T and Cukier W, 2008. The next digital divide: Online social network privacy. Privacy and Cyber Crime Institute, Ryerson University.2008.Mar.http://www.ryerson.ca/content/dam/tedrogersschool/privacy/Ryerson_Privacy_Institute_OSN_Report.pdf

[15] McGuire M, Dowling S, 2003. Cyber crime: A review of the evidence. Summary of key findings and implications. Home Office Research report. 2013 Oct 9; 75.

[16] Mathew AR, Al Hajj A and Al Ruqeishi K, 2010. Cyber crimes: Threats and protection. In 2010 International Conference on Networking and Information Technology 2010 Jun 11 (pp. 16-18).

[17] Moore T, Clayton R and Anderson R. “The economics of online crime”, Journal of Economic Perspectives, Vol. 23, No. 3, pp. 3-20.

[18] Nouh M, Nurse JR, Goldsmith M. 2006. Towards designing a multipurpose cybercrime intelligence framework. In 2016 European Intelligence and Security Informatics Conference (EISIC) 2016 Aug 17 (pp. 60-67). IEEE.

[19] Pahuja D, 2011. Cyber Crimes and the Law. Article published in LegalIndial.com on July 17, 2011. http://www.legalindia.com/ cyber-crimes-and-the-law/

[20] PWC, 2019. Cyber Security trends that India will Witness, https://www.pwc.in/consulting/cyber-security/blogs/seven-cyber-security-trends-that-india-will-witness-in-2019.html

[21] Symantec. 2019, Internet Security Threat Report Volume 24,https://docs.broadcom.com/doc/istr-24-2019-en

[22] Sharma V, “Cyberbullying in India’s Capital” in Global Journal of Enterprise Information System, Volume 10, Issue 2, April-June 2018, Pages 29-35, ISSN - 0975-1432.

[23] Sharma V, Manocha T, “Study on the readiness among Youth towards Industry 4.0” in Scopus Indexed Journal 'International Journal of Advanced Science and Technology'. ISSN - 2005-4238, Vol. 29 No. 3 (2020) http://sersc.org/journals/index.php/IJAST/article/view/7083

[24] Sharma V, Manocha T, “Cybercrimes - Trends and awareness: A study on youth” in BULMIM Journal of Management & Research (BJMR) Vol. 5 Issue 2 (2020).

[25] Sharma V, Manocha T, "Essential awareness of social engineering attacks for digital security" in peer reviewed Journal of Applied Management-Jidnyasa, Vol 13, Issue 1, 2021. (ISSN : 0976-0326).

[26] Garg,S.,Mahajan.Nand GhoshJ.(2022)”Artificial Intelligence as an emerging technology in Global Trade:the challenges and Possibilities,” in Innovative Management Using AI in Industry 5.0” By IGI Global Publishers DOI: 10.4018/978-1-7998-8497-2., pp 98-117

[27] MahajanN,Garg S, Pandita S,and Sehgal G(2022),” Smart Healthcare and digitalization: Technological and cybersecurity Challenges, pp 124-147