Awareness of Growing Cyber-crimes in Society 4.0

Vinita Sharma and Tanu Manocha***

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 of cyber-crimes among people so as 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 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*

1.0 Introduction

Society 5.0 was proposed in the 5th Science and Technology Basic Plan as a future society that Japan should aspire to. 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 centric approach which balances the economic advancements with the resolution of social problems that highly integrates cyber space and physical space. The current society which is prevailing is society 4.0 and is called as informational society and prior to Society 4.0 we have Society 3.0 , Society 2.0 and Society 1.0 which is termed as Industrial Society, Farming Society , and hunting society respectively.

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.

2.0 Literature Review

2.1 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.

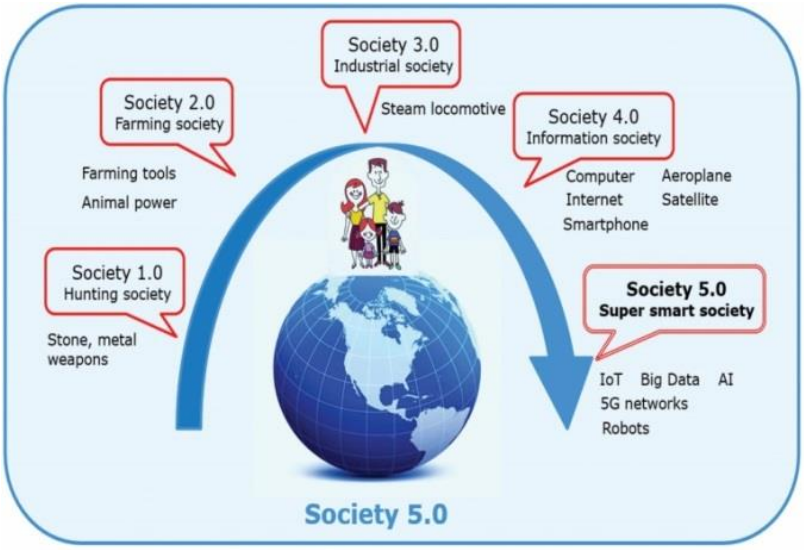
Symantec report published in January 2019 reveals that "Globally India is the third least honest country on the Internet". (Symantec, 2019) Among Indian cities, most cyber-crimes take place in Bangalore followed by Mumbai and New Delhi. Among Indian cities, most cybercrime takes place in Bangalore. 76% of Indians have been victims of some form of cybercrime.

**Corresponding author; Associate Professor, Department of IT, New Delhi Institute of Management, New Delhi, Delhi, India. (Email: vinitasharma75@gmail.com)*

***Research Scholar, Department of IT, Amity University, Noida, Uttar Pradesh, India. (Email: emailtotanu@gmail.com)*

60% have been victimized because of computer viruses and malware. 45% of cyber-crimes in India were never resolved. Over the last 5 years, there has been a 457% increase in cybercrime in India"

Figure 1 – Society 5.0



Source - ***https://myrepublica.nagariknetwork.com/news/toward-society-5-0/***

(ET, 2018) On 19th October, 2018 India faced a banking nightmare. The State Bank of India (SBI) blocked 6 lakh debit cards after a reported malware-related breach in a non-SBI ATM network. In what is possibly India's largest financial data breach, nearly 32 lakh debit cards across 19 banks, including HDFC Bank, ICICI Bank and Axis Bank, were compromised.

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 (Bendovschi A, 2015). According to (Chen et al, 2016) explains that there is no single universally accepted definition of cyber-crime, but several arguments may be found in literature over it. The European Commission defined it as, "criminal acts committed using electronic communications networks and information systems or against such networks and systems. (Chen, 2016) explains that definition incorporates about the crimes which were facilitated by computers and those that were committed against 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.

2.1.1 Types of cyber-crimes

Mike McGuire and Samantha Dowling, in 2013, suggested that cybercrimes can be explained easily after dividing into two different categories, which are, computer-enabled cyber-crimes and computer-dependent cyber-crimes. (Karali, 2015)

The most prevalent cyber-crimes in India may be listed as below -

1. Virus/Worms Attacks- which includes Worms, Trojan Horses and Denial of Service
2. Hacking
3. Identity Theft
4. Cyberstalking

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

2.2 Cyber-security - A prerequisite for Society 4.0

India's cyber security is going through a development phase, by using various innovative techniques and tools to protect from cyber-attacks and threats. According to PWC report 2019 "India's cyber security needs are not different from that of the rest of the world, there are a host of areas which require unique approach. Keeping in mind India's business landscape and her needs for cyber security tools and solutions, we have zeroed in on seven cyber security trends for the Indian market in 2019". (PWC, 2019)

2.3 Significance of awareness of cyber-crimes

Awareness about cyber-crime is essential for the youth (Levin et al., 2008). According to (Curtis and Colwell, 2000; Wang et al., 2008) explains that the risk in cyber space can be reduced by educating young people about the cyber- crime. 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 also to develop policies, rules and regulations, Chawki (2005).

Choi (2008) emphasizes on the " Effectiveness of university programs in promoting knowledge and values about cybercrime as these programs could improve future behavior of students' towards cybercrime in terms of safety and security. This would establish norms and adjust prospects for illegal or delinquent behaviors". According to the literature review, it indicates that age, gender and knowledge have significant impact on cyber-crime.

3.0 Research Methodology

After completion of the literature review, both primary data and secondary data were 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 collection questionnaire was developed and distributed randomly 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.

3.1 Analysis of primary data

Analysis of data is done, and it is an attempt to understand and connect to the different aspects of investigating different cyber-crimes.

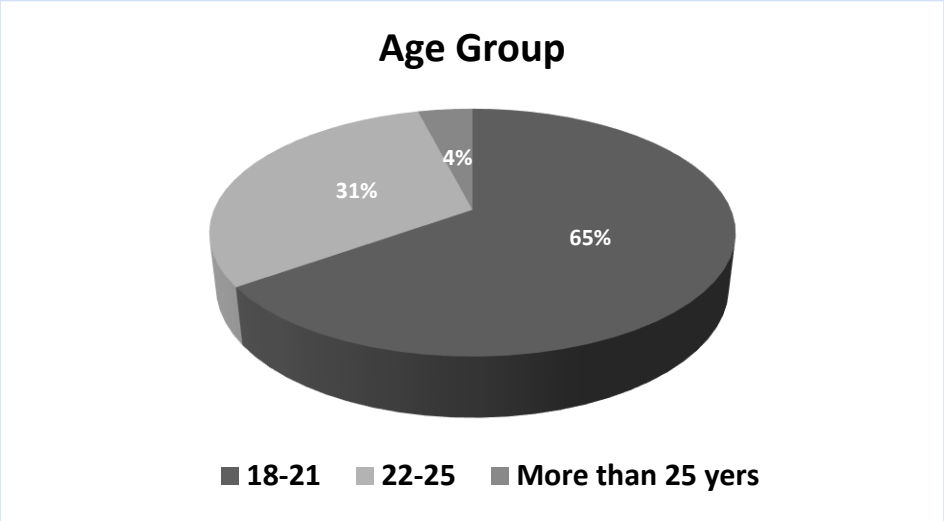
Analysis of data gave a clear picture of the level of awareness of respondents for cyber-crimes and its prevention. A brief description of questions and analyzed results from the questionnaire are as

below:

3.1.1 Age Group

The questionnaire was distributed among 134 participants. The chart clearly indicates that maximum respondents were 18-21 years of age is 65% whereas 31% of the respondents were between 22-25 years of age and 4% of respondents were more than 25 years.

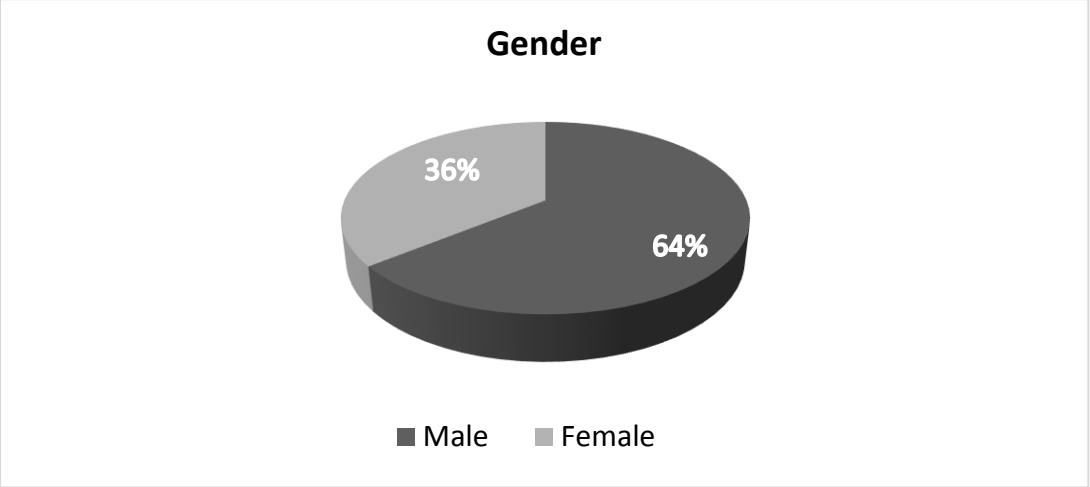
Figure 2 – Age Groups of Respondents



3.1.2 Gender

Gender plays an important role while doing such kind of analysis. It was observed that out of 134 respondents 36% were females and 68% were males.

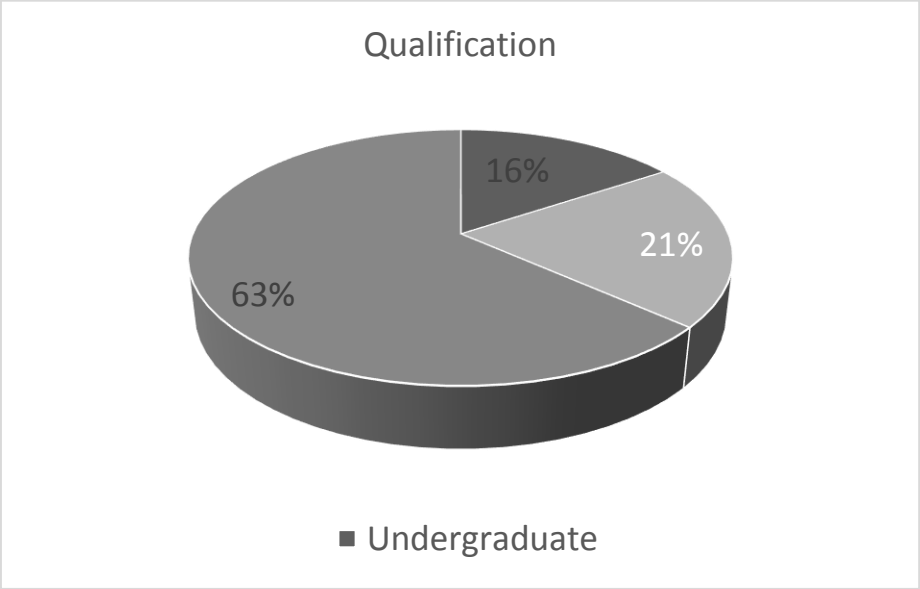
Figure 3 – Gender of Respondents



3.1.3 Qualification

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.

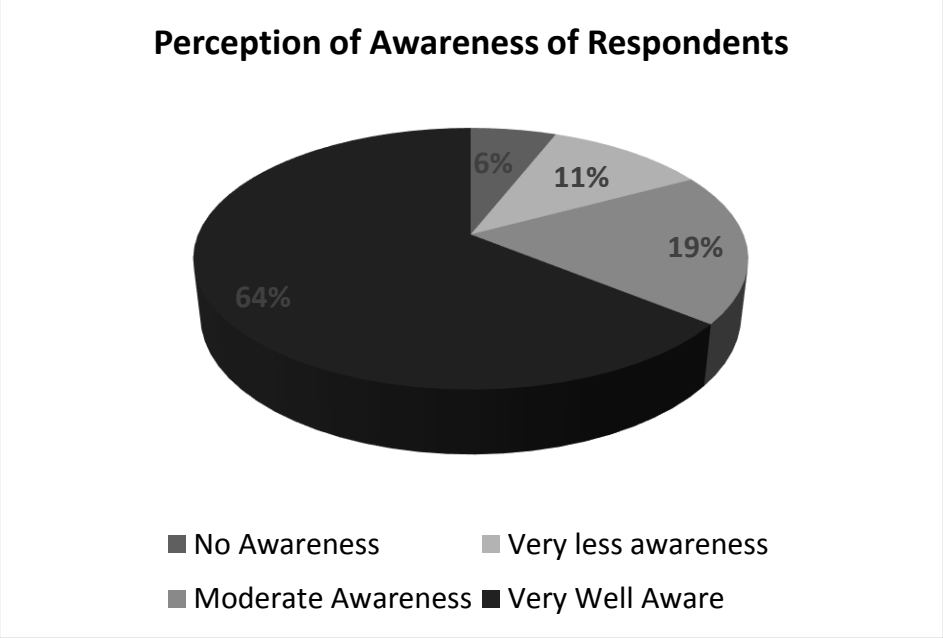
Figure 4 – Qualification of Respondents



3.1.4 Perception of Awareness of Respondents

- 64% of the total respondents had this opinion that they are very well aware of the cyber-crimes.
- 19% of the total sample had a perception that they were moderately aware of the different types of cyber-crimes.
- 11% had very less awareness of cyber-crime and 6% of them admitted that they do not know anything about cyber-crimes.

Figure 5 – Perception of Awareness of Cyber-crimes



3.1.5 Awareness of the respondents with various types of cyber-attacks

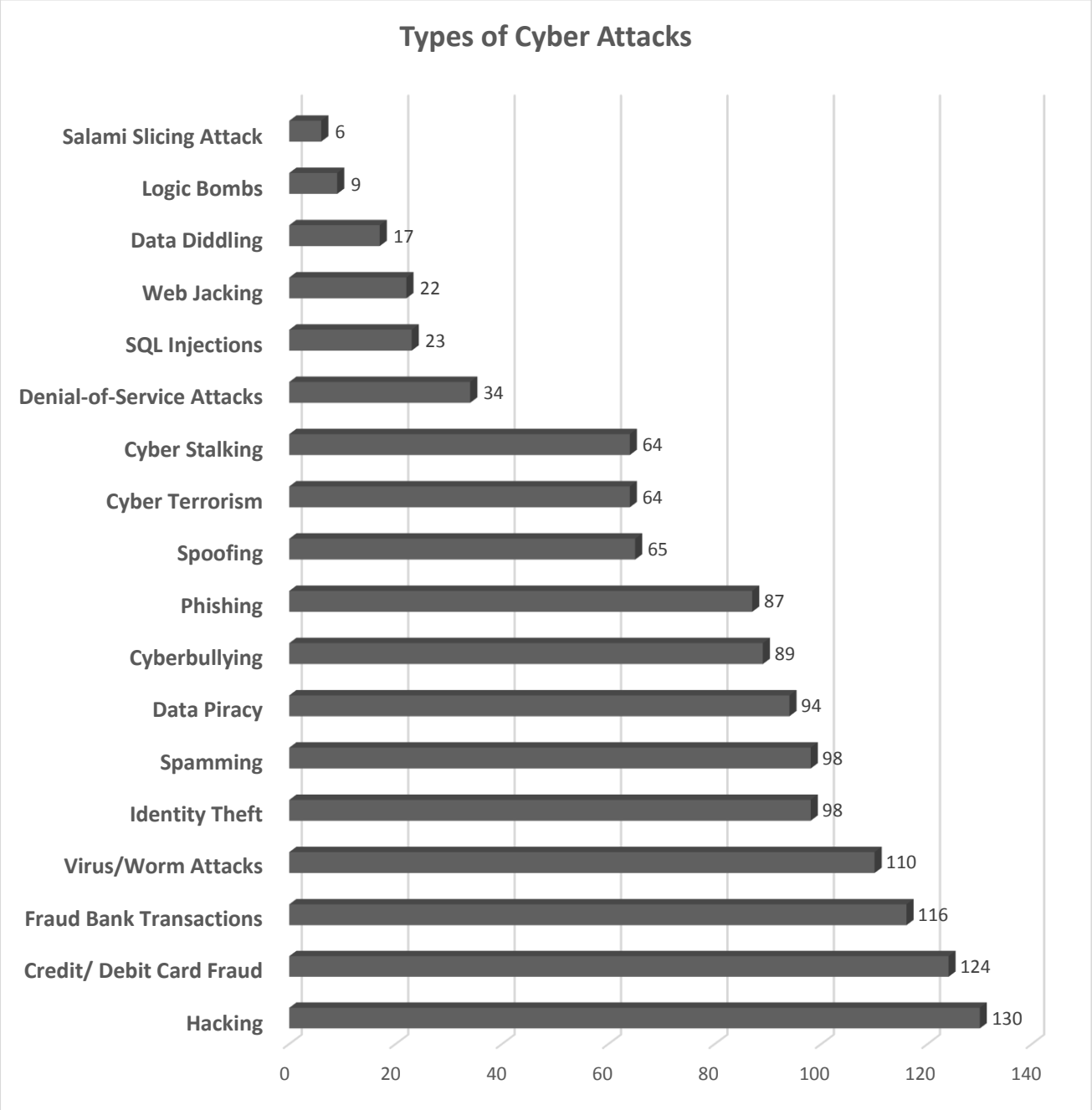
In the questionnaire, a list of 18 different types of cyber-attacks was provided to the

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.

Figure 6 – Best known Cyber-attacks

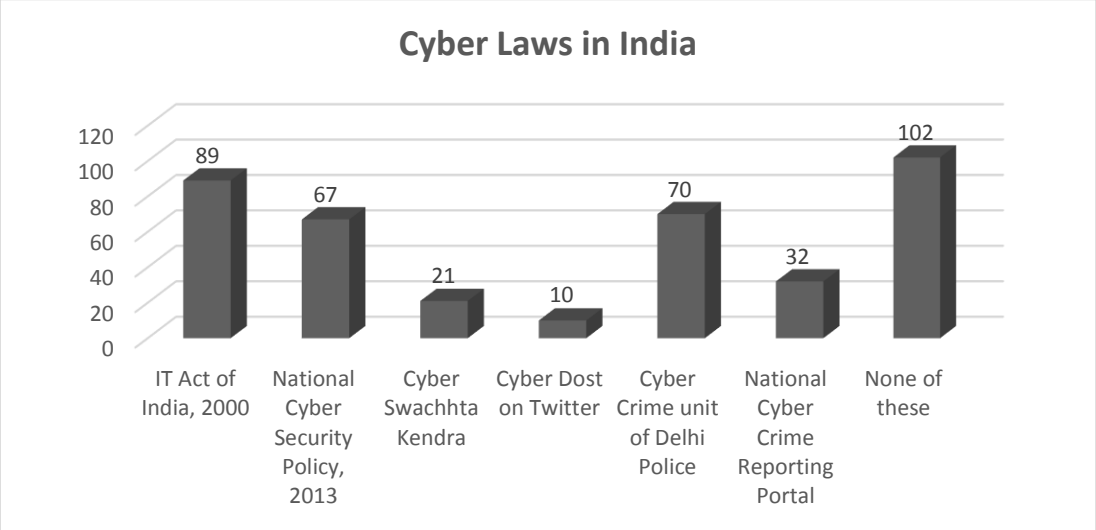


3.1.6 Awareness of cyber laws in India

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 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.

Figure 7 – Awareness of Cyber Laws



4.0 Conclusion

With the development of new emerging technologies which are leading to the emergence 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.

Cyber-crimes are increasing day by 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 life style 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.

References

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

Chawki M, 2005. “A critical look at the regulation of cybercrime”, ICFAI Journal of Cyberlaw, Vol. 3, No. 1, pp. 1-55.

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

Choi KS. Structural equation modeling assessment of key causal factors in computer crime victimization (Doctoral dissertation, Indiana University of Pennsylvania).

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.

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.

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/

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

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

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

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/

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

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.

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

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.

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).

Moore T, Clayton R and Anderson R. "The economics of online crime", Journal of Economic Perspectives, Vol. 23, No. 3, pp. 3-20.

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.

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/

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

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