

Impact of Cyber Crime: Issues and Challenges

Dr. Renu¹, Pawan²

¹Associate Professor, ²Student

¹UILS, Chandigarh University, Mohali, Punjab, India

²LLM, Chandigarh University, Mohali, Punjab, India

How to cite this paper: Dr. Renu | Pawan "Impact of Cyber Crime: Issues and Challenges" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-3, April 2019, pp.1569-1572, URL: <https://www.ijtsrd.com/papers/ijtsrd23456.pdf>



ABSTRACT

The facilities of computer technology have not come out without drawbacks. Though it makes the life so speedy and fast, but hurled under the eclipse of threat from the deadliest type of criminality termed as 'Cybercrime' without computers, entire businesses and government operations would almost cease to function. This proliferation of cheap, powerful, user-friendly computers has enabled more and more people to use them and, more importantly, rely on them as part of their normal way of life. As businesses, government agencies, and individuals continue to rely on them more and more, so do the criminals. Restriction of cybercrimes is dependent on proper analysis of their behavior and understanding of their impacts over various levels of society. Therefore, in the current manuscript a systematic understanding of cybercrimes and their impacts over various areas like Soci-eco-political, consumer trust, teenager etc. With the future trends of cybercrimes are explained.

Copyright © 2019 by author(s) and International Journal of Trend in Scientific Research and Development Journal. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0) (<http://creativecommons.org/licenses/by/4.0>)



KEYWORDS: Cybercrime, Consumer trust, Soci-eco-political, Security

INTRODUCTION

Cybercrime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It is also used to include traditional crimes in which computers or networks are used to enable the illicit activity.¹ The Cybercrime can halt any railway where it is, it may misguide the planes on its flight by misguiding with wrong signals, it may cause any important military data to fall in the hands of foreign countries, and it may halt e-media and every system can collapse within a fraction of seconds. The present study has been undertaken to touch some aspects, impact and prospects of this cybertechnology with special reference to threat poses of Cybercrime by India. Efforts have been made to analyze legal framework available for its control in India. To start with, it is, therefore, necessary to demarcate the dimensions of word 'crime'. Thus, it is beyond doubt that 'crime' is a relative phenomenon, universal in nature and essentially all societies from ancient to modern have been evidently demonstrating its presence.² Each society have been providing its own description of criminal behavior and conduct made punishable by express will of the political community ruling over the society and it was always

influence by religious-social-political economical values prevailing in the given society. Thus, from time immemorial the behavior that attracts 'penal liability' influenced and characterized by overall outcome of these standards. Parenthetically, just as concept of crime [has undergone] change with the growth of Information Technology so the categories of criminals who engage in such crimes. So far Indian society is concerned, particularly during ancient period, the definition of crime flagged by religious interpretation.³ The period was known for complete dominance of religion. All political and social activities in general and 'Crime' in particular, considered to be happened due to the presence of super-natural power. The Demonological theory of crime causation was an outcome of this period. Medieval period had evidenced the eras of renaissance and restoration, which delivered new, and a fresh look to 'crime'. The concepts like utilitarian, positive approach, analytical thinking, principles of natural justice, and thoughts of Lessie faire, hedonistic philosophy, and pain and pleasure theory outcome of this period which helped to open new horizons for the study of crime. Latter period paved the way for scientific & industrial revolution and rational way of interpretation dominated the thinking.⁴

IMPACTS OF CYBER CRIME

¹ Peter Grabosky and Russell Smith, *Crime in digital Age 3* (Federation Press., Sydney,1998)

² Dr.Jyoti Rattan,*Cyber laws and Information Technology 6* (Bharat law house pvt.ltd .,New Delhi,2014).

³ Dr.Amita Verma,*cyber crime and law 10* (Central law publication .,Allahabadh,2009).

⁴ *Supra* note 3, at 7.

Crime as an Evil Factor of Society

Despite crimeless society is myth, crime is omnipresent phenomenon, and it is non-separable part of social existence, one may get irritate by the question, 'Why there is too much ado about crime? 'No one can deny that crime is a social phenomenon, it is omnipresent, and there is nothing new in crime as it is one of the characteristic features of the all societies existed so far, may it be civilized or uncivilized, and it is one of the basic instincts of all human behavior! However, it should bear in mind that the social concern for high crime rate is not because of its nature, but due to potential disturbance it causes to the society.⁵ In addition, some individuals are victims of crime in a more specific sense. The victims of crime may lose anything that has value. Safety, peace, money, and property are perhaps basic values, because they contribute to the satisfaction of many wishes.

Impact of Cyber Crime over Socio-Eco-Political Riders

Conceptually, crime is a dynamic and relative phenomenon and subjected to the relative sociopolitical & economical changes occurring in existing system of society. Therefore, neither all-time suitable comprehensive definition encompassing all aspects of 'crime' is possible at any moment of time nor can a single definition be made applicable to different society. With its dynamicity, it is influenced by the changes occurring in the correlated phenomenon and value system generated by these changes. As evident in present scenario where money is more valuable than values, a definite hike in the corruption related offences are observed where social morality is low which influence the commission of crime attached less social stigma than ever before. Incidentally economic crime is on its peak. This clearly reflects that crime has its interdependency with other social phenomenon, economic systems and political machineries.⁶ Also, the population is one of the important factors influencing incidences of crimes. A positive correlation between the growth in incidences of crime and the population of the country has been observed. Besides population, the other factors influencing the crime are such as situation at a particular place, rate of urbanization, migration of population from neighboring places, unemployment, income inequality, [computer literacy in case of Cybercrime] etc. At the same time, the economic structure of give society is also influence the economic crimes. As every controlling system for crime has much to do with the political system which prescribe norms, make rules, create preventive measure, the political structure and system also influence the crime in given society. This clearly demonstrates that every definition of crime has correlation with the socio-economic and political factors.⁷

Impact of Cyber Crime over Teenager

These days a worst fear in teenager's eyes are Cyber Bullying. It is become common over past five years, generally from the age below eighteen are more susceptible and feared from Cyber Bullying as per inspection. It is becoming an alarming trend in our society. As per inspection of data, the worst fear of cybercrime is on teenager's female. Cyber Bullying is a fear when person receives threats, negative comments or negative pictures or comments from another

person. This is all done through core technologies described above mainly via online. Cyber Bullying can be done through chatting, instant messaging etc. Where website like Facebook, Orkut, Twitter user are more affected from Cyber Bullying.⁸ In my analysis generally feared person can reach a limit of depression, humiliation and threatens. Through this analysis we come to analyze that if person Bullied online he or she may be depressed up to the level of self-harming.⁹

Impact of Cyber Crime over Private Industry

Having to use three attributes to describe cybercrime I would use the words intrusive, silent and dangerous.¹⁰ Just the silent mode of this type of crimes is a major problem in combating the threat, in fact, very often the companies realize that they have been victims of frauds or attacks until long after the event occurred. The consequences are disarming and retrieve the situation is sometimes impossible, precisely the time gap between the criminal event and its discovery provides an advantage to those who commit crimes often unbridgeable that makes impossible any action of persecution.¹¹ We are assuming that the event is discovered by the victims and this is not always true, many companies are in fact over the years are victims of cybercrime, but they are not aware, a cancer that destroys from within.

Impact of Cyber Crime over Consumer Behavior

The information revolution, coupled with the strategic leveraging of the Internet, has exposed a number of relatively open societies to the dangers of cybercriminal and cyber terrorist acts, especially in commercial business transactions. With the development of e-commerce, this commercial dark side has become known as cybercrime and has taken on many forms that affect the perceptions of the way we shop online. Corporations should realize that these threats to their online businesses have strategic implications to their business future and take proper measures to ensure that these threats are eliminated or significantly reduced so that consumer confidence in the Internet as an alternative means of shopping is maintained. These counter measures, coined as cyber security, have been developed to ensure the safety of consumer privacy and information and allow for a carefree shopping experience.¹² There is need for the development of models that will allow corporations to study the impacts of cybercrime on online consumer confidence and to counter through leveraging the benefits associated with the latest developments in cyber security. With these two facets of e-commerce impacting the online consumer, corporations must ensure that the security measures taken will ultimately prevail to assure that consumers will continue to use the Internet to satisfy their shopping needs.¹³

Impact of Cyber Crime over Business

According to the FBI and the Department of Justice, cyber-crime is on the rise among American businesses, and it is

⁵ Sumanjit Das and Tapaswini Nayak, "Impact of cybercrime" 6 *IJESSET*, issue 2, ISSN: 22316604, (oct 2013).

⁶ Pavan Duggal, *Text Book on Cyber Law* 53 (Universal law Publication, Delhi, 2016).

⁷ Ibid.

⁸ Hemraj Saini, "cyber crime and their impacts: A review" 2 *IJERA*, Issue 2, ISSN:2248-9622, (2012).

⁹ *Supra* note 2, at 14.

¹⁰ R.C Mishra, *Cyber Crime: Impact in the New Millennium* 13 (Authorspress, 2002).

¹¹ Ibid.

¹² Animesh Sarmah and Roshmi Sarmah, "A Brief Study on Cyber Crime and Cyber law's of India" 4 *IRJET*, Issue 6, ISSN: 2395-0072, (2017).

¹³ *Supra* note 9, at 206.

costing them dearly. Cyber-crime includes a myriad of devious criminal practices designed to breach a company's computer security. The purpose of the electronic break and enter can be to steal the financial information of the business or its customers, to deny service to the company website or to install a virus that monitors a company's online activity in the future.

The-Cost-Of-Protection

Companies that want to protect themselves from online thieves have to pull out their wallets to do it. There are costs in identifying risks, building new and safer operating procedures, and buying protective software and hardware.¹⁴ For businesses with complex or sensitive operations, this often involves hiring a cyber-security consultant to develop a customized solution. Not only are the upfront costs of protection expensive, but the systems must be tested and monitored regularly to ensure that they are still impactful against emerging cyber-attacks. These costs are often passed on to the customer through higher prices of goods and services.

Lost-Sales

Cyber-crime isn't just for thieves anymore. A new subculture has emerged in the past few years: the cyber-activist. These are the online equivalents of protesters who chain themselves to buildings or trees. Their purpose is to shut down a company's online operations to send a message about the company's business practices. In the past two years, major corporations, such as PayPal and MasterCard, have been attacked in this way.¹⁵ In December 2010, the PayPal website was attacked by dozens of people claiming to be part of the group, Anonymous. They attempted to perpetrate a denial of service attack in retaliation for PayPal shutting down payment services to Wiki Leaks. More than a dozen hackers were arrested in that crime. While PayPal did not experience a full shutdown, many other businesses aren't so lucky. A denial of service attack results in fewer sales as customers cannot access the company's online store. It can even result in less revenue in the long-term if some customers decide to no longer do business with a company vulnerable to attack.

Impact of Cyber Crime over Youth

Cyber communication is society's newest way to interact. Online social networking websites, text messages and emails provide users with an impactful, quick way to communicate with people all over the world. Teens in particular spend hours online every day, on computers or personal electronic devices.

Friendships

Family-resource.com states that 48 percent of teens believe the Internet improves their friendships. With social networking sites becoming increasingly popular, youth are able to stay connected to real and online friends. Some teens believe cyber connections help them feel confident to be their true selves. Instant messaging programs, used by an estimated 13 million teens, allow conversations with friends to occur in real time. Online communication tools open the door for friendships with other teens near and far.

¹⁴ Pavan Duggal, *Mobile Crime and Mobile Law*, 79 (Saakshar Law Publication, New Delhi, 2013)

¹⁵ *Supra note 9*, at 207.

Writing

While teens are frequently online, using cyber forms of communication doesn't require formal writing skills. Quite the opposite actually occurs; youths often use shorthand, abbreviations or slang when writing online. The National Commission on Writing states that 85 percent of teens use social networking communication, but 60 percent of them don't see this form of communication as "writing." Teens should be aware of the difference between formal and informal writing, and understand when the latter is not appropriate (in school).

Cyber Bullying

Cyber bullying is a negative impact of online communication between youth. Victims of cyber bullying often experience rumors and lies spread on online social networks. Bullies may post inappropriate or embarrassing pictures of their victims. Another aspect of cyber bullying involves using mean text messages as harassment. The National Crime Prevention Council states that cyber bullying is a problem for almost half of American teens. In some extreme cases, teens have taken their own lives as a result of cyber bullying.¹⁶

Sexual Solicitation

Sexual solicitation is a growing concern for youth who use forms of cyber communication. It may occur in chat rooms or on social networking sites. Sexual solicitation occurs when an adult or peer tries to engage in an online sexual relationship. A teen may be asked to disclose personal information, view pornography or discuss something sexual online. About 70 percent of teens who are sexually solicited online are girls. Teens should be cautious in posting suggestive photos online and talking to strangers in chat rooms.¹⁷

CONCLUSION

The future of the Internet is still up for grabs between criminals and normal users. Fears of a cyber apocalypse still abound, while the potential extent of damage that can be caused by wide scale fraud is nearly unbounded. These anxieties should be rationally tempered with the knowledge that the problems are being addressed, although perhaps not fast enough. The usefulness of the Internet has proved itself in numerous and myriad ways that will hopefully be enough to ensure it does not become a wasteland of criminal activity and a bastion for the malicious. The government still has an important role to play, but most of the prevention needs to be done by commercial entities producing software and those with the ability to stop fraud. Relying on consumer education programs will only affect a percentage of possible victims. The others need to be automatically protected through measures that do not stress and require considerable participation. Security needs to be easy and impactful if it is doing work. Whether cybercrime is still a pertinent issue ten years from now is unknowable in a sense, but if the Internet will continue to grow, it must be solved so that the realities of cybercrime will be proportional to real-world crimes, if not better.

¹⁶ Karnika Seth, *Computer Internet and New Technology Law 135* (Universal Law Publication, Delhi, 2013).

¹⁷ Debarati Halder and K. Shankar, *Cyber Crime Against Women in India 142* (Saga Publication India Pvt.Ltd., New Delhi, 2017)

REFERENCES

- [1] Crime in the Digital Age by Peter Grabosky and Russell Smith, Sydney: Federation Press, 1998.
- [2] Peter Grabosky and Russell Smith, *Crime in digital Age* 3 (Federation Press., Sydney,1998)
- [3] Dr.Jyoti Rattan,*Cyber laws and Information Technology* 6 (Bharat law house pvt.ltd .,New Delhi,2014).
- [4] Dr.Amita Verma,*cyber crime and law 10* (Central law publication .,Allahabad,2009).
- [5] Sumanjit Das and Tapaswini Nayak, " Impact of cybercrime" 6 *IJESET*, issue 2, ISSN: 22316604, (oct 2013).
- [6] Pavan Duggal, *Text Book on Cyber Law* 53 (Universal law Publication, Delhi, 2016).
- [7] Hemraj Saini, "cyber crime and their impacts: A review" 2 *IJERA*, Issue 2, ISSN:2248-9622, (2012).
- [8] R.C Mishra, *Cyber Crime: Impact in the New Millennium* 13 (Authorspress, 2002).
- [9] Animesh Sarmah and Roshmi Sarmah, "A Brief Study on Cyber Crime and Cyber law's of India" 4 *IRJET*, Issue 6, ISSN:2395-0072, (2017).
- [10] Pavan Duggal, *Mobile Crime and Mobile Law*, 79 (Saakshar Law Publication, New Delhi, 2013).
- [11] Karnika Seth, *Computer Internet and New Technology Law* 135 (Universal Law Publication, Delhi, 2013).
- [12] Debarati Halder and K. Shankar, *Cyber Crime Against Women in India* 142 (Saga Publication India Pvt.Ltd., New Delhi, 2017).

