BioGecko

Vol 12 Issue 02 2023

ISSN NO: 2230-5807

An Ethical Angle of Cyber Crime Issues and Challenges in India

Dr.Sarang Javkhedkar[1], Dr. Anjali Shrungarkar[2], Dr.Atul P. Kulkarni[3]

[1]Dr. Ambedkar Institute of Management Studies and Research, Nagpur
[2]City Premier College,Nagpur
[3]Vishwakarma Intitute ofInformation Technology,Pune

Email: [1]sarangjavkhedkar@gmail.com, [2]sayalijavkhedkar@gmail.com, [3]atul.kulkarni@viit.ac.in

Abstract
The present paper is an attempt to bandy issues and challenges of Cyber Crime in India from an ethical perspective. Ethics is a branch of gospel, which deals with what is considered right or wrong. The ethics centers and program devoted to business ethics, legal ethics, bioethics, medical ethics, engineering ethics, and computer ethics have sprung up. Cybercrime is arising as a serious trouble. Computer Technology is one of the important general purpose Technologies in moment's age for several reasons. Moment it is used in nearly all the associations, institutions, and people. Computer technology makes the life so speedy and fast, but hurled under the decline of trouble from the deadliest type of crime nominated as' Cybercrime '. The advancement of IT brings so numerous installations to us; but also brings so numerous problems and challenges too and out of which Cyber Crime is a kind of offence, which deals with the cyber world, which includes computer security, information security, and mobile security too. The adding number of crimes in the field of Information Technology brings a big magnet to Cyber Crime to everyone.

Keywords Ethics, Cyber Crime, Issues and Challenges in India, Computer Security

1. Preface

Ethics is a branch of gospel, which deals with what is considered right or wrong. The ethics centers and program devoted to business ethics, legal ethics, bioethics, medical ethics, engineering ethics, and computer ethics have sprung up. Cybercrime is arising as a serious trouble. Cybercrime is a term used to astronomically describe felonious exertion in which computers or computer networks are a tool, a target, or a place of felonious exertion and include everything from electronic cracking to denial of service attacks. It is also use to include traditional crimes in which computers or networks are used to enable the lawless exertion. The Cybercrime can halt any road where it is, it may misguide the aeroplanes on its flight by misguiding with wrong signals, it may beget any important military data to fall in the hands of foreign countries, and it may halte-media and every system can collapse within a bit of seconds.

The present study has been accepted to touch some aspects, effect and prospects of this cyber technology with special reference to trouble acts of Cybercrime by India. Sweats have been made to dissect legal frame available for its control in India. To start with, it is, thus, necessary to define the confines of word 'crime '. Therefore it's beyond mistrustfulness that 'crime ' is a relative miracle, universal in nature and basically all societies from ancient to ultramodern have been putatively demonstrating its presence. Each society have been furnishing its own description of felonious geste and conduct made punishable by express will of the political community ruling over the society and it was always influence by religious-social- political provident values prevailing in the given society. Therefore from time immemorial the geste that attracts 'correction alliability' told and characterized by overall outgrowth of these norms.

Interjectionally, just as conception of crime (has experienced) change with the growth of Information Technology so the orders of culprits who engage in similar crimes. So far, Indian society is concerned, particularly during ancient period, the description of crime flagged by religious interpretation. The period was known for complete ominance of religion. All political and social conditioning in general and' Crime' in particular, considered to be happed due to the presence ofsuper-natural power. The Demonological proposition of crime occasion was an outgrowth of this period. Medieval period had substantiated the ages of belle epoque and restoration, which delivered new, and a fresh look to 'crime '. The generalities like utilitarian, positive approach, logical thinking, principles of natural justice, and studies of lessie faire, sybaritic gospel, and pain and pleasure proposition were

2. Objective

The main end and ideal of this study includes but not limited to as follows

- ▪ To know introductory about Cyber Crime and its characteristics;
- ▪ To know introductory about the challenges and hand of Cyber Crime;
- ▪ To learn introductory about the issues related to Cyber Crime compactly;
- ▪ To know introductory about the Cyber Crime affiliated act in the Indian environment.

3. Bracket of Cyber Crime

Data Interception A bushwhacker observers data aqueducts to or from a target in order to gather information. This attack may be accepted to gather information to support a after attack or the data collected may be the end thing of the attack. This attack generally involves smelling network business, but may include observing other types of data aqueducts, similar as radio. In utmost kinds of this attack, the bushwhacker is unresisting and simply observes regular communication, still in some variants the bushwhacker may essay to initiate the establishment of a data sluice or affect the nature of the data transmitted. Still, in all variants of this attack, and distinguishing this attack from other data collection styles, the bushwhacker is not the intended philanthropist of the data sluice. Unlike some other data leakage attacks, the bushwhacker is observing unequivocal data channels (e.g. network business) and reading the content. This differs from attacks that collect further qualitative information, similar as communication volume, not explicitly communicated via a data sluice.

Data revision sequestration of dispatches is essential to insure that data cannot be modified or viewed in conveyance. Distributed surroundings bring with them the possibility that a vicious third party can prosecute a computer crime by tampering with data as it moves between spots. In a data revision attack, an unauthorized party on the network intercepts data in conveyance and changes corridor of that data before retransmitting it.

Data Theft Term used to describe when information is immorally copied or taken from a business or other existent. Generally, this information is stoner information similar as watchwords, social security figures, credit card information, other particular information, or other nonpublic commercial

Network Crime Network snooping with the functioning of a computer Network by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing Network data. Network Sabotage' Network Sabotage' or unskillful directors trying to do the jobs of the people they typically are in charge of. It could be the over alone, or a combination of effects. However, if Verizon is using the help the children, hindering first asker's line also they might be using network problems as a reason to get the civil government to intermediate in the interest of public safety. Of course, if the civil government forces these people back to work what is the purpose of unions and strikes anyway.

Access Crime Unauthorized Access" Unauthorized Access" is an bigwig's view of the computer cracker resistance. The filming took place each across the United States, Holland and Germany." Unauthorized Access" looks at the personalities behind the computers defenses and aims to separate

the media exaggerate of the' outlaw hacker' from the reality. Contagion Dispersion vicious software that attaches itself to other software.(Virus, worms, Trojan steed, Time lemon, Logic Bomb, Rabbit and Bacterium are exemplifications of vicious software that destroys the system of the victim.

4. Reasons behind the Cyber Crime

There are numerous reasons why cyber-criminals are doing cyber-crime; chief among them are mentioned below-

- For the sake of recognition.
- For the sake of quick plutocrat.
- To fight a cause one thinks he believes in.
- Low borderline cost of online exertion due to global reach.
- Catching by law and enforcement agency is less effective and more precious.
- New occasion to do legal acts using specialized armature.
- No concrete non-supervisory measure.
- Lack of reporting and norms
- Difficulty in identification
- Limited media content.
- Commercial cybercrimes are done inclusively and not by individual persons.

5. Challenges of Cyber Crime

Endless discussion is there regarding the pros and cons of cybercrime. There are numerous challenges in front of us to fight against the cybercrime. Some of them then bandied below -

- Lack of mindfulness and the culture of cyber security, at individual as well as organizational position.
- Lack of trained and good force to apply the counter measures.
- Noe-mail account policy especially for the defense forces, police and the security agency labour force.
- Cyber-attacks have come not only from terrorists but also from bordering countries contrary to our National interests.
- The minimal necessary eligibility to join the police does not include any knowledge of computers sector so that they are nearly illiterate tocyber-crime.
- The speed of cyber technology changes always beats the progress ofgovt. Sector so that they are not suitable to identify the origin of thesecyber-crimes.
- Promotion of Research & Development in ICTs is not over to the mark.
- Security forces and Law enforcement labour force are not equipped to address high- tech crimes.
- Present protocols are not tone sufficient, which identifies the investigative responsibility for crimes that stretch internationally.
- Budgets for security purpose by the government especially for the training of law enforcement, security labour forces and investigators in ICT are less as compare to other crimes.

6. Way to Reduce Cyber Crime

There are so numerous conduct available to reducing Cyber Crime and cyber offence and out of which entourages are important similar as –

Legal Action as far as legal action is concerned, the following conduct may be helpful to reduce Cyber Crime and important to take into –

- ✓ Electronic Dispatches sequestration Act of 1986.
- ✓ Civil sequestration Act of 1974.
- ✓ Indian IT Act.
- ✓ Dispatches Act of 1934 streamlined 1996.
- ✓ Computer Fraud and Abuse Act of 1984.
- ✓ Computer Security Act of 1996.
- ✓ Economic Espionage Act of 1996.
- ✓ Health Insurance Portability and Responsibility Act of 1996.
- ✓ Personal Data sequestration and Security Act of 2007.
- ✓ Data Responsibility and Trust Act.
- ✓ Identify Theft Prevention Act.
- ✓ Data security Act of 2007

Mindfulness structure

Mindfulness structure is most important to reduce Cyber Crime and IT crime; therefore following effects are essential to follow–

- ➢ Creating changes in the word of the computing bias similar as computers, hunt and networking systems, changes of the word of other services similar as dispatch, social networking point, and other service grounded point registered by the aspirant or stoner.
- ➢ Reduction in use of dispatch in cyber café and other places and calculating bias.
- ➢ Open and communicating with the unknown computer and analogous device.

Technological Provisory

- ❖ Use of Anti-Virus software and system in the computer system or when network or telecommunication Systems.
- ❖ Use of internet safety tools, applicable time and as per machine demand.
- ❖ Use of Good firewall and sophisticated Network Designing.
- ❖ Keep off the Blue tooth and other RF bias.

7. Findings

1. IT Crime and Electronic Crime are synonymous with Cyber Crime and using fleetly for breaking reliable systems.
2. Still, numerous people aren't apprehensive of the strategy to use ”switch off “ Cyber Crime.
3. Cyber Crime is adding both in homemade form and as well as online form.
4. Moment Cyber Crime includes piecemeal from the computer and similar bias are television, ATM, Mobile Phone, I- cover and so on.

8. Conclusion

IT is one of the important and helpful tools currently. The new world of information society with global networks and cyberspace will inescapably induce a wide variety of social, political, and ethical problems. Numerous problems related to mortal connections and the communities come apparent, when utmost mortal conditioning are carried on in cyberspace. Some introductory ethical issues on the use of IT on global networks correspond of particular sequestration, data access rights, and dangerous conduct on the Internet. Though it has so numerous problems and downsides in numerous classes out of which Cyber Crime is most important and on the other hand,E-Crime and its world arising. Reduction in Cyber Crime is only possible when stoner will be much further apprehensive of the aspects of Cyber Crime and when they enrich their knowledge towards a reduction in cyber and electronic crime. The advancement of IT brings so numerous installations to us; but also brings so numerous problems and challenges too and out of which Cyber Crime is a kind of offence, which

deals with the cyber world, which includes computer security, information security, and mobile security too. The adding number of crimes in the field of Information Technology brings a big magnet to Cyber Crime to everyone.

Ethical norms also include those that enjoin merits of honesty, compassion, and fidelity. In addition, ethical norms include norms relating to rights, similar as the right to life, the right to freedom from injury, the right to choose, the right to sequestration, and right to freedom of speech and expression. Similar norms are acceptable norms of ethics because they are supported by harmonious and well-innovated reasons. Ethics refers to the study and development of particular ethical norms, as well as community ethics, in terms of geste, passions, laws, and social habits and morals, which can diverge from further universal ethical norms.

References

- Kubo, Takeaki, 1999, Internet Revolution & Japanese IT Industry, Symposium on Development of Information Industry in the Asia- Pacific Region, 5- 8 October 1999, Srilanka, runner 21- 93.
- Saracevic,T.(1996). Applicability reevaluated . Information wisdom Integration in perspectives. In Proceedings of the Alternate Conference on generalizations of Library and Information Science(pp. 201 – 218), Copenhagen, Denmark Royal School of Library and Information Science.
- Saracevic,T.(1975). Applicability A review of and a frame for the thinking on the notion in information wisdom. Journal of the American Society of Information Science, 26(6), 321 – 343.
- ACM, 1992, ACM Code of Ethics and Professional Conduct, Association of Computing Machinery, USA, October 1992.
- Stephan, Karl D, 2002, Is Engineering Ethics Optional?, IEEE Technology and Society, Volume 20, Number 4, runner 6- 12.
- Martin,S.B.(1998). Information technology, employment, and the information sector Trends in information employment 1970 – 1995. Journal of the American Society for Information Science, 49(12), 1053 – 1069.