International Journal of Advanced Trends in Engineering and Technology (IJATET)
Impact Factor: 5.965, ISSN (Online): 2456 - 4664
(www.dvpublication.com) Volume 3, Issue 1, 2018

CYBER CRIME: CHALLENGES, ISSUES, RECOMMENDATION AND SUGGESTION IN INDIAN CONTEXT

P. K. Paul* & P. S. Aithal**
* Raiganj University, West Bengal
** Vice Chancellor, Srinivas University, Mangalore, Karnataka

Cite This Article: P. K. Paul & P. S. Aithal, "Cyber Crime: Challenges, Issues, Recommendation and Suggestion in Indian Context", International Journal of Advanced Trends in Engineering and Technology, Volume 3, Issue 1, Page Number 59-62, 2018.

Abstract:

Information Technology is one of the important general purpose Technologies in today's age for several reasons. Today it is used in almost all the organizations, institutions, and people. The advancement of IT brings so many facilities to us; but also brings so many 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 increasing number of crimes in the field of Information Technology brings a big attraction to Cyber Crime to everyone. Cyber Crime is an important and valuable illegal activity nowadays. Initially internet and email are treated as the main tools of crime; however, over the time the number of weapons, tools, and happenings are increasing in this field. This paper discusses about Cyber Crime including nature, characteristics, and issues.

Key Words: Information, Information Technology, Cyber Crime, Cyber Space, Cyber Security, Information Science, Computer Forensic, Cyber Law & IT Law.

Introduction:

Cyber law is actually a law enacted by the concerned Government of the concerned country and state which allow for computer and cyber offence. Cyber Crime is the crime and other offensive activity such as computer crime, mobile crime, and IT crime may fall under the Cyber Crime. Cyber Law is the law and legal action which is essential or utilize for various kind of electronic crime and offence. Actually, people are still not aware about Cyber Crime and remedial for this kind of offence [01, 05]. Cyber Law is practically approved by the Government or constitutional unit or division for the concerned country or territory. The number of the incidents is increasing day by day and the periphery of Cyber Crime is also increasing rapidly. Virtually, the cyber law basically encompasses the laws which deal with Cyber Crime, Electronic Crime, Electronic Signature and intellectual property crime, data protection, information assurance, and so on. There are so many ways to reduce Cyber Crime and cyber related problems; such types of aspects are introduced in this paper briefly. Due to less awareness, people still do not take many precautions for the Cyber Crime [06, 07].

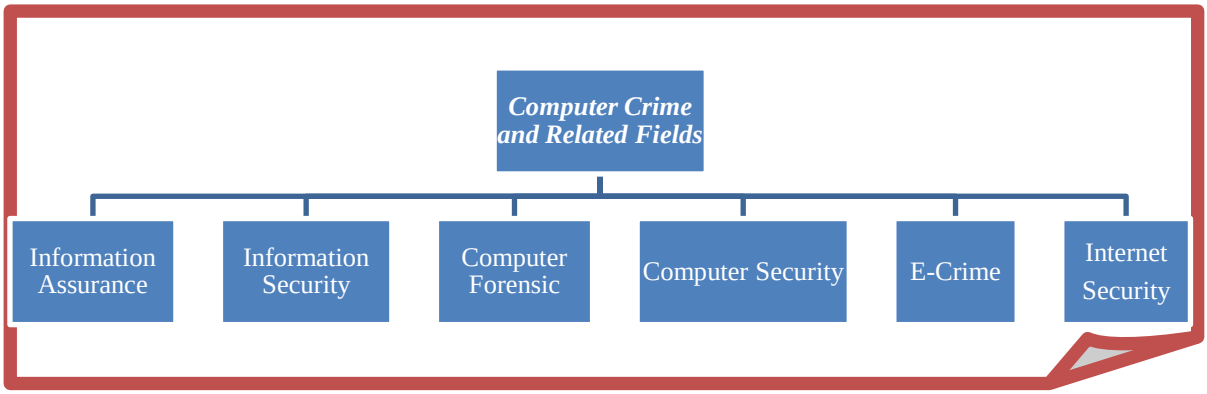

Figure 1: Depicted some allied and core field of Cyber Crime

Objective:

The main aim and objective of this study includes but not limited to as follows

- ✓ To know basic about Cyber Crime and its characteristics;
- ✓ To know basic about the challenges and facet of Cyber Crime;
- ✓ To learn basic about the issues related to Cyber Crime briefly;
- ✓ To know basic about the Cyber Crime related act in the Indian context.

Cyber Crime:

Cyber law is actually nothing but the legal and other electronic crime. In other sense, cyber law is actually legal aspect that deal with cyber related matter. Practically cyber is an important name in the field of computer science, legal studies, business and commercial studies [08, 09]. Cyber law and crime is a kind of interdisciplinary subject incorporated with IT, Computing, and legal studies. In generally, cyber space includes computer, networks, software, data storage devices like pen drive, hard disk, USB, and others. E-Crime is

mainly responsible for the emergence of cyber law. E- Crime includes all most all type of crime and criminal activities related to the electronic world. The field of E-Crime is increasing day by day and in almost all the fields [10, 11].

Cyber Crime and Types:

Cyber Crime is the main part of cyber world and Information Technology and Cyber Crime may be classified as follows

- ✓ E-Crime is one important type of Cyber Crime which includes mobile crime, television crime, video crime, and so on;
- ✓ Internet Crime is another important type of crime in which fake dealings basically happens;
- ✓ Computer crime is another which includes manipulation and changes in computer data; both as offline and offline way.

Cyber Crime: Some Examples

Following may be treated as Cyber Crime, Electronic Crime; directly and indirectly-

- ✓ Tampering and changes of document, content and database of the computer, laptop, mobile and so on.

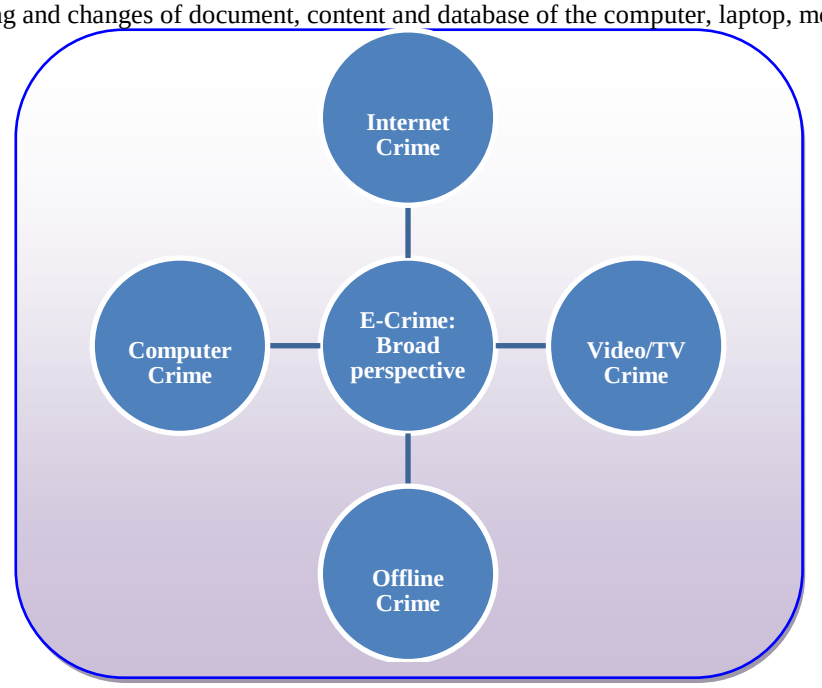

Figure 2: Depicted some examples of Electronic Crime

- ✓ Hacking computer or computer system or computer information and telecommunication networks and so on.
- ✓ Sending or store offensive information or message or content or even audio, video material may fall under the category of Cyber Crime.
- ✓ Cheating by personalization by using computer resources and similar resources.
- ✓ Creating and generating fake information or terrorism by using cyber tools or terrorist activities with the cyber weapon [13, 14].
- ✓ Publishing and dissertation of illegal, unethical and some one's material or document in the electronic form or similar form.
- ✓ Enter or access into unauthorized computing systems or IT systems.
- ✓ Sending threats message by email or SMS or any other electronic way or objects.
- ✓ Creating and distribution of false information or documents.
- ✓ Changes and replacement in document or content without prior permission or acknowledgement [15].
- ✓ Many time, we see in the television advertisement of selling something or identification of the person and sending SMS or like that, such type of dealing maybe fall under the category of Cyber Crime or Electronic Crime.
- ✓ Spreading virus or malware or similar object to the computer or in whole computer and information networks.
- ✓ Use of false information on the website or total fake website is another Cyber Crime and which shows about any person, organization or nation. In many cases, we can see such examples like- in Ministry, University or Railway as far as India is concerned.
- ✓ Uploading and spreading controversial information message and details to another person.
- ✓ Hacking password of another computer or information system or changes of content in email, social networking site such as Facebook and orkut, twitter and so on.

- ✓ Creating email account or social networking site for another name without acknowledgement is also fall under the category of Cyber Crime.
- ✓ Hacking website and changes web IP address or linkages with other website is also a kind of Cyber Crime [16, 17].

Way to Reduce Cyber Crime:

There are so many actions available to reducing Cyber Crime and cyber offence and out of which following are important such as-

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

- ✓ Electronic Communications Privacy Act of 1986.
- ✓ Federal Privacy Act of 1974.
- ✓ Indian IT Act.
- ✓ Communications Act of 1934 updated 1996.
- ✓ Computer Fraud and Abuse Act of 1984.
- ✓ Computer Security Act of 1996.
- ✓ Economic Espionage Act of 1996.
- ✓ Health Insurance Portability and Accountability Act of 1996.
- ✓ Personal Data Privacy and Security Act of 2007.
- ✓ Data Accountability and Trust Act.
- ✓ Identify Theft Prevention Act.
- ✓ Data security Act of 2007

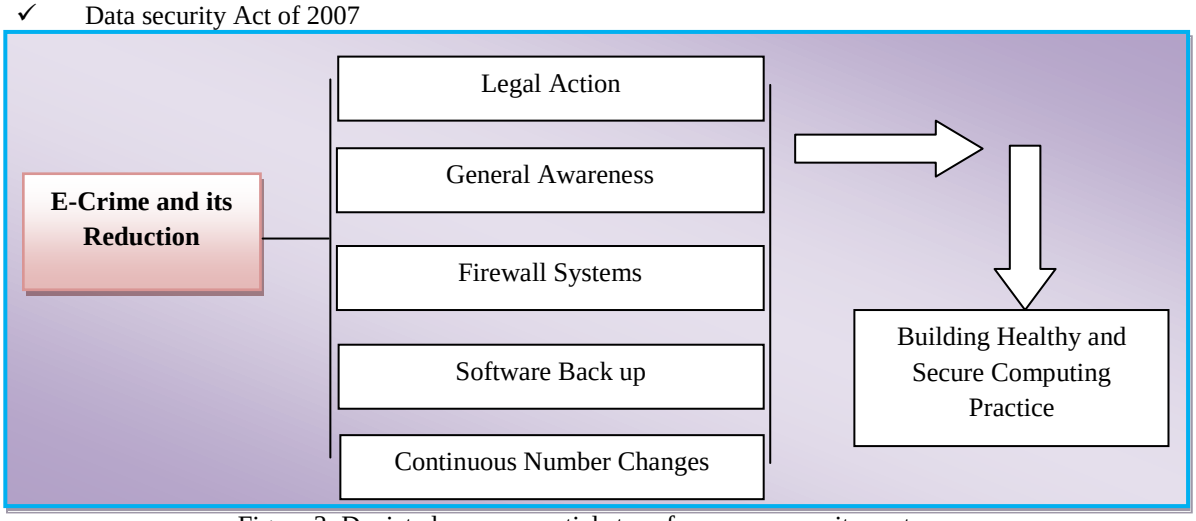

Figure 3: Depicted some essential steps for secure security system

Awareness Building: Awareness building is most important to reduce Cyber Crime and IT crime; thus following things are essential to follow

- ✓ Creating changes in the password of the computing devices such as computers, search and networking systems, changes of the password of other services such as email, social networking site, and other service based site registered by the applicant or user.
- ✓ Reduction in use of email in cyber café and other places and computing devices.
- ✓ Open and communicating with the unknown computer and similar device.

Technological Backup:

- ✓ Use of Anti Virus software and system in the computer system or when network or telecommunication Systems.
- ✓ Use of internet safety tools, appropriate time and as per machine requirement.
- ✓ Use of Good firewall and sophisticated Network Designing.
- ✓ Keep off the Blue tooth and other RF devices [19].

Findings:

- ✓ IT Crime and Electronic Crime are synonymous with Cyber Crime and using rapidly for breaking foolproof systems.
- ✓ Still, many people are not aware of the strategy to use 'switch off' Cyber Crime.
- ✓ Cyber Crime is increasing both in manual form and as well as online form.
- ✓ Today Cyber Crime includes apart from the computer and such devices are TV, ATM, Mobile Phone, I-Pod and so on.

Conclusion:

IT is one of the important and helpful tools nowadays. Though it has so many problems and drawbacks in many classes out of which Cyber Crime is most important and on the other hand, E-Crime and its world ar

also increasing day by day and unfortunately side by side the kind of crime with electronic gadgets are also emerging [11, 13]. Reduction in Cyber Crime is only possible when user will be much more aware of the aspects of Cyber Crime and when they enrich their knowledge towards a reduction in cyber and electronic crime.

References:

1. Cohen, E. B. (2004). Applying the Informing Science Framework to Higher Education: Knowledge Development, Management, and Dissemination. Konferencja Pozyskiwanie wiedzy i zarządzanie wiedzą (Proceedings of the Knowledge Acquisition and Management Conference) May 13-15, 2004 Kule, Poland.
2. Cohen, Eli B. and Nycz Malgorzata (2006). Learning Objects and E-Learning: an Informing Science Perspective. Interdisciplinary Journal of Knowledge and Learning Objects Volume 2, 2006
3. 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.
4. Michael Buckland and Ziming liu (1995).History of information science. Annual Review of Information Science and Technology vol. 30: 385-416.
5. P.K. Paul, " Information Scientist: Roles and Values with special Reference to their Appropriate Academic Programme and its availability in India:" International Journal of Information Dissemination and Technology, Vol. 2, No. 4, October-December-2012, Page-245-248, ISSN-2229-5984
6. Paul, P. K., D Chaterjee, R Bhatnagar, Uma Pricilda "Information Scientist: Contemporary innovative techno management roles with special reference to Information Scientist Vs Information Technologist: A Study", Indian Journal of Information Science and Applications [IJISA], Vol. 2. No. 1, Jan-Jun-2012, Academic Research Publication, New Delhi, Page-47-50, ISSN-2249-3689
7. Paul,P.K. , D Chatterjee, M Ghosh "Neural Networks: Emphasizing its Application in the World of Health and Medical Sciences" Journal of Advances in Medicine, Vol. 1 No. 2, July-Dec, ISSN-2277-9744 Page-17-23, New Delhi Publisher, New Delhi
8. Paul, P. K, Ashok Kumar, Dipak Chaterjee "Health Informatics and its Practice: Emerging Domain of Information Science-Indian Scenario" in Current Trends in Biotechnology and Chemical Research, Vol. 2 No. 2, July-Dec, 2012, Page- 83-87, ISSN-2249-4073
9. Prantosh Kr. Pau1, K L Dangwal, Asok Kumar Garg "Education Technology and Sophisticated Knowledge Delivery" Techno-Learn-International Journal of Education Technology, ND Publisher, New Delhi, Vol. 2, No. 2, Page-169-175 ISSN-2231-4105
10. Prantosh Kr. Pau1, K L Dangwal and Dipak Chaterjee, "Information Technology and Advance Computing and their interaction for healthy Education, Techning, and learning: The IKM Approach" Asian Journal of Natural and Applied Sciences,ISSN-2186-8468, Page- 70-77 V-1, No. 4, December-2012, Leena and Luna International, Oyama, Japan
11. Paul, P. K., M K Ghose, "Cloud Computing: Possibilities, Chalenges, and opportunitities with special reference to its emerging need in the academic and working area of Information Science", ICMOC, Procedia Engineering, 38 [2012], Page-2222-2227, DOI-10.1016/j.proeng.2012.6.267, 1877-7058 C-Published by- Elsevier,USA,
12. Saracevic, T. (1996). Relevance reconsidered. Information science: Integration in perspectives. In Proceedings of the Second Conference on Conceptions of Library and Information Science (pp. 201–218), Copenhagen, Denmark: Royal School of Library and Information Science.
13. Saracevic, T. (1975). Relevance: A review of and a framework for the thinking on the notion in information science. Journal of the American Society of Information Science, 26(6), 321–343.
14. Saracevic, T. (1979a). An essay on the past and future of information science education. I. Historical overview. Information Processing & Management, 15(1), 1–15.
15. Saracevic, T. (1979b). An essay on the past and future of information science education. II. Unresolved problems of 'extemalities' of education Information Processing & Management, 15(4), 291–301.
16. Vakkari, S.P. (1996). Library and information science: Content and scope. In J. Olaisen, E. Munch-Petersen, & P. Wilson (Eds.), Information science: From development of the discipline to social interaction. Oslo, Norway: Scandinavian University Press.
17. Vickery, B.C., & Vickery, A. (1987). Information science in theory and practice. London: Butterworths.
18. Wersig, G., & Neveling, U. (1975). The phenomena of interest to information science. Information Scientist, 9, 127–140.
19. White, H.D., & McCain, K.W. (1997). Visualization of literatures. Annual Review of Information Science and Technology, 32, 99–168.