"Effect of Cyber Crime on Indian Economy"

Kiran, Assistant Professor, School of Bioengineering and Biosciences, Lovely Professional University, Phagwara, Punjab

Gift Chichele , M.Sc. Forensic Science, School of Bioengineering and Biosciences, Lovely Professional University, Phagwara, Punjab

Introduction

The author has described Cyber Crimes as type of crimes which use computers and networks as targets or weapons (Milner, 1999). During 1960s It was called computer crimes since they involved large main frame computer systems which had limited internet or no internet at all (Parker, 1989). The most common criminals during that time were people who had access to those computers like disgruntled employees. However, as Li, J. X. wrote in his study, during this time the legislature did not provide any specific countermeasures against the phenomenon, leaving law enforcement agencies to deal with it within the traditional legal framework (Li, 2017). In our present time, the computer crimes have turned into cybercrimes due to ever increasing computer networks and personal computers. These crimes have adversely affected the economy, individual lives and society across the global. The study indicated that these crimes have note spared India as it has registered an alarming growth rate of 50% per year and ranked third position on the list of countries where cybercrimes are more prevalent in the world. Having this in mind, the researcher felt persuaded to carry out a research with the aim of assessing the levels of individual knowledge on the existing cybercrimes that are mostly common in India, and their impacts on the economy. In order for the researcher to fully analyse parameters in the study, he gave a detailed introduction of origins and evolution of cybercrimes, different categories of cyber crimes and the cyber crimes that are more prevalent in India.

The author carried out survey to collect data using questionnaires and the responses were quantitatively analysed using some statistical techniques. The results showed that cracking, software piracy, ATM fraud and pornography among others are prevalent crimes in India. The government is losing a lot of money in investigating into such cases and prosecuting the offenders. Sadly, most of the cases do not succeed in court due to lack of concrete evidence as the cases are more complex in nature. The author suggested that these crimes can be reduced if networks and data are defended and protected, criminal activities are detected investigated and brought them before the court of law for prosecution.

1.1. Categories of cyber crimes

Some of the examples of cyber-crimes highlighted in this article are spamming - sending an unsolicited emails especially adverts, identity theft - stealing someone's information, hacking – gaining an unauthorised access to someone's computer, phishing – fraudulent attempt to obtain someone's sensitive information, Denial of service(DOS) - making Internet services unavailable for users, Yahoo/yahoo extortion - advanced

free fraud 419, salami attacks - stealing money in small amounts in a cunning way, credit card fraud - ATM, plagiarism and software piracy, pornography and virus dissemination.

1.2. Cybercrimes most prevalent in India

The study setting was India, as such it was imperative to focus on the cybercrimes common in India. Some of the cases mentioned in this article are; Assault by Threat, Child pornography, Cyber laundering, Cyber stalking, Cyber terrorism, Cyber theft, Hardware Hijacking, Spam, Script kiddies, Insiders, Yahoo Attack, Salami Attack.

1.3. Methodology

In this article under review, data were collected through questionnaires in a survey. A sample of 60 computer users at the university of Centurian in the Department of Mathematics and Computer Science was randomly selected out of the targeted total population of 120. 55 out of 60 questionnaires were retrieved. Level of individual knowledge on cybercrimes was measured on the basis of cracking, software piracy, pornography, ATM fraud, Yahoo/ Cyber extortion.

1.4. Results and discussion

The study has found that 52.7% of the sampled population were aware that cracking, software piracy and ATM Fraud are cybercrimes. The rest of the parameters had scores below 50% which means there is low awareness on them yet the country is ranked number 3 on cybercrimes.

1.5. Conclusion

From the study, it is clear that there is still a section of people in India that do not know cybercrimes yet these crimes continue to negatively affect the economy of the country, resulting in high unemployment rate and inadequate social services. Further, they have damaged country's reputation at international level.

1.6. Recommendations

The study has proposed the following recommendations;

- That government should provide training to police so that they can be able to handle cyber related crimes.
- That the police should have central computer response wing to advise the state and other investigative agencies on computer crime investigations
- That the country should set up a cyber security regulatory body called national computer crime resource centre.
- That the Government to establish forensic commission that will be responsible for the training of forensics personnel/law enforcement agencies.

2.0. My Analysis of the article

2.1. Strengths in the study

- The research topic was well framed, narrow and so clear such that anyone reading it can easily understand it.
- The topic was timely, specific and relevant to India nation as it has registered an alarming growth rate of cybercrimes - 50% per year and was ranked third position on the list of countries where cybercrimes are more prevalent in the world. At this time, it was necessary to carry out the study to find out the contributing factors to such figures, how they are impacting the economy of the country and find the best ways to address the problems.
- The study gave an introduction of evolution of cybercrimes, their types and most common cybercrimes happening in India. This helps the reader to understand cybercrimes. He measured individual level of awareness on 5 cybercrimes cases that are so common in India. This was a good representation of cybercrimes cases happening in India.
- The methodology used in the study was relevant and in line with this type of study where the aim was to know individuals' level of knowledge on cyber related crimes.
- He selected the sample from a target population that was already conversant with cyber space and they may be the culprits or the direct victims of cyber-crimes. This was good because they can give relevant information.
- The research questions were structured in a simple way that do not consume time for respondent. That is why he retrieved more questionnaires from respondent.
- The study gives recommendations to government and other stakeholders on what should be done to ensure cybercrimes are minimised.
- The study respects the views of other people who did their studies on similar topic as evidenced by intext citations and reference included in the study.

2.2. Weaknesses

- The study does not show any data in form of qualitative collected during survey. He was supposed to collect data regarding the impact of those mentioned cyber crimes to an individual as respondent, society and government.
- The study reported cyber-crime annual growth rate as well as India ranking without citing the source which weakened the statement.

  He could also have gone to police departments to find out number of cases that are reported on a given period of time.

Bibliography

Li, J. X. (2017). Cyber Crime and Legal Countermeasures: A Historical Analysis. *International Journal of Criminal Justice Sciences (IJCJS)*, 197.

Milner, H. V. (1999). The political economy of international trade. *Annual Review of Political Sci-ence, 2,*, 91–114.

Parker, D. B. (1989). Computer Crime: Criminal Justice Resources Manual. *National Institute*, 5.

Rao, Y. S. (2014). Effect of Cyber Crime Indian Economy. *International Journal for Research in Technological Studie*, all.

Gary L Palmer.(2001). A Road Map for Digital Forensic Research. Technical Report DTR-T0010-01, DFRWS. Report for the First Digital Forensic Research Workshop (DFRWS).

Kruse II, Warren and Jay, G. Heiser (2002) Computer Forensics: Incident Response Essentials. Addison-Wesley.

National Institute of Justice.(July 2001) Electronic Crime Scene Investigation A Guide for First Responders. http://www.ncjrs.org/pdffiles1/nij/187736.pdf.

Mark Reith, Clint Carr and Gregg Gunsch.(2002)An Examination of Digital Forensic Models International Journal of Digital Evidence, Fall 2002,Volume 1, Issue 3.

Brian Carrier and Eugene H Spafford,(2003) Getting Physical with the Investigative Process International Journal of Digital Evidence.Fall 2003,Volume 2, Issue 2.