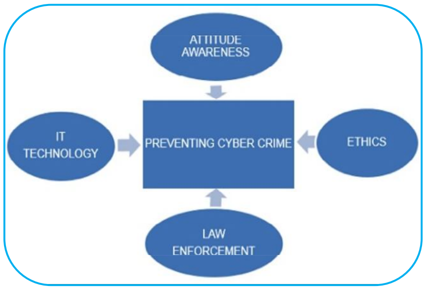
INDIAN STREAMS RESEARCH JOURNAL
ISSN NO : 2230-7850
IMPACT FACTOR : 5.1651 (UIF)
VOLUME - 12 | ISSUE - 4 | MAY - 2022

STUDY OF NETWORK SECURITY APPROACH FOR PREVENTION OF CYBER CRIME

Ajay Singh[1] and Dr. Jitendra Sheetlani[2]
[1]Research Scholar Computer Science Sri Satya Sai University of Technology and Medical Sciences Sehore Bhopal (M.P.)
[2]Prof. of Computer Science Sri Satya Sai University of Technology and Medical Sciences Sehore Bhopal (M.P.)

ABSTRACT:

Computer crime also referred as Cybercrime has increased in severity and frequency in the recent years and because of this, it has become a major concern for companies, universities and organizations. Worldwide governments, police departments and intelligence units have started to react. In this paper, we provide an overview of Cybercrime and examine the awareness among different respondents on the issue of Cyber Crime, to emphasize the severity of this problem and the urgent need to limit its impact worldwide.



KEY WORDS: Cyber Crime, Law, Internet Crime, Awareness.

INTRODUCTION

From personal computers in the home used to track checking accounts and keep household inventories in databases to large supercomputers that control space missions and run the world's largest companies, computers have become commonplace. The number of individuals who have access to the information on those computers has increased as the communications industry has undergone a revolution in recent years, and uncontrolled access to information presents a very real threat in most business and some government information.

When the Internet was developed, the founding fathers of the Internet hardly had any inclination that the Internet could also be misused for criminal activities. Today, there are many disturbing things happening in cyberspace. Obviously, it was just a matter of time before criminals discovered the advantages of computers and make it increasingly possible to get proprietary information of financial institutions and other firms.

Because of the highly significant role that computers play in modern life, there is a need to keep information on machines secure from tampering, from unauthorized dissemination, and from unauthorized removal.

DEFINITION OF CYBER CRIME

The term 'cybercrime' has not been defined in any Statute or Act. The Oxford Reference Online defines 'cybercrime' as crime committed over the Internet. The Encyclopedia Britannica defines 'cybercrime' as any crime that is committed by means of special knowledge or expert use of computer technology. So what exactly is Cybercrime? Cyber Crime could reasonably include a wide variety of criminal offences and activities. A generalized definition of cybercrime may be "unlawful acts wherein the computer is either a tool or target or both".

CBI Manual defines cybercrime as:

(i) Crimes committed by using computers as a means, including conventional crimes.
(ii) Crimes in which computers are targets.

The Information Technology Act, 2000, does not define the term 'cybercrime'. Cybercrime can generally defined as a criminal activity in which information technology systems are the means used for the commission of the crime.

Based on the United Nations General Assembly resolution of January 30, 1997, the Government of India passed the Information Technology Act 2000 (Act No.21 of 2000) and notified it on October 17, 2000. The Information Technology Act, 2000, is the first step taken by the Government of India towards promoting the growth of the E-commerce and it was enacted with a view to provide legal recognition to e-commerce and e-transactions, to facilitate e-governance and prevent computer-based crimes. It is a first historical step. However, the rapid increase in the use of Internet has led to a spate in crime like child pornography, cyber terrorism, publishing sexually explicit content in electronic form and video voyeurism. The need for a comprehensive amendment was consistently felt and after sufficient debate and much deliberation, the I.T. Amendment Act 2008 was passed. The ITAA 2008 got the President's assent in February 2009 and was notified with effect from 27.10.2009. The new IT Amendment Act 2008 has brought a large number of cybercrimes under the ambit of the law. Some of the significant points in the Amendment Act include introduction of corporate responsibility for data protection with the concept of 'reasonable security practices' (Sec.43A), recognition of Computer Emergency Response Team – India (CERT-In) as the national nodal agency empowered to monitor and even block web-sites under specific circumstances, introduction of technological neutrality replacing digital signatures with electronic signatures etc. Besides, the CERT-In will also assist members of the Indian Community in implementing proactive measures to reduce the risks of computer security incidents.

The IT Act provides legal recognition for transactions carried out by means of electronic data interchange, and other means of electronic communication, commonly referred to as "electronic commerce", involving the use of alternatives to paper-based methods of communication and storage of information. The IT Act facilitates electronic filing of documents with the Government agencies.

3. LITERATURE REVIEW

Cyber-crime or computer crime is considered to be any crime that uses a computer and a computer network (Matthews, 2010). A basic definition describes cybercrime as a crime where computers have the possibility of playing an important part (Thomas and Loader, 2000). The main factor in cyber-crime increase is the Internet. By use of Internet, cybercriminals often appeal to images, codes or electronic communication in order to run malicious activities. Among the most important types of Internet crimes we can mention: identity theft, financial theft, espionage, pornography, or copyright infringement. The cyber-crimes can be divided into two categories: the crimes where a computer network attacks other computers networks – e.g. a code or a virus used to disable a system, and, the second category, crimes where a computer network attacks a target population – e.g. identity theft, fraud, intrusions (Svensson, 2011).

Issues revolving around cyber-crime have become more and more complex. Computer criminal activities have grown in importance and institutions are more interested than ever in putting an end to these attacks. Progressions have been made in the development of new malware software, which can easily detect criminal behavior (Balkin et al., 2007). Moreover, high quality anti-virus systems are offered for free now in many countries at every purchase of a computer or an operating system.

4. OBJECTIVE AND HYPOTHESIS OF STUDY

The growing danger from crimes committed against computers, or against information on computers, is beginning to claim attention in national capitals. This study investigates whether or not people would use the Internet to report crime. The pin pointed objectives of the study is to find out awareness among different respondents on the issue of Cyber Crime. H1: It has been assumed that there is no association between Respondents Occupation and the level of awareness.

5. METHODOLOGY

5.1 Research Strategy

Quantitative research in the form of a survey instrument has been used to collect the data and descriptive statistics have been used to analyze and present the data. The decision to follow a quantitative research methodology was based on the fact that the results of the survey should be a representative sample of the total population.

5.2 Research Questions

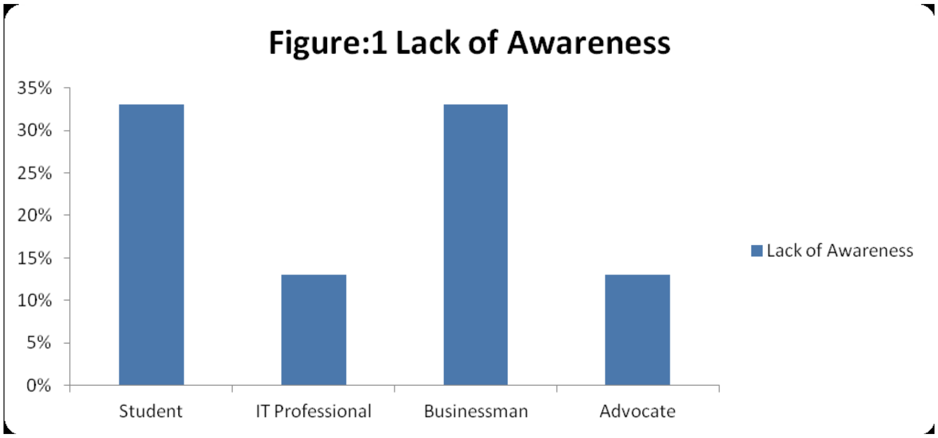
Due to the exploratory nature of the research, research questions were derived from the literature. These questions provided a basis for the research in order to find the awareness of cyber Crime among respondents. Also to find out what type of Cyber Crimes are occurring these days and what should be done to prevent Cyber Crime

5.3 Sample and Respondents

The primary target respondent was a working professional who was aware of the various computer crime and security issues within his/her organization. Typically, these were senior managers, IT administrators as well as any IT security consultants. Simple random sampling was the primary sampling method used when selecting the sample for this survey.

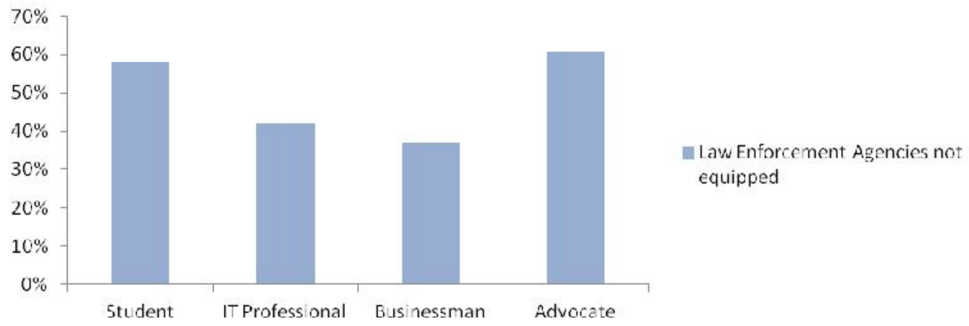
6. RESULT AND FINDINGS

In conducting the research, the author used SPSS 13.0 software program and take the hypothesis that there is no association between Respondents Occupation and the level of Cyber Crime Awareness.



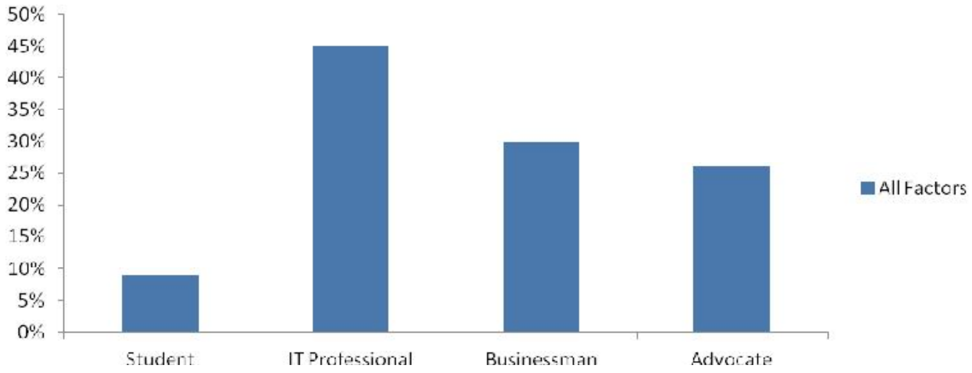
The Figure1 shows that, 33% Student, 13% IT Professional, 33% Businessman and 13% Advocate respondents think that major drawback, which prevent Cyber Crime from being solved in India, is Lack of awareness among people.

Figure:2 Law Enforcement Agencies not equipped



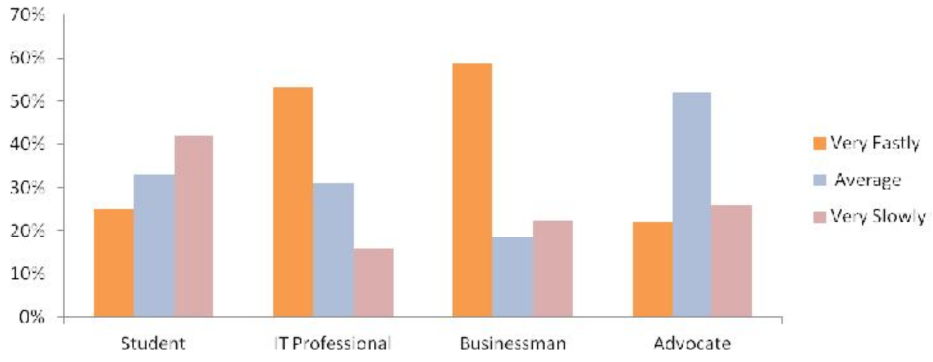
The Figure2 shows that, 58% student, 42% IT Professionals, 37% businessman and 61% advocates respondents are of view that Law enforcement agencies are not fully equipped

Figure 3: All Factors



The Figure 3 shows that, Rest 9% students, 45% IT Professional, 30% Businessman and 26% advocate respondents feels that all the factors are responsible which prevent cybercrime to be solved in India.

Figure:4 Spreading Cyber Crime



The Figure4 shows that, On the issue of spread of Disease Cyber Crime these days' 25% student, 53% IT Professional, 59% Businessman and 22% Advocates respondents feels that it is spreading very fastly and 33% student, 31% IT Professional,18.5% Businessman and 52% Advocates respondents said that it is spreading at average where as 42% student,16% IT Professional,22.5% Businessman and 26% Advocates believes that it is spreading very slowly

7. CONCLUSION-

Results revealed the importance of awareness as a tool to decrease/ prevent cybercrime. Therefore it is concluded that there is no association between the Respondents Occupation and Level of Awareness. This is due to the fact that it is a common misconception that leads to the underestimation of the threat that can be brought to the society. One of the most significant results is in relation to the possible reaction of the population to the threats of cybercrime. This is on the basis of the level of awareness of the members of the population on the issue of cybercrime. Some can dismiss the issue as unimportant due to the fact that the crime occurs in the virtual world that can be considered as unreal by some. This is due the fact that these individuals has less access to the cyber world and have no background information on the possible effects that can be incurred from the occurrence of cybercrime. There will always be new and unexpected challenges to stay ahead of cyber criminals and cyber terrorists but we can win only through partnership and collaboration of both individuals and government. There is much we can do to ensure a safe, secure and trustworthy computing environment. It is crucial not only to our national sense of well-being, but also to our national security and economy. It is not so easy and possible to eliminate cybercrime once for all in view of the latest scientific development. However, it is quite possible to combat and check the cybercrimes. To achieve that object, the first and foremost requirement is the awareness among the public about the cybercrimes and the precautions to prevent the same.

8. REFERENCES

1. Serban, C. (2011). Partnership in social marketing programs. Socially responsible companies and non-profit organizations engagement in solving society's problems. Amfiteatru Economic, XIII (29),pp. 104-116.
2. Svensson, P. (2011). Nasdaq hackers target service for corporate boards. Retrieved from http://news.yahoo.com/s/ap/20110205/ap_on_hi_te/us_nasdaq_hackers
3. Matthews, B. (2010). Computer Crimes: Cybercrime Information, Facts and Resources. Retrieved fromhttp://www.thefreeresource.com/computer-crimes-cybercrimeinformation-facts-and-resources
4. Balkin, J. M. et al. (2007). Cybercrime: digital cops in a networked environment. New York: New York University Press (NYU).
5. Thomas, D., and Loader, B. (2000). Cybercrime: law enforcement, security and surveillance in the information age. London: Routledge.