International Journal of Social Science and Economic Research

ISSN: 2455-8834

Volume:03, Issue:10 "October 2018"

CONSUMER VIGIL ON CYBER CRIME ISSUES AND CHALLENGES IN VILLUPURAM : A STUDY ON IMPACT LEVEL OF AWARENESS WITH SOCIAL MEDIA PARTICIPATION

Dr. R.RAMACHANDRAN

Assistant Professor, Department of Commerce, Annamalai University,
Annamalai Nagar – 608 002, Tamil Nadu, India

ABSTRACT

Cyber crime is not an old sort of crime to the world. It is defined as any criminal activity which takes place on or over the medium of computers or internet or other technology recognised by the Information Technology Act. Cyber crime is the most prevalent crime playing a devastating role in Modern India. Not only the criminals are causing enormous losses to the society and the government but are also able to conceal their identity to a great extent. There are number of illegal activities which are committed over the internet by technically skilled criminals. Taking a wider interpretation it can be said that, Cyber crime includes any illegal activity where computer or internet is either a tool or target or both. The present study aims to find out the consumer caution and vigil about cyber crime issues and challenges. A samples of 200 consumer selected randomly were studied. An interview schedule method of survey was used to find out the consumer awareness about cyber crime issues and challenges. Primary data were collected by using a structured interview scheduled and analysed with relevant interpretations. Anova, t-test, Correlation and regression analysis were applied to test the hypotheses. The findings and observations are the result and outcome of the analysis made during the research study.

Keywords: Cyber Crime, Vigil, Organization, Computer Technology, Demographic

INTRODUCTION

In today‘s world, an organization dependency on cyberspace is becoming an increasingly aspect of organizational security. The infrastructure of different organizations are interconnected in cyberspace, therefore the level of risk to security has increased dramatically. The threat to cyber security is growing at vast rate. Computer systems at colleges and Universities have become targets as they store same record as bank. The cyber crimes involve the use of computer, internet, cyberspace and the World Wide Web and give rise to the criminal activities. Cyber criminals are

ISSN: 2455-8834

Volume:03, Issue:10 "October 2018"

becoming more Sophisticated and are targeting consumers as well as public and private organizations. Cyber crimes are rises due to the lack of cyber security. All types of cyber crimes consist of both the computer and the person behind it as victims. Cyber crime could include anything such as downloading. Illegal music files to stealing millions of dollars from online bank accounts. Cyber crime could also creating and distributing small or large programs written by programmers called viruses on other computers or posting confidential business information on the Internet to harm the peoples. An important form of cyber crime is identity theft, in which criminals use the Internet to steal personal information from other users.

An example of one type of cyber crime is an *account takeover*. An incident occurred in 2012 at the South Carolina Department of Revenue that illustrates this cybercrime. Cybercriminals broke into the department‘s computer systems and stole 3.6 million Social Security numbers and 387,000 credit/debit card numbers this happens when cyber criminals compromise your computer and install malicious software, such as *key loggers*, which record key strokes, passwords, and other private information. This in turn allows them access to programs and web sites using your log-in credentials. Once these criminals steal your password, they may be able to breach your online bank account. These criminals can be anywhere in the world and may be able to transfer your money almost immediately.

The term cyber crime may be judicially interpreted in some judgments passed by courts in India, however it is not defined in any act or statute passed by the Indian Legislature. Cyber crime is an uncontrollable evil having its base in the misuse of growing dependence on computers in modern life. Usage of computer and other allied technology in daily life is growing rapidly and has become an urge which facilitates user convenience. It is a medium which is infinite and immeasurable. Whatsoever the good internet does to us, it has its dark sides too. Some of the newly emerged cybercrimes are cyber-stalking, cyber-terrorism, e-mail spoofing, e-mail bombing, cyber pornography, cyber-defamation etc. Some conventional crimes may also come under the category of cybercrimes if they are committed through the medium of computer or Internet.

During the period of 1950’s, it would be an astonished feeling for everyone who uses palmtops and microchips today, to know that the first successful computer was built and the size of the computer was so big that it takes the space of entire room and they were too expensive to operate. The functioning of these computer were not understandable to large number of people and only select people with expertise had direct access to such computers, and has the knowledge to operate them. For obvious reasons, the computer technology was extremely expensive and beyond the purchasing capacity of almost the entire population until IBM’s came into being wherein it introduced its stand-alone “personal computer” in 1981 and exposing many to the

ISSN: 2455-8834

Volume:03, Issue:10 "October 2018"

rewards of quick data access and manipulation that, up to that time, had been realized by few. The Personal computers become cheaper and become household item at the start of 21st century in India. The Internet was first started by the US department of defence, after World War II with the idea to have a network which could work in the event of disaster or war and securely transmit information. The First Network was known as ARPANET, with the development of Transmission Control Protocol/Internet Protocol, World Wide Web and Hypertext the internet become rage all over the world. With the growth of Internet the quality and variety of information grew. However at that point nobody anticipated the opportunities' the internet is going to provide the technology savvy criminals.

In India the internet services started by the state-owned Videsh Sanchar Nigam Limited in year 1995 and in 1998 the government has ended the monopoly of VSNL and market is opened to private operators. At that point, the internet users in India are 0.1% of total population, and now India has become the 2nd largest country in terms of internet users after china with 33.22% people using internet. The process of criminalization of human behaviour judged to be harmful the public is typically one that builds slowly in common law jurisdictions. Momentum gained through problem identification and pressures exerted mg special interest groups can easily span decades before undesirable actions are classified as "crime". In some instances, this process is accelerated through the occurrence of certain "catalyst events" that capture attention of the public and the attention of lawmakers.

The first recorded cyber crime took place in the year 1820. That is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since 3500 B.C. in India, Japan and China. The era of modem computers, however, began with the analytical engine of Charles Babbage. In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology. This is the first recorded cyber crime.

In the case of computer crime, legislators grew increasingly attentive is the 1980s as businesses became more dependent upon computerization and as catalyst event cases exposed significant vulnerabilities to computer crime violations. Criminals can now easily encrypt information representing evidence of their criminal acts, store the information and even transmit it with little fear of detection by law enforcement. Due to the extraordinary impact of the Internet, a computer crime scene can now span from the geographical point of the victimization (e.g., the victim's personal computer) to any other point on the planet, further complicating criminal investigative

ISSN: 2455-8834

Volume:03, Issue:10 "October 2018"

efforts. In effect, computer technology has dramatically altered the criminal justice terrain such that enterprising and opportunistic criminals have consciously turned to the computer to commit their illegal acts in situations in which the computer serves as the instrument of the crime, the means by which the crime is committed, as well as in cases in which the victim's computer, or computer system, is the target, or objective, of the act. And, as stated above, the presence of new computer technology aids cyber criminals in situations in which the computer's role is incidental to the crime; situations in which the computer is used to house and protect information that is evidence tying the offender to criminal acts. A commonality among these types of crimes is that the offender, to a great degree, depends upon the lack of technological skills of law enforcement to successfully commit the offenses and escape undetected. Based upon what empirical evidence has been available on self-assessed skills of investigators in this area, computer criminals would have good reason to feel some confidence in their chances to evade detection of their crimes.

As we advance towards the 21st century, it van be observed that the technological innovations have laid the way for the entire population using computer technology today, to experience new and wonderful conveniences in their daily life ranging from how to educated, shop, entertain, to availing the understanding of the business strategies and work flow. Our day to-day lives have been forever changed thanks to rapid advances made in the field of computer technology. These changes allow us to communicate over great distances in an instant and permit us, almost effortlessly, to gather and organize large amounts of information, tasks that could, otherwise, prove unwieldy and expensive. The technological treasures that have improved the quality of our lives, however, can reasonably be viewed as a doubled-edged sword. While computer technology has opened doors to enhanced conveniences for many, this same technology has also opened new doors for criminals.

Crime is a socially correlated phenomenon. No matter how much we try, we cannot experience a society without cybercrime. In actual sense, when we are not yet able to control the crime rate to the desirable minimum in the real world, how would it be possible to curb the same in the virtual world, as the same is comparatively more unreal, everlasting and legally less controllable. However with the time, nature and scope and definition of crime changes in a given society. Crimeless society is a myth and crime cannot be segregated from a society. Thus the nature of the crime depends upon the nature of a society.

Complexity of the society determines the complexity of the crime that evolves' around it. To understand the crime in a society, it is essential and crucial to verify all the factors which influence and contribute to the crime. The socio- economic and political structure of the society needs to understand the crime and the recourse that may curb the same. The preventive and

ISSN: 2455-8834

Volume:03, Issue:10 "October 2018"

corrective measures adopted by the machinery to control the crime and delinquent behaviour in the society are also taken into consideration while studying the nature and scope of a crime.

The advancement of the technology has produced new socio-economic and political problem in the society and instead of helping the state in controlling the problem it has created new complex situation which is difficult to understand and even more difficult to apply current law to face the situation. The state machinery is not equipped with enough sources and knowledge to handle the modern crime. Computers have transformed the modern society beyond expectations in last three to four decades. It has made life not only convenient but has also immensely helped different sections of the world come closer socially, economically and culturally. The Computer technology has made it possible to have access to all corners of the world while sitting in a room. Modern technology has put an end to the barriers of time and space. However, unlikely with the remarkable merits of having computers today, due to this the jurisdictional issue has been created in legal system.

Jurisdiction is one aspect which is very difficult to determine in transnational transaction over the internet. There was unmanageable ambiguity when courts were subjected to questions pertaining to jurisdiction law and were unable to decide the proper forum to entertain cases involving cyber crime as the cyberspace or virtual world is borderless if we compare it with physical world and that is why it is very difficult to control cybercrime. Through the local machinery we are not able to tackle the problem related with cyber crime because our machinery is not compatible to deal with transnational crimes. The law applicable to the territory is not advanced enough to regulate the cyber crime as their nature is far different from the existing crime.

Thus, the global dimension of cyber crime is made it difficult to handle and dealt with. The evolution of internet technology has given us so many advantages to deal with future problems and grow with rapid rate but also it has provided the scope for criminals to commit their crime with least chance of detection. The cyberspace has proved a boon to the deviant behaviour in the society. The concept of cyber crime has gained speed and we are facing great threat of its impact on world society. The human society is become vulnerable to cyber crime due to more and more dependence on technology. Cyber crime becomes a global phenomenon and hence the nationwide generalization of crime cannot workable in present scenario. Our understanding and regulation of cyber crime cannot be national but has to be international. It is necessary to enact new laws and prepare preventive and defensive mechanism globally, only then we can able to protect our society from this evil called ‘Cyber Crime’. Therefore, the threat of cyber terrorism throws serious challenge to world and its agencies. The terrorist organizations using technology to spread hatred among people and using it to recruit militants and train them using teaching tools. They are also launching websites which show them how to use weapons make bombs.

ISSN: 2455-8834

Volume:03, Issue:10 "October 2018"

RELATED REVIEW OF STUDIES

The responsibility of social scientist is to derive new outcome from the nature, concept and developed outcomes. Hence, every research work is in position to undergo to find out the research gap and hence following reviews are collected. Hemraj Saini and Yerra Shankar Rao (2012), "Cyber-Crimes and their Impacts: A Review", In the current era of online processing, maximum of the information is online and prone to cyber threats. There are a huge number of cyber threats and their behavior is difficult to early understanding hence difficult to restrict in the early phases of the cyber attacks. Cyber attacks may have some motivation behind it or may be processed unknowingly. The attacks those are processed knowingly can be considered as the cyber crime and they have serious impacts over the society in the form of economical disrupt, psychological disorder, threat to National defense etc. Restriction of cyber crimes is dependent on proper analysis of their behavior and understanding of their impacts over various levels of society. Therefore, the current manuscript provides the understanding of cyber crimes and their impacts over society with the future trends of cyber crimes.

T.C. Panda (2012), This manuscript put its eye not only on the understanding of the cyber crimes but also explains the impacts over the different levels of the society. This will help to the community to secure all the online information critical organizations which are not safe due to such cyber crimes. The understanding of the behavior of cyber criminals and impacts of cyber crimes on society will help to find out the sufficient means to overcome the situation. The way to overcome these crimes can broadly be classified into three categories: Cyber Laws (referred as Cyber laws), Education and Policy making. All the above ways to handle cyber crimes either are having very less significant work or having nothing in many of the countries. This lack of work requires to improve the existing work or to set new paradigms for controlling the cyber attacks.

Pooja Aggarwal, Piyush Arora and Neha (2014), "Review on Cyber Crime and Security", The evolution of Information Technology gave birth to the cyber space where in internet provides equal opportunities all the people to access any information. Due to increase in the number of netizens, misuse of technology is increasing which leads to cyber crimes. The cyber crimes are basically undertook by people in the age group from 13 to 25 years who all are well educated. Cyber crime refers to the unlawful acts where in the computer is either a tool or target or both. Cyber Security refers to mechanism by which computer –based equipments, information and services are protected from illegal and unauthorized access. The rules and regulations which are governing cyber space is known as Cyber Law which comprises of Information Technology Act 2000. There are cyber crime cells in every state to handle the cyber crime cases and to punish the netizens committing cyber crime. Cyber technology changes have been so rapid that there are laws which has some set of rules and guidelines that make the cyber activities legalized.

ISSN: 2455-8834

Volume:03, Issue:10 "October 2018"

Poonam (2014), In today's modern era, the computer system and internet are increasing worldwide, thus making it easy for the cyber criminals to access any information by using their expertise. Cyber crime is defined as the unlawful acts where in the computer are either a tool or target or both. Cyber crime is a menace that has to be tackled effectively. The need is to create awareness among the people about the cyber space, various forms of cyber crimes and preventive measures. It is rightly said, "Prevention is better than cure", thus it is advised to take precautions while operating on the internet. The internet users must adopt 5P mantra for their security, which is Precaution, Prevention, Protection, Preservation, Perseverance. The IT Act is an articulation of all existing laws with "e" added to most of the provisions. Cyber Law knowledge must be known among the people working on the computer systems, computer networks and information communication technology.

Alpna (2016), "Cyber Crime-Its Types, Analysis and Prevention Techniques", The user of computer system and internet are increasing worldwide in large number day by day, where it is easy to access any information easily within a few seconds by using internet which is the medium for huge information and a base of communications around the world .There has been tremendous growth in use of Internet. Due to this cyber crimes increases day by day. Cyber Crime is technology based crime committed by technocrats. This paper deals with Variants of cyber crime like terrorist attack, cyber extortion, crimes against individuals, crimes against property, and crimes against organization. It also includes impact on the real world and society, and how to handle cyber crimes.

Sona Malhotra (2016), Computer crime does have a drastic effect on the world in which we live. It affects every person no matter where they are from. This paper discussed different type's cyber attacks. Cyber attack techniques have been improved dramatically over time, especially in the past few years. Criminals have also adapted the advancements of computer technology to further their own illegal activities. Certain precautionary measures should be taken by all of us while using the internet which will assist in challenging this major threat Cyber Crime. There is a need to conduct research analysis of cyber crimes to find out a best approach to protect sensitive data and take appropriate action against the cyber attack.

Literature review is the basic phenomenon of in social science research and it pave way for to find out the Consumer Awareness about Cyber Crime Issues and Challenges in Villupuram. However, it is interesting to note that many research studies purports to different dimensions, exclusively in Cyber Crime Issues and Challenges. But this research paper concentrates on assessing the Cyber Crime Issues in prime impact factors in relation towards Consumer Awareness as an indicator for performance mechanism. Thus, this study realizes to new path for

ISSN: 2455-8834

Volume:03, Issue:10 "October 2018"

these parameters. And hence necessary primary and secondary data are collected over to emphasis the prominence and performance of its position in organization spectrum.

OBJECTIVES OF THE STUDY

The objectives of the study are:

- To analyses the Consumer, the significant causing factors and challenges over on demographic issues.
- To emphasis on the power of consumer on vigil and awareness on cyber crimes in the study area.

METHODOLOGY

The research study is basically empirical climate in nature. The main study was conducted on 200 consumers in Villupuram. Primary data, required for the present research work were collected by conducting direct interviews using questionnaire. It is planned to get the descriptive statistics and provided data and formulation of more refined studies. The universe of the present study is the consumers in the study area. The researcher has selected simple random sampling technique as a sample method for the study. The researcher used questionnaire for the purpose of data collection. The researcher issued the questionnaire to the respondents and got the response from them. The data collection was completed by July 2018. The collected data were analyzed later. The data collected by the researcher were edited and coded. Along with the data collected from interview schedule, researcher collected data through observation also. Through observation the consumers of the people was easily realized. It enhances the research to determine the respondents significant role causing factors and challenging over by demographic mechanisms. Thereby it enables to conduct analysis and interpretation with tools of analysis.

RESULTS AND DISCUSSION

This paper furnishes the analyses and interpretation of the collected data for **"Consumer Vigil on Cyber Crime Issues and Challenges in Villupuram : A Study on Impact Level of Awareness with Social Media Participation".** Necessary data are collected and tabulated for bringing out suitable analysis and conclusion.

ISSN: 2455-8834

Volume:03, Issue:10 "October 2018"

Table 1: F/t-ratio for Consumer Vigil on Cyber Crime Issues and Challenges on the basis of their age

(N=100)

Demographic Variables	Sub Samples	N	Mean	SD	F/t-value	Level of Significance
Age	Below 25 years	45	20.97	2.10	8.51	0.01
	26 to 35 years	35	21.89	1.90		
	Above 35 years	20	16.22	2.11		
Sex	Male	74	23.00	2.32	3.53	0.01
	Female	26	19.59	4.43		
Marital status	Married	39	13.81	4.29	8.72	0.01
	Unmarried	61	20.33	3.16		
Income	Low	62	26.19	4.38	3.60	0.05
	Middle	26	27.56	5.50		
	High	12	30.44	3.53		
Family type	Joint	42	17.62	2.87	4.19	0.01
	Nuclear	58	20.40	1.40		

Source : Field survey

Table 1 shows the Mean, SD and F-value of Consumer Vigil on Cyber Crime Issues and Challenges on the basis of their age. The calculated F-value (8.51) is statistically significant at 0.01 level. Therefore, result infer that the age groups influence the Consumer Vigil on Cyber Crime Issues and Challenges.

The Mean, SD and t-value of Consumer Vigil on Cyber Crime Issues and Challenges on the basis of their sex. The calculated t-value (3.53) is statistically significant at 0.01 level. Therefore, result infer that the sex groups influence the Consumer Vigil on Cyber Crime Issues and Challenges.

The Mean, SD and t-value of Consumer Vigil on Cyber Crime Issues and Challenges on the basis of their marital status. The calculated t-value (8.72) is statistically significant at 0.01 level. Therefore, result infer that the marital status groups influence the Consumer Vigil on Cyber Crime Issues and Challenges.

The Mean, SD and F-value of Consumer Vigil on Cyber Crime Issues and Challenges on the basis of their Income. The calculated F-value (3.60) is statistically significant at 0.01 level. Therefore, result infer that the income groups influence the Consumer Vigil on Cyber Crime Issues and Challenges.

ISSN: 2455-8834

Volume:03, Issue:10 "October 2018"

The Mean, SD and t-value of Consumer Vigil on Cyber Crime Issues and Challenges on the basis of their family type. The calculated t-value (4.19) is statistically significant at 0.01 level. Therefore, result infer that the family type groups influence the Consumer Vigil on Cyber Crime Issues and Challenges.

Table 2: Correlation between the awareness, Issues and challenges, Impact of social media and demographic variables

Demographic variables	Awareness about Cyber crime	Issues and challenges of cyber crime	Impact of social media
Age	0.320*	0.212**	0.327*
Sex	0.135*	0.142*	0.139*
Marital status	-0.329*	0.117*	0.019
Income	-0.240**	0.122*	0.014
Family type	0.230*	0.080	0.242*

Source : Field Survey

* Significant at 0.01 level ** Significant at 0.05 level

Awareness about cyber crime is positively and significantly related to age (0.320), sex (0.135), marital status (0.329), income (0.240) and family type (0.230). So there is a positive relationship between Awareness about cyber crime and demographic variables. Issues and challenges of cyber crime is positively and significantly related to age (0.212), sex (0.142), marital status (0.117) and income (0.122). So there is a positive relationship between Issues and challenges of cyber crime and demographic variables. Impact of social media is positively and significantly related to age (0.327), sex (0.139) and family type (0.242). So there is a positive relationship between Impact of social media and demographic variables.

Table 3: Stepwise regression analysis predicting awareness about cyber crime

Sl.No	Step/Source	Cumulative R^2	ΔR^2	Step t	P
1.	Age	0.042	0.039*	3.079	0.01
2.	Sex	0.053	0.050*	2.625	0.01
3.	Marital status	0.070	0.062*	2.014	0.01
4.	Income	0.081	0.070*	2.405	0.01
5.	Family type	0.103	0.084*	2.342	0.01

Source : Field Survey * P < 0.01

Constant value = 16.692

ISSN: 2455-8834

Volume:03, Issue:10 "October 2018"

Five variables namely age, sex, marital status, income and family type have significantly contributed for predicting the awareness about cyber crime. The variable age predictive value of awareness about cyber crime seems to be 0.042, when paired with the variable sex it is 0.053, with marital status 0.070, with income 0.081 and with family type 0.103. The predictive value of these variables separately is 0.01.

Table 4: Stepwise regression analysis predicting issues and challenges of cyber crime

Sl.No	Step/Source	Cumulative R^2	ΔR^2	Step t	P
1.	Marital status	0.027	0.018*	2.792	0.01
2.	Income	0.036	0.030*	2.342	0.01
3.	Family type	0.042	0.024*	2.634	0.01

Source : Field Survey * P < 0.01

Constant value = 21.614

Three variables namely marital status, income and family type have significantly contributed for predicting the issues and challenges of cyber crime. The variable marital status predictive value of issues and challenges of cyber crime seems to be 0.027, when paired with the variable income it is 0.036 and with family type 0.042. The predictive value of these variables separately is 0.01.

Table 5: Correlation between the organizational climate and social media

Related Variable	Social media
Awareness about cyber crime	0.345*

Source: Field Survey * Significant at 0.01 level

Awareness about cyber crime is significantly positive relationship with social media (0.345). So there is a positive relationship between Awareness about cyber crime and social media.

IMPLICATIONS AND CONCLUSION

In today's modern era, the computer system and internet are increasing worldwide, thus making it easy for the cyber criminals to access any information by using their expertise. Cyber crime is defined as the unlawful acts where in the computer are either a tool or target or both. Cyber crime is a menace that has to be tackled effectively. The need is to create awareness among the people about the cyber space, various forms of cyber crimes and preventive measures. It is rightly said, “Prevention is better than cure”, thus it is advised to take precautions while operating on the internet. The internet users must adopt 5P mantra for their security, which is Precaution, Prevention, Protection, Preservation, Perseverance. The IT Act is an articulation of

ISSN: 2455-8834

Volume:03, Issue:10 "October 2018"

all existing laws with “e” added to most of the provisions. Cyber Law knowledge must be known among the people working on the computer systems, computer networks and information communication technology. In this perspective, it is indentified that there is relevant gap on research to conduct on this issue and hence, Villupuram a vital place on transit on all regards over for good performance in determination of quality in benchmarking for all functionary factors in the place of e-business applications and taken as study base. From the data analysis and interpretation, the result concluded that the demographic groups influence the Consumer Vigil on Cyber Crime Issues and Challenges. There is a positive relationship between Awareness about cyber crime and demographic variables. There is a positive relationship between Issues and challenges of cyber crime and demographic variables. There is a positive relationship between Impact of social media and demographic variables. Five variables namely age, sex, marital status, income and family type have significantly contributed for predicting the awareness about cyber crime. Three variables namely marital status, income and family type have significantly contributed for predicting the issues and challenges of cyber crime. There is a positive relationship between Awareness about cyber crime and social media. Therefore to conclude that social media and demographic issues are making significant impact on cyber crime awareness and challenges over to be successful in their business decisions.

REFERENCES

Aghatise E. J. (2006): Level of Awareness of Internet Intermediaries Liability. (HND Project work) Unpublished. Auchi Polytechnic, Auchi, Edo State, Nigeria.

Alpna (2016), “Cyber Crime-Its Types, Analysis and Prevention Techniques”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 5, May 2016 ISSN: 2277 128X

Angel cruz,chief information security officer state of Texas, cyber security tips, monthly newsletter 2013,volume

Atul Kum ar, Sr. Analyst, Chiranshu Ahuja, Sr. Analyst, *Cyber Security Research Developments Global and Indian Context,* A NASSCOM® Initiative

Atul M. Tonge1, Suraj S. Kasture2, Surbhi R. Chaudhari3 IOSR Journal of Computer Engineering (IOSR-JCE) CSE, *Cyber security*: *challenges for society*, ISSN: 2278-0661, p- ISSN: 2278-8727Volume 12, Issue 2 (May. - Jun. 2013).

Baskerville, R., 1991, Risk Analysis: An Interpretive Feasibility Tool in Justifying Information Systems Security, European Journal of Information Systems, 1(2): 121-130.

ISSN: 2455-8834

Volume:03, Issue:10 "October 2018"

Berinato, S. (2002), Enron IT: A take of Excess and Chaos, CIO.com, March 5 http://www.cio.com/executive/edit/030502_enron.html, Visited: 28/01/2012

Bowen, Mace (2009), Computer Crime, Available at: http://www.guru.net/, Visited: 28/01/2012. By Jessica Stanicon (2009), Available at: http://www.dynamicbusiness.com/articles/articles-news/one-in-five-victims-of-cybercrime3907.html, Visited: 28/01/2012.

CAPEC (2010), CAPEC-117: Data Interception Attacks, Available at: http://capec.mitre.org/data/definitions/117.html, Visited: 28/01/2012.

Computer Hope (2012), Data Theft, Available at: http://www.computerhope.com/jargon/d/datathef.htm, Visited: 28/01/2012.

Crime Desk (2009), Million Online Crimes in the Year: Cyber Crime Squad Established, Available at: http://www.thelondondailynews.com/million-online-crimes-year-cyber-crime-squad-established-p-3117.html, Visited: 28/01/2012.

Cyber Trust and Crime Prevention, Mid-Term Review, November 2005 – January 2009, Available at: http://www.bis.gov.uk/assets/bispartners/foresight/docs/cyber/ctcp_midterm_ review.pdf, Visited: 28/01/2012

Cyberlawtimes (2009), Available at: http://www.cyberlawtimes.com/forums/index.php?board=52.0, Visited: 10/31/09

D. Ariz. (April 19, 2000), American Guarantee & Liability Insurance Co. v. Ingram Micro, Inc. Civ. 99-185 TUC ACM, 2000 U.S. Dist. Lexis 7299.

D'Amico, A., 2000, What Does a Computer Security Breach Really Cost?, The Sans Institute

DSL Reports (2011), Network Sabotage, Available at: http://www.dslreports.com/forum/r26182468-Network-Sabotage-or-incompetent-managers-trying-to-, Visited: 28/01/2012. en.wikipedia.org/wiki/Cyber_security_standards

Er. Harpreet Singh Dalla, Ms. Geeta HOD, Department of CSE & IT Patiala Institute of Engineering & Technology for Women, Patiala, *India*, *Cyber Crime – A Threat to Persons*, *Property*, Government and Societies, Volume 3, Issue 5, May 2013 ISSN: 2277 128X

ISSN: 2455-8834

Volume:03, Issue:10 "October 2018"

Forensic technology services cybercrime survey report 2014 kpmg.com/in

Gordon, L. A. et al., 2003, A Framework for Using Insurance for Cyber-Risk Management, Communications of the ACM, 46(3): 81-85.

Hancock, B., 2002, Security Crisis Management—The Basics, Computers & Security, 21(5): 397-401.

Harish Chander 2012, "Cyber Laws and IT Protection", PHI Learning

Hemraj Saini and Yerra Shankar Rao (2012), "Cyber-Crimes and their Impacts: A Review", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 2, Mar-Apr, pp.202-209.

Hemraj Saini and Yerra Shankar Rao (2012), "Cyber-Crimes and their Impacts: A Review", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 2, Mar-Apr, pp.202-209.

Hoffer, J. A., and D. W. Straub, 1989, The 9 to 5 Underground: Are You Policing Computer Crimes?, Sloan Management Review (Summer 1989): 35-43

IMDb (2012), Unauthorized Attacks, Available at: http://www.imdb.com/title/tt0373414/, Visited: 28/01/2012

India emerging as major cyber crime centre (2009), Available at: http://wegathernews.com/ 203/india-emerging-as-major-cyber-crime-centre/, Visited: 10/31/09

Jamal Raiyn, *A survey of Cyber Attack Detection Strategies*, International Journal of Security and Its Applications Vol.8, No.1 (2014).

Janhavi J Deshmukh and Surbhi R Chaudhari, *Cyber crime in Indian scenario – a literature snapshot*, International Journal of Conceptions on Computing and Information Technology Vol.2, Issue 2, April' 2014; ISSN: 2345 – 9808.

Kelly, B. J., 1999, Preserve, Protect, and Defend, Journal of Business Strategy, 20(5): 22-26.

Kevin G. Coleman (2011), Cyber Intelligence: The Huge Economic Impact of Cyber Crime, Available at: http://gov.aol.com/2011/09/19/cyber-intelligence-the-huge-economic-impact-of-cyber-crime/, Visited: 28/01/2012

ISSN: 2455-8834

Volume:03, Issue:10 "October 2018"

Leagal Info (2009), Crime Overview Aiding And Abetting Or Accessory, Available at: http://www.legalinfo.com/content/criminal-law/crime-overview-aiding-and-abetting-or-accessory. html, Visited: 28/01/2012

Longe, O.B. (2004): Proprietary Software Protection and Copyright issues in contemporary Information Technology. (M.Sc Thesis) Unpublished. Federal University of Technology, Akure, Nigeria.

Lyman, J., 2002, In Search of the World‘s Costliest Computer Virus, http://www. newsfactor.com/perl/story/16407.html. 2002.

Newswise (2009), China Linked to 70 Percent of World's Spam, Says Computer Forensics Expert, Available at: http://www.newswise.com/articles/view/553655/, Visited: 28/01/2012.

Nigel Jones, Director or the Cyber Security Knowledge Transfer Network, was featured in the daily telegraph (May 6, 2008), Cyber Security KTN,

Nilkund Aseef, Pamela Davis, Manish Mittal, Khaled Sedky, Ahmed Tolba (2005), Cyber-Criminal Activity and Analysis,White Paper, Group 2.

Oracle (2003), Security Overviews, Available at: http://docs.oracle.com/cd/B13789_01/ network.101/ b10777/overview.htm, Visited: 28/01/2012.

Panda T.C. (2012), “Cyber-Crimes and their Impacts”, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 2, Mar-Apr, pp.202-209.

Pooja Aggarwal, Piyush Arora and Neha (2014), “Review on Cyber Crime and Security”, *International Journal of Research in Engineering and Applied Sciences (IJREAS), ISSN : 2249-9210, © IJREAS, Vol. 02, Issue 01, Jan.*

Poonam (2014), “Review on Cyber Crime and Security”, *International Journal of Research in Engineering and Applied Sciences (IJREAS), ISSN : 2249-9210, © IJREAS, Vol. 02, Issue 01, Jan 2014*

Power, R., 2001, 2001 CSI/FBI Computer Crime and Security Survey, Computer Security Issues and Trends, 7(1): 1-18.

ISSN: 2455-8834

Volume:03, Issue:10 "October 2018"

Prasun Sonwalkar (2009), India emerging as centre for cybercrime: UK study, Available at: http://www.livemint.com/2009/08/20000730/India-emerging-as-centre-for-c.html, Visited: 10/31/09

PTI Contents (2009), India: A major hub for cybercrime, Available at: http://business.rediff.com/ slide-show/2009/aug/20/slide-show-1-india-major-hub-for-cybercrime.htm, Visited: 28/01/2012.

Ryder D. Rodney 2007, "Guide to Cyber Laws", Nagpur Wadhawa and Company.

S. Sai Sushanth, "Cyber Law: Various Aspects of Cyber Legal System", Cyber Times International Journal of Technology and Management.

Seema Vijay Rane & Pankaj Anil Choudhary, April 2012-September 2012, "Cyber Crime and Cyber Law in India", Cyber Times International Journal of Technology and Management, Vol. 5 Issue 2

Shantosh Rout (2008), Network Interferences, Available at: http://www.santoshraut.com/ forensic/ cybercrime.htm, Visited: 28/01/2012

Sheri R.K. & Chhabru S.T.N 2002, "Cyber Crime", New Delhi, Pentagon Press

Smith, R. G., Holmes, M. N. & Kaufmann, P. (1999): Nigerian Advance Fee Fraud., Trends and Issues in Crime and Criminal Justice, No. 121, Australian Institute of Criminology, Canberra (republished in The Reformer February 2000, pp. 17-19).

Sona Malhotra (2016), "Cyber Crime-Its Types, Analysis and Prevention Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 5, May 2016 ISSN: 2277 128X.

Sprecher, R., and M. Pertl, 1988, Intra-Industry Effects of the MGM Grand Fire, Quarterly Journal of Business and Economics, 27: 96-16.

Stephen Northcutt et al. (2011), Security Predictions 2012 & 2013 - The Emerging Security Threat, Available at: http://www.sans.edu/research/security-laboratory/article/security-predict 2011, Visited: 29/01/2012.

Sumanjit Das and Tapaswini Nayak, *"impact of cyber crime: issues and challenges*‖, International Journal of Engineering Sciences & Emerging Technologies, October 2013. ISSN: 22316604 Volume 6, Issue 2, pp: 142-153 ©IJESET.

ISSN: 2455-8834

Volume:03, Issue:10 "October 2018"

Sylvester, Linn (2001): The Importance of Victimology in Criminal Profiling. Available online at: http://isuisse.ifrance.com/emmaf/base/impvic.html

Vineet Kandpal and **R. K. Singh, *Latest Face of Cybercrime and Its Prevention In India*, International Journal of Basic and Applied Sciences Vol. 2. No. 4. 2013

Virus Glossary (2006), Virus Dissemination, Available at: http://www.virtualpune.com/citizen-centre/html/cyber_crime_glossary.shtml, Visited: 28/01/2012

Wow Essay (2009), Top Lycos Networks, Available at: http://www.wowessays.com/ dbase/ab2/ nyr90.shtml, Visited: 28/01/2012.

