Cybercrime: An Empirical Study of its Impact in the Society- A Case Study of Tanzania

J.A. Mshana
Assistant Lecturer,
Institute of Judicial Administration Lushoto,
Box 20 Lushoto
E-mail: jumamshana@gmail.com; jamshana@ija.ac.tz

Abstract: *The aim of the research is to examine the negative impact cybercrimes pose to the society. The concepts of cybercrimes are introduced and different types of cybercrimes are explored as examples of some of the impacts which caused by cybercrimes activities. Results from this study show that, there are many negative impacts which the society suffer from the cybercrimes and why the computer or networking are tools target for the crimes. The discussions are made from the findings and finally the paper addresses different measures which can be taken to combat these cybercrimes so that people still enjoy using the technology rather than stop them to use it.*

Keywords: Child Exploitation, Cybercrime, Computer Crime, Identity Theft, Stalking

INTRODUCTION

It is obvious that the ICT meets a variety of educational, entertainment, communications, commerce needs, and other areas just few to mention, for its users. õWith these benefits, though, this same technology has also ushered in a new wave of criminal activity called cybercrimeô (Saban, McGivern and Saykiewicz, 2002) defined as ócany illegal act fostered or facilitated by a computer, whether the computer is an object of a crime, an instrument used to commit a crime, or a repository of evidence related to a crimeô (Royal Canadian Mounted Police, 2000, in Hinduja and Schafer 2009) Cybercrimes are those crimes which are committed in the online or electronic environment.

As the Internet came into widespread commercial use, the nature of computer crimes began to shift. õWhile in some crimes, one component of the crime may have been committed using an electronic instrument, in other crimes, the crime as a whole is committed in the online or electronic environment. These crimes, known as cybercrimes, generally occur in the virtual community of the Internet or in cyberspaceô (Heather 2008, Newton 2008).

Viruses, worms, and Trojan horses are another serious threat. There is a variety of Cyber crime committed but these are the most prevalent and appear to be among the most troubling to computer users (Furnell, 2002 in Brett, 2008).

As it has been seen in the introductory part, there is no way any organization or country can avoid the uses of ICT since it needs to remain competitive in the

marketplace, but the biggest issue is how to deal with cybercrimes so as to minimize if not to reduce its threats. Therefore, the paper intends to explore the impact of cybercrimes in the society and the security measures which can be taken to prevent these threats.

DIFFERENT TYPES OF CYBERCRIMES

There are several ways we can categorize the various cybercrimes. We can divide them into two very broad categories: one, those crimes committed by violent or potentially violent criminals, and two, nonviolent crimes. Types of violent or potentially violent cybercrime include: Cyber terrorism; Assault by threat; Cyber stalking and child pornography (Chawki, 2005).

Cybercrimes include three main offending patterns (Wall, 2008). The focus of the offending can either be the integrity of the system (hacking) or the computer can be used to commit an offence, else the content of the computer itself can be the object of the offending.

Child exploitation: In 2005, the Virtual Global Task Force defined child sexual abuse online as the sharing and downloading of images of children being physically and sexually abused and approaching children online with the aim of developing a sexual relationship in the ôreal worldô, also known as ôgroomingô (Martellozzo, E., Nehring, D. and Taylor, H. 2010) .Child exploitation is not an invention of the Internet age by any means. However, the Internet has become the new playground for consumers of child pornography and a market place for those who provide it.

Harassment: The term is normally used to refer to the use of the Internet, e-mail, or other electronic communications devices to harass another person (Black and Kenneth, 2010).

Digital Piracy: The development of the personal computer has led to widespread use of the Internet, which allows for an exchange of information and the production of behaviours that include crime. One form of crime on the Internet is digital piracy. Gunter, Higgins and Gealt (2010) defined digital piracy as the act of copying digital goods that include software, documents, audio (including music and voice), and video for any reason other than to back up without explicit permission from and compensation to the copyright holder using computer technology.

Hacking: Unauthorized access may occur both on individualsô personal computers, as well as in the workplace. óOne major form of unauthorized access is known as hacking. Hacking is the act of gaining unauthorized access to a computer system or network and in some cases making unauthorized use of this accessô (Rushinek and Rushinek, 1993 in Kunz and Patrick, 2004).

Intentional Damage: The enterpriseôs communications networks can be harmed through zapping, the process of damaging or erasing data and information, causing problems for both the enterprise and the customer (Wienclaw, 2008).

Spam: Email spam could be one of the most prevalent crimes in the sense that almost every email user probably has received at least a few unsolicited commercial

emails at some point of time. Kunz and Patrick (2004) defined Spam mail as the distribution of bulk e-mail that offers recipients deals on products or services.

APPLICATION OF THE CYBER CRIMES THEORY

Based on the child exploitation as one among cyber crimes, the Routine Activity Theory (RAT) is applied to this study. The theory focused on environmental ñopportunities for crimeò. Essentially, when a potential criminal opportunity arises the act will occur at a juncture in time and space between a motivated offender and a suitable target for victimization. This crime will ultimately take place in a location that lacks a capable guardian to protect the ósuitable target,ô which is considered to be either a vulnerable person or oneôs unguarded property.

Thus, the absence of any one of these three situational factors should theoretically make the commission of a crime impossible (Davis, 2002 in Collins, Sainato & Khey 2011). As a result, routine activity theory is considered to be a macro-level theory applicable to numerous types of crime as it seeks to explain the criminal victimization process and not a criminalôs specific motivations (Akers & Sellers, 2009 in Collins, Sainato & Khey 2011).

The theory predicts that crime occurs when a motivated offender comes into contact with a suitable target in the absence of a capable guardian that could potentially prevent the offender from committing crime. Ngo and Paternoster (2011) said that, the theory posits that variations in crime rates could be explained by the supply of suitable targets and capable guardians, and from our understanding the theory is somewhat agnostic about the role of the supply of motivated offenders.

RESEARCH METHOD

The survey research method is used because bias was less likely as subjects were randomly assigned to treatments, and subjects and researchers were blind to the identity of the treatments. Questionnaire and interview were used for data collection. Researcher developed questionnaire on the basis of literature and related researches.

Surveys were used to gather information from the two educational institutions to represents youths, 15 musicians, 10 actors and 5 companies to explore different types of cybercrimes and their impacts. Data obtained from 100 students from each educational institution, 5 members of management from each company to make a total of 250 as sample size of the study. Out of 250 people 200 responded which is 80%. The survey respondents were small but informative and accurate because the instrument was reviewed before.

PROCEDURE

The researcher collected the data from the respondents through email and direct from the interview after the distribution of questionnaires to the five educational institutions and scoring was done after the collection of data. Five point rating scale was used to record score of all positive statements ranged from 5-1 for different response categories. Strongly agree (SA), Agree (A), Undecided (U), Disagree (DA) and Strongly Disagree (SDA). The data was analyzed in terms of percentage.

FINDINGS

The findings drawn out from the data analysis are as under:

Table 1: What are the impacts of cybercrime on the society?

S/N	Impacts	Response	Level of Agreement				
			SA	A	U	DA	SDA
1.	Child exploitation	N	120	70	0	10	0
		%	(60)	(35)	(0)	(5)	(0)
2.	Harassment	N	100	80	10	0	10
		%	(50)	(40)	(5)	(0)	(5)
3.	Digital Piracy	N	70	120	10	0	0
		%	(35)	(60)	(5)	(0)	(0)
4.	Hacking	N	80	80	10	20	10
		%	(40)	(40)	(5)	(10)	(5)
5.	Intentional damage	N	60	80	40	10	10
		%	(30)	(40)	(20)	(5)	(5)
6.	Spam	N	110	60	10	20	0
		%	(55)	(30)	(5)	(10)	(0)

Results of **Table 1** indicate that majority of respondents (95%) pointed out that cybercrimes affects children through pornography (child exploitation) while few (5%) respondents disagree with this opinion. A significant majority (90%) of respondents said that cybercrimes cause also harassment to the society. This is where a person can use either computer or mobile phone to abuse other people through short message text or social network like facebook. Also few respondents (5%) negated this effect to the society and the remaining (5%) were not aware on the crime.

Digital piracy is another impact caused by the cybercrimes on the society, the results show that majority (95%) of respondents responded positively to this while the remaining percentage (5%) of respondents were not sure.

Similarly, a sufficient number of respondents (80%) supported that hackers are the threat to the society which caused by cybercrimes. Most of respondents have been affected themselves or their fellows. Intentional damage was also declared by 70% that is one among the impacts of cybercrimes on the society. Similarly, a sufficient number of respondents (85%) supported that other effect of cybercrimes is spam electronic mail and only 10% negated the impact.

Table 2: Why computers or network are tools target or place for cybercrimes?

S/N	Reasons	Response	Level of Agreement				
			SA	A	U	DA	SDA
1.	Availability	N	100	80	10	10	0
		%	(50)	(40)	(5)	(5)	(0)
2.	Easy access	N	70	100	10	10	10
		%	(35)	(50)	(5)	(5)	(5)
3.	Affordable	N	60	100	20	10	10
		%	(30)	(50)	(10)	(5)	(5)

The researcher again wanted to explore out why the computer or network are tools target for cybercrimes. Results of **Table 2** indicates that 90% of respondents said it is because computers are available nowadays everywhere.

A significant respondents (85%) responded that it is easy to access computers which are connected to the internet. And in some cases people do access internet through their mobile phones easily because of the so called ódbundlesô which are provided by different mobile telecommunication companies.

Similarly, a sufficient number of respondents (80%) supported that nowadays computers or mobile phones are affordable and people may browse cheaply internet.

Table 3: What are the factors contributing to cybercrimes?

S/N	Factors	Response	Level of Agreement				
			SA	A	U	DA	SDA
1.	Growth of the Technology	N	90	70	0	20	20
		%	(45)	(35)	(0)	(10)	(10)
2.	Economic factor	N	100	60	20	10	10
		%	(50)	(30)	(10)	(5)	(5)

It is evident from **table 3** that majority of respondents (80%) said that the growth of technology is one among factors that contribute to the existing of cybercrimes. Similarly, a sufficient majority of respondents (80%) supported that economic is another factor.

DISCUSSION

Cyber crime is a term that covers a broad scope of criminal activity using a computer. At an organizational level, cyber crime may involve the hacking of customer databases and theft of intellectual property. Many users think they can protect themselves, their accounts, and their computers with anti-spyware and anti-virus software only. Cyber criminals are becoming more sophisticated and are targeting consumers as well as public and private organizations.

The effects of a single, successful cyber attack can have far reaching implications including financial losses, theft of intellectual property, and loss of consumer confidence and trust. The overall monetary impact of cyber crime on society and Government is estimated to be billions of dollars a year. As from Table 1, many impacts are shown and if you convert them in monetary value is when you get billions of dollars. ódRecent cases in the United Kingdom have brought to public light that women do exploit the Internet to sexually abuse childrenô (Martellozzo, E., Nehring, D. & Taylor, H. 2010). The risks that children may encounter when online are numerous and rather serious: exposure to inappropriate conversation; unwittingly becoming the subject of sexual fantasy; being sent indecent or obscene images; being asked to send indecent images of themselves or their friends; being engaged in sexually explicit talk; and being encouraged to perform sexual explicit acts on themselves or their friends. All these activities and risks form the new reality of cyberspace, where everyday hundreds of children are approached for

sexual abuse. As it can been seen in the findings, 95% of respondents declared that cybercrimes affect children through pornography.

Youths are using the Internet for playing games and communicating with friends, maintaining online blogs concerning their lives and interests, and using social networking sites to develop and maintain relationships. Each of these behaviours could potentially lead a young person to encounter harassment. Moore, Tarun and Lee (2010) wrote that, The Internet behaviours of young people could potentially cause them severe harm, with some recent media reports linking cyber bullying and online harassment to suicide-related deaths and attempted suicides among juveniles. The findings from Table 1 show that 90% of respondents agreed that cybercrimes cause harassment on the society. Nowadays people may use face book to harass other people. For example they can use your particulars e.g. names, date and place of birth, etc and create an account for you on face book and put naked pictures on your profile and once other people visit your profile see those pictures in your profile. The pictures can be edited by using graphic software regardless whether you were really naked or not.

Often, violence among youths involves some component of harassment, wherein individuals repeatedly experience some negative action by another young person who attempts to disrupt, injure, or otherwise cause discomfort for their victim. Chang Su & Thomas J. Holt (2010) added that, the impact of harassment can be quite severe, often causing depression and health concerns for victims and attempted suicide.

Digital Piracy is another impact which is also found from the findings. As it is seen clearly from Table 1; 95% of respondents agreed that cybercrimes affected the society through digital piracy and many actors/actress and musicians are suffering. According to a study by the International Federation of Phonographic Industries (2011), the music industry has seen a decline in sales of 31% from 2004 ï 2010. One potential cause of this loss is digital piracy, which is estimated to cost the music industry 12 billion dollars annually (Siwek, 2007). The cost is estimated to be 20 billion dollars for the movie industry (Siwek, 2006), and 8.3 billion for the software industry (International Data Corporation, 2010). The gaming industry also feels the negative impact of piracy (Kalning, 2007), although specific estimates are not as available for this industry.

In most countries including Tanzania the piracy in most cases occurs in music and videos, and this is the biggest problem many artists are complaining. The issue of piracy in Tanzania does not involve internet, but normally people copy illegally the work of artists (musicians, actors, etc) and distribute and sale them. Not only artists who suffer from this type of cybercrime, but also this involves the illegal copying of software from different vendors and distributing and sell them to other people.

Some of the most expensive and prolific victims of hacking have been businesses. Businesses are many times targeted for their customersô personal and financial data and often are targeted by their own employees, whether disgruntled or just

opportunistic. The results from Table 1 show that 80% of respondents said hacking is a major threat caused by cybercrimes on the society as well as the business. Also from table 3, the results show that hacking is due to the economic factor. This is supported by 80% of respondents.

> *Businesses lose billions of dollars yearly as a result of hacking and other computer breaches. Many times, the true cost cannot be evaluated because the effects of a security breach can linger for years after the actual attack (Washington. Edu, 2006)*.

Unauthorized access (hacking) may occur both on individualsô personal computers, as well as in the workplace. óOne major form of unauthorized access is known as hacking. Hacking is the act of gaining unauthorized access to a computer system or network and in some cases making unauthorized use of this accessô (Rushinek, 1993 in Kunz & Patrick, 2004).

Another side effect of the cybercrimes activities on the society and business in general is intentional damage of the data. As it can be observed from the findings in Table 1 70% of respondents agreed to this type of threat. This type of cybercrime can result in cost to the enterprise in the recovery of the data as well as from loss of good will from customers due to errors resulting from the data loss. Customers can also be harmed from data leakage if receipts or credits are not correctly posted to their accounts.

As the Internet has become an integral part of peopleôs lives around the world, criminals have increasingly adopted online strategies, such as stock spam e-mail campaigns to reach large numbers of potential victims cheaply and efficiently (Hu, Mclnish & Zeng, 2010). This is supported by the findings as it can be seen from Table 1 that 85% of respondents agreed that spam e-mail is another impact caused by cybercrimes. Although the majority of spam e-mail recipients ignore these fraudulent messages, a small percentage of recipients respond and lose money. óThe motivation of spam usually involves revenue generation, higher search ranking, promoting products and services, stealing information, and phishingô (Yu, 2011). Nowadays criminals have advanced in this type of crime and have been sending fee fraud e-mails in which the sender claimed to need assistance moving a large sum of money out of their country. Every user of the internet with email should be care with this crime.

As the discussion has been shown, the question we might ask ourselves is why computers or networking are tools target for these cybercrimes. As it shown in the findings from Table 2, there are almost three reasons as responded by 90% of respondents who said availability, 85% easy access and 80% said computers are affordable.

Availability and easy access to computer and internet have contributed much to the cybercrime activities. It is affordable to buy computer and to access internet and therefore many people are using technology in their daily activities whether at home or workplaces. Due to this advancement of using technology, the technology has become the tool target or place of criminal activities. óAs the Internet and computer-

mediated communications technologies are increasingly inexpensive and available, the opportunities for individuals to engage in harassment via electronic methods, or cyber harassment, have increased significantlyô (Chang Su & Thomas J. Holt, 2010) Photographic images from pictures or books can be input into a computer using scanners, devices that convert images into digital form that may be saved as files on a hard disk. Once these images have been converted to the softcopy, they can be put to the websites and if one has access to the internet has access to pornography.

Black & Kenneth (2010) in their article contributed that, Computer technology has revolutionized the distribution of pornography. Material can now be exchanged on small floppy disks or by way of the Internet rather than through the mail or personal contact. Furthermore, users and distributors are provided with substantial anonymity on the Internet. As the technology growth, the threat to the society increases. This is supported from the findings in Table 3 where by 80% of respondents said that one among factors which contribute to cybercrimes is technology growth. . óA recent survey conducted by Gartner Group of 160 retail companies selling products over the internet reveals that the amount of credit card fraud as 12 times higher online than in the physical retail worldô (Oates, 2001).

As the technology grows more and more efficiently, there is a directly proportional to the growth of the economy. Since cybercrimes normally work on the opportunities which occur on the systems, they use this loop hole of the growth of the technology to see how they can intrude the systems as a result the activities of cybercrimes increase more and more.

Technological advances have helped unintentionally promote this behaviour by making the ability to upload and download music easier and faster. Thus, these advances have resulted in a substantial amount of music being transferred illegally. Phonographic Industries (Gunter, Higgins and Gealt, 2010) has estimated that a third of all CDs are pirated. Internet criminals are well aware of these circumstances and combine both the weaknesses in computer security and internet knowledge with their own ever-growing skill base to succeed at their criminal occupations (Dingle, 2007; Mann 2007).

The development of multimedia network game industry affects the increase of cybercrime. As the Internet game industry prospers, many people are pampering themselves in variety of network games (Chawki, 2005). As this increase, cause the cyberspace to increase as well, which derive some crimes such as Internet fraud concerning game items and cyber money.

PREVENTIVE MEASURES FROM CYBERCRIMES

Preventing cyber-criminals activities is not an easy task. Tan (2002, p. 347 in Dion, M. 2010) said that cyber-criminals are often difficult to identify since they committed their crimes at the very long distance from their victims. Sometimes, the country in which they live and/or have their criminal activities does not have strong criminal laws against cyber-criminality. Despite of these challenges, some measures can be taken to account as the way of combating these cyber criminalsô activities as discussed in this section.

User identification & Authentication

User identification typically includes the use of user names and passwords. However, these simple tools can be very easy for a cyber criminal to break. Passwords can be made harder to break by various techniques including requiring longer character strings, the inclusion of numbers as well as letters, making them case sensitive, and requiring that they be changed at regular intervals (e.g., monthly, annually). Password should be changed with regular interval of time and it should be alpha numeric and should be difficult to judge (Kumar, 2008). The use of smart cards is expected to increase in the future since it requires both the card and a personal identification number known only to the card holder. Access is impossible without both pieces.

Using network scanning programs

For large to medium enterprises, the proven Virtual Private Network (VPN) technology over WLAN, which is a practical and scalable design can be used for the security. A VPN allows users on a public or un-trusted network, like the internet or WLAN to setup a secure connection to a private network. In a wired or wireless network, the user establishes a secure VPN tunnel to the VPN server when user authorization is successful. Then all the traffic sent through the tunnel is encrypted (Isack & Mohammed, 2007).

Using open source for security

Another way of preventing cybercrimes is through the uses of Open source software. Hoepman & Jacobs (2007) wrote that; open source enables users to evaluate the security by themselves, or to hire a party of their choice to evaluate the security for them. Open source even enables several different and independent teams of people to evaluate the security of the system, removing the dependence on a single party to decide in favour of or against a certain system.

Special law Protecting Computer Users

The paper has shown that, many countries do not have any special Act which has been established to combat computer crime activities. Though many countries have Communications Regulatory Authority (CRA), many of these regulatory authorities do not have any clear Act which protects computer users. For instance in Tanzania, The Tanzania Communications Regulatory Authority has come up with the ACT known as ôTHE ELECTRONIC AND POSTAL COMMUNICATIONS ACT, 2010ô (EPOCA) but it does not consider the protection of ICT users against cybercrimes.

CONCLUSION

Recent studies published on the evolution of principal cyber threats in the security landscape. They present concerning scenarios, characterized by the constant growth of cybercrimes activities. Even though the level of awareness of cyber threats has increased, and law enforcement acts globally to combat them, illegal profits have reached amazing figures. The impact to society has become unsustainable, considering the global economic crisis. Itôs necessary to work together to avoid the costs the global community suffers, which we can no longer sustain. The risk of business collapse is concrete, due to the high cost for enterprises in mitigating

counter measures, and the damage caused by countless attacks. Nowadays customers have come to expect that organizations have a presence on the Internet, including a website and e-mail capabilities. Use of the Internet is a risk that most companies have to take. The problem is to minimize the risks associated by so doing. If there is no technology, hopeful the cybercrimes would not be found anywhere. As it has been discussed in the paper, the preventive measures should be taken to prevent the society as well as the organizations from the cybercrimes instead of avoiding the uses of the technology.

REFERENCES

Black , G. Patrick and Hawk, Kenneth R. (2010) Computer and Internet crimes, San Francisco, California [Online] available from <http://www.fd.org/pdf_lib/WS2010/WS2010_Computer_Crimes.pdf> [March 29, 2011]

Brett Pladna (2008) The Lack of Attention in the Prevention of Cyber crime and How to Improve it [Online] available from < http://www.infosecwriters.com/text_resources/pdf/BPladna_Cybercrime.pdf> [April 30, 2011]

Chang Su and Thomas J. Holt (2010) *Cyber bullying in Chinese Web Forums- An examination of nature and extent*, International Journal of Cyber criminology Vol 4 Iss 1and2, pp 672ï 684 [Online] available from <http://www.cybercrimejournal.com/changuholt2010ijcc.pdf/> [September 15, 2011]

Chawki, Michael (2005) *Cybercrime in France: An Overview* [Online] available from<http://www.crime-research.org/articles/cybercrime-in-france-overview /> [February 28, 2011].

Collins, Jason D, Sainato, Vincenzo A. and Khey, David N.(2011) *Organizational Data Breaches 2005-2010: Applying SCP to the Healthcare and Education Sectors* Vol 5 Iss 1, pp 794-810 [Online] available from < http://www.cybercrimejournal.com/collinsetal2011ijcc.pdf> [February 14, 2012].

Dion, Michael (2010) *Advance Fee Fraud Letters as Machiavellian/Narcissistic Narratives*, International Journal of Cyber criminology Vol 4 Iss 1and2, pp 630ï 642 [Online] available from <http://www.cybercrimejournal.com/micheldion2010ijcc.pdf/> [September 14, 2011].

Erbschloe, Michael (2009) *Computer and Internet Crime - Research Starters Business,* [Online] available from <http://web.ebscohost.com/ehost/pdfviewer/pdfviewer?hid=105andsid=7142dd01-414d-4d45-8e62-b10e618961e2%40sessionmgr115andvid=1> [February 16, 2011].

Eric J. Sinrod and William P. Reilly (2000) cybercrimes: a practical approach to the application of federal computer crime laws; Santa Clara university school of law Journal vol16, number 2 [Online] available from < http://www.sinrodlaw.com/CyberCrime.pdf> [April 30, 2011].

Gunter, W., Higgins, G. and Gealt, R. (2010) *Pirating Youth: Examining the Correlates of Digital Music Piracy among Adolescents*, International Journal of Cyber criminology Vol 4 Iss 1and2, pp 657ï 671 [Online] available from <http://www.cybercrimejournal.com/whitneyetal2010ijcc.pdf/> [September 14, 2005] .

Heather, Newton (2008) Electronic Law: Research Starters Business [Online] available from <http://web.ebscohost.com/ehost/pdfviewer/pdfviewer?hid=105andsid=0af3d1fb-4a5b-43b3-9a63-88c64b0d59f9%40sessionmgr114andvid=1> [March 20, 2011].

Hinduja, Sameer and Schafer, Joseph A. (2009) "US cybercrime units on the world wide web", Policing: An International Journal of Police Strategies and Management, Vol. 32 Iss: 2, pp.278 ï 296 Available from < http://www.emeraldinsight.com/journals.htm?issn=1363-951Xandvolume=32andissue=2andPHPSESSID=9b6iln802cqem26pgpbll0pme0> [February 28, 2011].

Hoepman, Jaap-Henk; Jacobs, Bart (2007); increased security through open Source: *Communications of the ACM*, Jan2007, Vol. 50 Issue 1, p79-83, 5p [Online] available from <http://web.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=7a28b26e-60d2-4ee8-a9ff-d0f7f9f6cdef%40sessionmgr104andvid=1andhid=105>[April 30, 2011].

Hu Bill, Mclinish Thomas and Zeng Le (2010) *Gambling in Penny Stocks: The Case of Stock Spam E-mails*, International Journal of Cyber criminology Vol 4 Iss 1and2, pp 610ï 629 [Online] available from <http://www.cybercrimejournal.com/Huetal2010ijcc.pdf/> [September 15, 2011].

International Federation of Phonographic Industries (2011) IFPI *digital music report 2011: Music at the touch of a button*: Zurich, Switzerland: IFPI [Online] available from <http://www.ifpi.org/content/library/DMR2011.pdf> [April 15, 2014].

Issac, Biju ; Mohammed, Lawan A (2007) War Driving and WLAN Security Issues - Attacks, Security Design and Remedies: The Journal of *Information Systems Management*, Vol. 24 Issue 4, p289-298, 10p, [Online] available from < http://web.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=7andhid=105andsid=d9b6cd7d-57dd-42f8-89f2-dcf2f83440ea%40sessionmgr110> [April 30, 2011].

Kalning, K. (2007, May). Game piracy runs rampart on the Internet. *MSNBC* [Online] available from <http://www.nbcnews.com/id/18665162 > [April 15, 2014].

Kumar, V. S (2008) cyber crime prevention, detection [Online] available from <http://www.cidap.gov.in/documents/Cyber%20Crime.pdf> [February 17, 2011].

Kunz, Michael and Wilson, Patrick (2004) Computer Crime and Computer Fraud, University of Maryland Department of Criminology and Criminal Justice [Online] available from <http://www.montgomerycountymd.gov/content/CJCC/pdf/computer_crime_study.pdf> [March 29, 2011].

Marion, Nancy E. (2010) *The Council of Europe's Cyber Crime Treaty: An exercise in Symbolic Legislation,*, International Journal of Cyber criminology Vol 4 Iss 1and2, pp 699ï 712 [Online] available from<http://www.cybercrimejournal.com/marion2010ijcc.pdf/> [September 15, 2005].

Martellozzo, Elena., Nehring, Daniel and Taylor, Helen (2010) *Online child sexual abuse by female offenders- An Exploratory study*, International Journal of Cyber criminology Vol 4 Iss 1and2, pp 592ï 609 [Online] available from <http://www.cybercrimejournal.com/elenaetal2010ijcc.pdf/> [September 15, 2005].

Moore Robert, Tarun Naga and Lee Tina (2010) *Examining factors that influence a Youth's potential to become a Victim of Online Harassment*, International Journal of Cyber criminology Vol 4 Iss 1and2, p 685ï 698 [Online] available from <http://www.cybercrimejournal.com/mooreetal2010ijcc.pdf/> [September 15, 2011].

Newton, Heather (2008). *Electronic Law -- Research Starters Business*, p1-1, 19p [Online] available from <http://web.ebscohost.com/ehost/pdfviewer/pdfviewer?hid=105andsid=0af3d1fb-4a5b-43b3-9a63-88c64b0d59f9%40sessionmgr114andvid=1> [May 2, 2011].

Ngo, Fawn T. and Paternoster, Raymond (2011) *Cybercrime Victimization: An examination of Individual and Situational level factors* Vol 5 Iss 1 p 773ï 793 [Online] available from < http://www.cybercrimejournal.com/ngo2011ijcc.pdf>[February 15, 2012].

Oates, Brad (2001) *Cyber crime: how technology makes it easy and what to do about it*: Journal of Information Systems Management, Summer2001, Vol. 18 Issue 3, p92, 5p [Online] available from <http://web.ebscohost.com/ehost/pdfviewer/pdfviewer?hid=105andsid=40ff76e7-2b95-403c-a5e6-cca8db255632%40sessionmgr114andvid=1> [February 18, 2011].

Saban, Kenneth A.; McGivern, Elaine; Saykiewicz, Jan Napolean (2002); A critical look at the impact of cybercrime on consumer behaviour: *Journal of Marketing Theory and Practice*, Vol. 10 Issue 2, p29, 9p [Online] available from < http://web.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=e59a071f-c629-476c-97e0-283aa772d4d2%40sessionmgr112andvid=1andhid=105> [April 30, 2011].

Siwek, S. (2007) *The true cost of sound recording piracy to the U.S. economy.* [Online] available from <http://www.ipi.org/docLib/20120515_SoundRecordingPiracy.pdf> [April 15, 2014].

Siwek, S. (2006). *The true cost of movie picture piracy to the U.S. economy* [Online] available from <http://www.ipi.org/docLib/20120117_CostOfPiracy.pdf > [April 15, 2014].

Sonya Liew Yee Aun (2005); an introduction to cyber crimes: Malaysian Perspectives [Online] available from <http://www.maele.net/articles/ekom2005/Paper/Sonya%20Liew%20%20UK.pdf> [April 30, 2011].

Wall, David S. (2008) Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. International Review of Law, Computers and Technology; Vol. 22 Issue 1/2, p45-63, 19p [Online] available from < http://web.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=d9b6cd7d-57dd-42f8-89f2-dcf2f83440ea%40sessionmgr110andvid=5andhid=105> [April 30, 2011].

Wall, David S. (2005) The Internet as a conduit for criminal activity, In A. Pattavina (Ed.), Information technology and the criminal justice system (pp. 78-94) Thousand Oaks, CA: Sage..

Washington.edu (2006) History & Impact of Hacking: Final Paper [Online] available from < http://courses.cs.washington.edu/courses/csep590/06au/projects /hacking.pdf> [April 15, 2014].

Wienclaw, Ruth A. (2008) *Internet Security -- Research Starters Business* [Online] available from < http://web.ebscohost.com/ehost/pdfviewer/pdfviewer?hid=

105 andsid=56be29d8-2da9-4ecd-9429-c3b87bbdd88a%40sessionmgr114and vid =1> [February 15, 2011].

Yu, Szde (2011) *Email spam and the CAN-SPAM Act: A qualitative analysis* Vol 5 Iss 1 pg 715-735 [Online] available from < http://www.cybercrimejournal. com /Yu2011ijcc.pdf> [February 15, 2012].