ISSN No. 0976-5697

Volume 5, No. 8, Nov-Dec 2014

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

The Threat of Advancing Cyber Crimes in Organizations: Awareness and Preventions

Mr. Anil Kumar
Senior Lecturer,
Department of Computer Science,
Kabarak University, Kenya

Miss. Jaini Shah
Lecturer,
Department of Law,
Kabarak University, Kenya

Abstract:With the era of globalization, computers, mobile phones and the Internet have become part of our daily routine. As a result of this, online processing information is made available on the internet bringing in new threats in the form of cybercrimes. Such threats not only come in different faces, but they also have different execution methods making it difficult for cyber experts to find a viable solution. Due to the high rates of threats, nations around the globe have become concerned about their Netizens' online safety and have implemented several Acts of Parliament and International Instruments. However, most of the laws are still in A Mother's Womb which are in the process of evolution. There are several reasons why cyber- attacks are planned, as some have serious agendas tagged on them, while others are simply planned as pranks. This paper not only seeks to analyze the political, economic and social effects of cyber-crimes in organizations but also recommends how one can be made aware and prevent cyber-crimes in organizations as prevention is better than cure.

Keywords:Cybercrime, Hackers, Crackers, Cyber threat, Cyber-attack, Cyber Criminal, Cyber terrorists.

I. INTRODUCTION

As a Famous Lawyer once said- "a crime will happen where and only when the opportunity avails itself." For centuries now, we are only aware of traditional crimes such as murder, rape, theft, extortion and robbery. As the world has turned into a global village, science and technology has also advanced dramatically with the aid of computers and the internet. The internet has opened up a whole new virtual heaven for the people both good and bad, clever and naive to enter and interact with a lot of diverse cultures. Information dissemination, e-business and access to chatting with people around the globe are now possible at the click of a mouse. This has enabled users to carry out their malicious intentions including hacking, cracking and copyright theft.

What is Cybercrime? It is an illegal act as it is punishable by law. It is carried out by one when he or she uses a computer to carry out a criminal activity by hacking such as stealing governmental sensitive information for his or her own benefit e.g. financial fraud, identity theft, website defacement and cyber bullying.

Many organizations are under the wrong intuition that they can prevent this serious threat by simply using the best anti-virus or spyware. They have turned their eyes innocently by believing that cyber criminals are just like petty criminals, ignoring the fact that there are just like arrogant Terrorists.

II. BACKGROUND INFORMATION

Communicating online by using Internet as 'A Fast and Furious' Vehicle can be compared to a branded fashion label such as 'Dolce and Gabanna' as many people want to be associated with it.

Internet is the collection of millions of computers in a network worldwide. As the million users include organizations, Governments and internet users, they are all becoming victims of a number of cyber- crimes. As the world is now becoming a global village, both developed and developing countries have adopted computers as the best data storage devices. Although, the organizations have failed to train their employees effectively and often make errors which open doors to cyber-crimes. The cyber- attackers often use this to their advantage by using sophisticated techniques to attack their targets without their knowledge. These targets usually do not get to know that they have been stabbed on their backs as confidential organization information and government information is stolen rather than financial information. [1]

Types of Computer Crimes

- ***Computer assisted crimes-*** As the name suggests, these crimes are not carried out by the computer itself, but by a cyber-criminal who uses it as his/her vehicle to reach a destination. Examples of such crimes include fraud and child pornography.
- ***Computer specific or targeted crime*** – These crimes are directed at computers, networks, and the information stored on these systems (e.g., denial of service, sniffers attacking passwords).
- ***Computer is incidental*** - The computer is incidental to the criminal activity (e.g. customer lists obtained from the computer by traffickers for example in banks.)

Who commits cyber-crimes?

- ***Crackers:*** Intent on causing loss to satisfy hidden motives or just for fun. Computer virus developers/creators and virus distributors come under this category.
- ***Hackers:*** Explore other private secured networks or computer systems to get to know information for some purposes, out of mere curiosity, or in order to compete with their peers.

- ***Pranksters:*** They can be compared to 'Tom and Jerry' as they merely make jokes or play tricks on others for a short-term harm.
- ***Career criminals:*** Earn part or all of their income from crime. These individuals may be seen as mentally ill as most of them carry out this crime as a part-time job repeatedly after breaks.
- ***Cyber terrorists:*** Computer experts who paint their hands read by hacking into a Government or a valuable organization website. Most of them terrorize websites by flooding it with traffic.
- ***Cyber bulls:*** They cause nuisance on the Internet. Examples of cyber bull crimes include; posting fake profiles on web sites, using fake names in chat rooms, creating vicious forum posts, and sending cruel email messages.

III. STATEMENT OF THE PROBLEM

A single successful cyber-attack such as theft of intellectual property can have dreadful effects not just on the attacked organization but also the Government. These effects include, financial loss, losing customers and distraction of sensitive data. [2].

IV. PURPOSE OF THE STUDY

The main purpose of the study is to find ways of how cybercrime is advancing for example by accessing a private secured network in order to copy and destroy data; its effects on individuals, groups, organizations and the Government. This research paper will also help us to know who is responsible for cybercrimes.

WHO ARE RESPONSIBLE FOR CYBER- CRIMES?

1. Children or adolescents who want to impress others in their group by demonstrating mind-boggling skills.

2. Professional hackers or cyber-criminals who want to fulfill certain political or personal goals.

V. RESEARCH OBJECTIVES

It is always emphasized that a problem usually comes with its own seeds of solution. This statement signifies the need of defining the objectives of this research.

The main objective of this research is come up with an important solution that will curb the increase of cybercrime in organizations.

In order to achieve this, the organizations must:

- Understand how the internet and the cyber world operate.
- Be able to track and trace back where a cybercrime originated.
- Be able to examine the position of its intellectual property rights on the internet.
- Be able know its principle remedies in case of a cyber-attack.
- Understand each and every piece of its electronic evidence.
- Know the international rules of handling and curbing cyber-crimes.
- Be able to implement reforms and measures taken to control and prevent cybercrime.

VI. JUSTIFICATION OF THE STUDY

Organizations are not just losing sensitive information, money, and intellectual property, they are also loosing consumer confidence and trust [3]. Technology as a whole is a great thing and has a lot of advantages, for both the young and the old but it has its own threats which are being sown by new criminals who feel that they can escape unpunished. Cybercrime is an ongoing problem which is being discussed in organizations such as The ***United Nations (UN), The European Union (EU) and The Organization for Economic Cooperation and Development (OECD),***but organizations are still threatened by the issue of cyber-crimes. Due to this reason, we believe that the organizations must secure themselves on the ground by training and creating awareness for its employees on how to handle sensitive data such as customer's information and organizational information. The employees should also get a chance to understand the effects of cyber threats and the actions which they may undertake to protect their own information, as well as the information within theirorganization.

Effects of Cyber Crime:-

A. Economic Impact

As a Cybercrime is intended to damage the reputation of an individual, a private or a public organization, it also has a drastic side effect in the form of an economic impact.

An example is when a Finance Organization's system such as a Bank is hacked into. As we know, when we seal the deal of becoming a Bank's Client, we must both act in good faith. The good faith which must be adhered to by banks is not to leak a client's information to anyone as it may erupt into a cold war. When a cyber-criminal successfully hacks into the system, the bank's good faith is breached as the criminal may embezzle a client's funds or post the client's personal information on a particular website which eventually breaks the trust of the customer. This would literally spoil the bank's image as the client would be willing to find better prospects. [4]

According to previous research, the overall monetary impact of cyber-crimes on the society and the Governments at large is estimated to be billions of dollars a year [3].

B. Social Impacts

Trying to overcome a cybercrime attack for a developing country is not a good experience, as trying to mend the damage will cost millions of dollars which may not be readily available.

Due to cyber- attacks, the citizens of either developed or developing countries start avoiding the advent of technology as they feel insecure. This will murder 'Globalization' as people will not want to be a part of social networking. [4]

C. Political Impact

Cybercrime has a big effect in the political world, when Government computer networks are targeted and attacked. This decreases the ability of international organizations investing resources in developing countries. When this happens it increases white collar criminal activities, funding of anti-government regimes in order to stabilize the Government, which will definitely affect the political scenes in a country. [4]

VII. BENEFICIARIES OF THE STUDY

This study will help us to understand how to curb cybercrimes using the laws set in regulating the people who may think on prying on an organization's sensitive information. In enforcing these laws organizations will have great benefits.

- In understanding how cybercriminals work, it will increase the organization's chance of fighting back cybercriminals and not be the hosts of those cybercriminals.
- Organizations implementing cyber laws in their systems will see a big reduction of cybercrime attacks towards its operations.
- Organizations working together with the Government will see a stronger bond in enforcing the cyber laws that govern the cyber space, yielding to a good business relationship between the two, increasing profit margins.
- In implementing training and knowledge of cybercrime, organizations will improve their chances of curbing cyber-attacks since their employees will be aware and have better good understanding of its effects.
- It will help organizations to know and understand the techniques and ways in which the cybercriminals use to attack.
- Organizations will be able to understand the international laws that govern cyberspace in order to fight cybercrime. This will enable them to gain a better understanding of this emerging issue and gain support from its foreign enforces, making the organizations work efficiently in order to be effective.
- Organizations fighting cybercrime will improve the country's economic standard which will eventually enhance a better social environment between different communities increasing a better shared value expansion in social and economic progress.

VIII. RESEARCH METHODOLOGY

Research is a search for new knowledge or a scientific and systematic search for pertinent information on a specific topic.

Research Questions

What does an organization want to protect?

Organizations need to protect:-

1. Their customers' confidential and sensitive data

2. Their network, assets and resources.

Why are cyber-attacks on organization so often successful?

This is because many organizations do not pay much attention on their network security.

This is clearly evident from the fact that Organizations don't have guidance or procedures to audit any user's access to network. This makes it easy for any cybercriminal to gain access as there are no restrictions whatsoever.

What are the greatest challenges?

Organizations face numerous challenges in the field of cybercrime, including:-

1. New technology.

2. Cybercriminals coming up with new types of threats.

3. Organizations have poor security measures with limited funding in securing quality security machines and no qualified security experts who can monitor and close up all the open doors that may be used by the cyber-attackers.

Why are the most cyber-attacks gone undetected?

This is because most organizations don't have the resources that can detect a cybercriminal in their systems. For example, the organization may lack a cyber-security expert enabling the cybercriminal to access the organization's system without being detected

Why are cyber-attackers not getting jail terms?

This is because cybercrime is a global crime which makes it difficult to get or trace a cybercriminal because they might be situated in a different country or continent. Thus, making it difficult to collect evidence and prosecute such a criminal as each country enjoys its own sovereignty thus disabling one to access the effected organization's system. More over there is no international law that operates everywhere as many countries do not ratify international instruments such as conventions. Secondly, as the courts have their own jurisdiction disabling them from hearing cases outside their jurisdiction. Thirdly, the cyber-criminals may successfully escape after carrying out the heinous act. Lastly, one may not be able to extradite these criminals to another country to punish them as there might not be any harmonized domestic laws in relation to cyber-crime.

What are the motivations for the cybercriminals?

Cybercriminals have different reasons for attacking an organization's system or network; some are personal reasons for example retaliation to wrong termination or to gain more financially while some are political reasons.

What risk should the attacked be willing to take in other to get the target?

In order to catch the perpetrators of cybercrime organizations should be willing to take up some risks in opening up a dummy tunnel that leads to its network. This will fool the cyber-criminal by making him a victim of the trap enabling the organization to trace back the origin of the intrusion.

How can we end cybercrime and make our cyber space secure?

Cybercrime can be ended by enacting strict laws to govern the use of cyber space. Another method of fighting cyber-

crimes is securing network infrastructure, sensitive, confidential data and intellectual property.

Observation

In the methodology above, we collected data by observing an organization's networked environment, closely by taking into account the users who were interacting with the computers to serve customers. An observation was made on how they login to their systems and what security was abled while accessing the organization systems. We observed that most of the users don't follow protocol in keeping the intellectual property of the organization secure which made their computers vulnerable to cybercriminals.

IX. LITERATURE REVIEW

Intellectual property rights like copyrights, patents, trademarks and many more etc. are a reflection of the mind including symbols, names, images, literary and artistic works, inventions and designs. Infringement in cyberspace is a major concern to ***Justice Yatindra Singh*** who has made his own judgments on the issue [5].

Crimes against Intellectual Property: Laws falling under this category include offenses from the perspective of the information being protected. E.g. Use of intellectual property without consenting the owner or passing to define offenses involving the destruction, alteration, disclosure.

Cybercrimes such as online banking frauds, source code thefts, virus attacks, phishing attacks, email and website hacking to name but a few have become common place. Necessarily, all the good about technology can always be used in an adverse manner, and therefore, the role of the law is to maximize the good and minimize the adverse [6].

VivekSoodin his book "***Cyber Crimes, Electronic Evidence and Investigation: Legal Issues***" has suggested various strategies to curb cyber-crimes. He suggests that since cyber-crimes are technology based, the best way to curb these crimes is security technology. Fire-walls, anti-virus software and anti-intrusion systems are some of the effectively used security technologies. He concludes by saying that "protect yourself" is the best mantra against cyber-crimes. According to him, effective cooperation between the law enforcement agencies within the country and between many nations is necessary to challenge cyber criminals in order to punish them. Further he calls for strengthening extradition treaties and their implementation should be a must in this digital age [7].

NandanKamathin his book "***Law relating to Computers, Internet and E -commerce: A Guide to Cyber Laws and the Information Technology Act, 2000***" has commented on the emerging field of 'electronic evidence' in the cases of cyber-crimes. He has made an in-depth study about the admissibility and authenticity of electronic records, burden of proof in cyber offences, and other concepts like production and the effect of evidences such as video - conferencing, forensic computing and best evidence rule etc.

R.K. Chaubey in his book "***An Introduction to Cyber Crime and Cyber Law***" has emphasized on the significance of 'right to privacy' in digital age, stating that the new technologies have enhanced the possibilities of invasion into the privacy of individuals and provided new tools in the hands of eavesdroppers. Thus, individual privacy is at a greater stake than ever before. Computers and the internet can be used to steal huge amounts of data regarding people, then profiling and modifying it in various ways, in a manner which could violate an individual's privacy. He has examined the concept of privacy in the light of various national and international laws. He also discusses how the practices commonly used on the internet like cookies, web bugs, spamming could lead to the violation of privacy. He has also highlighted the importance of adopting privacy policy in the websites [8].

V.D. Dudeja in his book ***"Cyber Crime and the Law***" has highlighted the interplay of freedom of expression and the internet. Enumerating the reasonable restrictions on the freedom of expression has made him conclude that in the interests of privacy and security some restrictions should be put on the use of computers and internet because law has been able to recognize computer as a 'weapon of offence' as well as a 'victim of crime' leading to the emergence of cyber jurisprudence [9].

Muddaraju, N. and Ramesh in their article "***Cyber Crimes: Need an Effective Law***", has emphasized on the need for specific cyber legislations to effectively deal with cyber-crimes [10].

Paranjape, Vishwanath in his article "***Cyber Crime: A Global Concern***", has focused on the global nature of cyber-crimes and also presses the need for global measures to curb them [11].

Agarwal, S.C., in his article "***Training on Cyber Law, Cyber Crime and Investigation by Police: Need of Awareness and Requirements***", has stated that the law enforcement officials throughout the world are severely handicapped in tackling the new wave of cyber-crimes. He has gone to the extent of saying that you "either have to take a cop and make him a computer expert or take a computer specialist and make him a cop". He has suggested that a Cyber Crime Investigation and Training Cell in all the States for imparting training to the police personnel, public prosecutors and judicial officers should be set up. [12].

S.K. Verma and Raman Mittal in their book **"*Legal Dimensions of Cyber Space*"** have explained the basicconcepts of the cyber world like meaning, types, features and major components of computers; the history and development of the internet; merits and limitations of internet; various computer contaminants like virus, worms, Trojans etc. Emphasizing on the importance of computers and internet in day-to-day chores they have opined that "today it touches and influences almost every aspect of ourlives. We are in the information age and computers are the driving force [13]. We hardly do any activity that is not in some way dependent on computers." They further suggest that not only do we need to be computer-literate, but we also need to understand the myriad issues that surround our extensive and necessary dependence on computers. Commenting on the interlink of human-conflicts-law, they state that where humans are, crime and conflict of interests cannot be far behind, further, where crime and conflict of interests are, law must necessarily march in order totake control and regulate. Thus, they have made a detailed studyon the indispensable role of computer and internet, and the resultant cybercrimes.

Albert, J. Marcellai and Roberts S. Greenfield in their book "***Cyber Forensics-A Field Manual for Collecting, Examining and Processing Evidence of Computer Crimes***", have made a coherent and comprehensive study on various aspects of the electronic evidence including its collection, examination and evidentiary value. They have carved out an altogether new discipline of cyber forensics while focusing on cyber-crimes and cyber law [14].

Brian, Loader and Douglas, Thomas, in their book "***Cyber -Crime Law Enforcement, Security and Surveillance in the Information Age***", have emphasized on the enforcement of cyber-crime legislations by stating that "proper enforcement of law in its letter and spirit is more important than its enactment." Further, they have focused on the enhanced role of law enforcement agencies in investigating cyber-crimes [15].

Vakul Sharma in his book "***Information Technology; Law and Practice***" has evaluated the issue of jurisdiction in cyber space. While discussing the role of international law in deciding jurisdiction of cyber offences he has made references to various principles like territorial principle, nationality principle, protective principle, passive personality principle, effects principle and universality principle [16]. Further, he has made deep insight into the controversial issue regarding extradition of cyber criminals. Moreover, he has examined the US, European and Indian approaches towards personal jurisdiction at a greater length. [17]

Rodney D. Ryder in his book "***Guide toCyber Laws (Information Technology act, 2000, E-commerce, Data Protection and the Internet)*** has exhaustively dealt with the provisions of The Information Technology Act, 2000 as amended in 2008.He has pointed out some grey areas of the Act and has also suggested the remedial reforms in order to provide more teeth and nail to the Act.

The law stated in every book is to protect classified information, prohibit knowingly accessing a computer, without or exceeding authorization, and thereby obtaining classified information with intent to use or reason to believe that such information is to be used to the injury of the organization or to the advantage of any foreign organization.

Unlawful Destruction*:* criminal activities that alter damage, delete, or destroy computer programs or files. ***Brans Comb*** noted that such prohibitions, standing alone, might not always reach the problem of intrusive code, which may be introduced without immediate alteration of existing files and programs.

Use of a Computer to Commit, Aid, or assist a Crime: Laws of this type were passed to prohibit the use of a computer to facilitate other crimes, such as theft or fraud. Standing alone, however, these laws cannot deal with offenses that follow from, rather than precede, the emergence of computer technology.

Knowing and Unauthorized Use: Other statutes sought to criminalize acts of knowing and unauthorized use of computers or computer services.

Unauthorized Copying: Statutes in this category were enacted to criminalize the unauthorized copying of computer files or software and the receipt of goods so reproduced.

Unlawful Insertion: These laws, are common to a handful of states, prohibit the unauthorized insertion of data without regard to damage resulting there from.

Taking Possession: A few statues have criminalized taking possession of a computer or computer software.

X. PREVENTIONS TO MINIMIZE THE RISK OF BECOMING A CYBER CRIME VICTIM

Use strong passwords: Use separate ID/password combinations for different accounts, and avoid writing them down. Make the passwords more complicated by combining letters, numbers, and special characters. Change them on a regular basis [18].

Secure your computer:

Enable your firewall: Firewalls are the first line of cyber defense; they block connections from suspicious traffic and keep out some types of viruses and hackers.

Use anti-virus/malware software: Prevent viruses from infecting your computer by installing and regularly updating anti-virus software.

***Block spyware attacks*:** Prevent spyware from infiltrating your computer by installing and updating anti-spyware software.

Secure your mobile device: Be aware that your mobile device is vulnerable to viruses and hackers. Download applications from trusted sources only. Do not store unnecessary or sensitive information on your mobile device. Most importantly, keep the device physically secure; millions of mobile devices are lost each year. If you do lose your device, report it immediately to your carrier and/or organization. Some devices allow remote data erasing. Always protect your mobile device password [18].

Install the latest operating system updates: Keep your applications and operating system (e.g., Windows, Mac, Linux) current with the latest system updates. Turn on automatic updates to prevent potential attacks on older software.

Protect your data: Use encryption for your most sensitive files such as health records, tax returns, and financial records. Make regular backups of all of your important data.

Secure your wireless network: Wi-Fi (wireless) networks are vulnerable to intrusion if they are not properly secured. Review and modify default settings Avoid conducting sensitive transactions on these networks [18].

Protect your e-identity: Be cautious when giving out personal information such as your name, address, phone number, or financial information on the Internet. Ensure that websites are secure, especially when making online purchases, or ensure that you've enabled privacy settings (e.g., when accessing/using social networking sites, such as Facebook, Twitter, YouTube, etc.). Once something is posted on the Internet, it may be there forever.

Avoid being scammed: Never reply to emails that ask you to verify your information or confirm your user ID or password. Don't click on a link or file of an unknown origin. Check the source of the message; when in doubt, verify the source.

XI. KEY FINDING

This is the method involved in the collection and combination of data to interpret the findings collected from the field. It increases the relevance and makes us understand how organizations get attacked by the cybercriminals.

A. Nature of the crime

This explains the way cybercriminals identify the people or organizations who they can target, a clear indication is that if someone is in a network or connected to the internet he/she may fall a victim in one wayor another. Most organizations' computers are in a network layout to enable them to use the system to serve their customers or keep data and to be able to share resources such as printers, drives, fax machines etc. [19]

In a networked environment such as in the case of an organization, internet is part of the benefits that comes along with it, which is accessed by many employees without any knowledge that they are or might become targets to the prying eyes of a cybercriminal. In our key findings we found out that 99% of people access the internet while only 1% of the people do not. We also found out the different activities carried out while on the internet as seen below:-

Activity individual Access	Yes (%)	No (%)	Total (%)
Google search	88.3	11.7	100
Social media	78.8	21.2	100
Academic research	77.0	23.0	100
E-mail	74.0	26.0	100
Media/Entertainment& news	66.8	33.2	100
Sport	51.0	49.0	100
Games	36.0	64.0	100
Internet phoning	17.3	82.7	100
Pornography	8.3	91.7	100
Spamming	4.3	95.7	100
Piracy	3.5	96.5	100

Figure: 1, Activities carried out while on the Internet

It can be concluded that many people access ***Google search while*** others access internet for other reasons.

In this research, we found out that organizations know exactly the effects of cybercrime making them to be aware of cybercriminals. When asked whether they have heard of cybercrime a high percentage of the employees said 'yes' meaning that most of them are well conversed with the topic and would be able to answer any questions. The table below gives a response of 100 organization employees who were asked whether they knew what Cyber-crime is.

Heard of cybercrime	Frequency	Percentage
Yes	75	93.7
No	25	6.3
Total	100	100.0

Figure 2: Response as to whether they have heard of Cyber Crime.

There are several ways and tools a cybercriminal can use to attack or gain access to a targeted computer or server for example the use of the mathematical method. This is where a cybercriminal writes up or comes up with a program using a tree diagram or a statistical tool, which is then, linked to their victim's account without his/her knowledge, then the tree diagram keeps on checking without stopping until it gets the correct combination of the victim's PIN number.

The principal threats related to cyber-crime activities could be grouped into the following categories:

- Intrusion for monetary or other benefits
- Interception for espionage
- Network sniffer
- Data destruction
- Misuse of processing power
- Counterfeit items
- Evasion tools and techniques
- Password crackers.
- Key loggers.
- Exploits.
- Port scanner.
- Vulnerability scanner.

B. Advantages of the topic

As cybercrime continues to be a challenge, a greater need has arisen for people to shield themselves, by being more alert and secure in protecting unwanted ads or sites. Communication companies have become more reliable in developing secure software products to fight against harmful contents like viruses or computer hackers. Examples of these companies are the "Defend against Cybercrime! Frontier Communications' Frontier SecureTM Computer Security Protects Children and Data." The secure products which they create are stronger anti-virus protection packages. They always highlight in conferences and meetings with the public and media, that they will continue the fights with new shields so, so long as the hackers and viruses are being used in the cybercrime field [20]. The fight against cyber-crime for companies such as these ones will create more jobs for people who are interested in tracking down the criminals behind the cybercrimes.

It will also enhance technology in computer forensics to limit access to criminals when trying to break into a system. This will also be advantageous to organizations as it will:-

- Help the organizations in automating various tasks that cannot be done manually.
- Help the organizations organize data and information in a better way. This will enable important data and files to be stored in a secured mode.

XII. CONCLUSION

Cybercrime is regarded as merely a small threat or problem with the Government Authorities as it is usually placed at the end of the list in Parliament. From, the above findings, it can be seen that this is further from the truth and Governments must place more reliance on fighting this ' crime' by preventing it successfully. As the Governmental Authorities are not bothered, thus organizations are also taking it lightly. This means that the methods they use in fighting or tracking and combating these unwarranted cyber-attacks on the organizations are not proportionate to the threats posed by the cyber criminals. The higher chances of not solving the problem is that there are no reliable statistics on the problem, meaning it is hard to justify the increased powers that the Regulation of Investigatory Powers Act

which has been given is not in effect, hence be ineffective in dealing with the computer problems.[21]

The international treaties drawn by the authorities that deal with cybercrime are too vague making it ineffective in dealing with the problem. This means that civil liberties will be affected by the terms of the treaties since they could, conceivably, imply that everybody who owns a computer fitted with a modem or an internet connection could be suspected of being a cybercriminal. Attempts to outlaw the possession of hacking software could affect people, organizations or governments, who are trying to make the internet more secure which will not enable them to test their systems, pointing that the legislation could bring or do more harm than good.

The only certainty emerging from this analysis is that, with an exponential growth of cyber-criminal activity, this challenging fight could be won by law enforcement authorities. This should be done with the development of proper mitigation strategies, and a common legal framework enacted by a recognized International Organization such as The United Nations and applied harmoniously around the globe by sharing information obtained from investigations conducted by various co-operation bureaus around the globe.

XIII. RECOMMENDATIONS

1. Education is the most important strategy which can be used in combating crimes in the cyberspace. People can be educated in workshops and seminars which have been specially planned by organizations taking into account cyber safety. It is recommended that this should be done on a regular basis as new employees are always recruited. In doing so employees or system users will learn how to keep personal and organization information safe and the cybercriminal will flee from cybercrimes.

From the study it shows that most of these cybercriminals are mostly youths in tertiary institutions or they have graduated from tertiary institutions. It is recommended that tertiary institutes should introduce the study of cybercrime, cyber management, and its prevention as part of their curriculum courses in doing so we will be assured that it will take care of the present social changes.

2. It is also recommended that all Governments should act swiftly on their domestic cybercrime legislation and enact a comprehensive law on cybercrime. In order for the law to be effective and efficient, the Government should empower graduates by providing employment or funds to be able to employee themselves with their ideas on cyber-crime. [22]

3. The Governments should also make provisions for intensive training of law enforcement agencies on ICT so that they can track down the cyber criminals no matter how intelligent and cunning they may be.

4. For Government agencies, law enforcement agencies, intelligence agencies and security agencies to fight and curb cybercrime, it is recommended that there is a need for them to understand the technology and the individuals who engage in this criminal act. The findings showed that cyber criminals are part and parcel of our society, as such, prevention of cybercrime requires the cooperation of all the citizens and not the law enforcement agencies alone.

5. It is therefore, recommended that everyone should watch and report to law enforcement agencies quickly when they feel someone is engaging cybercrime. This enables the Government to bring the cyber criminals to the books of law.

6. It is recommended that the assets of the Cyber Criminal's should also be confiscated by the Governments and the imposition of longer prison terms should be enacted for cyber criminals in domestic legislation. This will serve as deterrence to those youths who want to indulge in such heinous crimes.

7. The innocent internet users should inculcate the habit of continuously updating their knowledge about the ever changing nature of ICTs, through this, they can not only be well informed about the current trends in cybercrimes, but they will also have the knowledge about different forms of the said crimes and how the cyber criminals carry out their bad activities, thus they can devise means of protecting their information from cyber criminals.

8. Internet users should be security conscious. In simple words, they must learn how to not provide personal or financial information to others unless there is a legitimate and assumed reason. They should not for instance, throw out cheques, old credit cards, driver's license, passports, receipts among other numerous documents which usually have personal data.

9. The internet services providers should not just provide broadband connection to their subscribers' users, but they should also monitor effectively what the subscribers are doing on the internet. They should provide their customers, especially financial institutions and cyber cafes with well-guided security codes and packages in order to protect their information and software from hackers and publishers.

XIV. REFERENCES

[1]. Saini H, and Rao S, (2012) Cyber-Crimes and their Impacts: T.C.Panda/Internatinal Journal of Engineering Research and Applications (IJERA) Vol.2, Issue 2, Mar-Apr 2012, pp.202-209Prof. Peter S. (2009) Literature Review on Internet Crime: For National Audit Office. (UK)

[2]. The Office of Angel Cruz, Chief Information Security Officer, State of Texas January 2013 | Volume 7, Issue 1

[3]. Angel Cruz, Chief Information Security Officer, State of Texas January 2013 | Volume 7, Issue 1

[4]. Nadia Khadam, (2010) Insight to Cybercrime

[5]. Justice YatindraSingh (5th Edition), 2012, Cyber Laws, Publisher: Jain Book Depot, ISBN 9350351802

[6]. Prof. Ashwani Kumar Bansal, 2010, Book Review: Cyber Laws, The Indian Journal of Law and Technology (vol 6), Universal Law Publishing Co

[7]. VivekSood, Cyber Crimes, Electronic Evidence and Investigation, legal issues (2010)

[8]. Dr R K Chaubey, 2009,An Introduction to Cyber Crime and Cyber Law

[9]. Dudeja V.D. *(2002): Cyber Crimes and Law- Crimes in Cyber*

[10]. Muddaraju, N. and Ramesh 2010, *Cyber Crimes: Need an Effective Law*, CRIMINAL LAW JOURNAL, 116 [1(3)], (February): p. 82
[11]. Paranjape, Vishwanath. 2007, Cyber Crime-A Global Concern, INDIAN POLICE JOURNALVol.54 (3), pp.20-27.
[12]. Agarwal, S.C, Feb., 2001, Training on Cyber Law,Cyber Crime and Investigation by Police: need of awareness and requirements, CBI Bulletin,Vol.9(2), ,pp.4-11
[13]. S.K. Verma and Raman Mittal (Pb), 2004, Legal Dimensions of Cyber Space, I.L.I. (Indian Law Institute)
[14]. Albert J. Marcella Jr., Robert S. Greenfield, and 2002 Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes ByAuerbach Publications
[15]. Brian D. Loader and Douglas Thomas (Apr 13, 2000), Cybercrime: Security and Surveillance in the Information Age, Kindle Edition
[16]. Vakul Sharma, February 28, 2011, Information Technology Law and Practice ISBN-13: 978-9350350003, Publisher: Universal Law Publishing Co Ltd; 3rd Revised edition edition
[17]. Lavorgna A, (2003) Criminal Behavior in the Internet Age: The social organization of Transnational Organized Crime. University of Torento – Italy.
[18]. The Office of Angel Cruz, Chief Information Security Officer, State of Texas September 2012 | Volume 6, Issue 8
[19]. Dr. McGuire M. and Dowling S. (2013) Cyber Crime: A review of the evidence (University of Surrey), Home Office.
[20]. Brown, I., Edwards, L. and Marsden, C., Information Security and Cybercrime, Law and the Internet, 3rd Ed., Oxford: Hart, 2009.
[21]. McConnell (2000) Cybercrime and Punishment: Archic Laws Threaten Global Information. Copyright 2000.
[22]. Schjolberg S.J. (2012) An International Criminal Tribunal for Cyberspace: Cybercrime Legal Work Group. Geneva, (2007-2008).

