On-line-Crimes and their Impacts : A Review

Rakesh Pariyani*

Abstract

In this present world of online processing, maximum of the information is available online and is prone to cyber threats. A huge number of cyber threats is being faced today and their behaviour is difficult for early understanding. Therefore, it is very difficult to restrict in the initial phases of these cyber attacks. Such attacks may have some intention behind them or may be processed unknowingly. All such attacks fall into the category of cyber crimes and they have serious impacts over the society in the form of economical disturbance, psychological disorder, social disturbances & threat to National defence etc. Restriction over these crimes depends on proper analysis of their behaviour and understanding of their impacts over various levels of the society. Therefore, the present article provides the understanding of basics of cyber crimes and their impacts over society with the future trends of cyber crimes.

I. Introduction

The present era is too fast that performance should be directly proportional to the time factor and it is possible only with the use of Internet today. The life is very busy today and Internet is the most important part of it. The term Internet can be defined as a group of many computers connected with a network of electronic connections among them and providing the information available on the main server. This term today is known to everyone, used by everyone, but apart from its benefits it has also another side which reflects its negative impacts also. These negative effects can be studied in the light of the term cyber crimes.

---

* Research Scholar, MLS University, Udaipur-313001, Presently posted as Civil Judge & Judicial Magistrate First Class, Palanpur, Gujarat.

Published in Articles section of www.manupatra.com

The term cyber crime means a crime committed by an act or omission in the violation of law forbidding or commanding it and for which punishment is imposed upon conviction. In other words, cyber crime means —Criminal activity directly related to the use of computers, specifically illegal trespass into the computer system or database of another, manipulation or theft of stored or on-line data, or sabotage of equipment and data[1]. Today, the world of cyberspace is expanding at a very rapid rate and the criminal activities are also expanding. Some of the kinds of Cyber-criminals are mentioned as below.

1. Crackers: These criminals have intention for causing loss to the victim to satisfy some antisocial motives or just for fun. The creators of computer viruses and their distributors fall into this category.
2. Hackers: These criminals enter into the computer system or database of victim to get the personal information hidden in those computer systems. Generally the object behind this crime is to get the personal information of the victim and thereafter use it for personal benefits.
3. Pranksters: The category of these criminals perpetrate tricks on others. They generally do not intend any particular or long lasting harm.
4. Career criminals: This group of criminals adopts cyber crimes as their career and these individuals earn part or all of their income from crime. In some cases they conspire with others or work within organized gangs such as the Mafia. As per the data available, the greatest organized crime threat comes from groups in Russia, Italy, and Asia. "The FBI reported in 1995 that there were more than 30 Russian gangs operating in the United States. According to the FBI, many of these unsavoury alliances use advanced information technology and encrypted communications to elude capture" [2].
5. Cyber terrorists: The criminals of this category attacks on a website, mail accounts, phone books etc for commission of crimes. They just send malware like viruses, Trojans, worms etc. to the victim so that their database get disturbed and their intention is to weaken down the information technology infrastructure of the country so that they become unreliable for the foreign investors and individuals who wish to become part of such victim country's IT system.

[1] Wow Essay (2009), Top Lycos Networks, Available at: http://www.wowessays.com/ dbase/ab2/ nyr90.shtml
[2] Bowen, Mace (2009), Computer Crime, Available at: http://www.guru.net/

6. Cyber bulls: The category which of these criminals commit crimes with the object of harassing victim through Internet. They generally send defamatory mails, posts which are vicious and making such a statement via Internet which causes harassment in any form to the victim.
7. Salami attackers: The criminals of this category attack through Internet for the commission of financial crimes. The main intention here is to make a little alteration in a single case which becomes unnoticed generally. Considering an example that if a bank employee inserts a program into bank's servers, which deducts a small amount from the account of every customer, such act is generally unnoticed, but the overall gain by the criminal is resulted into a huge loss to the victims.

In general cyber crimes can be categorized as follows-

1.1. Crimes related with Data

a. Data Interception

The attacker monitors data streams to or from a target in order to gather information from the victim. This attack is done to gather information to support a later attack or the data collected may be the end goal of the attack. Such attack usually involves sniffing network traffic. In most varieties of this attack, the attacker is passive and simply observes regular communication, however in some variants the attacker may attempt to initiate the establishment of a data stream or influence the nature of the data transmitted. However, in all variants of this attack, and distinguishing this attack from other data collection methods, the attacker is not the intended recipient of the data stream. Unlike some other data leakage attacks, the attacker is observing explicit data channels (e.g. network traffic) and reading the content. This differs from attacks that collect more qualitative information, such as communication volume, not explicitly communicated via a data stream[3].

b. Data Alteration

[3] CAPEC (2010), CAPEC-117: Data Interception Attacks,
Available at: http://capec.mitre.org/data/definitions/117.html

This is one of the major problems regarding privacy of communications. It is essential to ensure that data cannot be modified or viewed in transit. The distributed environments in cyber space bring with them the possibility that a malicious third party can perpetrate a computer crime by tampering with data as it moves between sites[4]. In such attack, an unauthorized party on the network intercepts data in transit and the data is altered before its retransmission. An example of this is changing the dollar amount of a banking transaction from $100 to $10,000.

c. Data Stealing

This term is most widely used to describe the situation when information is illegally copied or taken from a business or other individual. Commonly, this information is theft from user such as passwords, social security numbers, credit card information, other personal information, or other confidential corporate information. Since this information is illegally obtained, it is used by the criminal for commission of crime as soon as possible in order to prevent from being prosecuted or trapped[5].

1.2. Crimes related with Network

In this kind of crime the criminal tries to interfere with the network. Network Interfering is done with the functioning of a computer network by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing network data. It may affect the functioning of service providers[6].

1.2. Crimes related with Malafide Access

a. Unauthorized Access

[4]Oracle (2003), Security Overviews, Available at: http://docs.oracle.com/cd/B13789_01/ network.101/b10777/overview.htm.

[5] Computer Hope (2012), Data Theft, Available at: http://www.computerhope.com/jargon/d/ datathef.htm.

[6] DSL Reports (2011), Network Sabotage, Available at: http://www.dslreports.com/forum/r26182468-Network-Sabotage-or-incompetent-managers-trying-to-

"Unauthorized Access" means access by a person who is not authorised to look towards the database of the computer system. The criminal after entering into the database without authorisation may afterwards misuse that data[7].

b. Virus spreading

Virus are the programs made by criminals with mala fide intention. These malicious software's attach itself to other software (virus, worms, Trojan Horse, Time bomb, Logic Bomb, etc. are examples of malicious software that destroys the system of the victim[8].

1.3. Other Related Crimes

a. Aiding and Abetting On-line Crimes

There are three elements present in cases of aiding and abetting charges against an individual. First out of them is that another person who committed the crime. Second, the individual being charged having knowledge of the crime or the principals' intent. Third, the individual provided some form of assistance to the principal. An accessory in legal terms is typically defined as a person who assists in the commission of a crime committed by another or others. In most cases, a person charged with aiding and abetting or accessory has knowledge of the crime either before or after its occurrence. A person who is aware of a crime before it occurs, and who gives some form of aid to those committing the crime, is known in legal terms as an "accessory before the fact."[9]

b. Forgery and Fraud:

This category includes fraud committed by the website host by creating a fake websites or with the help of technique of cross site encrypting. The victim gets trapped into the net of criminal and fraud is committed to him. It is very much difficult to identify such forgery and fraud in many cases are being reported on cyberspace worldwide which are based on concept of these crimes.

[7] IMDb (2012), Unauthorized Attacks, Available at: http://www.imdb.com/title/tt0373414/.
[8] Virus Glossary (2006), Virus Dissemination, Available at: http://www.virtualpune.com/citizencentre/html/cyber_crime_glossary.shtml
[9] 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

c. Content-Related Crimes:

The crimes like cyber sex, unsolicited commercial communications, cyber defamation and cyber threats are included under content-related offenses.

Such crimes have a major and long-lasting impact on the economic position of the country because the compensatory costs are to be paid to the victim is in millions of dollars per year which is a significant amount to change the state of un-developed or under-developed countries to developed countries[10].

Recently, India was also ranked as the 14th country in the world hosting phishing websites[11]. Additionally, the rapidly increasing call centres in India have created more space for cyber criminals in this field. The words of Prasun Sonwalkar[12] reflects the threat of cyber crime in India —India is fast emerging as a major hub of cyber crime as recession is driving computer-literate criminals to electronic scams, claimed a study by researchers at the University of Brighton. Most of the countries of the world are lacking of strict cyber laws in the nation and it includes many of the African countries which are lack of the cyber policies and laws[13]. Due to these reasons many of cyber criminals escape even after they are caught by the investigating authorities because of absence of proper law in the country where he's being arrested. Countries like Kenya, Nigeria,Tunisia, Tanzania etc. are almost free from the cyber laws and policies.

Restriction of cyber crimes is dependent on proper analysis of their behaviour and understanding of their impacts over various levels of society. Therefore, in the current manuscript a systematic understanding of cyber crimes and their impacts over society with the future trends of cyber crimes are tried to be explained.

II. Impacts of Cyber-Crime

[10] By Jessica Stanicon (2009), Available at: http://www.dynamicbusiness.com/articles/articles-news/one-infive-victims-of-cybercrime3907.html.
[11] India emerging as major cyber crime centre (2009), Available at: http://wegathernews.com/203/indiaemerging-as-major-cyber-crime-centre/
[12] PTI Contents (2009), India: A major hub for cybercrime, Available at: http://business.rediff.com/slideshow/2009/aug/20/slide-show-1-india-major-hub-for-cybercrime.htm
[13] Cyberlawtimes (2009), Available at: http://www.cyberlawtimes.com/forums/index.php?board =52.0

The organised crime group uses Internet for major fraud and theft activities. Many trends can be seen in which these white-collar crimes are involved. The Internet based crime has become more prevalent because criminals have now moved away from traditional methods of crime and it is easier for them to earn a lot of amount related with these crimes. As per the statistical data of police Department also, these crimes have been increased up to a large extent and this is in sync with the national trend resulting from increased computer use, online business, and geeky sophisticated criminals. As per the data collected in the year 2012, cyber-crime generated a higher payback than drug trafficking, and it is set to grow further as the use of technology expands in developing countries.

Some of the major impacts of these crimes are mentioned in detail here as under –

2.1. Potential Economic Impact

These crimes make a large economical impact because of involvement of losses in millions of dollars per year. The 2011 Norton Cyber crime disclosed that over 74 million people in the United States were victims of cyber crime in 2010. These criminal acts resulted in $32 billion in direct financial losses. It was further analysed that about 65% of adults that are online have been victims of such crimes per day[14].

Since the consumers today have been dependent on computers, networks and Internet database therefore they restored and preserved information on the Internet is used by the criminal and therefore risk of being subjected to victimisation becomes high[15]. Everyday, new attacks on the confidentiality, integrity, and availability of computer systems can be heard. This could range from the theft of personally identifiable information to denial of service attacks. As the economy increases its reliance on the internet, it is exposed to all the threats posed by cyber-criminals. Today talks are traded to Internet, purchases are made using plastic money, banking transactions can be done online, and many such other activities are carried out through Internet and all these instances consist of chances of financial fraud by

[14] 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/

[15] PTI Contents (2009), India: A major hub for cybercrime, Available at: http://business.rediff.com/slideshow/2009/aug/20/slide-show-1-india-major-hub-for-cybercrime.htm

cyber criminals and hence affect the economy. Similar the disturbance of international financial markets create big impact on international economic position. Hence any attack on cyberspace related with financial activities send shock waves outside of the market which is the source of the problem. The productivity today is also at risk. Attacks from worms and viruses etc. take productive time away from the user. Machines may be made to perform slow, networks are jammed and another attack are done to negative by the organisation activities. In addition to all these, the potential fraud committed against online shoppers during transactions can also be considered to make laws to the economic zone and the breach of trust against the consumer repercussions and bear going into more detail.

2.2. Impact on Market Value

The cyber crimes make a greater impact on market value of the country also. The economic impact of security breaches is of interest to companies trying to decide where to place their information security budget as well as for insurance companies‘that provide cyber-risk policies[16]. Micro stated that —physical damage is not restricted to physical destruction or harm of computer circuitry but includes loss of use and functionality[17]. These kinds of damages affect more severely as many firms rely on information systems in general and the Internet in particular to conduct their business. Due to these reasons also, many insurance company are bound to compensate businesses for the damage caused by such cyber attacks or other security breaches. As the characteristics of security breaches change, companies continually reassess their IS environment for threats[18]. However, assessing the financial loss from a potential IS security breach is a difficult step in the risk assessment process for the following reasons:

1. It is not possible for many organisations to quantify their financial losses due to security breaches[19].

---

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

[17] 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.

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

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

2. Due to lack of historical data, many security breaches are unreported. In similar situation, companies are reluctant to disclose these breaches due to management embarrassment, fear of future crimes[20], and fear of negative publicity[21]. There exist that competitors exploiting these attacks and to gain competitive advantage also[22].
3. Additionally, there is a fear of negative financial consequences resulting from public disclosure of security breach[23].

The assessment of risks mentioned above can be performed by considering measures connected with traditional accounting such as the Return on Investment (ROI) approach[24]. This is very difficult to accomplish such crimes because the number of security incidents is low and there are no sincere returns to accomplish it. Accounting-based measures such as ROI are also limited by the lack of time and resources necessary to conduct an accurate assessment of financial loss. Instead, companies 'IT resources are devoted to understanding the latest technologies and preventing future security threats[25]. Therefore it can be said that there is a need for a different approach to cover such security breaches. One such approach may be to capture the capital market's expectations of losses resulting from security breach. Such approaches much reasonable because companies are generally impacted more by the public relations exposure as compared to the attack itself[26]. Further the managers have an object to maximise their market value by investing in projects and increase the shareholder value and minimise the risk of loss.

2.3. Impact on Consumer trust

[20] 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

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

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

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

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

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

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

The consumers hold the major impact of market and breach of their trust amounts to a huge impact on economic position through cyberspace. Since such attackers enter into others 'space and try and break the logic of the page, the end customer visiting the concerned page will be frustrated and discouraged to use the said site on a long term basis. The disputed site is termed as fraudulent but the master mind criminal is not recognised as its main cause. This makes the loss of confidence in the customer and in the internet and its strengths. According to reports sponsored by the Better Business Bureau Online, over 80% of online shoppers cited security as a primary worry when conducting business over the Internet. About 75% of online shoppers terminate an online transaction when asked for the credit card information. It is also a perception that the Internet is widespread with credit card fraud and security hazards are growing. It can be seen as a serious problem for e-commerce. Also, any concern over the credibility of an e-business in terms of being unsafe or cluttered makes a shopper reluctant to transact business. Even the slightest perception of security risk on e-commerce seriously paralyse is the potential of business.

2.4. Effect 0n National Security

Today, most of the countries have advanced computer system for their military system. But Information Warfare, including network attack, exploitation, and defence, isn't a new national security challenge. And, since 9/11 it has gained some additional importance. The crimes of this level are been increasing because of low-cost, highly effectiveness and deniability to the attacker. Malware are being spread misinformation is also being spread with it. The Internet has 90 percent junk and 10 percent good security systems[27]. When the criminals find systems that are easy easily breakable they simply hack the system and the terrorists and criminals use information technology to execute the criminal activities. Because of advanced technology such crimes may be committed from any part of the world and therefore criminals find loopholes in the security system of the country to be targeted and perform the task from part of other country other than their own country to confuse the victim during investigation. The Internet has helped funding of cyber crimes by

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

means of fraudulent bank transactions, money transfer etc. in developed countries by which these crimes are done. Greater encryption technology is helping these criminal activities.

III. Suggestive Areas

Most people become victims of these at one time or another, but there are ways to avoid or deal with cyber crime by protecting yourself appropriately. There are the some ideas by which we can get protected from these crimes and lead safe life. Cyber crime threats rise each year because too many people are unaware of the security risks involved when using the Internet. The Internet has become an integral part of society. Users need to learn how to protect themselves from online theft. Cyber crime involves unauthorized access to computer when you unwittingly install malware like viruses, worms, spyware or trojans. Without realizing it, can find ourself the victim of identity theft when we are tricked into giving out information to online criminals. User awareness helps us prevent cyber crime and protect our security online.

There are some suggestive measures which may be used in order to fulfil the lacuna in present cyber system in terms of its legal aspects as well as technological aspects.[28] It will assist us so that we may overcome with the rapidly increasing crimes through online tools. These suggestive measures include alterations in current laws as well as stringency in e-security system. The basis of these suggestive measures is proverb **"Prevention is always better than cure".**

1) One should avoid disclosing any personal information to strangers via e-mail or while chatting.

2) One must avoid sending any photograph to strangers by online as misusing of photograph incidents increasing day by day.

3) An update Anti-virus software to guard against virus attacks should be used by all the net users and should also keep back up volumes so that one may not suffer data loss in case of virus contamination.

[28] http://www.ehow.com/how_4967690_prevent-cyber-crime.html

4) A person should never send his credit card number to any site that is not secured, to guard against frauds. Similarly, other personal details should also be protected.

5) It is always the parents who have to keep a watch on the sites that your children are accessing, to prevent any kind of harassment or depravation in children.

6) Web site owners should watch traffic and check any irregularity on the site. It is the responsibility of the web site owners to adopt some policy for preventing cyber crimes as number of internet users are growing day by day.

7) Web servers running public sites must be physically separately protected from internal corporate network.

8) It is better to use a security programmes by the body corporate to control information on sites.

9) IT department should pass certain guidelines and notifications for the protection of computer system and should also bring out with some more strict laws to breakdown the criminal activities relating to cyberspace.

10) As Cyber Crime is the major threat to all the countries worldwide, certain steps should be taken at the international level for preventing the cybercrime.

11) A complete justice must be provided to the victims of cyber crimes by way of compensatory remedy and offenders to be punished with highest type of punishment so that it will anticipate the criminals of cyber crime.

12) Poor e-security or internet security can result in the corruption of files and can enable criminals and others to access personal and financial information. E-security measures provide protection from unwanted intentional and unintentional intrusion into computers, file corruption and data loss.

13) The negative programs like viruses, Trojans, worms are responsible for damage of data or computer system whose implications may vary up to the

most dangerous situation. Various tips shown in previous chapters may be followed so that such crimes may be prevented. Over all , the awareness among the people is required.

14) The softwares, antivirus, antispyware and antimalware should be made so hard so that they could detect any kind of scam, spam and phishing tactics. Also, the applications used by users like e-mails, social networking sites, mobile applications, ATM applications and telecom applications should be able enough to prevent the user from victimisation.

15) The firewall system , which is used by all the operating systems, should be updated time to time so that the increasing tactics of hacking, virus, Trojans any such unwanted material may be prevented by the user even without his knowledge. This may be the one of best efforts which can be done by users as all of them are not computer savvy. Similar efforts may also done in case of other tools like plastic money, ATM machine, mobile phones, SIM cards etc. & all other devices operating on-line.

16) The pillars of e-commerce authentication, confidentiality, integrity & non repudiation should be strictly followed so that such transactions may not affect economic growth of the nation. It may be done in following ways-

- Authentication - The sender of the document must be identified precisely and without any possibility of fraud.
- Confidentiality – The contents of the message may not be scanned by unauthorised parties.
- Integrity - Changes made in messages without according remarks must be impossible.
- Non repudiation – The sender of message is directly connected to the contents of message (and the recipient cannot deny that the message is received).

17) Data encryption techniques must be used during data transmission so that it can't be easily decoded. Focus on awareness & learning techniques of user may be done.

18) When children are on the Net , the appropriate use of filtering software supported by adult supervision should be there and more public awareness is required for it.

19) False E-mail identity registration should be treated as an offence.

20) Use of Voice-recognizer, Filter Software and Caller ID for Protection against Unauthorized Access should be done.

21) Development of Cyber Forensics and Biometric Techniques is the need of the time and we also need to establish a Computer Crime Research and Development Centre.

22) Extradition Treaty is the need of the hour because most of the crimes committed outside India can't be prosecuted unless accused is brought in India by this treaty.

23) Regulation of Social Networking Sites is required at utmost speed as such sites are somehow related with many offences reported in one or other way.

24) It is also need for periodical reviewing of licenses of Internet Service Providers (ISPs) or such other administrative control on them by statute.

25) Computer and Cyber crime related education and awareness is required among all, from youth to senior citizen, from poor to rich, from non-user to computer professional & from common man to judicial officers.

26) Spam blocker should be turned on. Most Internet providers provide a spam blocking feature to prevent unwanted messages, such as fraudulent emails and phishing emails, from getting to inbox.

27) Person should avoid getting taken in by common scams, such as foreign lotteries, phony sweepstakes and similar methods used by cyber criminals to

get your personal information and money. If it sounds too good to be true, it probably is.

28) Make online payments only on website that have an encrypted connection. Websites that have a security certificate start with "https://" and not "http://". You can verify whether the website is secure by looking for the small padlock icon in your browser window.

29) Proper knowledge of Computer and Internet Safety is required for all because organized identity theft groups constantly try to remotely load spyware, malware, Trojan horses, and botnets on victim computers. These programs transmit the keystrokes and other stored computer files to suspects.

30) Home wireless computer network should always be encrypted and strong passwords should be used to protect against unauthorised access.

31) No one should respond to emails from financial institutions requiring an update of personal and banking information.

32) No one should open unknown attachments or download questionable software. No one should open attachments or download any software from sites in which there are chances of the crime exist. Criminals may offer you free music, antivirus protection, or other applications. If we fall for it and download this, spyware may be installed on our computer.

33) Although secure or encrypted transactions have an icon of a miniature lock that appears on the Web browser, highly skilled scammers can replicate the miniature lock on sites, giving the false impression of a secure site. For this reason, in addition to the miniature lock image, one should look at the URL address of the Web page, it should change from “http” to “https”. This indicates that the website is a secure site for you to input your personal information.

34) Privacy Screens on laptop should be used while travelling.

35) It is suggested that there should be awareness programs and a children’s corner on the State Police websites, social networking websites and web

browsers where Internet safety tips in simple language can be explained to minors and helpline number or e-mail addresses provided for, in case of any problem. Further, records of every cybercafé should be so maintained that any information can be opted from a centralised location.

36) In appropriate cases, police officers may carry out undercover cyber patrol operations to identify internet criminals, lure them by posing as minors and arrest them. The exercise should be done in accordance with Section 72 and Section 72 (A) of Information Technology Act, 2000.

37) Apart from legal provisions for search under Section 100 and 165 Cr. P. C., Section 80 of IT (Amendment) Act, empowering any police officer not below the rank of a Police Inspector for search, can also be used appropriately. “Cyber Crime Investigation Manual" published by Data Security Council of India is a useful book and may be referred to.

38) Whenever any case comes before investigating agencies which requires information or help from outside India, CBI Interpol Division may be approached and provision of Mutual Legal Assistance Treaties and Letter of Rogatories (LRs) may be used.

39) Wherever any material which is covered under Section 67, Section 67 A and Section 67 (B) of Information Technology Act, 2000 and seen on the Web, which is covered under Section 69 (A) of the IT Act under ‘Public Order’ or ‘preventing incitement to commissioning of cognizable offence’ in such cases, police may consider invoking provisions of IT Procedure and Safeguards for Blocking of Information by Public Rules, 2009. Provisions of Section 67 (C) of IT Act should be used for preservation of evidence by intermediaries.

40) There should be clear-cut guidelines regarding Internet safety being issued from the websites hosting online gaming or children centric contents. Those transmitting, publishing or storing obscene material in contravention with the provisions of Section 67, Section 67 (A), Section 69, Section 69 (A) and Section 69 (B) of the IT Act, must be acted against.

41) In appropriate cases, police should keep a watch and thereafter request, if desired, Social Networking sites to remove undesirable contents. Most frequently visited and popular sites should be audited time to time for security concerns. Many of these are being used either for compromising of systems or for luring and incitement of children, which should be strictly prevented.

42) There is considerable potential for resolving certain problems of Internet content, especially civil issues like defamatory libel and copyright infringement by using on-line mediation and arbitration procedures.

In the present era of rapid growth, information technology is encompassing all walks of life all over the world. The use of Computers is increasingly spreading, and more and more users are connecting to the internet. The internet is a source for almost anybody to access, manipulate and destroy other's information. The rapid development of the Internet and computer technology globally has also led to the growth of new forms of transnational crimes especially those which are internet related. These criminal activities directly relate to the use of computers, specifically illegal trespass into the computer system or database of another, manipulation or theft of stored data, or sabotage of systems and data. Characteristic feature of these crimes are that these crimes are considered as illegal, unethical or unauthorized behaviour of people relating to the automatic processing and transmission of data by the use of Computer Systems and Networks. These crimes have virtually no boundaries and may affect any country across the globe within a fraction of second. Ways of tackling cyber crimes through legislation may vary from one country to another, especially when cyber crimes occur within a specific national jurisdiction with different definition and socio-political environment.[29]

IV. Conclusion

This article put its eye not only on the understanding of the on-line crimes but also explains the impacts over the different levels of the society. This will surely help the community to secure all the online information which are not safe due to such

[29] Andrew Grant-Adamson, Cyber Crime, Mason Crest Publishers, 2003.

cyber crimes. The understanding of the behaviour 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 , 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.

References

[1.] Wow Essay (2009), Top Lycos Networks, Available at: http://www.wowessays.com/ dbase/ab2/ nyr90.shtml.

[2.] Bowen, Mace (2009), Computer Crime, Available at: http://www.guru.net/

[3.] CAPEC (2010), CAPEC-117: Data Interception Attacks, Available at: http://capec.mitre.org/data/definitions/117.html

[4.] Oracle (2003), Security Overviews, Available at: http://docs.oracle.com/cd/B13789_01/ network.101/b10777/overview.htm.

[5.] Computer Hope (2012), Data Theft, Available at: http://www.computerhope.com/jargon/d/ datathef.htm.

[6.] DSL Reports (2011), Network Sabotage, Available at: http://www.dslreports.com/forum/r26182468-Network-Sabotage-or-incompetent-managers-trying-to-

[7.] IMDb (2012), Unauthorized Attacks, Available at: http://www.imdb.com/title/tt0373414/.

[8.] Virus Glossary (2006), Virus Dissemination, Available at: http://www.virtualpune.com/citizencentre/html/cyber_crime_glossary.shtml

[9.] 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

[10.] Shantosh Rout (2008), Network Interferences, Available at: http://www.santoshraut.com/ forensic/cybercrime.htm

[11.] By Jessica Stanicon (2009), Available at: http://www.dynamicbusiness.com/articles/articles-news/one-infive-victims-of-cybercrime3907.html.

[12.] 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.
[13.] India emerging as major cyber crime centre (2009), Available at: http://wegathernews.com/ 203/indiaemerging-as-major-cyber-crime-centre/
[14.] PTI Contents (2009), India: A major hub for cybercrime, Available at: http://business.rediff.com/ slideshow/2009/aug/20/slide-show-1-india-major-hub-for-cybercrime.htm
[15.] 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
[16.] Newswise (2009), China Linked to 70 Percent of World's Spam, Says Computer Forensics Expert, Available at: http://www.newswise.com/articles/view/553655/
[17.] Cyberlawtimes (2009), Available at: http://www.cyberlawtimes.com/forums/index.php?board =52.0
[18.] 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/
[19.] Gordon, L. A. et al., 2003, A Framework for Using Insurance for Cyber-Risk Management, Communications of the ACM, 46(3): 81-85.
[20.] 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.
[21.] Kelly, B. J., 1999, Preserve, Protect, and Defend, Journal of Business Strategy, 20(5): 22-26.
[22.] Berinato, S. (2002), Enron IT: A take of Excess and Chaos, CIO.com, March 5 http://www.cio.com/executive/edit/030502_enron.html.
[23.] Power, R., 2001, 2001 CSI/FBI Computer Crime and Security Survey, Computer Security Issues and Trends, 7(1): 1-18.
[24.] 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
[25.] Sprecher, R., and M. Pertl, 1988, Intra-Industry Effects of the MGM Grand Fire, Quarterly Journal of Business and Economics, 27: 96-16.

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

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

[28.] D‘Amico, A., 2000, What Does a Computer Security Breach Really Cost?, The Sans Institute

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

[30.] 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

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

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

[33.] Stephen Northcutt et al. (2011), Security Predictions 2012 & 2013 - The Emerging Security Threat, Available at: http://www.sans.edu/research/security-laboratory/article/security-predict2011

[34] Hemraj Saini, Yerra Shankar Rao, T.C.Panda / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com. Vol. 2, Issue 2,Mar-Apr 2012, pp.202-209