International Journal of Web Technology
Volume: 04 Issue: 01 June 2015 Page No.53-57
ISSN: 2278-2389

A Study on the Cyber-Crime and Cyber Criminals: A Global Problem

Esther Ramdinmawii[1], Seema Ghisingh[2], Usha Mary Sharma[3]
[123]Department of CSE & IT, Don Bosco College of Engineering and Technology, Assam, India
Email- jamjagai@gmail.com, seema.ghising@gmail.com, ushamary.sharma@gmail.com

Abstract- Today, Cybercrime has caused lot of damages to individuals, organizations and even the Government. Cybercrime detection methods and classification methods have came up with varying levels of success for preventing and protecting data from such attacks. Several laws and methods have been introduced in order to prevent cybercrime and the penalties are laid down to the criminals. However, the study shows that there are many countries facing this problem even today and United States of America is leading with maximum damage due to the cybercrimes over the years. According to the recent survey carried out it was noticed that year 2013 saw the monetary damage of nearly 781.84 million U.S. dollars. This paper describes about the common areas where cybercrime usually occurs and the different types of cybercrimes that are committed today. The paper also shows the studies made on e-mail related crimes as email is the most common medium through which the cybercrimes occur. In addition, some of the case studies related to cybercrimes are also laid down.
Keywords- financial crimes, cyber stalking, telecommunication frauds, e-mail related crimes, cyber criminals, email spoofing, email bombing.

I. INTRODUCTION

The term crime is denoted as [1] an unlawful act which is punishable by a state. However, certain purposes have no statutory definition provided. Crime is also called as an offense or a criminal offense. It is harmful not only to some individual but also to the community or the state. [2] Cyber crime has nothing to do with the law enforced. According to the authors in [3], cyber is a prefix used to describe a person, thing or idea as a part of the computer and information age. [4]It involves computer or computer networks. A computer network is basically the collection of communicating nodes that helps in transferring data across. The nodes at any given time could be a computer, the laptop, smart phones etc. [4] Cybercrime encompasses any criminal act dealing with computers and networks. [5] It includes crime conducted through the Internet. The Internet is basically the network of networks used across for communication and sharing of data. [6]Cybercrime also known as the computer crime is the use of an instrument for illegal ends, such as [5] committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy.With the advancement of the Internet technologies like the 2G and 3G, the global village is effectively sharing and communicating vital data(s) across the network. However, there are some who are intentionally trying to track and extract the vital and confidential information illegally for their personal use or for the financial achievement and many more.

II. CYBER CRIME

[7]Cybercrime encompasses a wide range of crimes including stealing people's identity, fraud and financial crimes, [2] pornography, selling contraband items, downloading illegal files etc. According to the authors in [2] and [8], any crime involving a computer and Internet is called cyber crime. Some of the popular and alarming crimes in the cyber world are discussed below:

A. Financial Crimes

With the increasing demand of the on-line banking, the financial crimes have become very alarming. Financial crimes include credit card frauds, stealing money from on-line banks etc. The criminals of credit card fraud get information from their victims often by impersonating a Government official or people from financial organizations asking for their credit information. The victims fall prey to this without proper inquiries and give away their credit card information to these criminals. In this ways, criminals may steal their identity and the consequences are mostly financially damaging.

B. Cyber Pornography

[8]Pornographic websites which allow downloading of pornographic movies, videos and pictures, on-line pornography magazines (photos, writings etc.), all come under this category. [5]The study made by the UK Home Affairs Committee Report on Computer Pornography (House of Commons, 1994) says that "Computer pornography is a new horror" (House of Commons, 1994:5). The US Carnegie Mellon University is also one such institute that has made a wide range of study and collected evidences on child and computer pornography.

C. Drug Trafficking

[2] Drug traffickers contribute a major part of cyber crime to sell narcotics using the latest technologies for encrypting mails. [7] They arrange where and how to make the exchange, mostly using couriers. Since there is no personal communication between the buyer and dealer, these exchanges are more comfortable for intimidated people to buy illegal drugs and even other items.

D. Cyber Terrorism

[7]Terrorism acts which are committed in cyberspace are called cyber terrorism. Cyber terrorism may include a simple broadcast of information on the Internet about bomb attacks which may happen at a particular time in the future. [2] Cyber terrorists are people who threaten and coerce an individual, an organization or even a government by attacking

International Journal of Web Technology
Volume: 04 Issue: 01 June 2015 Page No.53-57
ISSN: 2278-2389

them through computers and networks for their personal, political or social benefits.

E. Online Gambling

[8]On-line gambling offered by thousands of websites that have their servers hosted abroad. These websites are the one of the most important sites for money launderers.

F. Cyber Stalking

[9] 'Stalking' as has been defined in Oxford dictionary, means "pursuing stealthily". Cyber stalking is following an individual's or organization's whereabouts on the Internet. These may include sending threatening or non-threatening messages on the victim's bulletin boards, which may be by social networking sites or even through e-mails. According to David Wall [2], one of the prevalent forms of Cybercrime is Cyber stalking. This is basically a crime where the individual is constantly harassed by another individual example, sending constant mails to any individual with unsuitable contents and threat messages.

G. E-mail Spoofing and Phishing Scams

Cyber criminals often spoof e-mails of known and unknown individuals. [9]E-mail spoofing basically means sending an e-mail from a source while it appears to have been sent from another e-mail. E-mail spoofing is a very common cause of monetary damages. [10]The act that attempts to obtain vital information like passwords, details of credit cards by pretending to be a trustworthy entity in an electronic company is called phishing. Phishing e-mails are likely to contain hyper-links to the sites containing malwares.

III. TYPES OF CYBER CRIME

There are different types of cyber crime today. But the eight most common ones are:

A. Theft in the Services of Telecommunication

[9] Individuals and criminal organizations can gain access to the switchboards (PBX) [11] of an organization's switchboard and obtain the access to their dial-in or dial-out circuits. This allows them to make free calls to any local or distant number. [10] Theft of telecommunication services has been one of the earliest forms of cyber crime and is considered to be a misdemeanor. The criminal is usually asked to pay a fine with a short amount of jail time.

B. Piracy of Telecommunication

[8] Digital technology today, has allowed the perfect reproduction of prints and dissemination of graphics, sound and other multimedia combinations. This has been an important concern to the owners of the copyrighted materials. When the creators of a particular work are not able to gain profit from their own creations, it leads to severe financial loss and a great effect on creative efforts generally.

C. Dissemination of Offensive Materials

[8][10]These are the materials that are thought to be objectionable and exist in the cyberspace. [8]It includes materials which are of sexually explicit in nature, racist propaganda, explosive objects and devices, and codes for fabrication of the incendiary devices. Telecommunication services are also commonly used to harass, threaten and intrude the communications from phone calls to contemporary manifestation of cyber stalking. Computer networks can also prove to be of use in furtherance-of extortion. [10] The type of materials used, the location of the criminal who is disseminating the materials, and the victim's location all define the amount of fines and penalties to be paid.

D. Laundering E-money and Evasion of Taxes

[8]For quite a while, electronic funds transfers have been assisting in hiding and transportation of crimes. The origin of ill-gotten gains will greatly be concealed by the emerging technologies today. Taxation authorities may easily conceal those legitimately derived income. Central bank supervision will be bypassed by the development of the informal banking institutions or the parallel banking systems. [11] There is no separate law for this type of crime committed using computer and a network, but it falls directly under the laws which cover these offenses in general.

E. Extortion, Terrorism and Electronic Vandalism

[8]Unlike before, the western society of industries is depending upon a complex data processing and the telecommunications systems. Hampering or damaging these systems can lead to destructive consequences. [11]Vandalism in general can be considered as the denial of service attacks, bot-nets, or several other harmful network attacks. Extortion is the act of demanding the cease of an attack or the refrain of initiating an attack by means of money. The penalties for computer vandalism differs greatly according to the amount of damages and losses it cause, whereas the penalties of extortion are covered by the laws and rules of this type of felony.

F. Fraud in Sales and Investments

[8]The use and development of applications in digital technology becomes more fraudulent and is bound to increase as the electronic commerce becomes more and more prevalent. Cyberspace has now availed a lot of investment opportunities like bonds or stocks, sale and leaseback of automatic teller machines, telephone lotteries etc. [11]Fraudsters may use a wide variety of tools to spread their information on the Internet. They may create fake websites to appear legalized. [12]According to U.S. Securities and Exchange Commission, some of the investment scams that are targeted on Americans are:

- High-return or "risk –free" investments,
- Pyramid Schemes and
- "Ponzi" schemes.

G. Illegal Interception of Telecoms Signals

[5]The great and fast development in telecommunications allows new opportunities for electronic eavesdropping. [8] It ranges from the activities of surveillance of an individual to industrial and political espionage. The existing laws today, does not prevent one from monitoring a computer radiation from a distance.

H. Fraud in Transfer of Electronic Funds

[8]Electronic transfer systems are proliferating, and the same goes with the risks that such type of transactions may be intercepted or diverted. [13] There is no doubt that the E-fund transfer system has sudden and wide acceptance globally. With the usage of electronic fund transfer system, there is no doubt that this system will enhance the risk. The transfer of funds over the Internet may be diverted by the hackers. E-transfer is highly vulnerable in terms of crimes such as thefts and frauds.

International Journal of Web Technology
Volume: 04 Issue: 01 June 2015 Page No.53-57
ISSN: 2278-2389

There is no doubt that the technology in business service has benefitted both the business and the consumers to a greater extend. However, there is a darker side of this technological advancement as well due to Cybercrimes. Even though the organizations are aware of the types of cybercrimes; it is actually very difficult for them to understand the capacity of cybercriminals. It is indeed quite challenging for the organizations to understand the cybercriminal's next target and the value of their target. By the time the organizations understand they were targeted, it is already late and the damage has already incurred. Even though, organizations are taking efforts to prevent such cybercrimes, yet they fall into the hands of the cybercriminals. The graph in Fig.1 shows [14] the statistics of the total amount of monetary damage caused by having cybercrime from 2001 to 2013. This statistics was reported to IC3. In the year 2001, the total amount of loss incurred was 17.8 million U.S. dollars. Year 2009 showed a hike of about 559.7 million U.S. dollars and later by 2013 the monetary damage grew to 781.84 million U.S. dollars which is certainly alarming.

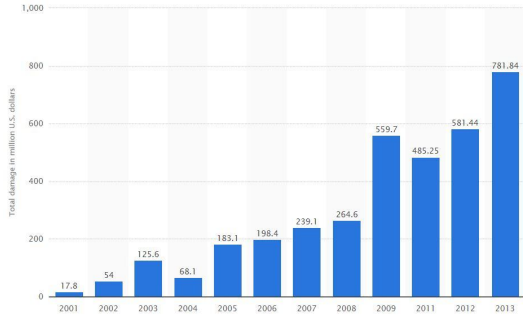

Figure 1. Amount of monetary damage caused by cyber crime from 2001 to 2013 (in million U.S. dollars) reported to the IC3[14]

Symantec – A famous Security Firm, carried out a detailed study and [15] has been able to find out the top ranked 20 countries that were facing and/or causing most of the activities of cybercrime. While gathering this list, Symantec observed and found the number of websites that host phishing sites. These phishing websites were designed in such a way that the end user could not distinguish the real sites from these fake ones. The design was made to trick users so that the computer user discloses their personal information or banking account information.

[15] In its further investigation, Symantec was successfully able to acquire the data including the number of bot-infected systems. These systems were meticulously controlled by the cybercriminals. The higher rate of cybercrime was found to be in the United States of America. This could be because the country is well facilitated with the broadband connection providing uninterrupted internet connection. Table 1 shows the countries that had been the victims of cybercrimes such as sharing malicious computer activities, spam messages, phishing etc. The table 1 shows, the six factors;

Share of malicious computer activity, Malicious code rank, Spam zombies rank, Phishing web site hosts rank, Bot rank and Attack origin, These factors contribute to authenticate its cybercrime ranking as conducted by Symantec security organization. [15]

TABLE I. COUNTRY LISTS WITH SIX CONTRIBUTING FACTORS TO CYBERCRIME [15]

Country	Share of Malicious Computer Activity	Malicious Code rank	Spam Zombies rank	Phishing website hosts rank	Bot rank	Attack origin rank
USA	23%	1	3	1	2	1
China	9%	2	4	6	1	2
Germany	6%	12	2	2	4	4
Britain	5%	4	10	5	9	3
Brazil	4%	16	1	16	5	9
Spam	4%	10	8	13	3	6
Italy	3%	11	6	14	6	8
France	3%	8	14	9	10	5
Turkey	3%	15	5	24	8	12
Poland	3%	23	9	8	7	17
India	3%	3	11	22	20	19
Russia	2%	18	7	7	17	14
Canada	2%	5	40	3	14	10
South Korea	2%	21	19	4	15	7
Taiwan	2%	11	21	12	11	15
Japan	2%	7	29	11	22	11
Mexico	2%	6	18	31	21	16
Argentina	1%	44	12	20	12	18
Australia	1%	14	37	17	27	13
Israel	1%	40	16	15	16	22

From the pie chart given at Fig. 2, it is quite evident that United States of America had suffered a lot due to cybercrime. The loss that had incurred has been tremendous other countries as well. China stands at the second position. Then the countries like Germany and Britain stood next, who had to bear the loss, occurred due to cybercrime. Countries like Brazil, Spain share almost the same percentage of cybercrime happening. Similarly, Italy, France, Turkey and Poland stands with the same percentage of cybercrime caused at their countries respectively. India share 3% of the malicious computer activities. Argentina, Australia and Israel share only 1% of the malicious computer activities. Mexico has the highest rank for hosting the phishing websites. Australia ranks the highest for bot- activities.

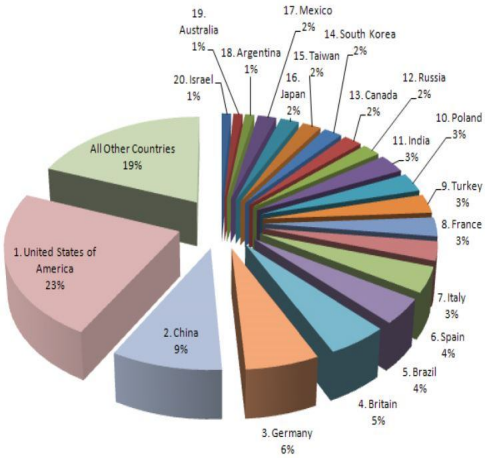

Figure 2. Top 20 Countries with Cyber Crime.[15]

International Journal of Web Technology
Volume: 04 Issue: 01 June 2015 Page No.53-57
ISSN: 2278-2389

IV. CRIMES ON THE INTERNET

[8]Crimes committed on the Internet by using the Internet and by means of the same, are mainly called Internet crimes. According to David Wall [2], the term Cybercrime symbolizes to the occurrence of the harmful activities done with the digital devices mainly over the Internet. The Cyber crime practically doesn't refer to the law and it is the concept that is created by the media to a greater extend. In general term computer crime is a crime that encompasses crimes such as phishing, bank robbery, credit card frauds, child pornography, kidnapping of children by means of chat rooms, creation or the distribution of viruses and so on. All these are facilitated crimes related to computers. Some crimes which are committed on the Internet are exposed to the world and some are hidden until they are perpetrated against someone or some company-

A. E-mail related crimes-

Electronic mail has rapidly become the world's most preferred means of communication. Across the globe, millions of e-mail messages are sent and received every day. E-mail, like any other means of communication, is also being misused by criminals. It has become a powerful tool for criminals due to the ease, the speed of transfer and its relative anonymity.

1) E-mail Spoofing: It is found in [8] that an e-mail that appears to originate from one source while it is actually being sent from another source is called e-mail spoofing. E-mail spoofing is usually committed by falsifying the e-mail address of the sender and/or the name. to send an e-mail, one usually has to enter the following informations:

The e-mail address of the receiver.

The e-mail addresses of the receivers (referred to as C for carbon copy).

The e-mail addresses of the persons who will receive a copy (referred as CC for carbon copy).

A subject for the message, which is a short title or a short description of the message.

2) E-mail Defamation: Cyber defamation or cyber slander often proves to be very dangerous and even fatal for anyone with even a little knowledge of computers to become blackmailers often by threatening their victims through e-mails.

3) E-mail Bombing: [8]E-mails account (in case of an individual) or servers (in case of a company) crashing due to a large amount of e-mails received by a victim is called e-mail bombing. This can easily be done by subscribing the victim's e-mail address to a large number of mailing lists which are the special interests group created to share and exchange data and information on a common topic of with one another through the help of e-mails. Mailing lists can generate a sufficient amount of e-mail traffics daily depending on the list. If a person unknowingly subscribes to multiple mailing lists, his incoming e-mail traffic becomes too large and can lead to the deletion of his account by his service provider.

4) Spreading Malicious Codes: The most common and fastest ways to spread malicious codes are often e-mails. With the help of e-mail, a virus called The Love Bug, spread to millions of computers within the 36 hours of its release from the Philippines. Trojans, viruses and worms or other computer contaminations are often binded with e-greeting cards which are e-mailed to unsuspecting persons.

5) E-mail Frauds: Financial crimes are commonly committed trough e-mail spoofing. It is becoming easier to assume an identity as well as to hide one's own identity. The criminal knows very well that there is minimum chance of his being identified.

6) Threats sent via e-mail: From [3], we find that the relative anonymity of e-mails offers technology savvy criminals a useful tool. Anyone with little knowledge of how to send an e-mail, can easily blackmail or threaten someone via e-mail without being identified.

V. WHO ARE CYBER CRIMINALS?

Cyber criminals range from a wide variety of age groups:

A. Kids(age group 9-16)

[9]Although it is hard to believe, kids can also be cyber criminals knowingly or unknowingly. The most amateur hackers comprises of teenagers. To these teenagers, it appears to be a matter of pride to be able to hack into a computer system or to a website. They may also commit the crimes without actually knowing that what they are doing is a crime.

B. Organized Hacktivists

[9] Hackers who come together with a particular motive are called hacktivists. These groups mostly operate on a political basis. While in other cases, [3] their motives may be social activism or religious activism or any other.

C. Disgruntled Employees

[9] It is hard to imagine how spiteful displeased employees can become. Up until now, these displeased employees have the option of having a strike against their employers. But now with the increase in dependence on computers and automation of processes, disgruntled employers can do a lot more harm to their employers by committing crimes via computers which can bring their entire system down.

D. Professional Hackers

[8] Extensive computerization has led to the storage of information in electronic form in business organizations. Hackers are employed by rival organizations to steal other industrial information and secrets which can prove to be beneficial for them. [9]If hacking can retrieve the required information from rival companies, the fact that physical presence required to gain access is considered unnecessary. This also leads to the temptation of companies hiring professional hackers to do their dirty jobs.

VI. CASE STUDY

Several cases of cybercrime have occurred recently in India. Some of these are described as follows:

A. Case I

An event occurred in April 2014, at Allahabad [16], India, where two under-graduate students, Vivek Kumar alias Kishan Dubey and Anand Mishra, were arrested for online fraud. These two students got hold of the ATM password of a man named Mahmood and had indulged themselves in credit card fraud amounting to Rs. 1.20 lakhs INR. The students were arrested and confessed to several of their frauds. According to

International Journal of Web Technology
Volume: 04 Issue: 01 June 2015 Page No.53-57
ISSN: 2278-2389

the Police, the two students would provide Delhi-based addresses for delivery of goods they had ordered online. Once the goods were delivered they would sell them to gullible buyers. This case had been registered under IPC Act, section 419 and 420, and under IT Act, section 66.

B. Case II

On the context of Cyber Stalking [17], in 2013, Police at Cyderabad arrested a youth, N Santosh Kumar alias Kiran, from Bangalore after he was charged for creating fake profile of a woman on Facebook. This youth also threatens the woman after she rejected his love proposal.Dejected, he made the fake profile and also chat with others in her name. He also made threat calls and send messages to the victim's family. A complaint was lodged by the victim's brother on August, 2013 with Cyber Crime Police and the accused was arrested.

C. Case III

This case is on E-mail Spoofing, [18] of late, one of the branch offices of the Global Trust Bank experienced a tough time. Many customers suddenly decided to withdraw their money and further close their own bank accounts. On investigating, it was discovered that someone had sent spoofed emails to these customers and others too mentioning the bank was soon getting closed as it is having tough time financially.

D. Case IV

[18] This case is about the E mail bombing (DoS); this case speaks about a foreigner; he was staying in Simla, India for many years almost thirty years. He wanted to benefit from a scheme introduced by the Simla Housing Board to buy land at a lower price. However, his application was not accepted as they mentioned that the scheme is meant only for citizens of India. On this, this man decided to retaliate. Subsequently, he sent out thousands of mails to the Simla Housing Board and repeatedly kept sending e-mails till their servers crashed.

VII. CONCLUSION

From this study made, it has been found that there are many ways and means through which an individual can commit crimes on cyber space. Cyber crimes are an offense and are punishable by law. In section 2, we have seen a brief discussion of the enlarging areas of cyber crimes. In section 3, we have seen the common types and areas where cyber crime occurs very frequently. We have also discussed the consequences of cyber crime that are causing tremendous financial losses in many countries, especially in the areas of sales and investments. Different fines and penalties have been laid down for this category of crime. Section 4 discusses about the different crimes on the net that are related to electronic mails. These crimes involve spoofing of mail, e-mail bombing and spreading malicious codes via e-mails. Furthermore, we have seen the different cyber criminals, ranging from the most amateur teenage hackers to the professional hackers that are often hired by rival organizations for hacking the into other company's system.

It is therefore very important for every individual to be aware of these crimes and remain alert to avoid any loss. To ensure justice to the victims and punish the criminals, the judiciary has come up with some laws known as Cyber Laws. Hence, it is advisable to each and every individual to know these laws. Besides, the cybercrime cannot be simply called as a Technological problem. Instead, it is an Approach based problem because it is not the computers that are harming and attacking the organizations instead it is the humans who are exploiting the technology to cause the damage. Therefore, it is we who need to be alert to figure out the different approaches that such criminals can take. There is a need to have intellectual mindset to sense such situation that may lead to such damages. The solution to such crimes cannot be simply based on the technology. The technologies can just be one such weapon to track and put a break to such activities to some extent.

[19]

REFERENCES

[1] en.wikipedia.org/wiki/Crime
[2] David Wall, "Cyber crimes and Internet", Crime and the Internet, by David S. Wall. ISBN 0-203-164504 ISBN 0-203-164504, Page no.1
[3] searchsoa.techtarget.com/definition/cyber
[4] www.merriam-webster.com/dictionary/cyber
[5] Bela Bonita Chatterjee, "Last of the rainmacs? Thinking about pornography in cyber space", Crime and the Internet, by David S. Wall. ISBN 0-203-164504, Page no.- 74.
[6] www.webopedia.com/TERM/C/cyber_crime.h ml
[7] www.britannica.com/EBchecked/topic/130595/ Cybercrime
[8] http://en.wikipedia.org/wiki/Computer_crime
[9] Gurjeet Singh and Jatinder Singh, "Investigation Tools for Cybercrime", International Journal of Computer, ISSN 0974-2247, Volume 4 Number 3, (2013) pp.141-154.
[10]en.wikipedia.org/wiki/Phishing
[11]www.ehow.com/facts_5144661_types_cyberc rime_penalties.html
[12]http://www.myretirementpaycheck.org/fraud/common-types-of-fraud.aspx
[13]Peter Grabosky and Russell Smith, "Telecommunication fraud in the digital age: The convergence of technologies", Crime and the Internet, by David S. Wall. ISBN 0-203-164504,Page no.29.
[14]http://www.statista.com/statistics/267132/total-damage-caused-by-by-cyber-crime-in-the-us/
[15]http://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/
[16]http://timesofindia.indiatimes.com/city/allahabad/Two-students-held-for-cyber-fraud/articleshow/34304971.cms
[17]http://ibnlive.in.com/news/youth-arrested-for-making-fake-facebook-profile-of-woman/418501-62-127.html
[18]http://satheeshgnair.blogspot.in/2009/06/selected-case-studies-on-cyber-crime.html#Email_spoofing_ 329149830155074