A Study on Cyber Crimes in Digital World

J. Vanathi
[1](Computer Science Department, T.S.Narayanaswami College of Arts & Science/ University of Madras ,India)
Email: vanathi_satish96@yahoo.com

S. Jayaprasanna
[2](Computer Science Department, T.S.Narayanaswami College of Arts & Science/ University of Madras ,India)
Email:aashisrikrish@gmail.com

Abstract--This paper puts forward the collective knowledge of Cyber crimes prevalent in Digital world to create awareness in our younger generation . I n an alarming trend many young and un employed youth are turning into crime. This paper focuses on the various crimes that take place in Cyberspace and the Laws pertaining to it . The cyber crimes rate in India and also the prevention measures to be implemented are discussed so that the young generation will protect themselves from being a victim of cyber crime. The inevitable uses of Internet in day to day life have increased the Cyber crimes.

Keywords*: Computer Forensics, Cyber security, Cyber-stalking, Phishing, Web jacking.*

*****

1. Introduction

Forensics is the term given to an investigation of a crime using scientific means. It is also used as the name of the application of scientific knowledge to legal matters. Forensic science has developed over the past 300 years or so, and its processes continue to improve and evolve today as science and technology find better and more accurate techniques. In 1929 the first American forensic lab was created in Los Angeles by the police department.

1.1 Computer Forensics

Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. Forensic investigators typically follow a standard set of procedures: After physically isolating the device in question to make sure it cannot be accidentally contaminated, investigators make a digital copy of the device's storage media. Once the original media has been copied, it is locked in a safe or other secure facility to maintain its pristine
condition. All investigation is done on the digital copy. The Internet history, web-based email, lost or deleted files, logging and registry files are examples of data the forensic accountant can utilize as evidence in their engagements by using the digital forensic techniques. There are four important components in Computer Forensics. They are

- Identifying
- Preserving
- Analysing
- Presenting

The advent of computers, internet and mobile phones and other high technology devices has led to the dramatic increase in white collar crimes worldwide. International trends have shown that there is an exponential increase in Cyber Crime with an increase in the availability of technology.

2. Cyber Crime

Cyber Crime is the use of computers and internet by criminals to perpetrate fraud and other crimes against consumer companies and consumers. Cyber crime is a legal wrong that can be followed by criminal proceedings which may result into punishment. Cyber criminal is a person who commits cyber crime. The cyber criminals may be children , adolescents they may be hackers, discontented employees, cheaters.

The first recorded cyber crime took place in the year 1820. In 1820 a textile manufacturer in France produced the loom, this device allowed the repetition of series in the weaving of special fabrics. This resulted in a fear amongst the employees that their employment and livelihood were being threatened. They committed acts of sabotage to discourage the owner from further use of technology. This is the first recorded cyber crime.

2.1 Reasons for Cyber crime

- Capacity to store data in comparatively small space.
- Easy to Access.
- Negligence
- Loss of Evidence
- Complex

3. Cyber Crime Classification

The subject of cyber crime may be broadly classified under the following groups.

- **Against Individuals.**
  - Harassment via e-mails.
  - Email spoofing
  - Defamation
  - Cheating & Fraud
  - Internet time Thefts

- Cyber-stalking

➢ **Against Organizations**.

- Possession of Unauthorized information.
- Cyber terrorism against the Government organization
- Unauthorized control over Computers.

➢ **Against Society**

- Pornography
- Trafficking
- Forgery
- Online Gambling.

3.1 Modes of Cyber Crimes:

- **Hacking**: It means unauthorized attempts to bypass the security mechanisms of an informationSystem or network. Hacker is a person who enjoys modifying and subverting systems.Hacking is possible because of free tools available on the Internet like Ping of Death, Netstat live, Ophcrack etc.
- **Data Theft** :Theft may be either by appropriating the data physically or by tampering them through virtual medium. The type of information illegally copied is user information such passwords, credit card information and other personal information.
- **E-mail Bombing:** E-mail bomb is a form of net abuse consisting of sending huge volumes of e-mail to an address in an attempt to overflow the mailbox where the email address is hosted in a denial-of-service attack. The email bomb can also cause serious damage such as system crashes and loss of Internet connectivity.
- **Denial of Service Attack:** DOS attacks involves flooding a computer with more requests than it **can** handle. This causes the computer to crash and **results** authorized users being unable to access the service offered by the computer. DOS attacks have blocked out websites like Amazon , CNN, Yahoo and eBay.
- **Web Jacking:** It takes place when a hacker forcefully gains control of a website by cracking the password. The actual owner does not have any control over the website but the hacker can change the contents of the websites. The Gold Fish case is an example of web jacking in which the site was hacked and the information related to Gold Fish was changed.
- **Email Spoofing :** It is sending an e-mail to another person so that it appears that the e-mail was by someone else. This technique is used by hackers to fraudulently send e-mail messages. Hackers use this method to disguise the actual email address from which phishing and spam messages are sent .
- **Phishing :** It is the criminally fraudulent process of attempting to acquire sensitive information such as usernames , passwords and credit card details by masquerading as a trust worthy entity in an electronic communication. Phishers attempt to steal your personal information by gaining access to users information by just logging into their account. Most of the Indian Banks are exposed to Phishing attacks.
- **Cyber Terrorism**: Any act of any person on the computer or network which threatens unity , sovereignity and security of the state can be called as cyber terrorism. Cyber terrorists use various tools such as Hacking , Cryptography , Virus , DOS attacks to unleash their terrorism.
- **Online Gambling** : Gaming is the act or practice of gambling on a game of chance and there is no skill involved in it. There are numerous websites that offer online GamblingOnline Gambling is legalised in several countries so the owners of the websites are safe in their home countries. The law related to gambling is applicable to online gambling also.
- **Child Pornography :** It refers to images or films and in some cases writings, depicting sexually explicit activities involving a child. The distribution of images on the internet is done easily through websites, chat , email and instant messaging. To report an incident involving child pornography, contact the website www.cybertipline.com operated by National center for Missing and Exploited children. This center will immediately forward the case to Law enforcement agency for further action.

4. Cyber Crimes in India

The National Crime Records Bureau (NCRB) have reported that 681 cyber crime related cases have been registered in Maharashtra in the year 2013 which has recorded a 44.6 percent rise in cyber crimes than the previous year.Under the new IT ACT in India the 3 states Maharashtra Karnataka and Andhra Pradesh (undivided) have occupied the top positions in cyber related crimes . The IT hub Pune has seen 97 cyber crimes in the year 2013.

Andhra Pradesh have registered 635 cases in 2013 which has seen a 48 percent increase compared to2012. Visakhapatnam has recorded 173 cases and Hyderabad has recorded 159 cases in the year 2013.In the state of Karnataka the cases registered in 2013 are 513 which is 24.5 per cent rise than the year 2012. The Bangalore City has

registered 399 cases in 2013 which has seen the highest number of cases in 2013 .The fourth place in cyber crimes is bagged by Uttar Pradesh which has recorded 372 cases which has witnessed a sharp rise of 81.5 percent in one year. The fifth place goes to Kerala state which has registered 349 cases in the year 2013. Compared to other bigger states very few cyber crimes have been registered in Tamil Nadu which amounts to 54 cases in 2013.

In the year 2013 Bihar have registered 23 cases . Gujarat have registered 61 cases and Odisha have registered 63 cases in the year 2013.

The Northern states of Mizoram , Nagaland and Sikkim have not seen a single case registered in Cyber crime in 2013. The Pink city Jaipur has seen 110 cyber crimes registered in 2013. In Kolkata nearly 84 cases have been registered in 2013. Our National Capital Delhi has recorded 131 cyber crimes in 2013 which has a sharp rise of 72.4 per cent compared to 2012. Other union territories Lakshadweep, Dadra Nagar and Haveli have not seen a single case of cyber crime in 2013.

Against the backdrop of rising incidents of hacking of military networks, Defence Minister AK Antony in his speech has said cyber space was the new domain of war and asked top Army brass to ensure security of critical information infrastructure of the force. He said rapid growth and dependence on information and communication networks had positioned the cyber world and space as the new domains of fighting a war. Hence, ensuring fool proof cyber security for information infrastructure would be a critical requirement for safer India.[12]

5. Information Act 2000

Information technology is one of the important law relating to Indian cyber laws. It had passed in Indian parliament in 2000. This act is helpful to promote business with the help of internet. It also set of rules and regulations which apply on any electronic business transaction. Due to increasing crime in cyber space, Govt. of India understood the problems of internet user and for safeguarding the interest of internet users, this act was made. The following are its main objectives and scope:-

5.1 Objectives :

1. It is objective of I.T. Act 2000 to give legal recognition to any transaction which is done by electronic way or use of internet.
2. To give legal recognition to digital signature for accepting any agreement via computer.
3. To provide facility of filling document online relating to school admission or registration in employment exchange.
4. According to I.T. Act 2000, any company can store their data in electronic storage.
5. To stop computer crime and protect privacy of internet users.
6. To give legal recognition for keeping books of accounts by bankers and other companies in electronic form.
7. To make more power to IPO, RBI and Indian Evidence act for restricting electronic crime.

5.2 Scope :

Every electronic information is under the scope of I.T. Act 2000 but following electronic transaction is not under I.T. Act 2000.

1. Information technology act 2000 is not applicable on the attestation for creating trust via electronic way. Physical attestation is must.
2. I.T. Act 2000 is not applicable on the attestation for making will of any body. Physical attestation by two witnesses is must.
3. A contract of sale of any immovable property.
4. Attestation for giving power of attorney of property is not possible via electronic record.[7]

5.3 Merits of I.T. Act 2000

1. Helpful to promote e-commerce
   - Email is valid
   - Digital signature is valid.
   - Payment via credit card is valid
   - Online contract is valid .
2. Enhance the corporate business
3. Filling online forms
4. High penalty for cyber crime

5.4 Demerit of I.T. Act 2000

1. Infringement of copyright has not been included in this law.
2. No protection for domain names.
3. The act is not applicable on the power of attorney, trusts and will.
4. Act is silent on taxation.
5. No, provision of payment of stamp duty on electronic documents.

5.5 Amendment IT Act 2008

The Information Technology Amendment Act, 2008 (IT Act 2008) is a substantial addition to India's Information Technology Act (ITA-2000). The IT Amendment Act was passed by the Indian Parliament in October 2008 and came into force a year later . The Act is administered by the Indian Computer Emergency Response Team.

Changes in the Amendment include: redefining terms such as "communication device" to reflect current use,validating electronic signatures and contracts, making the owner of a given IP address responsible for content accessed or

distributed through it; and making corporations responsible for implementing effective data security practices and liable for breaches.

5.6 Demerit of I.T. Act 2008

The Amendment has been criticized for decreasing the penalties for a few cybercrimes and for lacking sufficient safeguards to guard the civil rights of people.

6. Prevention for Cyber Crimes.

Prevention is always better than cure. It is essential thus that you just have sturdy Cyber security that protects your vital assets , clients details and your operational systems. Cyber security, which can be defined as the protection of systems, networks and data in cyber space,. Cyber space is unregulated and cyber criminals have a range of ways in which to attack organisations. It is essential therefore that you have robust cyber security that protects your critical assets, customer details and your operating systems. The three fundamental domains of effective cyber security are people , process and technology.

- Take Caution while sending photographs online particularly to strangers and friends as they could misuse the photos.
- Vital information should be kept as back up files for loss of data by virus.
- Credit card information must not be unconcealed to any website that is not secured .
- Use of firewalls is always beneficial.
- Avoid revealing personal information on the net to forestall cyber stalking.
- To prevent virus attacks guard your system with latest and updated antivirus software.
- Website owners ought to watch traffic and check any irregularity on the positioning.
- Audit systems and check logs to assist in detecting and tracing an intruder.
- Ensure that your browser's cache is cleared after an online transaction.
- Don't take anything from the Internet , or anywhere else , because it is almost always copyrighted.
- Save your file in ASCII or RTF format when sharing your documents with others to reduce the risk of transmitting micro viruses.
- Turn your computer off or on standby when not in use.
- For each system the user uses should have a password.
- Use advanced techniques like encryption , anonymous browsing, virtualization software , etc.

7. Challenges Faced in Cyber Crime.

- Bad guys just breach the law whereas good guys have to secure everything on every occasion..
- Insider frauds square measure tougher to notice than outsiders.
- Encryption is not making life simpler .
- Inadequate in-house manpower or skills to investigate/examine.
- Speed at which evidence is examined.
- Allign company policies with IT ACT and different GR compliances.
- Multi Country Jurisdiction and Treaties are not helping .
- Most of the time we think Fraud will not happen to us.

8. Conclusions

In a world where technology is growing rapidly, crimes in Computers are on the rise as well. Governments and Enterprises are spending millions of money each year to ensure that their information, Infrastructure , networks and data are properly protected against cyber crimes. Internet is being widely used for information, education, entertainment and socialization by younger generation .They have become addicts to social networking sites and are prone to be victims of cyber crimes. Our Indian Universities and Schools should introduce a subject on Cyber Crime awareness to our students to educate them .The parents and teachers should instill moral values in our children to be away from evil deeds . The awareness about cyber crimes should mainly be focused on rural children as they have less exposure than urban children. This would be an eye openner to the students to protect themselves from being a victim of cyber crimes. The future citizens have to bring a change in the society against cyber crimes especially cyber terrorism and safe guard our country like army personnel. Cyber security of India must be strengthened at the policy and legal fronts so that there is a holistic growth and development in this crucial field.

References

[1] Ashish Pandey : Cyber Crimes Detention and Prevention.
[2] Apurba Kumar Roy : Role of Cyber Law and its usefulness in Indian IT Industry
[3] Charles P. Pfleeger : Security in Computing.
[4] Edward Amorso : Fundamentals of Computer Security Technology.
[5] K. Rama Subramaniam : Cyber Crimes Trends to Watch .
[6] Prashant Malli : Cyber Law & Cyber Crimes.
[7] www.cyberlawportal.com
[8] http://www.cylab.cmu.edu/
[9] www.cisecurity.org
[10] www.cca,gov.in
[11] https://sites.google.com/site/cybercrimezbd/cybercrime-classified
[12] http://ibnlive.in.com/news/cyber-crimes