Cyber Crime: Threat, Prevention and Privacy

Patel Yagneshi B.

***Abstract* -** Privacy is a concern both for individuals and for society. Nowadays, Cybercrimes are responsible for the interruption of normal computer functions. Frequency of cyber crimes has increased over the last decade. Since users of computer system and internet are increasing worldwide in large number day by day. These crimes may be the conjunction of three factors: motivation, opportunity and the absence of guardianship. Understanding the threat of cybercrimes is a very important issue because technology holds a great impact on our society as a whole. This paper provides several aspects of Cybercrimes: the definition, reasons, methods, affect, and prevention. The purpose of this paper is to educate individuals about cybercrimes. It is necessary to keep balance between cyber-crime prevention and to ensure privacy. However, it is unclear to what extent this is possible using the ICTs available today. Still certain precaution should be taken by all of us while using the internet that will assist in challenging major threat of Cyber Crime.

I. INTRODUCTION

In our modern technology-driven age, it is very difficult to keep our personal information private. Details of data can be available to public databases due to interconnectivity. Technology continues make our daily lives easy; however, one of the main dangers of using technology is the threat of cybercrimes. Over the past twenty years, unscrupulous computer users have continued to use the computer to commit crimes.

Common internet users may be unaware of cybercrimes and due to this some innocent users fall victim to cybercrimes. These users do not know how they can protect themselves against such threats .When confidential information is lost or interrupted by improperly, it gives way to crimes such as hacking, e-mail bombing, DOS attacks, information theft, cyber terrorism and many more crimes which occur across borders.

It is important that civilians, law officials, and other associates of the justice system are well-informed about cybercrimes to reduce the threat. We have to look at security technologies and proposed cyber-crime prevention and methods.

II. WHAT IS CYBER CRIME

Cybercrime indicates to any illegal activities using or against computer systems, networks, and the internet. Although, there is no standard global definition.

It can include anything like downloading illegal music files, stealing millions of dollars from online bank accounts, spreading viruses on other computers etc.

III. REASONS OF CYBERCRIMES

There are many reasons for cyber-criminals to commit cyber-crime. Some of them are:

- Social Recognition: This is generally committed by youngsters. They just want to be famous among the media. They do not mean to hurt anyone in particular. They create some virus.
- Greed, Power, Revenge: These are career criminals and dangerous who are ready to commit any type of crime. They want to make quick money. They started the child pornography and attack on e-commerce sites to damage data like fraud with banking data. Sometimes they sell of the code to competitors.
- Fight: Cyber-terrorists come into this group. They are most dangerous. Their Primary goal is not just money but sending threat mails, destroying data stored in government information. The most wanted cyber-terrorist is Osama Bin Laden who is said to "use stereography to hide secret messages within pictures.
- Motivation: Growth in connectivity of computing and communications creates opportunities for criminals. As the internet becomes increasingly a medium of commerce, it will become increasingly a medium of fraud.

IV. METHODS OF COMMITTING

- Denial-of-Service (DOS): This attack makes a computer resource unavailable to its intended users and makes it functionally inefficient. E.g. Amazon, Yahoo, in November, 2010 wikileaks.org got a DoS attack.
- Malware or Malicious Software: It refers to programs such as viruses and worms that try to exploit computer systems or networks primary to business disruption, leakage of sensitive data, or unauthorized access to system resources. E.g. love bug virus, which affected at least 5 % of the computers around the world.
- Software and Information Piracy: It refers to misuse of copyright material and software.
- Industrial Espionage: Corporate rivals illegally access confidential information for competitive advantage, gain financial information, or misuse trade secrets.
- Cyber Extortion: It refers manipulating website links, or the threat of leaking customer or financial data.
- Spear Phishing: It refers to targeted of highly personalized bogus e-mails, aimed at a specific individual or organization.
- Spoofing: It refers to fooling people into entering personal details into a fake website.

- E-Mail Spoofing: A spoofed e-mail may be said to be one, which misrepresents its origin. It shows its origin to be different from which actually it originates.
- SMS Spoofing: Unwanted uninvited messages. Here a offender steals identity of another person in the form of mobile phone number and sending SMS via internet and receiver gets the SMS from the mobile phone number of the victim.
- Defamation: It involves any person with intent to lower down the person by hacking his mail account and sending some mails with using vulgar language to unknown persons mail account.
- Purchase Fraud: It refers to selling products through online channels which are never shipped.
- Identity Theft: It refers to obtaining personal data from individuals—such as social security number, address, or bank account details—which can be misused to open new accounts or obtain services in the name of the victim.
- Theft from Business: It refers to stealing revenue directly from businesses using online channels; for example, obtaining access to a firm's accounts and transferring the money illegally.
- Intellectual Property (IP) Theft: It involves stealing ideas, designs, specifications, trade secrets, or process methodologies.
- Fiscal Fraud: It describes fraud against the government, often through attacking government online channels, and includes theft, such as fraudulent claims for benefits, and evading taxes.
- Web jacking: This is where the hacker obtains access and can control web site of another person, where he or she can destroy or alter the information on the sites they see fit to them. Example was MIT (Ministry of Information Technology) was hacked by the Pakistani hackers whereas another was the 'gold fish' case, site was hacked.
- Cyber Squatting: It involves two persons claiming for the same Domain Name either by claiming that they had registered the name first on by right of using it before the other or using something similar to that previously. For example two similar names i.e. www.yahoo.com and www.yahhoo.com.
- Internet Time Thefts: Basically, Internet time theft comes under hacking. It is the use by an unauthorized person, of the Internet hours paid for by another person. The person who gets access to someone else's ISP user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the other person's knowledge.

V. AFFECT

There is tremendous rise in popularity of social media over the past ten years. As the Internet is an open medium, people create, and share their own information via conversations on blogs and sharing photos or videos on social networking websites like facebook, twitter etc. People use social media to advertise, recruit new employees, and maintain partnerships. Cyber criminals find the identity of interested peoples. They apply two ways - phishing and harming. They attract users via fake websites and asked to enter personal information like login information, phone numbers, addresses, credit card numbers, bank account numbers, and other information. The employee may, click on the message without thinking a second thought, and his computer can be hijacked. Cybercasing uses the Internet to determine the location of a desired victim using any available resource. In 2008, hackers sent messages to Facebook users stating, "Hey, I got a new Facebook account. I'm going to delete this one, so add my new profile." Upon clicking the hyperlink to add their friend's new account, the users were sent to a phishing page that was designed to collect their user information. The page looked identical to a Facebook® login page; however, is one of the signs of a phishing page. However, most people did not recognize this, and potentially thousands of Facebook® users had their accounts compromised by giving away their usernames and passwords.

VI. PREVENTION

Prevention of Cyber Crime is always better than cure. Authentication technologies have become essential which reduce the opportunity to commit computer-related crime.

- Most internet browsers email service, and Internet providers provide a spam-blocking feature to prevent fraudulent emails and phishing emails. However, every user must install and keep update of antivirus programs, firewalls. One should avoid disclosing any personal information to strangers, the person whom they don't know, via e-mail or while chatting or any social networking site.
- Encryption is good method to hide data like password and credit card information from unauthorized person. Encryption software runs your data through encryption algorithms to make it unintelligible to anyone who tries to hack into your computer.
- Avoid being susceptible to common frauds, such as letter asking for your help in placing large sums of money in overseas bank accounts, foreign lotteries.
- Type the address of your social networking site directly into your browser. Don't click a link to your site through email or another website because if you may enter your account name and password into a fake site, your personal information can be stolen.
- Educate children about the proper use of the computer and internet and monitor their online activities at home and school. A wise thing to is to use parental control software that limits the type of sites the user can gain access to. In schools, there should be restricted websites.
- Turn the geotagging feature off.
- Be careful about installing extras on your site. Many social networking sites allow you to download third-

party applications that let you do more with your personal page. Criminals sometimes use these applications to steal your personal information.

- United States Federal Government has been using data mining techniques to trying to detect terrorist's patterns and activities.
- Companies should work with a team of dedicated IT security experts who are knowledgeable and experienced with IT security. This can be an internal team or an external partner. Company should enhance employee knowledge by giving them training about awareness of the security threats like social engineering, tampering, and fraud. Companies should encrypt their sensitive data with AES encryption. Companies should also perform vulnerability scan of the external and internal network.
- Watermarking or fingerprinting digital data using steganographic techniques to help prove authorship or copyright infringements.
- Unilateral security options include secure portable devices, encryption of locally stored data, data concealment, watermarking and use of open source or certified software.
- Bilateral technologies include tools for negotiating security mechanisms and cryptographic and steganographic mechanisms for securing content.
- Trilateral technologies can be used if a third party is involved to fulfil a specific task for the other participating parties. A public-key infrastructure (PKI) to provide users with certified public keys of other users to test their digital signatures and to give users the ability to revoke their own public key if the corresponding private key has been compromised.
- In the modern cyber technology world it is very much necessary to make cyber law stricter in the case of cyber terrorism and hackers.
- Insurers must offer a specialized insurance policy to allow companies to transfer the risk arising from cybercrime. Insurance firms can only provide cover against cybercrime losses for which financial cost estimation can be achieved. It may be cover information asset damage including damage to the data, software, and systems of an organization. It protects against claims for losses from another organization or individuals.

VII. CONCLUSION

In conclusion, it is not easy to reduce cybercrime from the cyber-space. Even the well-prepared IT department sometimes fail to protect a company from a hacker. However, there are relatively simple measures that businesses can immediately implement to better protect their data. Individuals and businesses need to make sure they are educated about prevention from cybercrimes. Organizations should focus on implementing cyber-security plans addressing people, process and technology to ensure about integrity and confidentially of stored information. There is a desperate need for countries on a global scale to come together and decide on what constitute a cybercrime, and develop ways in which to persecute criminals across different countries. There is a need to convey modifications in the Information Technology Act so it can be more effective to fight cybercrimes.

VIII. REFERENCES

[1] http://www.esecurityplanet.com/trends/article.php
[2] http://www.haltabuse.org
[3] www.newworldencyclopedia.org/entry/Cybercrime
[4] www.bukisa.com/articles/206_internet-security-concepts
[5] http://en.wikipedia.org/wiki/Computer_crime
[6] http://www.wisegeek.com/what-is-cybercrime.htm
[7] http://www.internetfraud.usdoj.gov
[8] http://www.cpsr.org/cpsr/privacy/communications/wiretap/electronic_commun_privacy_act
[9] http://www.brighthub.com/internet/security-privacy/articles/65042.aspx
[10] http://www.securityweek.com/wikileaks-under-denial-service-attack-ddos
[11] http://crimesatcyber.blogspot.com
[12] http://news.softpedia.com/news/Internet-Fraud-384.shtml
[13] http://www.cyberlawindia.com
[14] http://ieeexplore.ieee.org/xpl/freeabs_all.jsp
[15] "How Cyber Insurance Might Ease Your (Network) Insecurity", Microsoft, http://www.microsoft.com/business/en-us/resources/ArticleReader/website/default.aspx
[16] "How Will You Survive a Data Security Breach" http://www.chubb.com/businesses/csi/chubb10600.pdf
[17] "How to recognize phishing email messages, links, or phone calls", Microsoft,
[18] http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx
[19] http://www.phishtank.com/what_is_phishing.php
[20] http://www.informationweek.com/news/security/vulnerabilities
[21] https://www.javelinstrategy.com
[22] http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm
[23] http://www.microsoft.com/security/online-privacy/social-networking.aspx
[24] http://www.naavi.org/pati/pati_cybercrimes_dec03.htm