GJCRT : Global Journal of Computer Science Research & Technology

ISSN (online): 2349- 0608

CYBER CRIME: IMPACT ON SOCIETY AND PREVENTION

Sukhmeen Kaur
HOD, PG Deptt.of Computer Science,
Khalsa College, Patiala.
Email: skhanjraw@rediffmail.com

Ramneek Kaur
PG Deptt.of Computer Science,
Khalsa College Patiala.
Email: ramneeksethi@yahoo.co.in

ABSTRACT

Cyber crime is emerging as a serious threat worldwide. Governments, police departments and intelligence units have started reacting to it seriously. Nowadays, Initiatives have been taken to curb cross border cyber threats considered to be more serious. Indian police has established special cyber cells across the country and have started educating the people about cyber threats. In the current era of online processing, maximum of the information is online and prone to cyber threats. There are so many cyber threats and their impact is difficult to understand at the first instance and hence difficult to restrict in the early phases of the cyber attacks. Cyber attacks may have some pre planned targets behind it or may be processed unknowingly. Those attacks which are processed knowingly can be considered as the cyber crime and they have serious impacts over the society in the form of economical disrupt, psychological imbalance, threat to National defense and infrastructure etc. Restrictions on cyber crimes are dependent on proper analysis of their behavior and understanding of their impacts over various levels of society. This paper is an attempt to provide a glimpse on various cyber crimes, their prevention and their impacts over society with the future trends of cyber crimes

Keywords: Cyber Attacks, Cyber Crimes, Potential Economic Impact, Consumer trust, National Security

INTRODUCTION

When any crime is committed over the Internet it is referred to as a cyber crime. The world of Internet today has become a parallel form of life and living. Public are now capable of doing things which were not imaginable few years ago. The Internet is fast becoming a way of life for millions of people and also a way of living because of growing dependence and reliance of the mankind on these machines. Internet has enabled the use of website communication, email and a lot of anytime anywhere IT solutions for the betterment of human kind. Internet, though offers great benefit to society, also present opportunities for crime using new and highly sophisticated technology tools. Today e-mail and websites have become the preferred means of communication. Organizations provide Internet access to their staff. By their very nature, they facilitate almost instant exchange and dissemination of data, images and variety of material. This includes not only educational and informative material but also information that might be undesirable or anti-social. Regular stories featured in the media on computer crime include topics covering hacking to viruses, web jackers, to internet pedophiles, sometimes accurately portraying events, sometimes misconceiving the role of technology in such activities. Increase in cyber crime rate has been documented in the news media. Both the increase in the incidence of criminal activity and the possible emergence of new varieties of criminal activity pose challenges for legal systems, as well as for law enforcement.

CYBER CRIMES

Hacking: This is a type of crime where in a person's computer is broken into so that his personal or sensitive information can be accessed.

*Theft***:** This crime occurs when a person violates copyrights and downloads music, movies, games and software.

*Cyber Stalking***:** This is a kind of online harassment wherein the victim is subjected to a barrage of online messages and emails. Typically, these stalkers know their victims and instead of resorting to offline stalking,

they use the Internet to stalk for cash transactions and banking services. In this cyber crime, a criminal accesses data about a person‟s bank account, credit cards, Social Security, debit card and other sensitive information to siphon money or to buy things online in the victim‟s name. It can result in major financial losses for the victim and even spoil the victim‟s credit history.

Malicious Software: These are Internet-based software or programs that are used to disrupt a network present in the system.

*Child soliciting and Abuse***:** This is also a type of cyber crime wherein criminals solicit minors via chat rooms for the purpose of child pornography. The FBI has been spending a lot of time monitoring chat rooms frequented by children with the hopes of reducing and preventing child abuse and soliciting.

Phishing: Phishing is just one of the many frauds on the Internet, trying to fool people into parting with their money. Phishing refers to the receipt of unsolicited emails by customers of financial institutions, requesting them to enter their username, password or other personal information to access their account for some reason. Customers are directed to a fraudulent replica of the original institution's website when they click on the links on the email to enter their information, and so they remain unaware that the fraud has occurred. The fraudster then has access to the customer's online bank account and to the funds contained in that account.

*Vishing***:** Vishing is the criminal practice of using social engineering and Voice over IP (VoIP) to gain access to private, personal and financial information from the public for the purpose of financial reward. The term is a combination of "voice" and phishing. Vishing exploits the public's trust in landline telephone services, which have traditionally terminated in physical locations which are known to the telephone company, and associated with a bill-payer. The victim is often unaware that VoIP allows for caller ID spoofing, inexpensive, complex automated systems and anonymity for the bill-payer. Vishing is typically used to steal credit card numbers or other information used in identity theft schemes from individuals.

*Cyber Squatting***:** Cyber squatting is the act of registering a famous domain name and then selling it for a fortune. This is an issue that has not been tackled in IT act 2000.

*Bot Networks***:** A cyber crime called 'Bot Networks', wherein spamsters and other perpetrators of cyber crimes remotely take control of computers without the users realizing it. Computers get linked to Bot Networks when users unknowingly download malicious codes such as Trojan horse sent as e- mail attachments. Such affected computers, known as zombies, can work together whenever the malicious code within them get activated, and those who are behind the Bot Neworks attacks get the computing powers of thousands of systems at their disposal. Attacker so often coordinates large groups of Bot-controlled systems, or Bot networks, to scan for vulnerable systems and use them to increase the speed and breadth of their attacks. Trojan horse provides a backdoor to the computers acquired. A 'backdoor" is a method of by passing normal authentication, or of securing remote access to a computer, while attempting to remain hidden from casual inspection. The backdoor may take the form of an installed program, or could be a modification to a legitimate program. Bot networks create unique problems for organizations because they can be remotely upgraded with new exploits very quickly and this could help attackers pre-empt security efforts.

CATEGORIES OF CYBER CRIME

- *Against Individuals and individual property*: Cyber crimes against individuals may be in case of Harassment via e-mails, Cyber Stalking, dissemination of obscene material, defamation, unauthorized control/ Access over computer system, indecent exposure, Email spoofing, cheating and Fraud, transmitting Virus, intellectual Property Crimes and Internet time thefts etc.
- *Against Government and organizations:* Cyber crimes against Government and organizations would be like unauthorized control/ access over computer system, possession of unauthorized information, cyber terrorism against the government organizations and distribution of pirated software etc.

- *Against Society***:** Cyber crimes against society are related to pornography (basically child pornography), polluting the youth through indecent exposure, trafficking, financial crimes, sale of illegal articles, online gambling and forgery etc.

The total cost to pay by victims against these attacks is in millions of millions Dollar per year which is a significant amount to change the state of un-developed or under-developed countries to developed countries. Some of the facts related to cyber crimes can be significantly marked by the information provided by a US base news agency Research study which has found that one in five online consumers in the US have been victims of cybercrime in the last two years. RSA, the security division of EMC have released their Quarterly Security Statistics Review concerning identity, theft online, phishing and malware, data breaches and data loss. The review found that 23 percent of people worldwide will fall for spear phishing attacks. Cybercrime costs businesses more than $600 million a year equating to $8 billion. The review also found that consumers are increasingly concerned about their safety online. The Identity Theft Resource Centre, 2009 Consumer Awareness Survey in the US found that 85 percent of respondents expressed concern about the safety of sending information over the Internet, while 59 percent expressed a need for improvement in the protection of the data they submit over websites. Reported cases of spam, hacking and fraud have multiplied 50-fold from 2004 to 2007.
Additionally, the booming of call centers in India has generated a platform for cyber criminal activity in harvesting data, the report maintained. A study by researchers at the University of Brighton, titled 'Crime Online: cyber crime and Illegal Innovation' reveals that India is fast emerging as a major hub of cyber crime as recession is driving computer-literate criminals to electronic scams. The study states that cyber crime in India, China, Russia and Brazil is a cause of "particular concern" and there has been a "leap in cyber crime" in India in recent years, partly fuelled by the large number of call centers.

IMPACT OF CYBER CRIME

Potential Economic Impact: As today„s consumer has become increasingly dependent on computers, networks as these are used to store and preserve, the risk of being subjected to cyber-crime is high. Some of the surveys conducted in the past have indicated as many as 80% of the companies„surveyed acknowledged financial losses due to computer breaches. The approximate number impacted was $450 million. Almost 10% reported financial fraud [14]. Each week we hear of new attacks on the confidentiality, integrity, and availability of computer systems. 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. Stocks are traded via internet, bank transactions are performed via internet, purchases are made using credit card via internet. All instances of fraud in such transactions impact the financial state of the affected company and hence the economy.

Impact on Consumer trust: 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. The perception that the Internet is rife with credit card fraud and security hazards is growing. This has been a serious problem for e-commerce.

Complicating the matter, consumer perceptions of fraud assess the state to be worse than it actually is. Consumer perception can be just as powerful - or damaging - as fact. Hence users„concerns over fraud prevent many online shoppers from transacting business. 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 or amateurish commerce seriously jeopardizes potential business

Areas Ripe for Exploitation & National Security: Modern military of most of the countries depends heavily on

advanced computers. Information Warfare, or IW, including network attack, exploitation, and defense, isn't a new national security challenge, but since 9/11, it has gained some additional importance. IW appeals because it can be low-cost, highly effective and provide deniability to the attacker. It can easily spread malware, causing networks to crash and spread misinformation.

Since the emphasis is more on non-information warfare, information warfare is definitely ripe for exploration. The Internet has 90 percent junk and 10 percent good security systems [32].

When intruders find systems that are easy to break into, they simply hack into the system. Terrorists and criminals use information technology to plan and execute their criminal activities. The increase in international interaction and the wide spread usage of IT has facilitated the growth of crime and terrorism. Because of the advanced communication technology people need not be in one country to organize such crime. Hence terrorists and criminals can find security loopholes in the system and can function from unusual locales instead of their country of residence.

Most of such crimes have been originating in developing countries. The wide spread corruption in these countries fuel these security hacks. The internet has helped fund such crimes by means of fraudulent bank transactions, money transfer etc. Greater encryption technology is helping these criminal activities.

*Future Trends***:** One of the biggest concerns is what if there is a hack into the critical systems in government, companies, financial institutions etc. This could lead to malware in critical systems leading to data loss, misuse or even killing the critical systems. Since the communication flow is easy via the internet, the crime organizations might merge and cooperate even more than they are currently.

It is feared that due to enhanced mobility, funds and people could transfer easily. The Internet is increasingly likely to be used for money laundering. As the Internet becomes the medium through which more and more international trade takes place, the opportunities for laundering money through over-invoicing and under-invoicing are likely to grow. Online auctions offer similar opportunities to move money through apparently legitimate purchases, but paying much more than goods are worth. Online gambling also makes it possible to move money especially to offshore financial centers. Recruitment into crime agencies over internet will be easier than before. Secret messages can be transferred over the internet to a large group of people very easily without being conspicuous.

Because much of the information technology companies are privately owned, the focus would be on making customer happy as opposed to worry about the transnational crime. In addition, legitimate civil liberties could be argued in favor of not monitoring the information technology. Social Media will provide the platform for the cyber crimes. More organizations will adopt social media as a core aspect of their marketing strategy. They will struggle to balance the need to be active as part of on-line social communities while balancing compliance and litigation risks associated with such activities. Similarly, organizations will have a hard time controlling online social networking activities of their users.

Attackers will continue to take advantage of the still-evolving understanding of online social networking safety practices to defraud people and organizations. Security vendors will position their products as solving all these problems; some of them will stand out by allowing organizations to granularly control and monitor on-line social networking activities, while being mindful of users' privacy expectations.

Humans are the weakest link, regardless of how technology changes attackers know they can always hack employees. In the year 2012 and 2013 these human attacks will only grow in
sophistication and numbers. Cyber attackers will always take the path of least resistance.

Organizations and management will finally start doing It„s the sensitive issue for the people relying on I Phones for their day today working that without issuing a dire warning that some worm will eat all the I Phones and convert the Androids to bricks. However, the biggest issue seems to be apps with spyware. Even

the apps that come loaded on the phone are likely to phone home, it is a sure thing with 3rd party apps. AT&T has proved they cannot be trusted by signing their customers up for Asurion road side assistance without even asking them. And it matters big time.

Memory Scraping Will Become More Common in the coming time. Wi-Fi technology will continue to grow, but other protocols will also emerge with widespread adoption suiting the needs of embedded technology with a variety of focus areas including Zig Bee Wireless HART and Z-Wave, as well as proprietary protocols.

More Cloud Computing issues will be at the eye of the cyber attackers. While there are many possible benefits to Cloud Computing, the honeymoon will end. Many organizations will soon discover that they do not have the flexibility they need for their businesses, and many others will discover that any security issues (from audit to compromise) are far more complex in the cloud. Many security professionals will come to terms with security risks of cloud computing.

CONCLUSION

This manuscript put its eye not only on the understanding of the cyber crimes but also explains the impacts over the different levels of the society. This will help to the community to secure all the online information critical organizations which are not safe due to such cyber crimes. The understanding of the behavior 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 (referred as 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.

PREVENTION OF CYBER CRIME

Prevention is always better than cure. It is always better to take certain precaution while operating the net. One should make the Precaution, Prevention, Protection, Preservation and Perseverance as part of cyber life. There are few suggestions given below that have to be kept in mind while working on computers and internet in case of persons who actively works on computers and internet

- Use strong passwords**:** Treat your password like you treat your tooth brush. Never give it to anyone.
- To prevent cyber stalking avoids disclosing any information pertaining to one. This is as good as disclosing your identity to strangers in public place
- Secure your computer and activate your firewall.
- Use anti-virus/malware software to Block spyware attacks
- Be Social-Media Savvy
- Secure your Mobile Devices Install the latest operating system
- Update Data: Use encryption for your most sensitive files such as tax returns or financial records, make regular back-ups of all your important data, and store it in another location.
- Secure your wireless network- Wi-Fi (wireless) networks at home are vulnerable to intrusion if they are not properly secured. Review and modify default settings. Public Wi-Fi, a.k.a. “Hot Spots”, is also vulnerable. Avoid conducting financial or corporate transactions on these networks.

- Protect your e-identity- Be cautious when giving out personal information such as your name, address, phone number or financial information on the Internet. Make sure that websites are secure (e.g. when making online purchases) or that you‟ve enabled privacy settings (e.g. when accessing/using social networking sites).
- Avoid being scammed.
- Call the right person for help.

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. Computer Hope (2012), Data Theft, Available at: http://www. computerhope.com/jargon/d/ datathef.htm,
4. By Jessica Stanicon (2009), Available at: http://www.dynamicbusiness.com/ articles/articles-news/one-infive victims-of-cybercrime3907.html
5. Prasun Sonwalkar (2009), India emerging as centre for cybercrime:
6. UK study, Available at: http://www.livemint.com/2009/08/20000730/India-emerging-as-centre-for-c.html
7. India emerging as major cyber crime centre (2009), Available at: http:// wegathernews.com/203/indiaemerging-as-major-cyber-crime-centre
8. 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
9. 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.
10. Gordon, L. A. et al., 2003, A Framework for Using Insurance for Cyber-Risk Management, Communications of the ACM, 46(3): 81-85.
11. 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.
12. Kelly, B. J., 1999, Preserve, Protect, and Defend, Journal of Business Strategy, 20(5): 22-26.
13. Nilkund Aseef, Pamela Davis, Manish Mittal, Khaled Sedky, Ahmed Tolba (2005), Cyber-Criminal Activity and Analysis, White Paper, Group 2.
14. 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,