UGC Approved Journal
© INNOVATIVE RESEARCH THOUGHTS | Refereed | Peer Reviewed | Indexed
ISSN : 2454 – 308X | Volume : 03 , Issue : 11 | October – December 2017

A Review of Cyber Crime Security : Issues And Challenges

Dr . Manish Bhardwaj
Assistant professor in law Vaish college of Law Rohtak

ABSTRACT
The internet's high degree of vulnerability has made online transactions untrustworthy. Cybercrime is growing more serious. In this work, we will define cyber-crime, explain the tools used by criminals to commit their evil deeds, identify the causes of "cyber-crime, how it can be eradicated, examine those involved and their motives, examine how to detect a criminal mail, and finally make recommendations to help curb the rising rate of cyber-crime and criminals.
Keywords: Cyber security, information, Internet, technology, people etc.

INTRODUCTION
The internet's high degree of vulnerability has made online transactions untrustworthy. Cybercrime is growing more serious. In this work, we will define cyber-crime, explain the tools used by criminals to commit their evil deeds, identify the causes of cyber-crime, how it can be eradicated, examine those involved and their motives, examine how to detect a criminal mail, and finally make recommendations to help curb the rising rate of cyber-crime and criminals.

CYBER – CRIME
These crimes are simple to perform, take few resources compared to the potential harms, may be done in a jurisdiction without being physically present and are frequently not obviously prohibited.
Cyber-crime ('computer crime') is any illicit activity directed by means of electronic operations that affects the security of computer systems and the data processed by them, said the Director of Computer Crime Research Centre (CCRC) in an interview on April 27, 2004. Environments in which information about people, things, events, phenomena or processes is represented mathematically or symbolically and exchanged across local and worldwide networks.
This wide word covers anything from electronic cracking to denial-of-service assaults that cost online retailers money. Mr. Pavan Duggal, President of www.cyberlaws.net and consultant, identified the different categories and forms of cybercrimes in a report.
Cybercrime is broadly classified into three types:
Personal cybercrime: Cybercrimes against people include sending child pornography and harassing someone using a computer such as email. Including pornography and indecent exposure, is one of the most serious Cybercrimes known today. The potential damage to mankind from such a crime is immense. If not regulated, this cybercrime might stunt the development of the next generation and cause irreversible damage.
separate cybercrime. Various forms of cyberbullying may and do occur. A person may be harassed for any reason. Cybercriminals who harass others are also cybercriminals. Cyber harassment as a crime relates to another area of citizen privacy infringement. The invasion of internet residents' privacy is a serious cybercrime. No one appreciates others entering the important and sensitive area of privacy that the internet affords the individual.
Property cybercrimes: The second kind of cybercrime is property cybercrime. Computer vandalism (destroying others' property) and spreading malicious programmes are examples. A

competing corporation, an industry heavyweight, stole the technical database from their systems with the aid of a corporate cyberspy.

In the third type of cybercrime, cybercrime against government is concerned. Cyberterrorism is one kind of this crime. The expansion of the internet has proven that people and organisations are using cyberspace to threaten foreign governments and intimidate populations. When someone cracks into a government or military controlled website, it becomes terrorism.

Cracking is a serious cybercrime. It's terrifying to learn that someone has hacked into your computer system without your knowledge or approval and altered sensitive data.

Various types of cyber-crimes include:

Unauthorized access of hosts- known as hacking. Hacking may take many forms, not all of which need technical expertise.

- Social engineering includes talking an authorised person into granting you computer access.
- There is a distinction between crackers or black hats who break into systems with malevolent purpose, and hackers or white hats who do it for fun or to improve their technical skill.

Spamming – • Email spam is becoming a big problem amongst organisations owing to the financial overhead it generates not just in terms of bandwidth use but also time spent downloading/ deleting junk messages. Aside from permuting email text, spammers are using graphics that is undetectable by spam filters.

Computer Fraud/ Phishing scams- Recently, sophisticated frauds targeting internet banking clients in South Africa have emerged. These are termed Phishing scams and require the offenders to masquerade as a trustworthy representative of an institution, usually the victim's bank.

Denial of Service Attacks- Not to be confused with computer hacking.

- A denial-of-service attack involves flooding a server or network with traffic, preventing regular users from accessing it.
- Distributed Denial of Service assaults employ several computers to attack, sometimes using zombie servers, which are trojan zed applications installed on different systems.

Viruses, Trojans and Worms- These three programmes are similar in that they are meant to infect computers without the user's consent, but they function in quite different ways.

- Many computer users have been frustrated by harmful viruses destroying their systems and data, however not all viruses are bad.
- A Trojan gives remote access to the machine it is installed on. Trojans come in many shapes and levels of sophistication.
- Worms exploit known flaws in frequently used software and are meant to spread across networks, but not necessarily destructively.

CAUSES OF CYBER – CRIME

There are various reasons why cybercriminals conduct cybercrime, but three stand out:

• Cybercrime may be undertaken for fame. This is usually done by teenagers who want to be seen as part of the big and strong males in society. • Another reason for cyber-crime is to generate fast money. • Thirdly, cyber-crime may be performed to fight a cause one believes in; to create

danger and most commonly damages that negatively impact the receivers. This is the most hazardous cybercrime cause.

WHO ARE INVOLVED?

Those involved in committing cyber-crimes are in three categories and they are:

IDEALISTS (Teenager). They are mainly untrained and unskilled youth aged 13–26 seeking social acclaim. They want media attention. Individually, their activities do little harm. Like rejecting several significant e-commerce servers in February 2000, causing substantial losses to these companies.

GREED – INSPIRED (Career Criminals). This sort of cyber-criminal is hazardous since they are dishonest and willing to commit any crime to get money. Then they created cyber-pornography, which includes both legal and illicit child pornography on the internet.

CYBER TERRORISTS They are the newest and most lethal. Their main motivation is not money, but a cause they support. To prove their case, they frequently send threatening emails and delete data housed in mostly government networks. Cyber-terrorism is comparable to dangers from nuclear, biological, or chemical weapons. The fact that they have no national borders and may operate from anywhere in the globe makes it tough to catch them.

A CRIMINAL MAIL

A criminal mail is another sort of cybercrime presently being investigated but not as popular as the others.

A criminal letter is frequently sent to networks to either corrupt or defraud the system. Detecting such messages requires security mechanisms that identify illicit trends in the network. Unisys Active Risk Monitoring System (ARMS) helps banks and other companies notice patterns of apparently unconnected occurrences that add up to criminal conduct, according to IDG News Service's Paul Roberts. With Actimize Technology Ltd's technology, enterprises may do extensive data mining and analysis on stored information and transaction data without transferring it to an external data warehouse. According to Katz, the atomize programme may be created on conventional server hardware with four to eight CPUs.

Terrorist organisations are adeptly utilising the internet to spread information about different terrorist activities that endanger human life. Cyber-terrorists may now breach computer systems using logic bombs (programmed devices that can be remotely detonated), electromagnetic pulses, and high-powered radio frequency rifles.

Modern high-speed communications, computers, and other technology are providing new criminal possibilities, crimes, and obstacles for law enforcement. From a financial perspective, Consumer debt growth may impact bankruptcy filings. Deregulatory reform, economic development, and globalisation are transforming anticompetitive behaviour.

Government Viewpoint: Criminal and civil justice issues increasingly cross-national borders, including treaty commitments, global environmental and trade agreements, and other foreign policy problems.

Social-Demographic Viewpoint

The numbers of adolescents and young adults, now the most crime-prone segment of the population is expected to grow rapidly over the next several years.

Computer as an instrument facilitating crime

A computer is used to facilitate crime. In the recent assault on Parliament, computers and the internet were utilised in a number of ways to accomplish the crime. Terrorists and criminals use internet tactics like e-mail and flash encrypted messaging globally. Electronic banking and commerce frauds are further instances. These crimes use computer programmes to aid the crimes, namely:

a) Fraudulent use of Automated Teller Machine (ATM) cards and accounts;
b) Credit card frauds;
c) Frauds involving electronic finds transfers;
d) Telecommunication Frauds; and
e) Frauds relating to Electronic Commerce and Electronic Data Interchange.

The private sector has an important role in securing the Nation's IT infrastructure by deploying sound security products and adopting good security practices. But the Federal government also has a key role to play by supporting the discovery and development of cyber security technologies that underpin these products and practices".

- **Software vulnerability**

Attackers use networks to go from one location to another, but software flaws in computers exacerbate the cyber security issue. The current software development processes do not provide high-quality, dependable, and secure software. Software development is still neither a science or a discipline, and it is not managed to reduce attack vulnerabilities. Today, like cancer, weak software may be infiltrated, updated, and spread over networks, causing harm to other systems.

- **Domestic and international law enforcement**

Attacks from hostile parties utilising Internet-connected machines hundreds of kilometres distant are as easy as if they were next door. This kind of assault is tough to track down, and even when it is, cross-border prosecution is challenging.

- **Education**

We must teach individuals that if they use the internet, they must constantly maintain and upgrade their security so they cannot be hacked, for example, to become DDoS agents or to distribute spam. We must also educate businesses and organisations on proper security management. Example: some big companies need all systems under their control to fulfil tight security standards. All internal PCs and servers get automatic upgrades, and no new systems are permitted online unless they meet the security standard.

- **Information security**

Information security refers to safeguarding data on a network as well as the network itself. The worrying increase in planned assaults on interdependent networks and information systems globally has necessitated major attention to key information infrastructure security programmes. Governments have always protected strategically vital facilities, but the digital revolution has changed everything. Business, government, and national defence have all evolved. These operations increasingly rely on an interconnected network of information technology infrastructures, increasing our vulnerability to emerging critical infrastructure threats.

CONCLUSION

All governments throughout the globe are concerned about cybercrime and cyber security. Nigeria, with the biggest proportion of African descent, has a vital role to play. Various studies indicate that this situation is rapidly deteriorating, and governments who fail to act quickly and sensibly will pay a high price. Develop thorough plans for handling sensitive data, records, and transactions and include robust security technology—such as firewalls, anti-virus software, intrusion detection tools, and authentication services are some of the measures that organisations may take to protect themselves.

REFERENCES

1. Douglas A. Barnes. Deworming the internet. Texas Law Review, 83:279_329, November 2004.
2. Aaron J. Burstein. Towards a culture of cybersecurity research. Harvard Journal of Law and Technology, 22:230_240, 2008.
3. Daniel J. Solove and Chris Jay Hoofnagle. A model regime of privacy protection. University of Illinois Law Review, 7:1083_1167, 2002.
4. Berkley l Joseph P, Liu. The data and the regulation of scientist research. Technology Law Journal, 18:501, 2003.
5. Goodman Seymour E and Herbert S. Towards a Safer and More Secure Cyberspace. National academies Press, 2007.
6. Euguene Volokh. Crime-facilitating speech. Stanford Law Review, 57:1095_1222, March 2005.
7. http://www.asianlaws.org/press/cybercrime.htm
8. http://www.dailytrust.com, 2008
9. http://news.softpedia.com/news/Nigerian-Phishers-Arrested-83024.shtml