Available online @ www.iaraindia.com
SELP Journal of Social Science - A Blind Review & Refereed Quarterly Journal
ISSN: 0975-9999 (P) 2349-1655 (O)
Impact Factor: 3.655(CIF), 2.78(IRJIF), 2.77(NAAS)
Volume. X, Issue 40
January - March 2019
Formally UGC Approved Journal (46622), © Author

CYBER CRIME IN DIGITAL ERA - ANEMPIRICAL STUDY

Dr. V. GOKILA
Assistant Professor in Commerce
Sri Ramakrishna College of Arts & Science for Women, Coimbatore

Abstract

In techno savy world, today relies heavy use of electricity and numerous us electronics to keep every day running smoothly. No matter where one goes, there is some sort of technology that has a drastic impact on life. In the fast growing world as both sides of the coin internet has its own advantages and disadvantages (cyber crime).This research paper discusses about the cybercrime in the digital world. Cybercrime is nothing but computer acts as an objector a subject of crime. This research paper helps us discuss about the aspects of cybercrime in digital Era.

Key Words: Cybercrime, Technology, Digital Era.

Introduction

It is not unusual for teenagers in this digital world to get involved in cyber activities at early stages. In this technological world all are well interested in using gadzets from early age. The children of small age do it for fun without knowing the later risks and penalties they have to suffer. Cyber crime isn't a victimless crime and it is taken seriously by law enforcement. This arises due to high usage of computers, digital devices and internet. Over 40 years, cybercrime still doesn't universally accepted definition in literature. There are millions of computer connected to the internet everyone appreciates the use of internet but there is other side of the coin (i.e.,) cybercrime by the use of internet.

The term cybercrime can be defined "as an act committed or omitted in violation of a law forbidding or commanding it and for which punishment is imposed upon conviction". The purpose of this research paper is discussing the digital era and understanding the cybercrime.Itprovides an overview on the relevant topics.This research paper concludes with data's collected from primary and secondary sources.

Objectives:

- To know about the digital era.
- To provide overview ofcybercrime.
- To know the pros and cons of cyber-crime.

Research Methodology

Primary Data

Primary data was used for the study and it was collected by means of structured questionnaire from the people who were all the internet users .The data was collected from 88 respondents were taken into consideration of the study .The data was collected through online survey. Percentage analysis was used to analyze the data so collected.

Secondary Data

Secondary data was also used for the study. After searching the important websites and blogs relevant information was downloaded and examined to address the objective of the study.

LIMITATION:

1. The study is based on convenient sampling which is a type of non-random sampling. Hence the limitations of non-random samplings are applicable.
2. The inclination and opinion of youth may change from time to time. Hence, the result of the project may be applicable only in the present situation.

Cyber-Crime

Cyber crime is defined as a crime in which a computer is the object of the crime or is used as a tool to commitan offense. Cyber criminals may use computer technology to access personal information, business trade secrets or use the internet for exploitative ormalicious purposes. Criminals can also use computers for communication and document or data storage. Criminals who perform the sail legal activities are often referred to as hackers. Cyber crime may also be referred to as computer crime.

CommonForms of Cyber Crime

- ❖ Phishing: using fake email messages to get personal information from internet users.
- ❖ Misusing personal information (identity theft)
- ❖ Hacking: shutting down or misusing websites or computer networks
- ❖ Spreading hate and in citing terrorism
- ❖ Distributing child pornography
- ❖ Grooming: making sexual advances to minors.

Pros and Cons of Cyber crime:

P	C
Improved securityofcyberspace Increase in cyber defense Increase in cyber speed Allows more option to save data Betterresponsetimetonational crisis	Improved hacker speed and ability Interconnectedcomputers Improved viruses, malware and worms Increasein“cyberwarefare” Possibly More anonymity between hackers

There are a lot of cases of Computer Assisted crime where computer is the instrument for committing crime. Some of them are discussed below:

Data Piracy

This involves reproduction of digital data and easy distribution of print, graphics, sound and multimedia combinations even the use of copyrighted material either for personal use.

Pornography/Child Pornography

It is the unethical and illegal distribution of sexually implicit material especially involving children.

Illegal Interception of Material

Data transfer over the net has resulted in greater speed and capacity but also greater vulnerability. It is now easier for unauthorized people to gain access to sensitive information. It has many forms like:

Internet Time Thefts

Phishing, spoofing or spam (unsolicited mail) wherein a perpetrator sends fictitious mails which appears official causing the victim to release personal information

Online Credit card fraud, E- Bank theft: Illegal acquisition of credit card number for online purchases or bank account details where the perpetrator diverts funds to account accessible to criminal.

There are other situations of computer oriented cyber crime where computer is the Target of Crime Like

Hacking

Information theft from computer storage device or hard disk and stealing username, password and altering information is called hacking

Forgery

It includes reproduction of documents, certificates, identity thefts and fake currency. Altering Websites: Here the hacker deletes some pages of a website, uploads new pages with the similar name and controls the messages conveyed by the web site.

Cyber terrorism

It involves E-murder or homicide or suicide or Spyware.

Causes of Cyber Crimes

Ease of access

The problem encountered in guarding a computer system from unauthorised access is that there is every possibility of violating the technology by stealing access codes, recorders, pins, retina imagers etc. that can be used to fool biometric systems and bypass firewalls to get past many a security system.

Cyber Hoaxes

Cyber Crimes can be committed just to cause threats or damage one's reputation.

This is the most dangerous of all causes. The involved believe in fighting their cause and want their goal to be achieved. They are called cyber terrorists.

Negligence

There are possibilities of not paying attention in protecting the system. This negligence gives the criminals control to damage the computer.

Revenge or Motivation

The greed to master the complex system with a desire to inflict loss to the victim. This includes youngsters or those who are driven by lust to make quick money and they tamper with data like e-commerce, e-banking or fraud in transactions.

Poor Law Enforcing Bodies

Due to lack in cyber laws of many countries, many criminals get away without being punished.

CyberCrimes Committed for Publicity

Generally committed by youngsters where they just want to be noticed without hurting someone's sentiments.

CYBER LAW

Cybercriminals + computer technology= difficulties to apply the law

PavanDuggal, acknowledged as one of the top four Cyber Lawyers in the world, gave a definition of Cyber law in1996, which is broadly accepted, as follows:–

Simply speaking, Cyber law is a generic term, which refers to all the legal and regulatory aspects of Internet and the World Wide Web. Anything concerned with or related to or emanating from any legal aspects or issues concerning any activity of netizens and others, in Cyberspace comes within the ambit of cyber law**.**

ANALYSISAND INTERPRETATION:

The following are the results of primary data Collected from various sectors of respondents:

Gender:

86.4% of the respondents are female aware of cyber crime.

Software Installed:

51.1 % of respondents have installed antivirus software in their PC/ MAC.

Safe Online:

The study lights on the fact that 48.9% of the respondents feel safe that their in formations are safe online.

Password Protection

The study reveals that 42% of respondents agree that they need password protection in concern with the information security.

Money Loss due to Cyber Crime

Majority 83% of the respondents had not ever lost money due to Cybercrime.Trojan or malware affects 5.57% of users, 10.2% are affected by auto-generated emails and 3.4% are affected by publishing obscure on their profile.47.7%of respondents have reported that cyber law towards cyber criminals are not clear and laws to be made strict.

Cyber Security

Cyber security or IT security is the protection of computer systems from theft or damage to their hardware, software or electronic data, as well as from disruption or misdirection of the services they provide.

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.

All of these things make it more difficult to deal with cyber-crime. Some of the future trends predicted by Stephen Northcutt &Friends are briefly summarized in the followed text. Improved Social Engineering Attacks will be the trend for the coming era. Attackers will increasingly make use of social-engineering tactics to bypass technological security controls, fine-tuning their techniques to exploit natural human predispositions.

This will bring us closer to merging the line between external and internal threat agents, because social engineering will allow external attackers to quickly gain an internal vantage point despite traditional perimeter security measures. 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 something about it to secure the human. 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. This has been around for a long time, but is more aggressively targeting data such as credit card records, passwords, PIN's, keys, as of late. The reason they are successful is that they get around PCI/GLBA/HIPAA/ETC security requirements that data must be encrypted while in transit and at rest. Data in transit is decrypted on the system and often stored in memory during the lifetime of a process, or at least during a decryption routine. Depending on how a process cleans up after itself, it may stay resident even after the fact.

The data is encrypted on the hard disk, but again, the RAM likely maintains the clear text version of the data. Browsers are notorious for leaving things sitting around in memory during web sessions. The RAM Scraping malware also targets encryption keys in memory to decrypt anything for session data to encrypted files. As far as the emerging security threat part, we are seeing RAM scraping more commonly now as attackers focus on client-side attacks, shifting away from server-side attacks. Browsers are often mis configured, allowing malware to get onto a user's system, stealing credit card data and passwords. They are mostly an annoyance where if a customer or fraud department detects fraudulent transactions, the account must be credited and changed. This requires the banks to write-off these transactions, which can add up quickly. AV products can't keep up with the aggressive rate and polymorphic characteristics of this type of malware.

We discover a ton of new malware every week, reverse it to some extent, and send the details to AV vendors to be added as a new signature. The other emerging component is the threat of RAM scraping malware targeting Point of Sale (POS) systems.

Wireless adoption will continue, branching out into a larger number of purpose-focused protocols that fit the needs of individual technology. 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 ZigBee, WirelessHART and Z-Wave, as well as proprietary protocols.

With this growing alternate wireless adoption, we're already seeing some of the past mistakes from earlier failed protocols repeated. Based on this exposure, and the trend of Wi-Fi failure and improvement, we'll see history repeating itself where vendors are quick to the market to capitalize on new opportunities, failing to critically examine the lessons from earlier wireless technologies.

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.

They will do so under pressure from the businesses they support, as companies will continue to migrate to cloud platforms. The infosec community will better understand cloud environments, while the technologies implementing cloud platforms will reach an acceptable level of maturity. Security professionals will continue to apply extra scrutiny to scenarios that involve processing sensitive or regulated data in shared cloud environments. Security Continues to become part of Virtual Infrastructure.

As more and more organizations add virtualization technologies into their environment, particularly server and desktop virtualization, security will be more embedded in the native technologies, and less of an "add-on" after the implementation is complete. For server virtualization, new firewalls and monitoring capabilities are being integrated into some of the leading platforms now. For desktop virtualization, native integration with remote access technologies and client-side sandbox capabilities are common. Vendors will continue to push the envelope and offer new tools to enhance virtual environments, but virtualization platforms will evolve to easily allow existing security technologies to interoperate more natively, as well. In addition, security architecture design will be a "must have" element of virtual infrastructure planning and deployment, not a "nice to have".

Conclusion

All the way through the research on cyber crime in digital era concludes saying that there arises cybercrime problems in higher risks nowadays.“Where there will there is a way” according to this saying there is also equal preventive measures in controlling digital crimes and that can make a positive sense. There is 100% cyber-attack proof. High technology can be a high touch.

Reference

1. AmmarYassirandSmithaNayak, Cybercrime: Athreatto Network Security IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.2, February 2012.
2. Cyber-Crimes and their Impacts: A Review ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 2, Mar- Apr2012, pp.202-209.
3. http://cyberlawcybersecurity.com/cyber-law/
4. https://www.techopedia.com/definition/2387/cybercrime
5. SoumyaSatishRevankar, Cyber Crime and Cyber Security, International Research Journal of Engineering and Technology (IRJET), Volume: 04Issue: 11|Nov-2017 www.irjet.netp-ISSN: 2395-0072 e-ISSN: 2395-00.