CYBER CRIME AND COMPUTER CRIME INFORMATION TECHNOLOGY

BY

DR. ALFRED ABHULIMHEN-IYOHA

CHIEF MAGISTRATE, EDO STATE JUDICIARY, BENIN CITY, NIGERIA.

PhD LAW, PhD STRATEGIC STUDIES, DIPLOMA CHRISTIAN THEOLOGY.+2348055968440, Email:aaiyoha@yahoo.com

JULY 2020

CYBER CRIME AND COMPUTER CRIME INFORMATION TECHNOLOGY

Nowadays, computer is used for different purposes depending on the persons skill and wants. When you look at the population of the people who use computers in the world, the number is very surprising. It increases everyday and as every second passes, technologies are increasing. Lets take China for example an article which says "There are nearly 300 million inter users only in China"[1]. So with this population of computer and cyber users, there is no wrong in saying cyber and computer crime will keep increasing as it is networked internationally, which makes computer criminals to get access to it easily. As government and Businessmen rely on computers so do criminals.

The first recorded cyber crime was in 1820. This is not surprising because the first form of computer is Abacus which has been around since 3500BC. By looking at this fact their will be no doubt in saying that cyber crime and computer crime will keep increasing day by day.[2]

INFORMATION TECHNOLOGY (IT)

Information technology (IT) is the use of computers to store, retrieve, transmit, and manipulate data,[3] or information, often in the context of a business or other enterprise.[4] IT is considered to be a subset of information and communications technology (ICT). An information technology system (IT system) is generally an information system, a communications system or, more specifically speaking, a computer system – including all hardware, software and peripheral equipment – operated by a limited group of users.

---

[1] *Eliza Strickland, New York Times, population of internet users in china, 1 July, 2009)(1)*
[2] *Ibid pp 4.*
[3] Daintith, John, ed. (2009), "IT", *A Dictionary of Physics*, Oxford University Press, *ISBN 9780199233991, retrieved 1 August 2012*
[4] *"Free on-line dictionary of computing (FOLDOC)". Retrieved 9 February 2013.*

Humans have been storing, retrieving, manipulating, and communicating information since the Sumerians in Mesopotamia developed writing in about 3000 BC,[5] but the term *information technology* in its modern sense first appeared in a 1958 article published in the Harvard Business Review; authors Harold J. Leavitt and Thomas L. Whisler commented that "the new technology does not yet have a single established name. We shall call it information technology (IT)." Their definition consists of three categories: techniques for processing, the application of statistical and mathematical methods to decision-making, and the simulation of higher-order thinking through computer programs.[6]

The term is commonly used as a synonym for computers and computer networks, but it also encompasses other information distribution technologies such as television and telephones. Several products or services within an economy are associated with information technology, including computer hardware, software, electronics, semiconductors, internet, telecom equipment, and e-commerce.[7]

Based on the storage and processing technologies employed, it is possible to distinguish four distinct phases of IT development: pre-mechanical (3000 BC – 1450 AD), mechanical (1450–1840), electromechanical (1840–1940), and electronic (1940–present).[8] This article focuses on the most recent period (electronic), which began in about 1940.

2.0 DEFINITION OF CYBER CRIME AND COMPUTER CRIME

2.1 CYBER CRIME

---

[5] Butler, Jeremy G., *A History of Information Technology and Systems*, University of Arizona, *retrieved 2 August 2012*
[6] Leavitt, Harold J.; Whisler, Thomas L. (1958), *"Management in the 1980s"*, Harvard Business Review, **11**
[7] Chandler, Daniel; Munday, Rod (10 February 2011), "Information technology", *A Dictionary of Media and Communication* (first ed.), Oxford University Press, *ISBN 978-0199568758, retrieved 1 August 2012*, Commonly a synonym for computers and computer networks but more broadly designating any technology that is used to generate, store, process, and/or distribute information electronically, including television and telephone.
[8] Butler, Jeremy G., *A History of Information Technology and Systems*, University of Arizona, *retrieved 2 August 2012*

Cyber crime is a crime that is committed using a computer, network or hardware device. The computer and the internet serve as a target victim or as a tool to commit a lot of crimes. Cyber crime does not only mean stealing of millions as many people think. Cyber crime constitutes a lot of crimes such as fraud, cyber stalking, unauthorized access, child pornography, forgery, and etcetera. Looking at it that way, the major crime that Government, Industries, and people around the world are concerned about are cracking, piracy, phreaking, cyber stalking, cyber pornography, cyber terrorism, etcetera.

Cyber crime also involves traditional crimes that take place via the internet. Cyber crime is the latest and the most complicated problem in the cyber world. There are organized and individual hackers.[9] The individual hackers normally do this sort of things to prove themselves to be good in computer programming and other breaching softwares while the organized crimes are always done for monetary purposes, like hacking into big companies, business organizations or even Banks.[10]

2.2 COMPUTER CRIME

Computer crime is a crime that is committed with the help of a computer. These crimes have been around since before the coming of computer but now as the world is changing crime can also be a situation computers are used to assist in crime activities. When this kind of crime is committed it doesn't have to result in any loss of data and also the data in the computer doesn't have to be modified.

Computer crime can also be a situation whereby data on a computer is accessed without the administrators permission. It doesn't mean that data in the computer have to be modified or

---

[9] *"The chief Executive Officer Lieutenant-Colonel Jazri said that in the past two years there has been at least 4000 complaints filed in the country of Malaysia , mostly consisted of hack threats, fraud, denial of services and other computer problems such files lost or corrupted by viruses." (Sanooaung, More than 4,000 cybercrime cases reported in Malaysia within two years, January 17, 2009.) (2)*

[10] *As (Parthasarathi pati, cyber crime, page 2, Indian printing press,2006) (3) said "Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber crime".*

as a result got lost. The worst time of computer crime is that which occurs without any indication that data has been accessed.

Computer crime are now done in groups, because they have now realize that if such crimes are organized, their will be low-level of risk and ease of stealing. Computer crime is mostly done by rogue hackers and crackers, majority of who are employees of an organization.[11]

3.0 DEFINITION OF TERMS INVOLVING COMPUTER AND CYBER CRIME

FRAUD:

Fraud is normally caused by extorting money from individuals by way of tricking them. Fraudsters are on the rise in the world, they execute this act by way of email etcetera and it usually comes in form of big business organization or individual.

BLACK HAT:

Is a word used for a hacker who breaks into a computer or network or even creates computer viruses. Black hats are sort of the villains of the computer world.

IDENTITY THEFT:

Identity theft is using of some ones personal data illegally, meaning without his knowledge. If a persons identity has been stolen, is may be very devastating because a lot of activities may be taking place without the owner knowing. They use a persons name, social security Number, birthday or even using some ones international passport to create new credit cards or collect loans which will affect the owners record.

---

[11] *Beverly Bright(2009) "Internet Crime has risen from $68 million in 2004 to $265 million in 2008. The statistics on Internet fraud indicates the seriousness of the problem." Computer Crime Is On The Rise: Help Is Available For Cyber Crime.*

PHISHING:

Phishing is an e-mail fraud in which the phishers sends millions of messages to different people. The message will look as if it was sent by a genuine source, it will look very real. What they normally ask is your financial information from the message recipients.

PHARMING:

Pharming is a way hackers use to trick people using the internet Unlike phishing, pharmers use a technique of changing an IP address of a web-site, so when you type a web- site thinking that its sending you to the right site, it then diverts hackers fake link page. What they do is that they use the same Domain name but different IP address so you will end up filling a page that is fake and they will have all your information.

DENIAL-OF-SERVICE ATTACK:

Denial of Service attack is a situation whereby computer resources are made unavailable to organization or intended users. Mostly, DOS does not usually result of information or other security loss. This attack may make inter sites or services from working properly.

MALWARE:

Malware is a software made to penetrate or damage a computer system without the owners giving permission to penetrator.

HACKING:

Hacking is a word used to describe breaking into computer systems without the owners consent. It is also the unauthorized trespassing in the internet world.[12]

---

[12] *Example: "some Russian hackers known as Russian Business Network stole 10s of millions of Dollars from US Banks and are still at large, the FBI are still investigating the case"(Bubbie Johnson, The age. 'Russian hacks stole from US Banks. Dec 25, 2009.) (5)*

SPYWARE:

Spyware is a computer software that is being installed which takes control of partial interaction between the user and his computer without the user knowing. Spyware programs can store personal information. It also redirects web browser activities which may cause more harmful Viruses to your computer. This sort of spywares can cause problems like slowing down the connection speed and even loss of internet or other programs.

4.0 FUTURE OF CYBER CRIME

Looking at the future of cyber crime in Asia and where cyber criminals are heading, you will see that cyber criminals (attackers) are always a step a head of the authorities. Cyber criminals always find a new way of committing crimes. They always find a way to by-pass the authorities. Authorities should increase the skill-level of international police so as to catch up with this sort of crime committers.

In Asia, the cases of cyber crime are high because of their population and their exposure to computer; about 85-90% of Asians have access to computers. When looking at how cyber crime is growing, you can say that cyber crime will keep getting worst. Relying on the current law and technical protection is not sufficient for the computer worlds well being.

Protection measures most be taken for people to secure themselves from cyber crime for example “People should know when and where to do their online Banking. A person may be doing his thing not knowing that the computer has spywares which can store all his data”. These problems can be solved by installing up to date Anti-virus and configuring your firewalls is also very important.

In china, 25% of major cyber crimes are committed as cyber frauds. There are about 300 million internet users in only China, what if we look at the whole world? How many bad eggs

will we find? What these cyber criminals put in mind is that they urgently want to get rich by all means which will lead to no good. And know the fastest way to steal from people and escape is using cyber fraud.[13]

5.0 SCENARIOS OF CYBER CRIMES

There are a lot of examples involved in cyber crime. These are some of the examples:

- A case was filed in which 250,000 was stolen from a Bank in Indonesia through a fake computerized Bank Account.
- The police in India arrested an unemployed computer operator together with his friend, a host of a five star hotel allegedly stealing and misusing the total hotel customers credit card numbers.
- The host copied down the information on the credit card and passes it to his computer operator friend. And what the friend normally does is that he uses the details to purchase a different websites online.

Cyber pornography has been rated as the biggest and largest business on the internet today.

The CEO of an online auction website "bazee.com" was arrested by the Delhi police for disobeying Indias laws on cyber pornography. This was so because a student was using bazee website to sell a Video showing two students having sexual intercourse. The website was responsible for the being of everything that goes on in the site. So the CEO was arrested for distributing porn videos.

A professional on software from Bangalore (India) was arrested for misappropriating the source code of a product that was developed by his employers. He then started his own company and used the stolen code to launch his new software product.

---

[13] *Eliza Strickland, New York Times, population of internet users in china, 1 July, 2009)(1)*

In 2003, a computer user in China got hold of a source code for a game called LINEAGELL from a website that was unprotected. In 2004, he then started selling the codes to different people. He was warned by the South Korean company who owned the code legally. But despite their warnings, he was still reluctant and was even trying to expand his illegal Business. The South Korean company realized that they were loosing $250,000 a month, that when they filed a case. The US FBI arrested the suspects and the web-sites were shut down.

6.0 PREVENTION OF CYBER CRIME

Hacking Techniques

- Password compromised
- Make your password difficult to guess
- Profiling
- Using of random passwords
- Malware
- By using of Anti-virus, And spyware software
- Lost laptops
- Secure your system by pass wording your laptop
- Software Vulnerability
- By Knowing the location of all your softwares and how its used
- Password observers
    - beware of your surrounding
    - type fast
- Firewall
    - Make sure it is always on.

- Upgrade or replace

- Bribed Staff
- Never share your password
- Windows Vulnerability
- Install windows updates
- No License

- Change to retrieve source software
- Buy License

Prevention Measures

These are the preventions:

Using of spam blocker is a way to stop receiving unwanted e-mails. There is always a spam blocking feature provided by most of the internet providers. Fraudulent, phishing e-mails are example of mails blocked if you use the spam blocker.

Make sure you install well recommended Anti-virus software. Its not only installing the Anti-virus but up-dating it regularly and scanning your computer at least once a week or two (2) In order to remove unwanted programs like malware, viruses, spyware, and a lot more. AVG is free security software for those who prefer free versions.

Always be cautious of giving out your personal information to web-sites you know nothing about, mostly those who request your bank account details, name, mailing address or even social security number are all fraudsters.

Using of parental control software to limit your children's whereabouts online is a very wise thing to do, checking on them regularly while they are online and also checking the

browsers is another way of knowing what your kids are always doing and with whom are they interacting with.

Always keep your computer firewalls protection feature on because it prevents hackers from penetrating through your computer.

Police should be trained not only in the field but also in the technology wise with all its technicalities. Looking at a lot of books and journals and the law behind

Cyber criminals, you will find out that the sentence for a black hat hacker is between 1-5 years in prison. I think if the Government will use these culprits they can do well to the society by giving them another chance in a community service punishment. Their punishment should be helping the Government to nab such criminals because they know all the maneuvers involved in hacking or cracking.

Companies, Banks, and big organizations should make it a habit of changing their security measures on regular bases.

7.0 CONCLUSION

In conclusion to this paper, what computer and cyber crime will become in the future is not predictable. Things that have been happening before is not what will happen in the future, because everyday there is an advancement in the computer world.

There are a lot of cyber crimes victims who refuse to report petty crimes, because they feel what they have lost are too small, they feel its better to loose than to be embarrassed.

I hope that the people this society will take this case very seriously. Computer crime should be stopped. Reports should be filed immediately no matter how small a crime is because other people may learn from your mistakes.