FEDERAL UNIVERSITY OF TECHNOLOGY, MINNA, NIGERIA

CENTRE FOR OPEN DISTANCE AND e-LEARNING (CODeL)

SCHOOL OF INFORMATION & COMMUNICATION TECHNOLOGY

COURSE TITLE: CYBERCRIMES AND COUNTERMEASURES

COURSE CODE: CSS 311

COURSE DEVELOPMENT

CSS 311

CYBERCRIMES AND COUNTERMEASURES

Course Developer/Writer
Mr. Ojeniyi Joseph Adebayo
Department of Cyber Security Science
School of Information & Communication Technology,
Federal University of Technology, Minna, Nigeria.

Course Editor
Prof. Sanjay Misra
Department of Cyber Security Science
School of Information & Communication Technology,
Federal University of Technology, Minna, Nigeria.

Programme Coordinator
Mr. Ojeniyi Joseph A.
Department of Cyber Security Science
School of Information & Communication Technology,
Federal University of Technology, Minna, Nigeria.

Instructional Designers
Prof. Gambari, Amosa Isiaka
Dr. Falode, Oluwole Caleb
Centre for Open Distance and e-Learning,
Federal University of Technology, Minna, Nigeria.

Editor
Miss Chinenye Priscilla Uzochukwu
Centre for Open Distance and e-Learning,
Federal University of Technology, Minna, Nigeria.

COURSE GUIDE

Introduction

CSS 311: Cybercrimes and Countermeasures is a 3 credit unit course for students studying towards acquiring a Bachelor of Technology in Cyber Security Science and other related disciplines. The course is divided into 4 modules and 15 study units. The course started with the introduction of software engineering issues and associated terms to software engineering. The course then proceeds and deals with the processes that have to be followed in order to develop robust software. The course went further to deal with the concepts of system engineering and engineering processes that are important to the development of software. Other modules of the course discussed software requirements, requirements engineering process and system design; that is the strategic design to follow to have sophisticated software. The course concluded by examining software verification, validation, testing, debugging and decommissioning. These are the final processes to execute to ensure error-free and standard software.

The course guide therefore gives you an overview of what the course; CSS 326 is all about, the textbooks and other materials to be referenced, what you expect to know in each unit, and how to work through the course material.

What you will learn in this Course

The overall aim of this course, CSS 326 is to introduce you to the basic concepts of software engineering to acquaint students with the basic knowledge of software development strategies.

This course highlights different processes that are essential to the development and management of software engineering. This course will also introduce you to the practical terms and definitions of software engineering.

Course Aim

The aim of this course is to introduce students to the basics and concepts of Software Engineering. It is believed the knowledge will enable the student to acquire basic knowledge of software development strategies and software management skills. It will help the reader to understand that it is important to note that in designing software, specific software development processes have to be followed so as to have robust and error-prone free software and a nation's virile economy. It will also help software developer to realize several requirements, requirements engineering processes and system engineering procedures vita to software development.

Course Objectives

It is important to note that each unit has specific objectives. Students should study them carefully before proceeding to subsequent units. Therefore, it may be useful to refer to these objectives in the course of your study of the unit to assess your progress. You should always look at the unit objectives after completing a unit. In this way, you can be sure that you have done what is required of you by the end of the unit. However, below are overall objectives of this course. On completing this course, you should be able to understand:

(i) Software engineering techniques and software development principles

(ii) Basic techniques of developing software

(iii) Communicating and interacting with database systems.

(iv) Showcase some practical knowledge of software development principles

(v) Understand what are requires to develop robust software.

(vi) The application of engineering principle to the development of software.

(vii) Categories of system models use in modelling and designing specific software applications and processes.

(viii) System engineering principles to develop maintainable and reliable system.

Working through this Course

To complete this course, you are required to study all the units, the recommended textbooks, and other relevant materials. Each unit contains some self assessment exercises and tutor marked assignments, and at some point in this course, you are required to submit the tutor marked assignments. There is also a final examination at the end of this course. Stated below are the components of this course and what you have to do.

Course Materials

The major components of the course are:

1. Course Guide
2. Study Units
3. Text Books
4. Assignment File

5. Presentation Schedule

Study Units

There are 16 study units and 4 modules in this course. They are:

Module 1 Software Engineering Issues

Unit 1 Introduction to Software Engineering

Unit 2 Software Life cycle

Unit 3 Software Process Model

Unit 4 System Engineering

Module 2 Requirements

Unit 1 Software Requirement

Unit 2 Requirement Engineering Process

Unit 3 System Models

Module 3 System Design

Unit 1 Design Principle

Unit 2 Architectural

Unit 3 Object Oriented Design

Unit 4 Computer Software Aided Design

Module 4 Verification and Validation

Unit 1 Software Verification

Unit 2 Software Validation

Unit 3 Software Testing

Unit 4 Software Debugging and Decommissioning

Recommended Texts

These texts and especially the internet resource links will be of enormous benefit to you in learning this course:

1. Software engineering Schaum's series 3rd Edition, Murray R. Spiegel and Larry J. Stephens

2. Sommerville (2000), Software Engineering, 6th edition

3. Roger S. Pressman (2005), Software Engineering; A practitioner's Approach, McGraw-Hill, ISBN: 007-124083-7 Sixth Edition.

Assignment File

The assignment file will be given to you in due course. In this file, you will find all the details of the work you must submit to your tutor for marking. The marks you obtain for these assignments will count towards the final mark for the course. Altogether, there are tutor marked assignments for this course.

Presentation Schedule

The presentation schedule included in this course guide provides you with important dates for completion of each tutor marked assignment. You should therefore endeavour to meet the deadlines.

Assessment

There are two aspects to the assessment of this course. First, there are tutor marked assignments; and second, the written examination. Therefore, you are expected to take note of

the facts, information and problem solving gathered during the course. The tutor marked assignments must be submitted to your tutor for formal assessment, in accordance to the deadline given. The work submitted will count for 40% of your total course mark.

At the end of the course, you will need to sit for a final written examination. This examination will account for 60% of your total score.

Tutor Marked Assignments (TMAs)

There are TMAs in this course. You need to submit all the TMAs. The best 10 will therefore be counted. When you have completed each assignment, send them to your tutor as soon as possible and make certain that it gets to your tutor on or before the stipulated deadline. If for any reason you cannot complete your assignment on time, contact your tutor before the assignment is due to discuss the possibility of extension. Extension will not be granted after the deadline, unless on extraordinary cases.

Final Examination and Grading

The final examination for CSS 326 will be of last for a period of 2 hours and have a value of 60% of the total course grade. The examination will consist of questions which reflect the Self-Assessment Questions and tutor marked assignments that you have previously encountered. Furthermore, all areas of the course will be examined. It would be better to use the time between finishing the last unit and sitting for the examination, to revise the entire course. You might find it useful to review your TMAs and comment on them before the examination. The final examination covers information from all parts of the course.

The following are practical strategies for working through this course

1. Read the course guide thoroughly
2. Organize a study schedule. Refer to the course overview for more details. Note the time you are expected to spend on each unit and how the assignment relates to the units. Important details, e.g. details of your tutorials and the date of the first day of the semester are available. You need to gather together all these information in one place such as a diary, a wall chart calendar or an organizer. Whatever method you choose, you should decide on and write in your own dates for working on each unit.
3. Once you have created your own study schedule, do everything you can to stick to it. The major reason that students fail is that they get behind with their course works. If you get into difficulties with your schedule, please let your tutor know before it is too late for help.
4. Turn to Unit 1 and read the introduction and the objectives for the unit.
5. Assemble the study materials. Information about what you need for a unit is given in the table of content at the beginning of each unit. You will almost always need both the study unit you are working on and one of the materials recommended for further readings, on your desk at the same time.
6. Work through the unit, the content of the unit itself has been arranged to provide a sequence for you to follow. As you work through the unit, you will be encouraged to read from your set books.
7. Keep in mind that you will learn a lot by doing all your assignments carefully. They have been designed to help you meet the objectives of the course and will help you pass the examination.
8. Review the objectives of each study unit to confirm that you have achieved them.

If you are not certain about any of the objectives, review the study material and consult your tutor.

9. When you are confident that you have achieved a unit's objectives, you can start on the next unit. Proceed unit by unit through the course and try to pace your study so that you can keep yourself on schedule.

10. When you have submitted an assignment to your tutor for marking, do not wait for its return before starting on the next unit. Keep to your schedule. When the assignment is returned, pay particular attention to your tutor's comments, both on the tutor marked assignment form and also written on the assignment. Consult you tutor as soon as possible if you have any questions or problems.

11. After completing the last unit, review the course and prepare yourself for the final examination. Check that you have achieved the unit objectives (listed at the beginning of each unit) and the course objectives (listed in this course guide).

Tutors and Tutorials

There are 8 hours of tutorial provided in support of this course. You will be notified of the dates, time and location together with the name and phone number of your tutor as soon as you are allocated a tutorial group. Your tutor will mark and comment on your assignments, keep a close watch on your progress and on any difficulties you might encounter and provide assistance to you during the course. You must mail your tutor marked assignment to your tutor well before the due date. At least two working days are required for this purpose. They will be marked by your tutor and returned to you as soon as possible.

Do not hesitate to contact your tutor by telephone, e-mail or discussion board if you need help. The following might be circumstances in which you would find help necessary: contact your tutor if:

• You do not understand any part of the study units or the assigned readings.

• You have difficulty with the self- test or exercise.

• You have questions or problems with an assignment, with your tutor's comments on an assignment or with the grading of an assignment.

You should endeavour to attend the tutorials. This is the only opportunity to have face to face contact with your tutor and ask questions which are answered instantly. You can raise any problem encountered in the course of your study. To gain the maximum benefit from the course tutorials, have some questions handy before attending them. You will learn a lot from participating actively in discussions.

GOODLUCK!

TABLE OF CONTENTS

CONTENTS PAGE

Module 1 – Cybercrime Activities

Unit 1 Definition of Cyber and Cybercrime Activities

1.0 Introduction

Widespread of technology and access to the Internet are shaping the way business activity is done today. While these phenomena are known to have brought global business to a whole new level, they have also brought with them, the mixed blessing called "cybercrime." **Cybercrime** has the following base words, 'cyber' and 'crime'. Of a truth, you are conversant with the word, 'crime', '**cyber'** could different meanings depending on its context. In this context, however, cyber means network space which could either be closed or open. Closed cyber could mean Intranet or local network while open cyber stands for Internet, where users are unknown giving ample opportunity to anonymous criminality. According to Science Dictionary, cyber could also be prefix meaning computer or computer networks, as in cyberspace. **Cyberspace** means an electronic medium through which online communication or transaction takes place. Consequently, **cybercrime** can be said to be any crime committed in the cyberspace.

Businesses, governments and individuals have all played victim to cybercrime. Many have attempted a definition of "cybercrime." Fafinski, & Minassian (2008) quoting Wall (2007), define cybercrime as "the transformation of criminal or harmful behavior by networked technology", while Wilson (2007) puts it simply as a "crime that is enabled by, or that targets computers". Other synonyms exist like "computer crime" and "internet crime", are also found in literature. Cybercrimes can range from criminal activity against data to content and copyright infringement (Gordon & Ford, 2006). As the United Nations says "Globalization opens many opportunities for crime, and crime is rapidly becoming global, outpacing international cooperation to fight it…"

2.0 Learning Outcomes/Objectives: At the end of this unit, you should be able to:

(i) familiar with the term **cyber** and **cybercrime** activities;

(ii) know why they are cybercrime;

(iii) be able to group cybercrime based on the two broad accepted classifications of cybercrime activities.

3.0 Main Content

3.1 Definition of Cyber and Cyber Crime Activities

As you have rightly informed in the introduction section, cyber means computer, computer networks, computer or digital related situation.

Cybercrime activities are those criminal activities that specifically target a computer or network for damage or infiltration and also refer to the use of computers as tools to conduct criminal activities. Cybercrime activities could be classified as

"computer-aided" and "computer-focused"

3.2 Computer-Aided Crimes

These are crimes accomplished with the help of computer. It can also be referred to as computer-assisted crimes. Some of them are as follows:

3.2.1 Denial of service Attack (DoS)

This is an act by the criminal, who floods the bandwidth of the victim network or fills his e-mail box with spam mail depriving him of the services he is entitled to access or provide short for ***d****enial-****o****f-****s****ervice* attack, a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. Many DoS attacks, such as the *Ping of Death* and *Teardrop attacks*, exploit limitations in the TCP/IP protocols. For all known DoS attacks, there are software fixes that system administrators can install to limit the damage caused by the attacks. But, like Virus, new DoS attacks are constantly being dreamed up by Hacker.

3.2.1 Virus Dissemination

Malicious software that attaches itself to other software. (virus, worms, Trojan Horse, Time bomb, Logic Bomb, Rabbit and Bacterium are the malicious codes.

3.2.2 Software Piracy

Theft of software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original.

3.2.3 Net Extortion

This is the process of seizing, getting or copying data of high value or secrecy in order to threaten its damage, exposure or reputation tarnishing for huge sum of money.

3.2.4 Phishing

The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the users information. Phishing, also referred to as brand spoofing or carding.

3.2.5 Cyber trespassing

This type of crime includes following a victim online. Cyber Criminals send a program to the victim's machine, which after getting downloaded in stealth or hidden capture all the information from the victim's machine and send it to the criminal. The information collected by the cybercriminal is then used against the victim for harassing, black mailing etc.

3.2.6 Cyber Contraband

Selling of illegal items by use of computer system, preferably having internet connectivity.

3.2.7 Cyber terrorism

Terrorist use technology to spread terrorism across the world. Some websites provide unwarranted information about making ammunitions, hacking techniques, spreading arms and ammunitions by using secret codes.

3.2.8 Cyber laundering

Cyber criminals lure the victim by sending email's assuring them that they have won a lottery and asking the victim to pay token amount to get the lottery amount. They ask personal information from the victim such as Name, Age, Address, Bank Account, Occupation etc. This information collected is then used against the victim for commiting the crime. The lottery amount is never received by the victim, nor the token amount is returned back.

3.2.9 Cyber Theft

This type of crime involves stealing internet time.

3.2.10 Cyber Pornography

This is one of the most prominent crime taking place on the internet. Cyber criminals make websites which promote nudity on the internet. There are many websites on the internet which promote this heinous crime. Another way by which criminals promote pornography on the internet is by cutting and pasting two or more photographs from pornographic sites and merging with the photograph of the victim. This is called as morphing. Special care has to be taken by individuals, groups while putting photographs on the websites. Whenever photographs are put on the internet features such as cut, copy, paste and print screen should be disabled.

3.2.11 Email bombing

This kind of activity refers to sending large numbers of mail to the victim, which may be an individual or a company or even mail servers there by ultimately resulting into crashing.

3.2.12 Data diddling

This kind of an attack involves altering raw data just before a computer processes it and then changing it back after the processing is completed. The electricity board faced similar problem of data diddling while the department was being computerized.

3.2.13 Salami attacks

This kind of crime is normally prevalent in the financial institutions or for the purpose of committing financial crimes. An important feature of this type of offence is that the alteration is so small that it would normally go unnoticed. E.g. the Ziegler case wherein a logic bomb was introduced in the bank's system, which deducted 10 cents from every account and deposited it in a particular account.

3.2.14 Denial of Service attack

The computer of the victim is flooded with more requests than it can handle which cause it to crash. Distributed Denial of Service (DDoS) attack is also a type of denial of service attack, in which the offenders are wide in number and widespread. E.g. Amazon, Yahoo.

3.2.15 Logic bombs

These are event dependent programs. This implies that these programs are created to do something only when a certain event (known as a trigger event) occurs. E.g. even some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date (like the Chernobyl virus).

3.2.16 Trojan attacks

This term has its origin in the word 'Trojan horse'. In software field this means an unauthorized programme, which passively gains control over another's system by representing itself as an authorized programme. The most common form of installing a Trojan is through e-mail.

3.2.17 Web jacking

This term is derived from the term hijacking. In these kinds of offences the hacker gains access and control over the web site of another. **Hacker** is someone gains unauthorized access to computer system or confidential information. Web jacker may even mutilate or change the information on the site. This may be done for fulfilling political objectives or for money. Of recent many sites were web jacked. Out of uncounted number was the site of Bombay crime branch which was also

web jacked. Another case of web jacking is that of the ‘gold fish’ case. In this case the site was hacked and the information pertaining to gold fish was changed. Further a ransom of US $ 1 million was demanded. Thus web jacking is a process whereby control over the site of another is made backed by some consideration for it.

3.3 Computer-Target/Focused Crime

These are cybercrimes attacks meant to disrupt the functionality of the computer (the effect of this crime is directly felt by the system).

3.3.1 Viruses

This type of malicious code requires you to actually do something before it infects your computer. This action could be opening an email attachment or going to a particular web page.

3.3.2 Worms

Worms propagate without user intervention. They typically start by exploiting a software vulnerability (a flaw that allows the software's intended security policy to be violated), then once the victim computer has been infected the worm will attempt to find and infect other computers. Similar to viruses, worms can propagate via email, web sites, or network-based software. The automated self-propagation of worms distinguishes them from viruses.

3.3.3 Trojan horses

A Trojan horse program is software that claims to be one thing while in fact doing something different behind the scenes. For example, a program that claims it will speed up your computer may actually be sending confidential information to a remote intruder.

3.3.4 Physical Destroying the System in other to Destroy Evidence

Even in the traditional law today, for a criminal court to set upon any lawsuit there must be genuine evidence or witnesses

4.0 Conclusion

As we can see cybercrime is so numerous hence reasons why cyber security should be in inevitable especial in a nation such as Nigeria that is ranked as one of the nations where cybercrime is exceedingly high.

5.0 Summary

You have been exposed to the definitions of the words cyber and cybercrime. In simple terms, **cyber** means relating to computer or computer networks either open or close. Then, cybercrime is the crime committed in relation to computer or computer networks.

We also defined Cybercrime activities as those criminal activities that specifically target a computer or network for damage or infiltration. More so, the computers could be used as tools to conduct criminal activities. Cybercrime activities could be ether be classified as, and it could be classified as either *"computer-assisted" or "computer-focused"*

6.0 Self-Assessment Exercises

7.0 Tutor-Marked Assignments

8.0 References

United Nations Human Development Report, 1999

Audal, J., Lu, Q., & Roman, P. (2008). Computer Crimes. *The American Criminal Law Review, 45(2),* 233-274.

Bakos, Y. (1998, August). Emerging Role of Electronic Marketplaces on the Internet. *Communications of the ACM, 41(8),* 35-42.

Balfour, D. L. & Marini, F. (1991). Child and Adult, X and Y: Reflections on the Process of Public Administration Education. *The American Society of Public Administration, 51(6),* 478-485.

Brown, K. V. (2001, June). The Determinants of Crime in South Africa. *The South African Journal of Economics, 69(2),* 269-298.

Buettner, T., & Spengler, H. (2003). Local Crime Determinants: Distinguishing Between Resident and Non-resident Offenders. *Darmstadt Discussion Papers in Economics, 120.*

Buonanno, P. (2006). The Socioeconomic Determinants of Crime: A Review of the Literature. *University of Milan-Bicocca, Working Paper Series, 63.*

Cantor, D. & Land, K.C. (1985, June). Unemployment Rates and Post-World War II United States: A Theoretical and Empirical Analysis. *American Psychological Review, 50(3),* 317-332.

D'Ovidio, R. (2007). The Evolution of Computers and Crime: Complicating Security Practice. *Security Journal, 20,* 45-49.

Emigh, J. (2004). Cybercrime Can Have Real-World Ramifications. *Access Control Security Systems, 47(1),* 36-37.

Unit 2 – Categorization of Cybercrime Activities

1.0 Introduction

In the unit 1, you have learnt the meaning of cyber and cybercrime activities. In addition, basic classification of cybercrime was introduced. There are number of common attacks and methods of committing a computer related crime. Some of these are less sophisticated than others are, committed by someone with limited knowledge of computers. Others require programming skills and/or an advanced knowledge of how computers and various software can work together to commit a crime. In other to understand cybercrime better, categorization of cybercrime activities had to a role to play. Basically cybercrime had been categorized into three (3) major groups namely: Cybercrimes against persons, Cybercrimes against property (Business and Non business Organization) and Cybercrimes against government.

1.0 Learning Outcome/ Objectives: At the end of this unit, you should be able to:

(i) categorize cybercrime activities;

(ii) highlight some of the major difference between them.

(iii) explain some of the crime base on the categorization.

2.0 **Main Content**

3.1 Categorization Based on Targets

According to Mr. Pavan Duggal, who is the President of cyberlaws.net and consultant, from wide research and study of cybercrime, cybercrime has been clearly defined into various categories. Basically into 3 major categories:

(i) Person-oriented cybercrimes.

(ii) Property-oriented cybercrimes.

(iii) Government-oriented cybercrimes.

3.1.1 Person-Oriented Cybercrimes

This is the category of cybercrimes that are targeted towards the personality of individual or aimed at causing emotional, financial loss or any other form of damage. At the initial stage, the damage caused may be minor but if not checked could be amplified. Even in situations where minimal pain, the scars may cut across generations. Some of the examples of crimes under this category are:

- Email spoofing
- Spamming,
- Cyber Defamation,
- Harassment & Cyber stalking,
- Phishing
- Intellectual Property crimes
- Unauthorized Accessing of Computer
- Cyber Stalking
- Cyber/Child Pornography
- Email account hacking
- Email scams
- Virus attack and so on.

Have a look at the following real life scenarios:

A minor girl was lured after deception to a private place through cyber chat (chat room) by a man, who, along with his friends, attempted to gang grape her. As some passersby heard her cry, she was rescued.

Taking Virus attack as another example wherein the damage was not done to a person but to the masses is the case of the Melissa virus. The Melissa virus first appeared on the internet in March of 1999. It spread rapidly throughout computer systems in the United States and Europe. It was estimated that the virus caused 80 million dollars in damages to computers worldwide. In the United States alone, the virus made its way through 1.2

million computers in one-fifth of the country's largest businesses. David Smith pleaded guilty on Dec. 9, 1999 to state and federal charges associated with his creation of the Melissa virus. There are numerous examples of such computer viruses few of them being "Melissa" and "love bug".

Violation of privacy of online citizens is a Cybercrime of a grave nature. No one likes any other person invading the invaluable and extremely touchy area of his or her own privacy, which the medium of internet grants to the citizen.

3.1.2 Property-Oriented Cybercrimes

These are crimes that are targeted towards organization of corporate existence. It could be targeted towards business or non-business organizations. The essence of this category of crime is to cause a low output or slow down their business. It is destruction of others' property. These include some of which have explained in the unit 1:

- Intellectual Property crimes
- Credit Card Fraud
- Theft of computer source code
- Software piracy
- Unauthorized Accessing of Computer
- Denial of Service
- Virus attack
- Email Bombing
- Salami Attack
- Trojan Horse
- Data diddling

3.1.3 Government-Oriented Cybercrimes

In this type of crime the government is the target, mostly to steal security and high profile information. This includes:

- Cyber Terrorisms
- Web hacking

- Tax evasion and money laundry
- Cyber defamation

The third category of Cyber-crimes relate to Cybercrimes against Government. Cyber terrorism is one distinct kind of crime in this category. The growth of internet has shown that individuals and groups to threaten the international governments as also to terrorize the citizens of a country are using the medium of Cyberspace. This crime manifests itself into terrorism when an individual "cracks" into a government or military maintained website.

Cracking is amongst the gravest Cyber-crimes known till date. It is a dreadful feeling to know that a stranger has broken into your computer systems without your knowledge and consent and has tampered with precious confidential data and information. Coupled with this the actuality is that no computer system in the world is cracking proof. It is unanimously agreed that any and every system in the world can be cracked. The recent denial of service attacks seen over the popular commercial sites like E-bay, Yahoo, Amazon and others are a new category of Cyber-crimes, which are slowly emerging as being extremely dangerous.

3.2 Categorization Based on the Object of Legal Protection

According to the Council of Europe Convention on Cybercrime, four different types of cybercrime offenses were identified. They are:

- Offences against the confidentiality, integrity and availability of computer data and systems;
- Computer-related offences;
- Content-related offences; and
- Copyright-related offences

3.2.1 Offences against the Confidentiality, Integrity and Availability of Computer Data and Systems:

All offences in this category are directed against (at least) one of the three legal principles of confidentiality, integrity and availability. Unlike crimes that have been covered by criminal law for centuries (such as theft or murder), the computerization of offences is relatively recent, as computer systems and computer data were only developed around sixty years ago. The effective prosecution of these acts requires that existing criminal law provisions not only protect tangible items and physical documents from manipulation, but also extend to include these new legal principles. This section gives an overview of the most commonly occurring offences included in this category.

- Illegal Access (Hacking, Cracking)

The offence described by "hacking" refers to unlawful access to a computer system, one of oldest computer-related crimes. Following the development of computer networks (especially the Internet), this crime has become a mass phenomenon. Famous targets of hacking attacks include the United States National Aeronautics and Space Administration (NASA), the United States Air force, Pentagon, Yahoo, Google, eBay and the German Government. Examples of hacking offences include: Breaking the password of password-protected websites; and

• Circumventing password protection on a computer.

- Data Espionage

Sensitive information is often stored in computer systems. If the computer system is connected to the Internet, offenders can try to access this information via the Internet from almost any place in the world. The Internet is increasingly used to obtain trade secrets more often. The value of sensitive information and the ability to access it remotely makes data espionage highly interesting. In the 1980s, a number of German hackers succeeded in entering United States government and military computer systems,

obtain secret information and sell this information to agents from the Soviet Union. Offenders use various techniques to access victims' computers, including:

- use of software to scan for unprotected ports;
- use of software to circumvent protection measures; and
- "social engineering".

Especially the last approach "social engineering", which refers to a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures, is interesting as it not based on technical means.

- Illegal Interception

Offenders can intercept communications between users (such as e-mails) or intercept data transfers (when users upload data onto webservers or access web-based external storage media) to record the information exchanged. Offenders can target any communication infrastructure (e.g., fixed lines or wireless) and any Internet service (e.g. e-mail, chat)

- Data Interference

Computer data are vital for private users, businesses and administrations, all of which depend on the integrity and availability of data. Lack of access to data can result in considerable (financial) damage. Offenders can violate the integrity of data and interfere with them by:

- Deleting data; and/or
- Suppressing data; and/or
- Altering data; and/or
- Restricting access to them.

One common example of the deletion of data is the computer virus.

- System Interference

The same concerns over attacks against computer data apply to attacks against computer systems. More businesses incorporating Internet services into their production processes, with benefits of 24-hour availability and worldwide accessibility. If offenders succeed in preventing computer, systems from operating smoothly, this can result in great financial losses for victims. Attacks can be carried out by physical attacks on the computer system. If offenders are able to access the computer system, they can destroy hardware. For most criminal legal systems, remote physical cases do not pose major problems, as they are similar to classic cases of damage or destruction of property. However, for highly profitable e-commerce businesses, the financial damages caused by attacks to the computer system are often far greater than the mere cost of computer hardware.

3.2.2 Content-related Offences

This category covers content that is considered illegal, including child pornography, xenophobic material or insults related to religious symbols. The development of legal instruments to deal with this category is far more influenced by national approaches, which can take into account fundamental cultural and legal principles. For illegal content, value systems and legal systems differ extensively between societies. The dissemination of xenophobic material is illegal in many European countries, but can be protected by the principle of freedom of speech in the United States. The use of derogatory remarks in respect of the Holy Prophet is criminal in many Arabic countries, but not in some European countries.

- Erotic or Pornographic Material

Sexually-related content was among the first content to be commercially distributed over the Internet, which offers advantages to retailers of erotic and pornographic material including:

• Exchange of media (such as pictures, movies, live coverage) without the need for cost-intensive shipping;

• Worldwide access, reaching a significantly larger number of customers than retail shops;

- Racism, Hate Speech, Glorification of Violence

Radical groups use mass communication systems such as the Internet to spread propaganda. Besides propaganda, the Internet is used to sell certain goods e.g. Nazi-related items such as flags with symbols, uniforms and books, readily available on auction platforms and specialized web-shops.

- Religious Offences

A growing number of websites present material that is in some countries covered by provisions related to religious offences e.g., anti-religious written statements. Although some material documents objective facts and trends (e.g., decreasing church attendance in Europe), this information may be considered illegal in some jurisdictions. Other examples include the defamation of religions or the publication of cartoons.

- Illegal Gambling and Online Games

Internet games and gambling are one of the fastest-growing areas in the Internet

- Spam and Related Threats

“Spam” describes the emission of unsolicited bulk messages. Although various scams exist, the most common one is e-mail spam. Offenders send out millions of e-mails to users, often containing advertisements for products and services, but frequently also malicious software.

3.2.3 Copyright- and Trademark-related Offences

One of the vital functions of the Internet is the dissemination of information. Companies use the Internet to distribute information about their products and services. In terms of piracy, successful companies may face problems on the Internet comparable to those that exist outside the network. Their brand image and corporate design may be used for the marketing of counterfeit products, with counterfeiters copying logos as well as products and trying to register the domain related to that particular company. Companies that distribute products directly over the Internet can face legal problems with copyright violations. Their products may be downloaded, copied and distributed.

- Copyright-related Offences

With the switch from analogue to digital, digitalization has enabled the entertainment industry to add additional features and services to movies on DVD, including languages, subtitles, trailers and bonus material. CDs and DVDs have proved more sustainable than records and video-tapes. Digitalization has opened the door to new copyright violations. The basis for current copyright violations is fast and accurate reproduction. Before digitalization, copying a record or a video-tape always resulted in a degree of loss of quality. Today, it is possible to duplicate digital sources without loss of quality, and also, as a result, to make copies from any copy. The most common copyright violations include:

- Exchange of copyright-protected songs, files and software in file-sharing systems;
- The circumvention of Digital Rights Management systems;

- Trademark-related Offences

Trademark violations are similar to copyright violations, a well-known aspect of global trade. Violations related to trademarks have transferred to cyberspace, with varying degrees of criminalization under different national penal codes. The most serious offences include:

• The use of trademarks in criminal activities with the aim of misleading targets; and

• Domain or name-related offences. The good reputation of a company is often linked directly with its trademarks. Offenders use brand names and trademarks fraudulently in a number of activities, including phishing, where millions of e-mails are sent out to Internet users resembling e-mails from legitimate companies e.g., including trademarks. Another issue related to trademark violations is domain-related offences such as cyber-squatting, which describes the illegal process of registering a domain name identical or similar to a trademark of a product or a company

3.2.4 Computer-related Offences

This category covers a number of offences that need a computer system to be committed. Unlike previous categories, these broad offences are often not as stringent in the protection of legal principles, including:

• Computer-related fraud;

• Computer-related forgery, phishing and identity theft; and

• Misuse of devices.

- Fraud and Computer-related Fraud

Computer-related fraud is one of the most popular crimes on the Internet, as it enables the offender to use automation and software tools to mask criminals' identities. Automation enables offenders to make large profits from a number of small acts. One strategy used by offenders is to ensure that each victim's financial loss is below a certain limit. With a 'small' loss, victims are less likely to invest time and energy in reporting and investigating such crimes. One example of such a scam is the Nigeria Advanced Fee Fraud

- Computer-related Forgery

Computer-related forgery describes the manipulation of digital document for example, by:

• Creating a document that appears to originate from a reliable institution;

• Manipulating electronic images (for example, pictures used as evidence in court); or

• Altering text documents.

The falsification of e-mails includes the scam of "phishing" which is a serious challenge for law enforcement agencies worldwide. "Phishing" seeks to make targets disclose personal/secret information.

- Misuse of Devices

Cybercrime can be committed using only basic equipment. Committing offences such as libel or online fraud needs nothing more than a computer and Internet access and can be carried out from a public Internet café. Offences that are more sophisticated can be committed using specialist software tools.

- Combination Offences

There are a number of terms used to describe complex scams covering a number of different offences. Examples include:

• Cyber terrorism;

• Cyber laundering; and

• Phishing;

Cyber terrorism

Today it is known that terrorists use ICTs and the Internet for:

• Propaganda;

• Information gathering;

• Preparation of real-world attacks;

• Publication of training material;

• Communication;

• Terrorist financing;

• Attacks against critical infrastructures.

- Cyber warfare

Cyber warfare describes the use of ICTs in conducting warfare using the Internet. It shares a number of features in common with cyber terrorism. Discussions originally focused on the substitution of classic warfare by computer-mediated or computer-based attacks. Network-based attacks are generally cheaper than traditional military operations and can be carried out even by small states

- Cyber laundering

The Internet is transforming money laundering. With larger amounts, traditional money-laundering techniques still offer a number of advantages, but the Internet offers several advantages. Online financial services offer the option of enacting multiple, worldwide financial transactions very quickly.

4.0 CONCLUSION

From the above discussions, we can clearly categorize cybercrime and activities. In addition, the two categorize used is so related to each other. In court of law or in life experience the understanding of this categorizes will go a long way in either prosecuting or protecting one's self from an intruder.

5.0 SUMMARY

- Cybercrime can be categorized depending on the focus either base on Targets or base on the object of legal protection.
- Base on Targets categorization: there are three categories:
    - Persons-Oriented Cybercrimes
    - Property-Oriented Cybercrimes
    - Government-Oriented Cybercrimes
- ✓ Base on the object of legal protection: we have four different types of offences:
    - Offences against the confidentiality, integrity and availability of computer data and systems;
    - Computer-related offences;
    - Content-related offences; and
    - Copyright-related offences
- ✓ Computer virus, Denial of Service, Hacking are the most common tool of an intruder from either side of the categorization.

6.0 TUTOR MARKED ASSIGNMENT AND MARKING SCHEME

6.1In your own words not more than one sentence, what can you say about categorization of Cybercrime.

Tips: Answers must contain- understanding of cybercrime.

6.2From the discussing above Cybercrime are categorized from two points of view, explain why?

Tips: Answers must contain- means of prosecution, defense, countermeasures.

6.3What are the two points of view or consideration in categorizing cybercrime?

6.4Discuss in detail one categorization of cybercrime you understand.

Tips: at least the example of two each of the categorization mention must be explained.

6.5 From your study and reasoning so far, which classification do you think is the best? Support your with good point.

Tips: Answers must contain- compare and contrast with a personal judgment or conclusion.

6.6 Categorize the various cybercrimes you know into any of the categorize from this material.

7.0 REFERENCES

Unit 3 – Analyses of Cybercrime Stages

1.0 Introduction

As you are now acquainted with the meaning and classification of cybercrimes in units 1 and 2, here we will be carrying out analyses of some criminal activities in the cyberspace. There are stages, levels, motives and/or risk assessment involved in cybercrimes. Also, we have vulnerability level, threat level, attack level and exploit level. All these and more you will learn in the body of this unit.

2.0 Learning outcomes and objectives: At the end of this unit, you should be able to:

(i) identify incident of a cybercrime;

(ii) analyse the level of the incident;

(iii) assess the risk level of the incident.

3.0 Main content

Analysis of cyber criminality simply means assessing the damage extent or potentiality of the launched incident or prospective cybercrime. There are several classifications for this analysis. Some analysis classifications are based on intent, damage potential, skill set and so on.

Another analysis divides cybercrime activities into the curious, the meddler and the criminal. David Aucsmith puts forward a more thorough multidimensional cybercrime analysis classification. This is based on skill level and motivation.

3.1 David Aucsmith Analysis Classifications

The model of David Aucsmith is explained with the aid of the graph below.

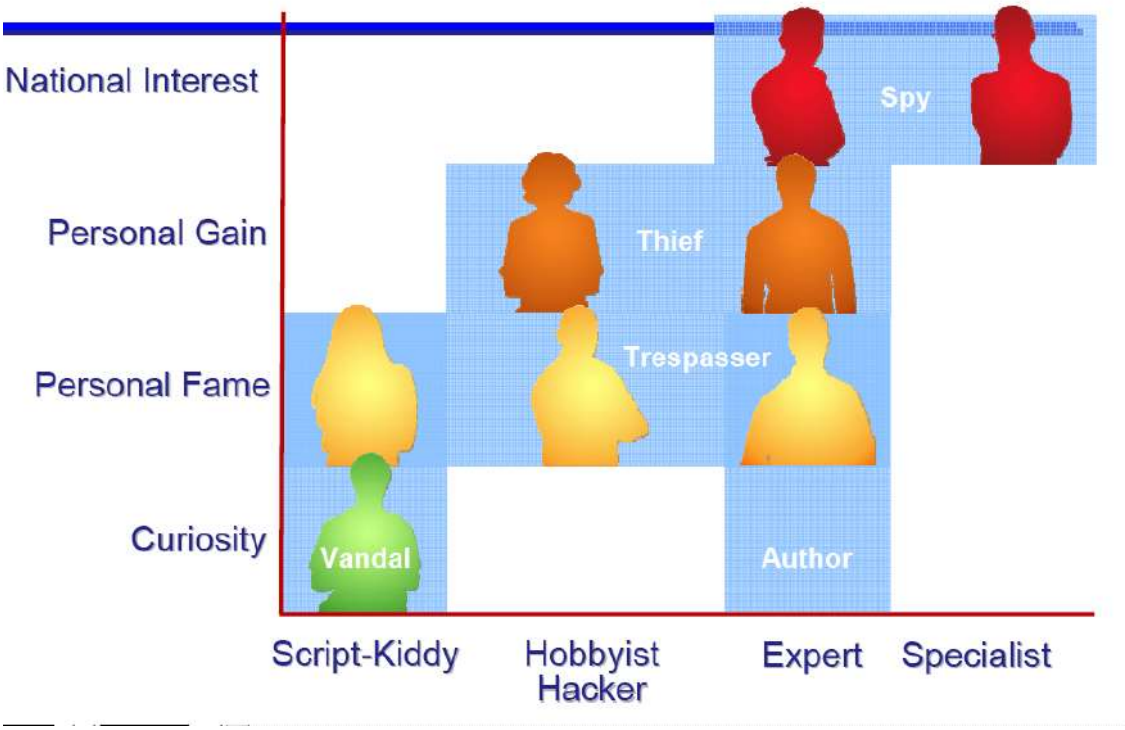

Figure 1: David Aucsmith Cybercrime Analysis Model

The ladder of cybercrime analysis in the model above starts with 'Vandal' who is relatively inexperienced with little or no programming skill. This analytical categories just reflect mere curiosity without malicious intention. Their primary intention may later climb to the level of personal fame. Also, the ability to write scripts could be used as avenues of developing malicious codes such as viruses, worms, Trojans and so on.

In the model, 'Trespassers' are those who are also driven by the desire for fame but range in their skills all the way to expert. Financial gain is not his motivating factor but just showing the world that he can break into secure places of the world through his acquired skills. It might just be an addiction which he shows no care for any personal reputation damage encountered or even ruin to their personal life.

When cybercrime activity is properly examined and analysed, it could be not be for personal fame but some gain-factors may be in it. This is the level of being a thief. A **thief**, as the name implies, is mainly interested in some sort of an illegal gain. According

to Aucsmith's analysis, it is the fastest growing cybercrime. They could use tools developed by others to perpetrate their criminal intention or use self-made tool. Some of the specific and distinctive examples are cyber extortion, economic data espionage, tax evasion, cyber money laundering, salami slicing and so on.

- Given the following list of cybercrime activities, carry out analysis classification on them based on Trespasser or Thief levels: virus, salami slicing, worm, Trojan, cyber laundering
  - At the trespasser's level, there is no any personal gain or financial gain, the examples of such cybercrimes in the list given are virus, worm and Trojan while those that involve financial gains are at the thief level, they are: salami slicing and cyber laundering.

Spy level is the advanced stage of cyber criminality in which national and international interests come to play. Many allied, sponsors, external backups and hidden interests have been introduced. One major example of such is cyber terrorism.

3.2 Thematic Model of the Questionnaire

This model is elaborated using the chart below:

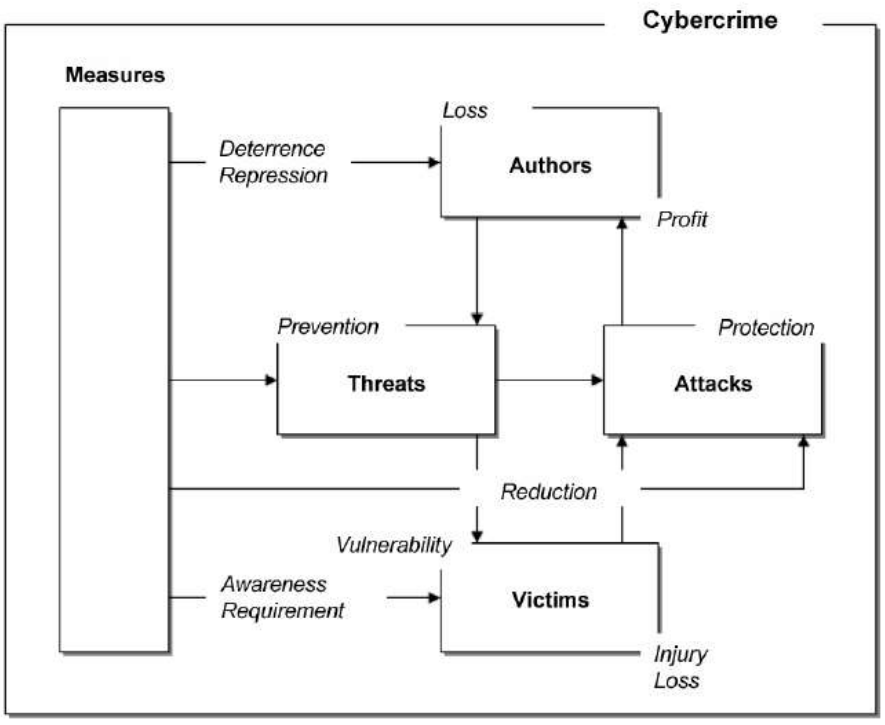

Figure 2: Thematic Model of the Questionnaire

In this model, there are basically four measures. They are Authors, Threats, Attacks and Victims. **Author** is the measure of being inventors of cybercrimes. It is the point of initiating criminality in a cyberspace. At this stage, deterrence measure could be used to stop or mitigate the authorship of new cybercrimes.

Threat is the measure portray having potential of launching an attack. It might be the result of removal, destruction, disruption, interruption, modification of image or data. Preventive measure could be used to avert the occurrence of a potential attacks before they are launched.

Attack is the stage of launching the real damage or negative tendency and due to vulnerability there is a victim. After an attack is effected, protective measure could be used to reduce the extent of damage.

A victim is the measure that shows the state of being harmed by threats that lead to attacks. More vulnerability awareness created will help in minimizing the effects at this stage.

CONCLUSION

Cybercrimes analysis could have several yardsticks, however the David Aucsmith and Thematic for the Questionnaire models considered in this unit can be used to analytically assess cybercrime risk level and the mitigation steps to be taken. Early detection of crime or criminal intention will help in avoiding or reducing eventual damage.

SUMMARY

The two models considered in this unit are David Aucsmith and Thematic for the Questionnaire.

David Aucsmith Models highlights some key areas of assessment:

Vandal's stage: it is just the level of curiosity.

Trespasser's stage: is the stage of personal fame and no financial pain involved

Thief's stage: this is the stage at which personal and financial gains are motivating factors

Spy stage: it is a national interest gain where collaborative efforts of cybercrimes come to play.

On the other hands, thematic model emphasises on authors, threats, attacks and victims which could be respectively deterred, prevented, protected and vulnerability-proofed in order to mitigate against these yardsticks of cyber criminals.

TUTORED MARKED ASSIGNMENTS AND MARKING SCHEME

References

Unit 4 – Effects of Cybercrimes

Introduction

As you have learnt in the previous units, cybercrime which is referred to as computer crime, e-crime and electronic crime. It is also defined as a criminal act where a computer or computer network serves as the location, means, target or as the source of the activity. Types range from outside parties who hack into a computer network to phishing programs which give users a false sense of security, prompting them to divulge sensitive information.

Effects of these crimes are not farfetched, putting into consideration the following questions:

(i) Would you like to have yourself, organization, corporation or business responsible for cyber-crime, without you knowing?

(ii) Would you like to be prosecuted for something you did not do?

(iii) Would you like to be sued for privacy violations?

(iv) Would you like to be the base of operations for major crime?

(v) Would you like to become another survey statistics?

(vi) Would you like to loose clients due to lack of public confidence in your Information Technology system?

(vii) Would you like to be the VICTIM?

All these questions will help us in assessing the effects cybercrimes have on our corporate existence.

2.0 LEARNING OUTCOMES/OBJECTIVES

At the end of this unit, you should be able to:

(i) **I**dentify the new face of crime i.e. cybercrime

(ii) Enumerate the adverse effects of these crime

(iii) Suggest available solutions to prevent these effects from occurring

3.0 **MAIN CONTENT**

Some of the effects of cybercrimes using the questions above as yardsticks are discussed as follows. Even though, some effects are not quantifiable, the losses caused are not small. In this sense, we view the effects of cybercrime activities in terms of the general damage caused or based on categories of the crimes as you have learnt in unit 2.

3.1General Effects of Cybercrimes

3.1.1 Loss of Revenue

One of the main effects of cybercrime on a company is a loss of revenue. This loss can be caused by an outside party who obtains sensitive financial information, using it to withdraw funds from an organization. It can also occur when a business's e-commerce site becomes compromised while inoperable, valuable income is lost when consumers are unable to use the site.

3.1.2 Wasted Time

Another major effect or consequence of cybercrime is the time that is wasted when IT personnel must devote great portions of their day handling such incidences. Rather than working on productive measures for an organization, many IT staff members spend a large percentage of their time handling security breaches and other problems associated with cybercrime.

3.1.3 Damaged Reputations

In cases where customer records are compromised by a security breach associated with cybercrime, a company's reputation can take a major hit. Customers whose credit cards or other financial data become intercepted by hackers or other infiltrators lose confidence in an organization and often begin taking their business elsewhere.

3.1.4 Reduced Productivity

Due to the measures that many companies must implement to counteract cybercrime, there is often a negative effect on employees' productivity. This is because, due to security measures, employees must enter more passwords and perform other time-consuming acts in order to do their jobs. Every second wasted performing these tasks are a second not spent working in a productive manner.

3.1.5 Frustrated Consumer Trust

Since cyber criminality breaks into the web pages disrupting the logic of the information, the end users are always left to suffer the consequences. They are frustrated and at times made to pay hard for it, thereby losing confidence in such sites. This makes the customers to have no trust over such sites and in internet transactions in general. Several reports have shown that many internet users have been left with techno-phobia.

3.2 EFFECTS BASED ON CATEGORIES OF CRIMES

The effects of cybercrime activities could also be viewed on the basis crime categories learnt in unit 2. Two broad cybercrime categories studied are based on targets and objects of legal protection.

3.2.1 Cybercrime Effects based Person

Some activities of cyber criminals targeted against person have damaged the reputation and the integrity of the concerned person(s). There was a case of course mate that took her colleague pill and put it in nude site just for character assassination. In similar vein, social networking websites like facebook, twitter, and so on have become viable tools in adversely attacking the personality of individuals.

3.2.2 Effects of Cybercrimes based on Property

Cybercrimes against property have caused a lot of economic losses and have potentially killed or destroyed prospective productive initiatives. Cyberspace that is supposed to be a fertile environment for economic booming has been turned otherwise by the activities of cyber criminals specially targeted against property other than theirs. The cybercrimes such as intellectual property, credit card fraud, source code theft to mention but a few have made incurred great losses on the property owners. These incidents projected danger signals to the upcoming users.

3.2.3 Government-oriented Effects of Cybercrimes

3.2.4 Effects on Confidentiality, Integrity and Availability of Data

3.2.5 Computer-related Cybercrime Effects

3.2.6 Content-related Cybercrime Effects

3.2.7 Copyright-related Cybercrime Effects

4.0 CONCLUSION

In the end I may conclude that computer crime is a strict criminal act and it should be punished strictly and there should be strict laws against cyber criminals like there are should be punishment against them as there is punishment for other criminals who have committed crimes like stealing etc. computer crime cannot be stopped at this level but immunity can be used to keep safe from it or at least harm could be a lesser.

5.0 SUMMARY

Cyber crime affects more than the financial integrity of a business. There are many very real and damaging consequences associated with Internet crime. Understanding the effects of cyber crime is an important first step in comprehending the necessity of security measures on a computer network.

When you use credit card at a store the transitions are encrypted and sent to the internet and the internet is available globally. Hackers are smart and they can decrypt the information in a few time.

There are few solutions to keep safe from computer crime and they could be a little help for the attacks, antivirus and antispyware tools, firewalls, Cryptography. After theses cyber ethics and law has been formulated to stop these kinds of things. And after these the internet service providers must provide secured internet connections to keep the users safer from the cyber-attacks.

6.0 TUTOR MARKED ASSESSMENT AND MARKING SCHEME

Assessment

- Highlight various reasons the protection and security of a company, individual or group is important? 10mks

(1b) State an example of an attack to buttress this. 2mks

(2).As a cyber security personnel, suggest possible security measures a

I a company should put in place 4mks

Ii an individual should observe 4mks

TOTAL MKS= 20mks

Answers

(1)The protection and security of a company, individual or group is important putting into consideration the above listed adverse effects, recovering from each of the effects entails so many lost of resources most rampantly is great financial losses in every attack.

(ii) Example : On Tuesday 18th March Data thieves enter into the computer of Hanford and sweet bay supermarkets and stole $4.2 million and debit card numbers.

HINT: students should provide different attacks, there are thousands of attacks

- Security measures that should be put in place by

I a company must put in place

1. The use of firewalls, antivirus
2. Establishment of Virtual Private Network
3. Use of Intrusion Detection software's e.g snort

(ii) an individual should ensure the use of a genuine antivirus, firewalls, enable windows defender, regular windows update

7.0 REFERENCES

(1) **Effects of cybercrime by** Meaghan Ringwelski, eHow Contributor

(2) Effects of cybercrime against women in India by advocate debarati

(3) computer crime and its effect © 2003 - 2012 - Law Teacher

(4) Copyright ©2012 A&L Computer Software Ltd.

Unit 5 – Current and Future Trends of Cybercrimes

1.0 Introduction

Cybercrime is evolving at an astounding pace, following the same dynamic as the inevitable penetration of computer technology and communication into all walks of life. Whilst society is inventing and evolving, at the same time, criminals are deploying a remarkable adaptability in order to derive the greatest benefit from it. To avoid giving cybercriminals the initiative, it is important for those involved in the fight against cybercrime to try to anticipate qualitative and quantitative changes in its underlying elements so that they can adjust their methods appropriately.

2.0 Learning Outcomes/Objectives

At the end of this unit, you should be able to:

(i) Current trends of cybercrimes;

(ii) Future trends of cybercrimes;

(iii) Give a distinct difference between the current and future trends.

3.0 main content

DEFINITION OF CYBERCRIME

Etymologically, *"cybercrime"* combines the term *"crime"* with the root *"cyber"* from the word *"cybernetic"*, from the Greek, "*kubernân*", which means to lead or govern. The *"cyber"* environment includes all forms of digital activities, regardless of whether they are conducted through networks and without borders. This extends the previous term "*computer crime*" to encompass crimes committed using the Internet, all digital crimes, and crimes involving telecommunication networks. This more recent terminology covers a wide variety of facets, leading to different approaches, depending on the dominant culture of the experts, making it appear either reduced or expanded, in different dimensions, dealing with emerging issues that also reflect its diversity. Some of the kinds of Cyber-criminals are mentioned as below:

- Crackers: These individuals are intent on causing loss to satisfy some antisocial motives or just for fun. Many computer virus creators and distributors fall into this category.
- Hackers: These individuals explore others' computer systems for education, out of curiosity, or to compete with their peers. They may be attempting to gain the use of a more powerful computer, gain respect from fellow hackers, build a reputation, or gain acceptance as an expert without formal education.
- Pranksters: These individuals perpetrate tricks on others. They generally do not intend any particular or long lasting harm.
- Career criminals: These individuals earn part or all of their income from crime, although they Malcontents addicts, and irrational and incompetent people: "These individuals extend from the mentally ill do not necessarily engage in crime as a full-time occupation. Some have a job, earn a little and steal a little, then move on to another job to repeat the process. In some cases they conspire with others or work within organized gangs such as the Mafia.
- Cyber terrorists: There are many forms of cyber terrorism. Sometimes it's a rather smart hacker breaking into a government website, other times it's just a group of like-minded Internet users who crash a website by flooding it with traffic.
- No matter how harmless it may seem, it is still illegal to those addicted to drugs, alcohol, competition, or attention from others, to the criminally negligent.
- In general cyber crimes can be categorized as follows-
- 3.1 DATA CRIME
- a. <u>Data Interception</u>
- An attacker monitors data streams to or from a target in order to gather information. This attack may be undertaken to gather information to support a later attack or the data collected may be the end goal of the attack. This attack usually involves sniffing network traffic, but may include observing other types of

data streams, such as radio. In most varieties of this attack, the attacker is passive and simply observes regular communication, however in some variants the attacker may attempt to initiate the establishment of a data stream or influence the nature of the data transmitted. However, in all variants of this attack, and distinguishing this attack from other data collection methods, the attacker is not the intended recipient of the data stream. Unlike some other data leakage attacks, the attacker is observing explicit data channels (e.g. network traffic) and reading the content. This differs from attacks that collect more qualitative information, such as communication volume, not explicitly communicated via a data stream.

- b. Data Modification

- Privacy of communications is essential to ensure that data cannot be modified or viewed in transit. Distributed environments bring with them the possibility that a malicious third party can perpetrate a computer crime by tampering with data as it moves between sites. In a data modification attack, an unauthorized party on the network intercepts data in transit and changes parts of that data before retransmitting it. An example of this is changing the dollar amount of a banking transaction from $100 to $10,000. In a replay attack, an entire set of valid data is repeatedly interjected onto the network. An example would be to repeat, one thousand times, a valid $100 bank account transfer transaction.

- c. Data Theft

- Term used to describe when information is illegally copied or taken from a business or other individual. Commonly, this information is user information such as passwords, social security numbers, credit card information, other personal information, or other confidential corporate information. Because this information is illegally obtained, when the individual who stole this information is apprehended, it is likely he or she will be prosecuted to the fullest extent of the law

- 3.2 NETWORK CRIME
- a. Network Interferences
- Network Interfering with the functioning of a computer Network by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing Network data.
- Network Sabotage
- 'Network Sabotage' or incompetent managers trying to do the jobs of the people they normally are in charge of? It could be the above alone, or a combination of things. But if Verizon is using the help the children, hindering first responders line then they might be using network problems as an excuse to get the federal government to intervene in the interest of public safety. Of course if the federal government forces these people back to work what is the purpose of unions and strikes anyway.
- 3.3 ACCESS CRIME
- a. Unauthorized Access
- "Unauthorized Access" is an insider‘s view of the computer cracker underground. The filming took place all across the United States, Holland and Germany. "Unauthorized Access" looks at the personalities behind the computers screens and aims to separate the media hype of the 'outlaw hacker' from the reality
- b.Virus Dissemination
- Malicious software that attaches itself to other software. (virus, worms, Trojan Horse, Time bomb, Logic Bomb, Rabbit and Bacterium are examples of malicious software that destroys the system of the victim

3.4 CURRENT TRENDS OF CYBER CRIMES

3.4 .1 TROJAN WARS WILL CONTINUE, BUT ZEUS WILL PREVAIL AS THE TOP FINANCIAL MALWARE

RSA has been observing the Trojan landscape throughout 2011, and Zeus 2.0 has continued to dominate as the leading financial Trojan throughout the year. Indisputably the most widely spread financial malware in the world, Zeus is responsible for around 80% of all attacks against financial institutions today and is estimated to have caused over $1 billion in global losses in the last five years.

Other Trojan/malware trends expected to continue in 2012 include:

For mobile platforms: A growing trend in the world of cybercrime codes will further carry Zeus (ZitMo) and Spyo) over to the various mobile platforms, with the purpose of having these banking.Trojans steal data such as SMS codes. “InfoStealers” for the mobile platform are also likely to emerge with Trojans designed to keylog touch-screen input and monitor data traffic through the mobile device.

3.4 .1.1 Privately-owned and geo-specific Trojan development

In 2011, cybercriminals demanded more customized Trojans, built for the types of fraud operations they planned to execute. For example, in 2011, there was an increased development of private Trojans as well as codes adapted to specific geographies. The Shiz Trojan, targeted at Russian banking applications, is just one example.

3.4 .1.2 Banking Trojans will be sold in varying business models

The sophisticated business models used by cybercriminals has allowed tools and services once reserved for the cybercrime elite to be made available on the black market as commodities. The more savvy criminals offer their goods and services to those who may be starting out or are in need of set-up and instructions. Whether selling off-the-shelf botnets, Trojans by the binary, or Zeus recompiles, the underground is loaded with tools to allow any “newbie” cybercriminal to launch an attack.

3.4.2 Cyber criminals will find new ways to monetize non-financial data,

Cybercriminals continue to understand the value of non-financial data harvested by their Trojans and are already actively looking for ways to monetize this information. Not only is victims' information being traded in the underground, but access to victims' computers is increasingly being offered for sale, as well. Some examples of non-financial data for sale in the underground today are as follows:

3.4.2.1 Utility Statements

Exemplifying interest in non-financial data include cybercriminals seeking access to billing statements of consumer's utility accounts, including accounts with gas and electricity providers, as well as telecommunication providers. Perpetrators likely collect these details in order to trace additional personally identifiable information (PII) or facilitate other forms of identity theft such as the opening of new bank accounts or obtaining personal loans.

3.4.2.2 Medical Records

Numerous instances of fraudsters seeking "fresh" medical records were also traced possibly for such cash out operations as selling patient databases to law firms or to commit insurance billing fraud. Currently, the three types of non-financial information most widely traded in the underground consist of spam mailing lists, dates of birth (DOB), and unfiltered Trojan logs.

3.4.3 FRAUD-AS-A-SERVICE VENDORS WILL BRING NEW INNOVATIONS

The fraud underground is a vivid marketplace where different types of vendors create tools, share methods for making money, and find ways to sell anything they can create and monetize per the market's demand. Fraud-as-a-service (FaaS) is the one area of the underground economy which has seen the most consistent innovation throughout 2011.

Comparable to legitimate hosted software service (SaaS) providers, those who create and provide the fraud supply chain with the latest Trojan codes and plug-ins offer their work and associated services to those who require turnkey solutions, set-up, instructions and support. Fraud-as-a-service will continue to evolve in all directions, making it easier to find, buy and pay for "off the shelf" services that continue to make it easier for cybercriminals to commit fraud. RSA expects a series of new technologies, services, and business models to emerge in the underground as FaaS continues to grow

3.4.4 OUT-OF-BAND METHODS WILL FORCE CYBER CRIMINALS TO INNOVATE.

Strong authentication at login has become necessary to protect online financial accounts. However, cybercriminals are consistently developing new attack methods that can bypass login authentication – and even two-factor authentication systems. Some attacks that have continued to evolve throughout 2011 are man-in-the-browser Trojans and SMS forwarding.

3.4.4.1 Man-in-the-browser Trojans

Man-in-the-browser (MITB) Trojans first emerged in 2007 as a way for cybercriminals to overcome two-factor authentication – specifically one-time passwords. A MITB Trojan works by intercepting data as it passes over a secure communication

between a user and an online application. In just a short time, MITB Trojans have advanced so quickly that most of the available kits for sale on the black market come programmed with functionality to fully automate the process from infection to cash out.

3.4.4.2 SMS Forwarding

Some financial institutions have implemented out-of-band SMS authentication as an additional layer of security for confirming high-risk transactions. Referred to by some as a "man-in-the-mobile" attack, SMS forwarding shows the rapid evolution of Trojan development.

3.4.5 Hacking will drive Enterprises to re-evaluate their security postures

Hacktivism was further popularized in 2011 as groups such as Anonymous, LulzSec, and AntiSec took on governments and major global corporations through highly-publicized hacking incidents. The goals of hacktivism are most often driven by a politically charged agenda with the intent to cause fear, intimidation, or public humiliation.

A general profile of these anti-establishment vigilantes follows:

3.4.5.1 Motivations:

Ego, populist agenda, self-declared moral code, front for other organizations

3.4.5.2 Methods:

Bribery, recruitment of insiders, malware and hacking tools that target a specific systems or set of data, denial-of-service tools

3.4.5.3 Target:

Large corporations, governments, supply chains, security or media outlets that oppose their agenda or moral code

3.4.5.4 Inherent Risk:

Varies depending on the nature of protected information and the public profile of potential targets

3.4.6 Cooperation and information sharing between International Law Enforcement agencies will continue to become more integral to fighting cyber crime's cyber-gangs and botnet operators.

Cybercrime victims are often targeted by botmasters operating from within a country other than their own. Perpetrators' infrastructures are usually dispersed over numerous locations, with bulletproof hosting services purchased in one country, domain registrations performed by providers in another country, and money mules often recruited using bogus job ads appealing to residents of the target country. Furthermore, the botnets used to disguise an attack's "mother ship" web servers, more often than not comprise machines scattered around the globe. In addition, commercially-available Trojan kits, sold in fraudster forums, are coded by malware authors of diverse nationalities.

3.5 FUTURE TRENDS OF CYBER CRIMES

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 [33] are briefly summarized in the followed text.

3.5.1 Laptop encryption

Laptop encryption will be made mandatory at many government agencies and other organizations that store customer/patient data and will be pre-installed on new equipment. Senior executives, concerned about potential public ridicule, will demand that sensitive mobile data be protected. This development provides a reasonable safety blanket to protect against an epidemic of laptop and PDA theft.

Whether the data on the stolen (or lost) laptops is ever read, the mere theft makes the company and its executives subject to security breach disclosure laws and public ridicule.

3.5.1.1 PDA smart phones

Theft of PDA smart phones will grow significantly. Both the value of the devices for resale and their content will draw large numbers of thieves.

3.5.2 Attack targets

3.5.2.1 Targeted cyber attacks

Targeted attacks will be more prevalent, in particular against government agencies. Targeted cyber attacks by nation states against US government systems over the past three years have been enormously successful, demonstrating the failure of federal cyber security activities. Other antagonistic nations and terrorist groups, aware of the vulnerabilities, will radically expand the number of attacks. Targeted attacks on commercial organizations will focus on military contractors and businesses with valuable customer information.

The most common technique used in targeted attacks against military sites is spear phishing. Spear phishing uses fake emails sent to the employees of a target organization. The email seems to come from a key manager of the target and orders each recipient to load a piece of spyware or to provide log-in information that the attackers use to break in and steal important data.

3.5.2.2 Cell phone worms

Cell phone worms will infect at least 100,000 phones, jumping from phone to phone over wireless data networks. Cell phones are becoming more powerful with full-featured operating systems and readily available software development environments. That makes them fertile territory for attackers fuelled by cell phone adware profitability.

3.5.2.3 Voice over IP (VoIP) systems

Voice over IP (VoIP) systems will be the target of cyber attacks. VoIP is an immature technology that is often deployed hastily in organizations that do not understand the security challenges they will face. A new type of phishing attack is also using VoIP technology to get bank credentials to steal money.

The attacker sends an email to a potential victim saying that a bank doesn't want the victim to use the internet but needs some data verified and gives a phone number to call that seems to be in the correct (local) area code (VoIP technology allows people anywhere in the world to appear to have a local phone number in any location they choose).

The victim calls the number and is asked to key in or say their account number and password. The criminals use the data to empty the victim's bank account.

3.5.3 Attack techniques

3.5.3.1 Spyware

- Spyware will continue to be a huge and growing issue. The spyware developers can make money so many ways that development and distribution centres will be established throughout the world.

3.5.3.2 Security vulnerabilities

Zero-day vulnerabilities will result in major outbreaks resulting in many thousands of PCs being infected worldwide. Security vulnerability researchers often exploit the holes they discover before they sell them to vendors or vulnerability buyers like 'Tipping Point'.

The ranks of security researchers is growing rapidly, in part because they can sell what they find to Verisign's defense or 3Com's Tipping Point. Sadly by the time the researchers sell their discoveries, most have already been used by someone as zero-day attacks breaking into high-value sites.

3.5.3.3 Rootkits

The majority of bots will be bundled with rootkits. The rootkits will change the operating system to hide the attack's presence and make uninstalling the malware almost impossible without reinstalling a clean operating system.

Rootkit sophistication is soaring. Ed Skoudis, SANS Hacker Exploits course director, tells of a tool called the Blue Pill that uses new virtualization features of recent AMD processors to create a practically undetectable rootkit as a virtual machine hypervisor, subverting a system at an extremely deep level, far below the operating system itself.

4.0. 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.

5.0. SUMMARY

If you have read this far, you will have seen that attacker sophistication seems to be ahead of defensive tools. That is the nature of the war between hackers and defenders: the attackers are always a step ahead. But by making the attackers' job harder and harder and by increasing the length of gaol sentences for cybercrime and improving international police co-operation and skill levels, we can continue to keep up with the attackers and, over time, begin to turn the tide.

6.0 Tutor marked assignment and marking scheme

1. What is cyber crime

2. List the major kind of cyber crimes
3. In details explain the resons for cyber crime
4. In your own simple english define a trojan horse
5. Explain : hacking will drive enterprises to re-elvaluate their security posture under the following heading

   motivation

   methods

   target

   inherent risk

6. Define the following terms

access crime

Network crime

data crime

sms forwarding

targeted cyber attack

REFERENCE

- http://www.bloomberg.com/news/2011-12-13/china-based-hacking-of-760-companies-reflects-undeclaredglobal-cyber-war.html
- Cyber Trust and Crime Prevention, Mid-Term Review, November 2005 – January 2009, Available at:

http://www.bis.gov.uk/assets/bispartners/foresight/docs/cyber/ctcp_midterm_review.pdf

- D'Amico, A., 2000, What Does a Computer Security Breach Really Cost?, The Sans Institute
- Stephen Northcutt et al. (2011), Security Predictions 2012 & 2013 - The Emerging Security Threat, Available at: http://www.sans.edu/research/security-laboratory/article/security-predict

Module 2 – Cybercrime Modes of Operation

Unit 1 – Modes Operandi of Cyber criminality

1.0 INTRODUCTION

Throughout the past several decades there have been numerous advances in Electronic resources. Technologies such as cellular phones, pagers, home computers, the Internet, websites, and palm pilots have added another dimension to crime. That Dimension involves increased methods at criminals' disposal to commit certain crimes Along with increased locations in which crimes can occur. For example, property crimes no longer have to involve face-to-face contact between the criminal and the victim. In the past, property crimes usually involved a criminal breaking into a victim's house or grabbing a purse from a person on the street. Today, criminals can commit property crimes from the comfort of their own homes against people who live on the other side of the world through the use of computers. Computer crime poses a daunting task for law enforcement agencies because they are highly technical crimes. Law enforcement agencies must have individuals trained in computer science or computer forensics in order to properly investigate computer crimes. Additionally, states must update and create legislation, which prohibits computer crimes and outlines appropriate punishments for those crimes. Computer crimes will likely become more frequent with the advent of further technologies. It is important that civilians, law enforcement officials, and other members of the criminal justice system are knowledgeable about computer crimes in order to reduce the threat they pose.

2.0 LEARNING OUTCOMES/OBJECTIVE

- To enlighten the masses and clarify the areas of illegal activities and redefine the term" cybercrime" for the next decade.

- To note the place cybercrime has and how will it be related to other forms of crimes and offenses, including counterfeiting, financial and economic crimes, child pornography, drug trafficking, human beings trafficking, terrorism, and other crimes.

- What will be the overall impact of technological changes and breakthroughs, including cloud computing, virtual systems, mobile systems, cryptology, steganograph and malware, on the control – or rather on the rise – of this phenomenon?

- To be abreast of current and emerging threats and the new expected forms of cybercrime, along with their level of sophistication.

- What changes can be expected in the distribution of threats to the confidentiality integrity, availability, and accountability of information and systems.

- Given the various modes of operation of cybercrimes, it might be possible to identify a pattern to counter such attacks.

- In what ways can our current institutional and initial training plans be adapted to respond to all aspects of cybercrime, from ordinary risk to cyber war.

- What trend will companies and individuals follow in terms of applying security standards and controlling the implementation of corresponding measures and procedures?

3.0 Definition and Aspects of Cybercrime Modus Operandi

Etymologically, "cybercrime" combines the term "crime" with the root "cyber" from the word "cybernetic". The "cyber" environment includes all forms of digital activities, regardless of whether they are conducted through networks and without borders. This extends the previous term "computer crime" to encompass crimes committed using the Internet, all digital crimes, and crimes involving telecommunications networks. This more recent terminology covers a wide variety of facets, leading to different approaches, depending on the dominant culture of the experts, making it appear either reduced or expanded, in different dimensions, dealing with emerging issues that also reflect its diversity.

Criminal Aspect of Cybercrime

From a criminal dimension, some experts say that there is no need to change or redefine this term, but rather a need to clarify what it encompasses, using the Council of Europe's Convention on Cybercrime. They emphasize the coexistence of common law offenses from the real world with other offenses that are more related to the virtual world or even more specific, such as online identity theft. The proportions of the various types of offenses committed or seen in light of public sensitivities are subject to change. The next ten years will certainly bring the development of the financial aspect – including money laundering, despite it already being easy to circumvent the traditional banking system using the Internet – involving organized crime groups, often on an international level, and the importance of keeping personal data secure.

Others, however, prefer the term "digital technology crime", which includes offenses and lawsuits that involve digital technology. Others still point out that the term "cybercrime" rather oversimplifies matters, given the distribution of damage caused, mainly related to causes outside of computing, and the various procedures involved.

Technological Aspect of Cybercrime

From a technological dimension, other experts point out the need for a comprehensive term, such as "electronic crime" or "e-crime", thanks to the convergence of ICT, including mobile technology, telephony, memory, surveillance systems, and other technologies, including nanotechnology and robotics, which must be taken into account from now on. These electronic media will be targeted increasingly more often and will also be used to conceal, commit, or support crimes and offenses. Only the positive actions for which one or more means were used to commit one of the elements of the offense can be included.

3.1 Modis-Operandi

Before most cybercrimes take place, the hackers or crackers usually prepare and plan for the attack in other for it to be successful. Hacking involves more than just penetrating and patching. Proven techniques are usually put in place to help guide ht criminal along the hacking highway and ensure that they end up at the right destination. Because these cyber-criminals are highly skilled in computer usage and manipulation, planning a methodology that supports their hacking goals is what separates the professionals from the amateurs. In these material, Most cyber-criminals will be referred to as hackers unless stated otherwise. The reason for this is because hacking is probably the most common cyber-crime.

Setting the Stage

In the past, hacking was mostly a manual process. Now, tools can automate various tasks. These tools allow criminals to focus on performing the tests instead of on the testing methods. They gather information — often small pieces — and assemble the pieces of the puzzle. These criminals often start at point A with several goals in mind, hack (repeating many steps along the way), and move closer until they discover security VULNERABILITIES at point B. The goals and how they achieve them are different. In addition hacker will eventually attempt to assess all information-security

VULNERABILITIES and how to EXPLOIT them. Today's attackers can come from any angle against any system, not just from the perimeter of the network and the Internet. They usually Test every possible entry point, including partner, vendor, and customer networks, as well as home users, wireless LANs, and modems.

Most hi-tech cyber-criminals usually start from a ground zero-level with nothing but the organization or individual name and no other information that gives you a leg up, such as:

- IP addresses
- Host names
- Software versions
- Firewall rules
- Phone numbers
- Employee names

All cyber-criminals have to worry about covering their tracks or evading intrusion-detection systems, because everything you're doing is illegitimate.

A couple of methodologies are now cited to serve as a case-study.

3.2 Social Engineering

Typically in social engineering, criminals pose as someone else to gain information they otherwise can't access. These cyber-criminals then take the information obtained from their victims and wreak havoc on network resources, steal or delete files, and even commit industrial espionage or some other form of fraud against the organization they're attacking. Social engineering is different from physical-security issues, technical attacks, but they are related.

Here are some examples of social engineering:

- False support personnel claim that they need to install a patch or new version of software on a user's computer, talk the user into downloading the software, and obtain remote control of the system.

- False vendors claim to need to make updates to the organization's accounting package or phone system, ask for the administrator password, and obtain full access.
- False contest Web sites run by hackers gather user IDs and passwords of unsuspecting contestants. The hackers then try those passwords on other Web sites, such as Yahoo! and Amazon.com, and steal personal or corporate information.

- False employees notify the security desk that they have lost their keys to the computer room, are given a set of keys, and obtain unauthorized access to physical and electronic information.

- Sometimes, social engineers act as forceful and knowledgeable employees, such as managers or executives. Other times, they may play the roles of extremely uninformed or naïve employees.

3.2.1 How Criminals Performing Social-Engineering Attack

The process of social engineering is actually pretty basic. In general, social engineers find the details of organizational processes and information systems to perform their attacks. With this information, they know what to pursue. Hackers typically perform social-engineering attacks in four simple steps:

1. Perform research.

2. Build trust.

3. Exploit relationship for information through words, actions, or technology.

4. Use the information gathered for malicious purposes.

I. Perform research.

Social engineers typically start by gathering public information about their victim. Many social engineers acquire information slowly over time so they don't raise suspicion. Obviousness is a tip-off when defending against social engineering.

Using the Internet Today's basic research medium is the Internet. A few minutes on Google or other search engines, using simple key words such as the company name or specific employees' names, often produces a lot of information. You can find even more information in SEC filings at www.sec.gov and at sites such as www.hoovers.com and finance.yahoo.com. In fact, many organizations — especially upper management — would be dismayed by what's available. By using this search-engine information and browsing the company's Web site, the hacker often has enough information to start.

II. Building trust

Trust so hard to gain, so easy to lose. Trust is the essence of social engineering most humans trust other humans until a situation occurs that forces them not to. We want to help one another, especially if trust can be built and the request for help is reasonable. Most people want to be team players in the workplace and don't know what can happen if they divulge too much information to a "trusted" source. This is why social engineers can accomplish their goals. Of course, building deep trust often takes time. Crafty social engineers gain it within minutes or hours. How do they build trust?

- Likability: Who can't relate to a nice person? Everyone loves courtesy. The friendlier the social engineer — without going overboard — the better his chances of getting what he wants. Social engineers often begin by establishing common interests. They often use information they gained in the research phase to determine what the victim likes and act as if they like those things as well.

- Believability: Of course, believability is based in part on the knowledge that social engineers have and how likable they are. But social engineers also use impersonation — perhaps posing as a new employee or fellow employee that the victim hasn't met. They may even pose as a vendor that does business with the organization. They often modestly claim authority to influence people. The most common social-engineering trick is to do something nice so that the victim feels obligated to be nice in return or to be a team player for the organization.

III. Exploiting the relationship

After social engineers obtain the trust of their unsuspecting victims, they coax them into divulging more information than they should. They do this through face-to-face or electronic communications that victims feel comfortable with, or they use technology to get victims to divulge information.

IV. Using the Information For Malicious Use

Finally after all the necessary information is gotten, it is most often used for malicious purpose.

3.2.2 Social-Engineering Countermeasures

There are only a few good lines of defense against social engineering. Even with strong security systems, a naïve or untrained user can let the social engineer into the network. Never underestimate the power of social engineers.

Policies

Specific policies help ward off social engineering long-term in these areas:

- Classifying data
- Hiring employees and contractors and setting up user IDs

- Terminating employees and contractors, and removing user IDs
- Setting and resetting passwords
- Handling proprietary and confidential information
- Escorting guests

These policies must be enforceable and enforced — for everyone within the organization. Keep them up to date and tell your end users about them.

User awareness

The best line of defense against social engineering is an organization with employees who can identify and respond to social-engineering attacks. User awareness begins with initial training for everyone and follows with security awareness initiatives to keep social-engineering defenses on everyone's mind. Align training and awareness with specific security policies.

3.3 PASSWORDS

Password hacking is one of the easiest and most common ways hackers obtain unauthorized computer or network access. Although strong passwords that are difficult to crack (or guess) are easy to create and maintain. Users often neglect this; therefore, passwords are one of the weakest links in the information-security chain. Passwords rely on secrecy. After a password is compromised, its original owner isn't the only person who can access the system with it. That's when bad things start happening.

Criminals have many ways to obtain passwords. They can glean passwords simply by asking for them or by looking over the shoulders of users as they type them in. Hackers can also obtain passwords from local computers by using password-cracking software. To obtain passwords from across a network, hackers can use remote cracking utilities or network analyzers and off course using Social engineering.

Password Vulnerabilities

When you balance the cost of security and the value of the protected information, the combination of user ID and secret password is usually adequate.

However, passwords give a false sense of security. The bad guys know this and attempt to crack passwords as a step toward breaking into computer systems. One big problem with relying solely on passwords for information security is that more than one person can know them. Sometimes, this is intentional; often, it's not. You can't know who has a password other than the owner. Knowing a password doesn't make someone an authorized user.

Here are the two general classifications of password vulnerabilities:

- Organizational or end-user vulnerabilities: This includes lack of password awareness on the part of end users and the lack of password policies that are enforced within the organization.
- Technical vulnerabilities: This includes weak encryption methods and insecure storage of passwords on computer systems.

Before computer networks and the Internet, the user's physical environment was an additional layer of password security. Now that most computers have network connectivity, that protection is gone.

Organizational password vulnerabilities

It's human nature to want convenience. This makes passwords one of the easiest barriers for an attacker to overcome. Almost 3 trillion (yes, trillion with a t and 12 zeros) eight-character password combinations are possible by using the 26 letters of the alphabet and the numerals 0 through 9. However, most people prefer to create passwords that are easy to remember. Users like to use such passwords as "password," their login name, or a pet's name.

Unless users are educated and reminded about using strong passwords, their passwords usually are

- Weak and easy to guess.
- Seldom changed.
- Reused for many security points. When bad guys crack a password, they try to access other systems with the same password and user name.
- Written down in insecure places. The more complex a password is, the more difficult it is to crack. However, when users create more complex passwords, they're more likely to write them down. Hackers can find these passwords and use them against you.

Technical password vulnerabilities

You can often find these serious technical vulnerabilities after exploiting organizational password vulnerabilities:

- Weak password-encryption schemes. Hackers can break weak password storage mechanisms by using cracking methods that I outline in this chapter. Many vendors and developers believe that passwords are safe from hackers if they don't publish the source code for their encryption algorithms. Wrong persistent, patient hacker can usually crack this security by obscurity fairly quickly. After the code is cracked, it is soon distributed across the Internet and becomes public knowledge. Password-cracking utilities take advantage of weak password encryption. These utilities do the grunt work and can crack any password, given enough time and computing power.
- Software that stores passwords in memory and easily accessed databases.
- End-user applications that display passwords on the screen while typing.

3.4 Technical Cyber-Crime Methodology

This is the counterpart to social engineering modes of cyber-crime. It involves using various tools to gain access into a system as opposed to social engineering. In this category, we have things like:

a. Denial of Service
b. Unauthorized access
c. Malware

3.4.1 Denial of Service

A denial of service attack is a targeted effort to disrupt a legitimate user of a service from having access to the service. This may be accomplished through a number of methods. Offenders can limit or prevent access to services by overloading the available resources, changing the configuration of the service's data, or physically destroying the available connections to the information.

3.4.2 Unauthorized Access

Unauthorized access is a prerequisite to many forms of computer crimes and computer fraud. This form of crime amounts to electronic intrusion, or gaining access to resources via a computer resource without permission. Unauthorized access may occur both on individuals' personal computers, as well as in the workplace. One major form of unauthorized access is known as hacking. Hacking is "…the act of gaining unauthorized access to a computer system or network and in some cases making unauthorized use of this access." (Rushinek & Rushinek, 1993) As stated previously, unauthorized access may be a gateway to commit other offenses.

3.4.3 Malicious Software

Viruses and malicious programs can potentially impact a massive amount of individuals and resources. These programs are intended to cause electronic resources to function abnormally and may impact legitimate users access to computer resources. For instance,

the “Melissa” virus released in early 1999 contaminated 1.2 million computers used by U.S. businesses, impacted computer resources throughout the U. S. and Europe, and is estimated to have created eighty million dollars in damages worldwide (Computer Crimes and Intellectual Property Section, 2003).These are the three main classes of malware.

- Viruses
- Worms
- Trojans

1.0 CONCLUSION

The past several decades have brought a vast increase in the availability of electronic resources. With this increased availability has come a new form of criminal activity that takes advantage of electronic resources, namely computer crime and computer fraud. Currently, these new forms of crime are burgeoning and pose a new and lasting challenge to law enforcement agencies at all levels in how to prevent, investigate, and prosecute these crimes. Law enforcement agencies from the local to the federal level are beginning to institute specific units devoted to handling computer-related offenses, but there does not currently exist a uniform method to define and address computer crime and computer fraud.

But in reality these units cannot function fully unless they know how cyber-criminals operate. It is in these aspects that this material can be of use.

5.0 SUMMARY

With this case study, we intend to analyze what the current level of understanding is regarding computer crime and computer fraud.

What is being done by law enforcement agencies to deal with these offenses. Using this information, we provided specific recommendations regarding computer-related offenses in the future including:

- Uniform definition
- Organizational requirements and procedures
- Tools necessary to successful operation of computer crime units

6.0 Tutor Marked Assignment and Marking Scheme

- Introduction and definition of cyber-crime---------- 25%
- Ability to state learning objectives---------- 15%
- Discussion of social engineering and Countermeasures---------- 30%
- Explanation and discussion of passwords and its vulnerabilities---------- 20%
- List and explain the various forms of malware---------- 10%

7.0 REFERENCES

- CERT. Denial of Service Attacks.

  http://www.cert.org/tech_tips/denial_of_service.html (accessed 22 November 2004).

- Computer Crime Research Center. About Computer Crime Research Center.

  http://www.crime-research.org/about/ (accessed 23 November 2004).

- Haantz, S. WCC Issue: Computer Crime: Computer as the Instrumentality of the Crime. National White Collar Crime Center. September 2002.

- National Institute of Justice. JUSTNET - Justice Technology Information Network.
  http://www.nlectc.org/assistance/justnet.html (accessed 22 November 2004).

- National Security Institute. Code of Iowa 1989.
  http://nsi.org/Library/Compsec/computerlaw/Iowa.txt (accessed 15 October 2004).

- PBS. Computer Crime Laws.
  http://www.pbs.org/wgbh/pages/frontline/shows/hackers/blame/crimelaws.html
  (Accessed 3 November 2004).

- Thompson, David. "1997 Computer Crime and Security Survey". Information
  Management and Computer Security. 6.2 (1998)

Module 3 – Countermeasures

Unit 1 – Cybercrime countermeasures

1.0 Introduction

This module attempts to define cyber crimes, various classifications of cyber crimes and their counter measures.

2.0 Objectives.

This module introduces the student to the subject of cyber crime and counter measures. The core objective of this module is to familiarize the reader with:

- What is cyber crime;
- Types of cyber crime activities;
- Classifications of cyber crime activities;
- Damages cause by cyber criminals; and
- Measures to be taken to prevent cyber criminals;

3.0 Main content

3.1 Definitions of Cybercrime

Despite the fact that the word "Cybercrime" has entered into common usage, many people would find it hard to define the term precisely. Furthermore, there is no catch all term for the tools and software which are used in the commission of certain online crimes.

Most reports, guides or publications on cybercrime begin by defining the term "cybercrime". One common definition describes cybercrime as any activity in which computers or networks are a tool, a target or a place of criminal activity. Some definitions try to take the objectives or intentions into account and define cybercrime more precisely, defining cybercrime as "computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic

networks". These more refined descriptions exclude cases where physical hardware is used to commit regular crimes, but they risk excluding crimes that are considered as cybercrime in international agreements such as the "Convention on Cybercrime". For example, a person who produces USB-devices containing malicious software that destroy data on computers when the device is connected commits a crime.

Cyber Crime

Cyber crime is the current and perhaps the most complicated problem in the cyber world.

Cyber crime may be said to be those species, of which, genus is the conventional crime, and

Where either the computer is an object or subject of the conduct constituting crime. 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.

However, the act of deleting data using a physical device to copy malicious code has not been committed through global electronic networks and would not qualify as cybercrime under the narrow definition above. This act would only qualify as cybercrime under a definition based on a broader description, including acts such as illegal data interference.

This demonstrates that there are considerable difficulties in defining the term "cybercrime". The term "Cybercrime" is used to describe a range of offences including traditional computer crimes, as well as network crimes. The fact that there is no single definition of "cybercrime" need not be Important, as long as the term is not used as a legal term. However, the definition is broader, including activities such as fraud, unauthorized access, child pornography, and cyber stalking. The United Nations Manual on the Prevention and Control of Computer Related Crime includes fraud, forgery, and unauthorized access.

3.2 Types of cyber crime activities includes;

1. Virus, Trojan and worms
2. Email bombing
3. Email account hacking
4. Credit card fraud
5. Music piracy
6. Software piracy
7. Salami slicing
8. Source code theft
9. Email/Website spoofing
10. Intellectual property theft
11. Email scam
12. Online sales of illegal articles
13. Theft of confidential information
14. Web defacement
15. Unauthorized access
16. Denial of service
17. Phishing
18. Data diddling
19. Online share trading fraud
20. Tax evasion and money laundering
21. Cyber pornography/Child pornography
22. Cyber terrorism
23. Cyber laundering

3.3 Classifications of cyber crime activities;

Many authors have classified cybercrime activities in various ways, some classify it as:

- Financial and Nonfinancial crime

- Traditional and Nontraditional crime

Other as:

- Cyber Crime against individual
- Cyber Crime against property
- Cyber Crime against organization
- Cyber Crime against society

Others as:

- Offences against the confidentiality, integrity and availability of computer data and systems;
- Computer-related offences;
- Content-related offences; and
- Copyright-related offences;

Let's look at the last classification briefly:

3.3.1 Offences Against the Confidentiality, Integrity and Availability of Computer Data and Systems

All offences in this category are directed against (at least) one of the three legal principles of confidentiality, integrity and availability. Unlike crimes that have been covered by criminal law for centuries (such as theft or murder), the computerization of offences is relatively recent, as computer systems and computer data were only developed around sixty years ago. The effective prosecution of these acts requires that existing criminal law provisions not only protect tangible items and physical documents from manipulation, but also extend to include these new legal principles. This section gives an overview of the most commonly occurring offences included in this category.

Illegal Access (Hacking, Cracking)

Data Espionage

Illegal Interception

Data Interference

System Interference

3.3.2 Content-related Offences

This category covers content that is considered illegal, including child pornography, xenophobic material or insults related to religious symbols. The development of legal instruments to deal with this category is far more influenced by national approaches, which can take into account fundamental cultural and legal principles. For illegal content, value systems and legal systems differ extensively between societies. The dissemination of xenophobic material is illegal in many European countries, but can be protected by the principle of freedom of speech in the United States. The use of derogatory remarks in respect of the Holy Prophet is criminal in many Arabic countries, but not in some European countries. These legal challenges are complex, as information made available by one computer user in one country can be accessed from nearly anywhere in the world. If “offenders” create content that is illegal in some countries, but not in the country they are operating from, prosecution of the “offenders” is difficult, or impossible. There is much lack of agreement regarding the content of material and to what degree specific acts should be criminalized. The different national views and difficulties in prosecuting violations committed outside the territory of an investigating country have contributed to the blocking of certain types of content on the Internet. Where agreement exists on preventing access to websites with illegal content hosted outside the country, states can maintain strict laws, block websites and filter content. There are various approaches to filter systems. One solution requires access providers to install programs analyzing the websites being visited and to block websites on a black list. Another solution is the

installation of filter software on users' computer (a useful approach for parents who wish to control the content their children can view, as well as for libraries and public Internet terminals). Attempts to control content on the Internet are not limited to certain types of content that are widely accepted to be illegal. Some countries use filter technology to restrict access to websites addressing political topics. Open Net Initiative reports that censorship is currently practiced by about two dozen countries.

Erotic or Pornographic Material (excluding Child-Pornography)

Child Pornography

The use of virtual currencies and anonymous payment

The use of encryption technology

Racism, Hate Speech, Glorification of Violence

Religious Offences

Illegal Gambling and Online Games

Libel and False Information

Spam and Related Threats

Other Forms of Illegal Content

3. Copyright- and Trademark-related Offences

One of the vital functions of the Internet is the dissemination of information. Companies use the Internet to distribute information about their products and services. In terms of piracy, successful companies may face problems on the Internet comparable to those that exist outside the network. Their brand image and corporate design may be used for the marketing of counterfeit products, with counterfeiters copying logos as well as products and trying to register the domain related to that particular company. Companies that

distribute products directly over the Internet can face legal problems with copyright violations. Their products may be downloaded, copied and distributed.

3.3.3 Copyright-related Offences

With the switch from analogue to digital, digitalization has enabled the entertainment industry to add additional features and services to movies on DVD, including languages, subtitles, trailers and bonus material. CDs and DVDs have proved more sustainable than records and video-tapes. Digitalization has opened the door to new copyright violations. The basis for current copyright violations is fast and accurate reproduction. Before digitalization, copying a record or a video-tape always resulted in a degree of loss of quality. Today, it is possible to duplicate digital sources without loss of quality, and also, as a result, to make copies from any copy. The most common copyright violations include:

• Exchange of copyright-protected songs, files and software in file-sharing systems;

• The circumvention of Digital Rights Management systems;

File-sharing systems are peer-to-peer based network services that enable users to share files, often with millions of other users. After installing file-sharing software, users can select files to share and use software to search for other files made available by others for download from hundreds of sources. Before file-sharing systems were developed, people copied records and tapes and exchanged them, but file-sharing systems permit the exchange of copies by many more users. Peer-to-Peer (P2P) technology plays a vital role in the Internet. Currently, over 50 per cent of consumer Internet traffic is generated by peer-to-peer networks. The number of users is growing all the time – a report published by the OECD estimates that some 30 per cent of French Internet users have downloaded music or files in file sharing systems. File-sharing systems can be used to exchange any kind of computer data, including music, movies and software. Historically, file-sharing systems have been used mainly to exchange music, but the exchange of videos is becoming more and more important. The technology used for file-sharing services is

highly sophisticated and enables the exchange of large files in short periods of time. First-generation file-sharing systems depended on a central server, enabling law enforcement agencies to act against illegal file-sharing in the Napster network. Unlike first-generation systems (especially the famous service Napster); second-generation file-sharing systems are no longer based on a central server providing a list of files available between users. The decentralized concept of second generation file-sharing networks makes it more difficult to prevent them from operating. However, due to direct communications, it is possible to trace users of a network by their IP-address. Law enforcement agencies have had some success investigating copyright violations in file-sharing systems. More recent versions of file-sharing systems enable forms of anonymous communication and will make investigations more difficult. File-sharing technology is not only used by ordinary people and criminals, but also by regular businesses. Not all files exchanged in file-sharing systems violate copyrights. Examples of its legitimate use include the exchange of authorized copies or artwork within the public domain. Nevertheless, the use of file-sharing systems poses challenges for the entertainment industry. It is unclear to what extent falls in sales of CD/DVDs and cinema tickets are due to the exchange of titles in file-sharing systems. Research has identified millions of file-sharing users and billions of downloaded files. Copies of movies have appeared in file-sharing systems before they were officially released in cinemas at the cost of copyright-holders. The recent development of anonymous file-sharing systems will make the work of copyright holders more difficult, as well as law enforcement agencies. The entertainment industry has responded by implementing technology designed to prevent users from making copies of CDs and DVDs such as Content Scrambling Systems (CSS), an encryption technology preventing content on DVDs from being copied. This technology is a vital element of new business models seeking to assign access rights to users more precisely. Digital Rights Management (DRM) describes the implementation of technologies allowing copyright-holders to restrict the use of digital media, where customers buy limited rights only (e.g., the right to play a song during one party). DRM offers the possibility of implementing new business models

that reflect copyright-holders' and users' interests more accurately and could reverse declines in profits. One of the biggest difficulties with these technologies is that copyright protection technology can be circumvented. Offenders have developed software tools that enable the users to make copy-protected files available over the Internet free of charge or at low prices. Once DRM protection is removed from a file, copies can be made and played without limitation. Efforts to protect content are not limited to songs and films. Some TV stations (especially Pay-TV channels) encrypt programmes to ensure that only paying customers can receive the programme. Although protection technologies are advanced, offenders have succeeded in falsifying the hardware used as access control or have broken the encryption using software tools. Without software tools, regular users are less able to commit offences. Discussions on the criminalization of copyright violations not only focus on file-sharing systems and the circumvention of technical protection, but also on the production, sale and possession of "illegal devices" or tools that are designed to enable the users to carry out copyright violations.

3.3.4 Trademark-related Offences

Trademark violations are similar to copyright violations, a well-known aspect of global trade. Violations related to trademarks have transferred to cyberspace, with varying degrees of criminalization under different national penal codes. The most serious offences include:

• The use of trademarks in criminal activities with the aim of misleading targets; and

• Domain or name-related offences. The good reputation of a company is often linked directly with its trademarks. Offenders use brand names and trademarks fraudulently in a number of activities, including phishing, where millions of e-mails are sent out to Internet users resembling e-mails from legitimate companies e.g., including trademarks. Another issue related to trademark violations is domain-related offences such as cyber-squatting, which describes the illegal process of registering a domain name identical or similar to a trademark of a product or a company. In most cases, offenders seek to sell the domain for

a high price to the company or to use it to sell products or services misleading users through their supposed connection to the trademark. Another example of a domain-related offence is “domain hijacking” or the registration of domain names that have accidentally lapsed.

3.3.5 Computer-related Offences

This category covers a number of offences that need a computer system to be committed. Unlike previous categories, these broad offences are often not as stringent in the protection of legal principles, including:

• Computer-related fraud;

• Computer-related forgery, phishing and identity theft; and

• Misuse of devices.

3.3.6Fraud and Computer-related Fraud

Computer-related fraud is one of the most popular crimes on the Internet, as it enables the offender to use automation and software tools to mask criminals’ identities. Automation enables offenders to make large profits from a number of small acts. One strategy used by offenders is to ensure that each victim’s financial loss is below a certain limit. With a ‘small’ loss, victims are less likely to invest time and energy in reporting and investigating such crimes. One example of such a scam is the Nigeria Advanced Fee Fraud. Although these offences are carried out using computer technology, most criminal law systems categorize them not as computer-related offences, but as regular fraud. The main distinction between computer-related and traditional fraud is the target of the fraud. If offenders try to influence a person, the offence is generally recognized as fraud. Where offenders target computer or data-processing systems, offences are often categorized as computer-related fraud. Those criminal law systems that cover fraud, but do not yet include the manipulation of computer systems for fraudulent purposes, can often still prosecute the abovementioned offences. The most common fraud scams include:

3.3.7 Online Auction Fraud

Online auctions are now one of the most popular e-commerce services. In 2006, goods worth more than USD 20 billion were sold on eBay, the world's largest online auction marketplace. Buyers can access varied or specialist niche goods from around the world. Sellers enjoy a worldwide audience, stimulating demand and boosting prices. Offenders committing crimes over auction platforms can exploit the absence of face-to-face contact between sellers and buyers. The difficulty of distinguishing between genuine users and offenders has resulted in auction fraud being among the most popular of cybercrimes. The two most common scams include:

• Offering non-existent goods for sale and requesting buyers to pay prior to delivery; or

• Buying goods and asking for delivery, without intention to pay.

In response, auction providers have developed protection systems such as the feedback/comments system. After each transaction, buyer and sellers leave feedback for use by other users as neutral information about the reliability of sellers/buyers. In this case, "reputation is everything" and without an adequate number of positive comments, it is harder for offenders to persuade targets to either pay for non-existent goods or, conversely, to send out goods without receiving payment first. However, criminals have responded and circumvented this protection through using accounts from third parties. In this scam called "account takeover", offenders try to get hold of user names and passwords of legitimate users to buy or sell goods fraudulently, making identification of offenders more difficult.

3.3.8 Advance Fee Fraud

In Advanced Fee Fraud, offenders send out e-mails asking for recipients' help in transferring large amounts of money to third parties and promise them a percentage, if they agree to process the transfer using their personal accounts. The offenders then ask them to transfer a small amount to validate their bank account data (based on a similar

perception as lotteries – respondents may be willing to incur a small but certain loss, in exchange for a large but unlikely gain) or just send bank account data directly. Once they transfer the money, they will never hear from the offenders again. If they send their bank account information, offenders may use this information for fraudulent activities. Evidence suggests that thousands of targets reply to e-mails. Current researches show, that despite various information campaigns and initiatives advance fee frauds are still growing – with regard to the number of victims as well as with regard to the total losses.

3.3.9Computer-related Forgery

Computer-related forgery describes the manipulation of digital documents - for example, by:

• Creating a document that appears to originate from a reliable institution;

• Manipulating electronic images (for example, pictures used as evidence in court); or

• Altering text documents.

The falsification of e-mails includes the scam of “phishing” which is a serious challenge for law enforcement agencies worldwide. “Phishing” seeks to make targets disclose personal/secret information. Often, offenders send out e-mails that look like communications from legitimate financial institutions used by the target. The e-mails are designed in a way that it is difficult for targets to identify them as fake e-mails. The e-mail asks recipient to disclose and/or verify certain sensitive information. Many victims follow the advice and disclose information enabling offenders to make online transfers etc. In the past, prosecutions involving computer-related forgery were rare, because most legal documents were tangible documents. Digital documents play an ever more important role and are used more often. The substitution of classic documents by digital documents is supported by legal means for their use e.g., by legislation recognizing digital signatures Criminals have always tried to manipulate documents. With digital forgeries, digital documents can now be copied without loss of quality and are easily

manipulated. For forensic experts, it is difficult to prove digital manipulations, unless technical protection is used to protect a document from being falsified.

3.4.0 Identity Theft

The term identity theft – that is neither consistently defined nor consistently used – describes the criminal act of fraudulently obtaining and using another person's identity. These acts can be carried out without the help of technical means as well as online by using Internet technology. In general the offence described as identity theft contains three different phases:

• In the first phase the offender obtains identity-related information. This part of the offence can for example be carried out by using malicious software or phishing attacks.

• The second phase is characterized by interaction with identity-related information prior to the use of that information within criminal offences. An example is the sale of identity-related information. Credit card records are for example sold for up to 60 US dollars.

• The third phase is the use of the identity-related information in relation with a criminal offence. In most cases the access to identity-related data enables the perpetrator to commit further crimes. The perpetrators are therefore not focusing on the set of data itself but the ability to use them in criminal activities. Examples for such offence can be the falsification of identification documents or credit card fraud. The methods used to obtain data in phase one cover a wide range of acts. The offender can use physical methods and for example steal computer storage devices with identity-related data, searching trash ("dumpster diving") or mail theft. In addition they can use search engines to find identity-related data. "Googlehacking" or "Googledorks" are terms that describe the use of complex search engine queries to filter through large amounts of search results for information related to computer security issues as well as person information that can be used in identity theft scams. One aim of the perpetrator can for example be to search for insecure password protection systems in order to obtain data from this system. Reports highlight the risks that can go along with the legal use of search engines for illegal

purposes. Similar problems are reported with regard to file-sharing systems. The United States Congress discussed recently the possibilities of file-sharing systems to obtain personal information that can be abused for identity theft. Apart from that the offenders can make use of insiders, who have access to stored identity-related information, to obtain that information. The 2007 CSI Computer Crime and Security Survey shows that more than 35 per cent of the respondents attribute a percentage of their organization's losses greater than 20 per cent to insiders. Finally the perpetrators can use social engineering techniques to persuade the victim to disclose personal information. In recent years perpetrators developed effective scams to obtain secret information (e.g. bank account information and credit card data) by manipulating users through social engineering techniques. The type of data the perpetrators target varies. The most relevant data are:

• Social Security Number (SSN) or Passport Number – The SSN that is for example used in the United States is a classical example of a single identity-related data that perpetrators are aiming for. Although the SSN was created to keep an accurate record of earnings it is currently widely used for identification purposes. The perpetrators can use the SSN as well as obtained passport information to open financial accounts, to take over existing financial accounts, establish credit or run up debt.

• Date of birth, address and phone numbers – Such data can in general only be used to commit identity theft if they are combined with other pieces of information (e.g. the SSN). Having access to additional information like the date of birth and the address can help the perpetrator to circumvent verification processes. One of the greatest dangers related to that information is the fact that it is currently on a large scale available in the Internet – either published voluntarily in one of the various identity-related for a or based on legal requirements as imprint on websites.

• Password for non-financial accounts – Having access to passwords for accounts allows perpetrators to change the settings of the account and use it for their own purposes. They

can for example take over an email account and use it to send out mails with illegal content or take over the account of a user of an auction platform and use the account to sell stolen goods.

• Password for financial accounts – Like the SSN information regarding financial accounts is a popular target for identity theft. This includes checking and saving accounts, credit cards, debit cards, and financial planning information. Such information is an important source for an identity thief to commit financial cybercrimes. Identity theft is a serious and growing problem. Recent figures show that, in the first half of 2004, 3 per cent of United States households fell victim to identity theft. In the United Kingdom, the cost of identity theft to the British economy was calculated at 1.3 billion British pounds every year. Estimates of losses caused by identity theft in Australia vary from less than 1 billion USD to more than 3 billion USD per year. The 2006 Identity Fraud Survey estimates the losses in the United States at 56.6 billion USD in 2005.426 Losses may be not only financial, but may also include damage to reputations. In reality, many victims do damage to reputations. In reality, many victims do not report such crimes, while financial institutions often do not wish to publicize customers' bad experiences. The actual incidence of identity theft is likely to far exceed the number of reported losses. Identity theft is based on the fact that there are few instruments to verify the identity of users over the Internet. It is easier to identify individuals in the real world, but most forms of online identification are more complicated. Sophisticated identification tools (e.g., using biometric information) are costly and not widely used. There are few limits on online activities, making identity theft easy and profitable.

3.4.1 Misuse of Devices

Cybercrime can be committed using only fairly basic equipment. Committing offences such as libel or online fraud needs nothing more than a computer and Internet access and can be carried out from a public Internet café. More sophisticated offences can be committed using specialist software tools. The tools needed to commit complex offences

are widely available over the Internet, often without charge. More sophisticated tools cost several thousand dollars. Using these software tools, offenders can attack other computer systems at the press of a button. Standard attacks are now less efficient, as protection software companies analyze the tools currently available and prepare for standard hacking attacks. High-profile attacks are often individually designed for specific targets. Software tools exist to:

• Carry out DoS attacks;

• Design computer viruses;

• Decrypt encrypted communication; and

• Illegally access computer systems.

A second generation of software tools has now automated many cyber-scams and enables offenders to carry out multiple attacks within a short time. Software tools also simplify attacks, allowing less experienced computer users to commit cybercrime. Spam-toolkits are available that enable virtually anybody to send out spam emails. Software tools are now available that can be used to up- and download files from file-sharing systems. With greater availability of specially-designed software tools, the number of potential offenders has risen dramatically. Different national and international legislative initiatives are being undertaken to address cyber scam software tools – for example, by criminalizing their production, sale or possession.

3.4.2 Combination Offences

There are a number of terms used to describe complex scams covering a number of different offences.

Examples include:

• Cyber terrorism

• Cyber laundering and

• Phishing

Cyber terrorism

Back in the 1990s the discussion about the use of the network by terrorist organizations was focusing on network-based attacks against critical infrastructure such as transportation and energy supply ("cyber terrorism") and the use of information technology in armed conflicts ("cyber warfare"). The success of virus and botnet attacks has clearly demonstrated weaknesses in network security. Successful Internet-based attacks by terrorist are possible, but it is difficult to assess the significance of threats and at that time the degree of interconnection was small compared to the current status and it is very likely that this – apart from the interest of the states to keep successful attacks confidential – is one of the main reasons why very few such incidents were reported. Today it is known that terrorists use ICTs and the Internet for:

• Propaganda;

• Information gathering;

• Preparation of real-world attacks;

• Publication of training material;

• Communication;

• Terrorist financing;

• Attacks against critical infrastructures.

4.0 Damages or dangers cause by cyber criminals include the following;

- Lost of confidential information
- Theft of one's intellectual property

- Lost of money in bank (through e-banking)
- Threat to individual, cooperate organizations or government agencies
- Destructions of one's image (personality)
- Gaining illegal access to one's system or network to Modify and delete important information e.t.c.

5.0 Preventive or counter measures

- Network Ingress filtering can be to prevent the downstream networks from injecting packets with faked or "spoofed" addressed into the Internet. Although it may not stop the attack, it will make identifying the source host easier and terminate it immediately. Provides more information on Ingress Filtering.
- Disable external ICMP_ECHO traffic entirely. This does have serious implications to normal network management since it does affect network communication management within the local segment. However, this can be configured to allow internal ping traffic and disable packets coming from the outside
- Disable ICMP_ECHO_REPLY traffic on a Cisco router. Security implications make this a prudent choice.
- Ensure that the routers are configured to not send ICMP_UNREACHABLE error packets to hosts that do not respond to ARPs.
- It is clear that a tight application gateway firewall with a strict policy is essential. Ideally DNS resolving should be only done on the WWW/FTP proxies and access given to WWW with prior proxy authentication only. Mails should be on a separate server. A secure solution would be to set up a second network which is connected to the internet, and the real one kept separated.
- The first line of defense is to educate users regarding the dangers of installing applications downloaded from the Internet and to take great caution if they have to open any mail attachment.

- The second line of defense can be antivirus products that are capable of recognizing Trojan signatures. Ensure that these updates are regularly applied over the network.
- The third line of defense comes from keeping application version updated by following security patches and vulnerability announcements.
- Treat Access Points As Entrusted - Access points need to be identified and evaluated on a regular basis to determine if they need to be quarantined as untrusted devices before wireless clients can gain access to internal networks. This determination means appropriate placement of firewalls, virtual private networks (VPN), intrusion detection systems (IDS), and authentication between access point and intranets or the Internet.
- Access Point Configuration Policy - Administrators need to define standard security settings for any 802.11b access point before it can be deployed. These guidelines should cover SSID, WEP keys and encryption, and SNMP community words.
- Access Point Discovery - Administrators should regularly search outwards from a wired network to identify unknown access points. Several methods of identifying 802.11b devices exist, including detection via banner strings on access points with either Web or telnet interfaces. Wireless network searches can identify unauthorized access points by setting up a 2.4 GHz monitoring agent that searches for 802.11b packets in the air.
- The first countermeasure against password guessing should rightly address the ports used by the NETBIOS protocol - namely TCP and UDP port 135-139 - to unauthorized access. Disable bindings to Wins client on any adapter. Apart from what the administrator can do, users need to be made aware of their contribution to the situation. Users can thwart password guessing to a great extent by choosing complex password. This can include letters, numerals and symbols. However, the prime deterrent in choosing complex passwords is that they are often hard to remember. Users would not like to be locked out of their systems obviously. A

best practice is to choose the first letter of every word in a phrase - such as 'Serena Williams holds four Grand Slam titles', resulting in a password 'SWhfGSt'. Windows can enforce choosing complex passwords. Users must be made to change their passwords at regular intervals or as often as they choose within an interval.

- Network and Web server logs can hold the trace evidence of computer system attacks. Server log entries can reveal whether systems have been attacked, how they were attacked, and whether the attacks were successful. The purpose of log analysis is to look for unusual events that occur on the network, patterns of abnormal behavior such as unauthorized log-ins, long log entries, and repeated unsuccessful attempts to access systems. Especially take note of failed logon attempts, events registered with identifiers 529 or 539 and the logging patterns that fall out of the ordinary for regular users.

- There are many log-analysis tools available that report network events, ranging from commercial products such as Event Reporter to free programs such as Backlog and NT Systemlog. Moreover, log-parsing programs such as Logsurfer, Swatch, and several application-specific tools monitor system logs for attack signatures.
- Using Windows 2000 Kerberos authentication only in a native, single forest environment network (no legacy clients) with all applications supporting Kerberos;
- Ensuring physical security best practices; Ensuring that network access points are inaccessible to passersby;
- Setting LAN Manager Authentication Level to "Send NTLM responses only". The NTLM response is not susceptible to SMBCapture attack; SMBCapture will maintain it is capturing but, when sent to Lophtcrack, the hashes will not crack within a reasonable time frame.

6.0 Conclusion

Cyber crime has poised a lot of concern to developing organization, agencies and the world at larger. Apart from conventional crime and security threat on life and properties, cyber criminals have taken a new dimension in the criminal activities. With the fast growing technology advancement, the use of computer and related devices, crimes are carried out in the space. Therefore the readers should be careful with the activities on the internet and the preventive measures to be taken when they come across such things or activities.

7.0 Summary

- Cyber crime may be said to be those species, of which, genus is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime.

Cyber crime activities include the following;

1. Virus, Trojan and worms
2. Email bombing
3. Email account hacking
4. Credit card fraud
5. Music piracy
6. Software piracy
7. Salami slicing
8. Source code theft
9. Email/Website spoofing
10. Intellectual property theft
11. Email scam
12. Online sales of illegal articles
13. Theft of confidential information

14. Web defacement

Cyber crime are based on the classification;

- Offences against the confidentiality, integrity and availability of computer data and systems;
- Computer-related offences;
- Content-related offences; and
- Copyright-related offences;

Corrective or preventive measures should be taken against cyber criminals these include;

- The use of anti spywares against viruses, worms and Trojans.
- The use of authentication and authorization to identify and verify those granted access to system resources e.t.c.

QUESTIONS;

1. What is cyber crime?
2. List ten (10) cyber crime activities you know?
3. List the possible classifications of cyber crime you know?

ANSWERS;

- Despite the fact that the word “Cybercrime” has entered into common usage, many people would find it hard to define the term precisely. Furthermore, there is no catch all term for the tools and software which are used in the commission of certain online crimes. Therefore, cyber crime may be said to be those species, of which, genus is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime.
-
    - Email scam
    - Online sales of illegal articles

- Theft of confidential information
- Web defacement
- Unauthorized access
- Denial of service
- Phishing
- Data diddling
- Online share trading fraud
- Tax evasion and money laundering

- Financial and Nonfinancial crime

- Traditional and Nontraditional crime

Or:

- Cyber Crime against individual
- Cyber Crime against property
- Cyber Crime against organization
- Cyber Crime against society

Or:

- Offences against the confidentiality, integrity and availability of computer data and systems;
- Computer-related offences;
- Content-related offences; and
- Copyright-related offences;

REFERENCE:

1. Ethical Hacking (EC-Council Exam 312-50): Student Courseware

by International Council of Electronic Commerce Consultants

OSB © 2004.

2. Council of Europe Convention on Cybercrime.
   Commonwealth Model Law on Computer and Computer Related Crime.
   Draft Stanford Convention.
3. Aghatise, E.J (2006): Cyber crime Definition. Computer Crime Research Center. June 28, 2006. Available online at www.crime-research.org
4. Longe, O.B.& Chiemeke, S.C. (2006): The Design and Implementation of An E-Mail Encryptor for Combating Internet Spam. Proceedings of the Ist International Conference of the International Institute of Mathematics and Computer Sciences. Pp 1 – 7. Covenant University, Ota, Nigeria. June, 2006
5. Longe O.B & Longe F.A (2005): The Nigerian Web Content: Combating the Pornographic Malaise Using Content Filters. Journal of Information Technology Impact, Vol. 5, No. 2, pp. 59-64, 2005
6. [Longe, O.B (2006): Web Journalism In Nigeria: New Paradigms, New Challenges. Journal of Society and Social Policy. Calabar, Nigeria (In Print)
7. Peter, G & Grace, D. (2001): Red Flags of Fraud. Trends and Issues in Crime and Criminal Justice, no. 200, Australian Institute of Criminology, Canberra. Available online at http://www.aic.gov.au
8. Sackson, M. (1996): Computer Ethics: Are Students Concerned. First Annual Ethics Conference. Available online at http://www.maths.luc.edu/ethics96/papers/sackson.doc

Unit 2 – Categories of Cybercrime Countermeasures

1.0 INTRODUCTION

When we are talking about categories of cybercrime countermeasures we need to understand what cyber crime is. By definition Cyber crime, or computer crime, refers to any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Some of this crime are hacking, copyright infringement, identity theft, child pornography, and child grooming e.t.c. there are also problems of privacy when confidential information is lost or intercepted, lawfully or otherwise. Now go to cybercrime countermeasures, a cyber countermeasure is defined as an action, process, technology, device, or system that serves to prevent or mitigate the effects of a cyber attack against a computer, server, network or associated device. Now that we know the definition we can now go to the categories of the cybercrime we which are Technical, Counter-Terror Social Network Analysis and Intent Recognition (CT-SNAIR), Economic, Legal and Behavioral.

2.0 LEARNING OUTCOMES/OBJECTIVES

At the end of this lesson the reader should be able to

- ✓ Define cybercrime.
- ✓ Define cybercrime countermeasures.
- ✓ Know the categories of cybercrime countermeasures.
- ✓ Explain in detail all the categories of the cybercrime countermeasures we have.

3.0 MAIN CONTENT

3.1 Categories of cybercrime countermeasures

In my introduction I define Cybercrime countermeasures as an action, process, technology, device, or system that serves to prevent or mitigate the effects of a cyber attack against a computer, server, network or associated device. Some

of countermeasures that exist that can be effectively implemented in order to combat cyber-crime and increase security are:-

3.2 Technical

There are a variety of different technical countermeasures that can be deployed to thwart cybercriminals and harden systems against attack.

These technical measures are

3.2.1 Firewalls-- network or host based, are considered the first line of defense in securing a computer network by setting.

3.2.2 Access Control Lists (ACLs) --determining which what services and traffic can pass through the check point.

3.2.3 Antivirus-- can be used to prevent propagation of malicious code. Most computer viruses have similar characteristics which allow for signature based detection. Heuristics such as file analysis and file emulation are also used to identify and remove malicious programs. Virus definitions should be regularly updated in addition to applying operating system hotfixes, service packs, and patches to keep computers on a network secure.

3.2.4 Cryptography-- techniques can be employed to encrypt information using an algorithm commonly called a cipher to mask information in storage or transit. Tunneling for example will take a payload protocol such as Internet Protocol (IP) and encapsulate it in an encrypted delivery protocol over a Virtual Private Network (VPN), Secure Sockets Layer (SSL), Transport Layer Security (TLS), Layer 2 Tunneling Protocol (L2TP), Point-to-Point Tunneling Protocol (PPTP), or Internet Protocol Security (IPSec)to ensure data security during transmission. Encryption can also be employed on the file level using encryption protocols like Data Encryption Standard(DES), Triple Data Encryption

Algorithm (3DES), or Advanced Encryption Standard (AES) to ensure security of information in storage.

3.2.5 Network vulnerability testing-- performed by technicians or automated programs can be used to test on a full-scale or targeted specifically to devices, systems, and passwords used on a network to assess their degree of secureness. Furthermore network monitoring tools can be used to detect intrusions or suspicious traffic on both large and small networks.

3.2.6 Physical deterrents-- such as locks, card access keys, or biometric devices can be used to prevent criminals from gaining physical access to a machine on a network. Strong password protection both for access to a computer system and the computer's BIOS are also effective countermeasures to against cyber-criminals with physical access to a machine.

3.3 Counter-Terror Social Network Analysis and Intent Recognition (CT-SNAIR)

The Counter-Terror Social Network Analysis and Intent Recognition (CT-SNAIR) project uses the Terrorist Action Description Language (TADL) to model and simulate terrorist networks and attacks. It also models links identified in communication patterns compiled from multimedia data, and terrorists' activity patterns are compiled from databases of past terrorist threats. Unlike other proposed methods, CT-SNAIR constantly interacts with the user, who uses the system both to investigate and to refine hypotheses.

Multimedia data, such as voice, text, and network session data, is compiled and processed. Through this compilation and processing, names, entities, relationships, and individual events are extracted from the multimedia data. This information is then used to perform a social network analysis on the criminal network, through which the user can detect and track threats in the network. The social network analysis directly influences

and is influenced by the intent recognition process, in which the user can recognize and detect threats. In the CT-SNAIR process, data and transactions from prior attacks, or forensic scenarios, is compiled to form a sequential list of transactions for a given terrorism scenario.

The CT-SNAIR process also includes generating data from hypothetical scenarios. Since they are imagined and computer-generated, hypothetical scenarios do not have any transaction data representing terrorism scenarios. Different types of transactions combine to represent the types of relationships between individuals.

The final product, or target social network, is a weighted multiplex graph in which the types of edges (links) are defined by the types of transactions within the social network. The weights within these graphs are determined by the content-extraction algorithm, in which each type of link is thought of as a separate graph and "is fed into social network algorithms in part or as a whole. Links between two individuals can be determined by the existence of (or lack of) the two people being mentioned within the same sentence in the compiled multimedia data or in relation to the same group or event.

The final component in the CT-SNAIR process is Intent Recognition (IR). The goal of this component is to indicate to an analyst the threats that a transaction stream might contain. Intent Recognition breaks down into three subcategories: detection of "known or hypothetical target scenarios," prioritization of these target scenarios, and interpretation "of the resulting detection.

3.4 Economic

The optimal level of cyber-security depends largely on the incentives facing providers and the incentives facing perpetrators. Providers make their decision based on the economic payoff and cost of increased security whereas perpetrators decisions are based on the economic gain and cost of cyber-crime. Potential prisoner's dilemma, public goods, and negative externalities become sources of cyber-security market failure when

private returns to security are less than the social returns. Therefore the higher the ratio of public to private benefit the stronger the case for enacting new public policies to realign incentives for actors to fight cyber-crime with increased investment in cyber-security.

3.5 Legal

In some countries, a number of legal statutes define and detailed the conditions for the prosecution of a cybercrime and are used not only as a legal counter measures but also functions as a behavioral check against the commission of a cyber crime. In the United States as a case study a number of legal statutes define and detail the conditions for prosecution of a cyber-crime. Many of the provisions outlined in these acts overlap with each. This are some of the acts

- **The Computer Fraud and Abuse Act :-** The Computer Fraud and Abuse Act passed in 1986 is one of the broadest statutes in the US used to combat cyber-crime. It has been amended a number of times, most recently by the US Patriot Act of 2002 and the Identity theft enforcement and Restitution Act of 2008. Within it is the definition of a "protected computer" used throughout the US legal system to further define computer espionage, computer trespassing, and taking of government, financial, or commerce information, trespassing in a government computer, committing fraud with a protected computer, damaging a protected computer, trafficking in passwords, threatening to damage a protected computer, conspiracy to commit a cyber-crime, and the penalties for violation.
- **The Digital Millennium Copyright Act:-** The Digital Millennium Copyright Act passed in 1998 is a United States copyright law that criminalizes the production and dissemination of technology, devices, or services intended circumvent Digital Rights Management(DRM), and circumvention of access control.
- **The Electronic Communications Privacy Act:-** The Electronic Communications Privacy Act of 1986 extends the government restrictions on wiretaps from

telephones. This law is generally thought in the perspective of what law enforcement may do to intercept communications, but it also pertains to how an organization may draft their acceptable use policies and monitor communications.

- **Identity Theft and Aggravated Identity Theft:-** The Identity Theft and Aggravated Identity Theft statute is a subsection of the Identification and Authentication Fraud statute. It defines the conditions under which an individual has violated identity theft laws.
- **Internet Spyware Prevention Act:-** The Internet Spyware Prevention Act (I-SPY) prohibits the implementation and use of spyware and adware. I-SPY also includes a sentence for "intentionally accessing a computer with the intent to install unwanted software.

3.6 Behavioral

Behavioral countermeasures can also be an effective tool in combating cyber-crime. Public awareness campaigns can educate the public on the various threats of cyber-crime and the many methods used to combat it. It is also here that businesses can also make us of IT policies to help educate and train workers on the importance and practices used to ensure electronic security such as strong password use, the importance of regular patching of security exploits, signs of phishing attacks and malicious code, etc.

Financial agencies such as banks and credit bureaus are starting to require verification of data that identity thieves cannot easily obtain. This data includes users' past addresses and income tax information. In the near future, it will also include the data located through use of biometrics. Biometrics is the use "of automated methods for uniquely recognizing humans based upon … intrinsic physical or behavioral traits. These methods include iris scans, voice identification, and fingerprint authentication. The First Financial Credit Union has already implemented biometrics in the form of fingerprint authentication in their automated teller machines to combat identity theft. With a similar purpose, Great Britain has announced plans to incorporate computer chips with biometric

data into their passports. However, the greatest problem with the implementation of biometrics is the possibility of privacy invasion.

4.0 CONCLUSION

In conclusion cybercrime countermeasures that exist should be effectively implemented in order to combat cyber-crime and increase security. And cyber crime is a strict criminal act and any one cut in this act should be punished strictly also it is very importance to create a public awareness of the crime and the countermeasure available to the public.

5.0 SUMMARY

- Cyber crime, or computer crime, refers to any crime that involves a computer and a network.
- A cyber countermeasure is defined as an action, process, technology, device, or system that serves to prevent or mitigate the effects of a cyber attack against a computer, server, network or associated device.
- Countermeasures that exist are Technical, Counter-Terror Social Network Analysis and Intent Recognition (CT-SNAIR), Economic, Legal and Behavioral.
- Technical involve different technical countermeasures that is deployed to thwart cybercriminals and harden systems against attack which are Firewalls, Access Control Lists (ACLs), Antivirus, Cryptography techniques, network vulnerability testing and Physical deterrents.
- The Counter-Terror Social Network Analysis and Intent Recognition (CT-SNAIR) project uses the Terrorist Action Description Language (TADL) to model and simulate terrorist networks and attacks.
- Economic Countermeasures make use of the optimal level of cyber-security depends largely on the incentives facing providers and the incentives facing perpetrators.

- Legal Countermeasures In some countries, a number of the legal statutes define and detailed the condition for the prosecution of a cybercrime.
- Behavioral countermeasures can also be an effective tool in combating cyber-crime. Public awareness campaigns can educate the public on the various threats of cyber-crime and the many methods used to combat it.

6.0 TUTOR MARKED ASSIGNMENTS AND MARKING SCHEME

6.1 Assessment Test

Answer all

1. In which type of countermeasure is a number of legal statutes define and detail the conditions for prosecution of a cyber-crime? **(5 marks)**

A. Behavioral

B. Economic

C. Legal

D. Legal behavioral

2. Which of this is not in the categories of cybercrime countermeasures? **(5 marks)**

A. The Counter-Terror Social Network Analysis and Intent Recognition

B. Legal behavioral

C. Technical

D. Economic

3. Define Cybercrime and countermeasure **(10 marks)**

4. Explain in detail categories of cybercrime countermeasure that we have. **(10 marks)**

6.2 Answers to Assessment Test (Marking Scheme)

1. C. Legal Countermeasures In some countries, a number of the legal statutes define and detailed the condition for the prosecution of a cybercrime. **(5 marks)**

2. B. Legal behavioral (there is nothing like legal behavioral we have only have Legal Countermeasures and behavioral Countermeasures). **(5 marks)**

(Check for the answer of question three and four in the lesson) **(10 marks each)**

ATTENDANCE (10 marks)

TOTAL (40 marks)

7.0 REFERENCES

1. Firewall http://www.tech-faq.com/firewall.html
2. Weinstein, C., et al. (2009) Modeling and Detection Techniques for Counter-Terror Social Network Analysis and Intent Recognition. Proceedings from the Aerospace Conference. Piscataway, NJ: IEEE. p. 2.
3. Moore, R. (2005) "Cybercrime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.
4. Coleman, Kevin. "Cyber Attacks on Supply Chain Systems". defensetech.org. http://defensetech.org/2009/04/15/cyber-attacks-on-supply-chain-systems

Unit 3 – Detection of Cybercrimes

1.0 INTRODUCTION

Criminal activity has been in existence from time immemorial. Decades ago, these activities were perpetrated only in the commission of conventional crimes as in stealing, robbery, burglary etc. As time evolved and technology advanced, criminal activities took a new dimension in tune with modern communication methods.

In recent times, owing to the widespread of computer systems and the dependence on computerized systems in communication, crimes commission which would have otherwise been executed using crude conventional means have also metamorphosed into being committed using several computerized techniques.

Unfortunately, for those at the receiving end of these crimes, technology has eased the commission of the crimes, and made more difficult the detection. The detection of Cyber Crime is an evolving phase of the cyber era and as a result, lacks a clear-cut and defined approach. Cases of Cyber Crime detection have resulted by chance but this detection can be enhanced by skill and up-to-date knowledge acquisition on the operations of cyber criminals.

Nevertheless, recent experience has shown some informal techniques used by computer users, administrators, network professionals and other persons concerned with computers in detecting cybercrime activities. This write-up looks at cybercrime with a view of identifying some detection methods.

2.0 LEARNING OBJECTIVES

Upon completion of this chapter, the student will be able to:

- List methods of cybercrime detection;
- Explain several techniques used in cybercrime detection;

- Differentiate between the detection methods;
- Explain clearly the difference between conventional crime detection and cybercrime detection;

3.0 DETECTION OF CYBER CRIME

The detection of cybercrime is an ever-evolving process and as such, lacks precisely defined methods. The following however, are some cybercrime detection techniques:

3.1 INACCURACIES

Inaccuracies are apparent. The commission of cybercrimes over long periods of time results in the cyber criminals lagging in their precautionary measures. They tend to neglect detection precautions which they initially would not have taken for granted. They also get greedy, especially in financial crimes and make detectible mistakes. Upon discovery, their close acquaintances could get nervous and turn the criminals in. This possibility is increased if more people are aware of the consequences of cybercrime indictment as well as those of being accessories to these crimes. These inaccuracies in the actions of the criminals leave traces which if discovered and thoroughly scrutinized by security professionals, could lead to the crime detection.

3.2 MONITORING AND SURVEILLANCE SYSTEMS

An internet monitoring and surveillance unit with personnel trained in modern computer network monitoring system operations and techniques could serve as an independent agency with the sole responsibility of detecting cybercrimes through the use of several detection tools and techniques

3.3 AUDITING

Regular and thorough system auditing is important. Proper auditing could reveal hidden inconsistencies in a system. In recent times, computer crimes have been seen to be committed by the victims close associates, employees of a victim organization or

individuals in close contact with the victim system, as opposed to farfetched criminals such as hackers on a distant network. A proper audit could uncover criminal tracks by detecting inconsistences which could result in unveiling the identity of these offenders.

3.4 USE OF INTRUSION DETECTION SYSTEMS (IDS)

Cybercrime activities could be detected using such technical measures as *SNORT.* Snort is an open source tool which exists for monitoring network attacks. Its development started in the late 1990s and has now evolved into a reliable intrusion detection software.

3.5 GOVERNMENT AGENCIES

The use of government established crime detection agencies such as the Police, EFCC and ICPC in uncovering cybercrime activities could be the *light bulb* in some cases of cybercrime detection. These agencies comprise of various personnel who are specialized in several areas of cybercrime investigations. Suspicious and irregular activities such as uneven wealth distribution amongst a common income earning level can act as a signal to the commission of cybercrime.

4.0 CONCLUSION

The level of expertise possessed by cyber criminals is on an unbelievable increase. If this is not matched by corresponding technologically oriented up-to-date detection methods, these cyber criminals would easily have a *safe haven* in which they would execute their heinous activities without any opposition.

All computer users should be aware of some basic cybercrime detection techniques which would make visible the flaws of these criminals, thereby sabotaging their efforts.

5.0 SUMMARY

Cybercrime detection methods include but are not limited to

- **Inaccuracies:** This involves the use of careless mistakes of cyber criminals in finding their activities out.

- **Monitoring and surveillance systems:** This describes setting up of computer network monitoring agencies with trained staff capable of detecting cyber crimes
- **Auditing:** Involves executing measures to check inconsistencies in a system
- **Use of Intrusion Detection Systems(IDS):** IDSs include the use of technical tools such as software for detecting network intrusions
- **Government agencies:** Agencies such as The Police, EFCC and ICPC could be the *light bulbs* that may just be needed in spotting cyber crimes

6.0 TUTOR MARKED ASSIGNMENTS AND MARKING SCHEME

1(a) Explain Cyber Crime detection. 2.5marks

(b) List 5 detection methods. 2.5marks

2(a) Which in your opinion is the most effective of the methods listed above and explain your selected option. 2.5marks

(b)Suggest a detection method for cybercrimes in your immediate Environment. 2.5marks

7.0 REFERENCE

1. Lloyd Doney, *NonProfits Are Not Immune to Computer Crime.*

2. Nibal Idlebi and Matthew Perkins, *Practical Application of Cyber Crime Issues.* United Nations Economic and Social Commission of Western Asia (UN-ESCWA), Information and Communication Technology division.

3. Walter Johnson (An eHow contributing writer), *Ways To Detect Cyber Crime or Terrorism.*

Unit 4 – Prevention of Cybercrimes

1.0 INTRODUCTION

In today's world we use computers for everything; searching the internet, online shopping, accessing bank accounts, Email, and online gaming as some examples. Communication is faster and more reliable than in the past which has allowed more to be accomplished in a given day. The problem is just like anything else; vulnerability. There are individuals that hack into computers as well as the networks of businesses and government agencies. The problem is that sensitive data can be stolen and/or destroyed. There needs to be more focus on the security of computers and the internet. This paper will focus on the prevention of cybercrime as well how cyber security can be improved.

2.0 LEARNING OUTCOME AND OBJECTIVE

The main objectives of this course material is to

- Educate students on cyber crime
- The form in which it takes
- How to prevent each crime
- What resources are needed to prevent cyber crime

3.0 CYBER CRIME AND ITS PREVENTION

3.1 WHAT IS CYBER CRIME?

Cyber crime is regarded as computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks. Cyber crime can be referred to as illegal activities that takes place online such activities include fraud, spam. Identity theft, computer viruses and worms, cyber stalking, drug trafficking, sexual predators, malware or spyware, phishing schemes and the like.

3.2 PREVENTION OF CYBER CRIME

3.2.1 TERMINATE YOUR ONLINE SESSION COMPLETELY:

Closing your browser window or typing in a new website address without logging out may give others a chance of gaining access to your account information. Always terminate your online session by clicking on the "Log out or Sign Out" button to terminate your online session. Avoid using the option of "remember" your username and password information.

3.2.2 CREATE BACKUP OF IMPORTANT DATA:

Backup of all the important files whether personal or professional should be created. Getting used to back up your files regularly is the first step towards security of your personal computer.

3.2.3 USE SECURITY PROGRAMS:

If your system does not have data protection software to protect you online, then by all means buy internet security program for your computer. Today, almost all new computer systems come with some kind of security programs installed.

3.2.4 PROTECT YOUR PASSWORD:

Try creating a password that consists of a combination of letters (both upper case and lower case), numbers and special characters. Password should be changed regularly. Do not share your password with other people.

3.2.5 USE YOUR OWN COMPUTER:

It's generally safer to access your financial accounts from your own computer only. If you do use some other computer, always delete all of the "Temporary Internet Files", â€œcookiesâ€• and clear all of your "History" after you log off your account.

3.2.6 ONLINE SHOPPING ON SECURE WEBSITE:

Make sure that you do online shopping on a secure website, like those with a url that starts with "https" and/or have a TRUSTe or VeriSign seal. If you don't see these anywhere on the site, you run the risk of submitting credit card information and other personal information to a site that may be a fraud.

3.2.7 MONITORING OF CHILDREN ONLINE ACTIVITIES:

Children should only have access to a computer located in a central area of your home and you should regularly check all browser and email activity. A wise thing to do is to use parental control software that limits the types of sites the user can gain access to.

3.2.8 PREVENTION OF EMAIL SPOOFING:

A simple rule in using this communication tool is not to open any links in emails from people you do not know. Hackers do use E-mail as the main target seeking to steal personal information, financial data, security codes and other. Do not use the link sent to you if you need access to the website, visit the website by typing the address in your menu bar.

3.2.9 ENCRYPTION OF IMPORTANT FILES AND DATA:

Encrypt important data you don't want compromised. Utilize encryption software, which "garbles" your data to make it unintelligible to anyone who tries to hack into your computer system.

3.3 RESOURCES NEEDED AND HOW USE IT TO PREVENT CYBER CRIME

The resources needed to prevent cyber crime include the following:

- Spam blocker
- Anti-virus software
- Firewall protection
- Encryption software

3.3. 1 SPAM BLOCKER:

Turn on spam blocker. Most internet providers provide a spam blocking feature to prevent unwanted messages, such as fraudulent emails and phishing emails from getting into email inbox.

3.3.2 ANTI-VIRUS SOFTWARE

Make sure you have adequate and efficient antivirus software for your computer, such as McAfee, Norton anti-virus or other similar programs and make sure its is regularly

updated and scan your computer once in a week to locate and eliminate malware, spyware, viruses and other problems.

3.3.3 FIREWALL PROTECTION

Use your computer firewall protection feature which is a digitally created barrier that prevents hackers from getting into a computer system. Make sure it's always turned on.

3.3.4 ENCRYPTION SOFTWARE

Encryption software helps encrypts files or data you don't want to be compromised. Use encryption software which "garbles" your data to make it unintelligible to any1one who tries to hack in your computer system

4.0 CONCLUSION

The problems with cyber crime; how to improve efforts of prevention; and the response to cyber crime are what help us to look at the dangers of cyber space. The Internet is a very powerful tool and effective means of communication but it is vulnerable just like anything else. The way to protect it for now is for everyone to be smart and follow preventive measures; individuals, institutions, and government alike should all follow these measures.

5.0 SUMMARY

Cyber crimes may pose the most potentially damaging threat to IT-related activities, transactions, and assets. We see this threat as under-recognized and under-rated among the risks that organizations face, and thus believe that many organizations are unprepared to detect, address, or protect themselves from these threats. But these threats can be prevented by many ways such as cautious of providing information, securing online payment, avoidance of scams and monitoring of child's computer activities.

6.0 QUESTIONS:

1. What is cyber crime?
2. What can be done to prevent cyber crimes?
3. Discuss four(4) ways of preventing cyber crime

6.1 ANSWERS:

Cybercrime is regarded as computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks. Cybercrime can be referred to as illegal activities that takes place online such activities include fraud, spam. Identity theft, computer viruses and worms, cyber stalking, drug trafficking, sexual predators, malware or spyware, phishing schemes and the likes

Terminate Your Online Session Completely:

Closing your browser window or typing in a new website address without logging out may give others a chance of gaining access to your account information. Always terminate your online session by clicking on the "Log out or Sign Out" button to terminate your online session. Avoid using the option of "remember" your username and password information.

Create Backup of Important Data:

Backup of all the important files whether personal or professional should be created. Getting used to back up your files regularly is the first step towards security of your personal computer.

Use Security Programs:

If your system does not have data protection software to protect you online, then by all means buy internet security program for your computer. Today, almost all new computer systems come with some kind of security programs installed.

Protect Your Password:

Try creating a password that consists of a combination of letters (both upper case and lower case), numbers and special characters. Password should be changed regularly. Do not share your password with other people.

7.0 REFERENCES

Govil, J. (2007). Ramifications of Cyber Crime and Suggestive Preventive Measures.IEE43

http://www.crimepreventiontips.org/self-defense-methods/cybercrime-part-3.html
http://expertscolumn.com/content/cyber-crime-and-its-prevention

http://www.ehow.com/how_4967690_prevent-cyber-crime.html

Unit 5 – Cure and Recovery from Cybercrime Exploits

(1) INTRODUCTION

Since Internet fell into widespread use, cyber-criminals(i.e people that operate or use computer system or network for bad act or with bad intention) have been exploiting(i.e to use a system as an opportunity to gain an advantages fo your self) holes, threats and vulnerabilities in computer systems. Which has caused so many damages to the an organization, company, individual, goverment e.t.c.

Cybercrime exploit simple means how cyber-criminals take advantages of a particular program or devise to lunch a crime in the cyberspace.

Recovery from cybercrime exploit is a situation whereby a victim of cybercrime can be able to prevent, detect, response and recover from cybercrime exploit

(2) Objectives

At the end of this course the reader:

Should be able to know how cybercrime exploit can be recorver.

Should know how cyber-criminals exploit cybercrimes.

Should be able to detect, prevent,recorver andresponce.

(3) MAIN CONTENT

3.1 Cybercrime exploit can be recorvered by detect, prevent and responce.

Let take it one after the other:

3.2 prevention from cybercrime exploit: It is the act of stopping, keep from happening or arising our computer system or network to vulnerable to cybercrime exploit.

3.2.2How can we prevent from cybercrime exploit

By bringing to an existence law enforcement teams that organize seminar to people to practice security awareness training, system hardening, monitoring and policy analysis to

protect against computer crime to an individual and organization. Security awareness training empowers organizations to defend against attack, teaching about security threats and response.

System hardening and monitoring work at the technical level to fix vulnerabilities and scan for abnormalities associated with an attack.

Policy analysis at the managerial level involves an ongoing review of security practices, training and personnel to find and fix weaknesses that could be exploited by computer criminals.

3.3 Detection of cybercrime exploit: It is the process of discover or investigate a cybercrime exploit.

3.3.2 how to detect cybercrime exploit

The goal of cyber-criminals is to move undetected into computer systems, and to exploit without anyone even noticing

By installs monitoring systems in networks, and devotes personnel to auditing systems in order to quickly detect a breach.

The sooner a breach is detected by authorities, the less damage is likely to be done, and the easier the recovery. Because of this, law enforcement encourages organizations to be proactive in installing and maintaining their monitoring and detection systems.

3.4 Response to cybercrime exploit

3.4.1 Responce to cybercrime exploit: I t simply define as what we do as reply or as a reaction to a particular cybercrime exploit.

3.4.2 how to respond to cybercrime exploit

When a computer crime occurs and is detected, quick response by law enforcement is key.

The stages of response include: evaluation (determining the method of entry, the type of attack and the impact), isolation (isolating the network or computer system from further damage), auditing (analyze the system for damage) and reporting (notifying the necessary personnel of the breach and the impact.

An accurate and complete report is crucial to ensuring that the computer crime is not repeated

(4) CONCLUTION

In conclution, recovering from a computer crime takes patience and determination. At this step, law enforcement serves the organization by providing a set of useful recommendations to protect against future computer crime

Following the initial stages of recovery, it is the organization's responsibility to implement the changes--Prevention, Detection and Response--to respond to future computer crime threats.

(5) SUMMARY

In summary, cybercrime exploit can be recovered through many means, modes or operation, but hear we specify on modes or operation such as prevention, detection and response.

It has been discussed that prevention is the act of stopping, keep from happening or arising our computer system or network to vulnerable to cybercrime exploit and it operate by making public awareness to the user the sign of cybercrime exploit.

Then, we discuss the use of detection to cybercrime exploit which we said is the It is the process of discover or investigate cybercrime exploit and cybercrime exploit can be detected by frequently installing monitoring systems in network.

And the last recovery from cybercrime exploit we discussed about is the response which is the what we do as reply or as a reaction to a paticular cybercrime exploit and the response is been done by the what we do as reply or as a reaction to a paticular cybercrime exploit.

And the response can be done through evaluation, isolation, auditing and reporting.

Recovering from a computer crime takes patience and determination. At this step, law enforcement serves the organization by providing a set of useful recommendations to protect against future computer crime.

(6) TUTOR MARKED ASSIGNMENT AND MARKING SCHEME

Questions

1. What do you understand by the following terms
2. Cybercrime

2 Cybercrime exploit

3. Explain how we can recover from cybercrime exploit through the use of:

(i) prevention

(ii) detection

(iii) responce

(7) REFRENCES

University of south Carolina: law enforcement and computer security

Us department of justice: cyber crime