CYBERCRIME AND IT-GOVERNANCE

Prof. OBADIAH OGHOERORE ALEGBE PhD

Electronics Engineer

Professor of Computer Engineering Universidad Nacional de Tres de Febrero Buenos Aires Argentina

Professor of Information Engineering Universidad de Belgrano Buenos Aires Argentina

Professor Collegium Ovirium Buenos Aires Argentina

Table of Contents:

Chapter 1.

Introduction.

Simply put, cybercrime is any crime committed over the cyberspace. Since it is over the cyberspace, it means using computers to commit crimes.

Illegal music download, stealing of money from online bank account are cybercrimes.

Creation and distribution of viruses all over the networks and the internet and posting of confidential reports of others over the internet are also cybercrimes.

Another terrible cybercrime is Identity Theft by which criminals use the internet to steal from others their personal information. This is usually done through Phishing and Pharming. They create fake websites and ask users for personal information which include social security number, personal identity number, pictures, bank account numbers. Credit card number and key. They also ask for username and login data with which they go into the business transaction of users and cause robbery.

Cybercrime are in thousands and only limited by the imagination of a human being. Computer structure and its communications infrastructure has become a feast theatre for criminals and the limit to their destruction is not measurable.

In this case the computer has become an agent of committing crimes. It also is helpful in crime detection and prevention.

There are different types of cybercrimes, below are two types:

1. A user innocently downloads a file containing Trojan Horse virus unto his computer, the Trojan Horse installs a keystroke logger into the computer. The keystroke logger is used to steal private information such as used in internet banking and email passwords.

2. Another very serious type of cybercrimes are cyberstalking, harassment, child intimidation, extortion, manipulation of stock market, industrial and corporation espionage and terrorist activities planning. Chartrooms are used to deceive victims and lure them into fake relationship which could end up in kidnapping. Instant messages can also be venue of committing crimes.

Cybercrime use current telecommunication networks to offend individuals or groups by defaming them over the internet through email, chat rooms and fake websites. Also taken as crime is cracking into other people's software, copyright infringement, child pornography, child grooming, revelation of private and confidential information. In fact cybercriminals are a danger to national security.

Cybercrime uses computer networks to commit fraud by misinterpreting facts to deceive others which could lead other to lose benefits.

Harassment can contain derogatory statements and obscenities based on race, religion, ethnic origin, tribe, bullying, sexual orientation, gender through emails con publications over the www.

Cyberthreats are threats carried out over the internet by publication on webpages or my emails and messaging.

Cyber terrorism exist and it creates software that destroy documents published over the internet and also can break across security of networks to destroy documents especially in State Digital storage.

Cyberextortion are extortion carried out through the internet which could be by email, messaging among others.

There are organized cybercriminals that attack big corporations producing heavy losses on their finance.

Chapter 2.

Security Policies and Procedures.

We stated in chapter 1 some examples of the various ways of cybercrimes. We here will review some security policies that can be useful to reduce attack by cybercriminals.

Security policies are setup to protect network and information. Policies really depend on the establishment to be protected. The Establishment must state what it is to protect before setting up policies. We are going to state here just ideas of security policy.

Policies, Standards and Procedure can be amended at any time depending of the evolution of technology and attacks.

Scope:

There is need for policies, Standards and Procedures to be set be set for the security practices to protect Establishments and Institutions.

Audience:

This policies are applicable to all members of the Establishment that have access to computers within the establishment or accessing it form any where.

Compliance:

Every user must comply with the policy rules in order prevent risk to the asset of the Institution.

Information will be divided into two types: Sensitive Information and Public Information.

Policy on Sensitive Information:

Sensitive information cn be spoken. Written and preserved electronically or in printed form , they must all be protected from being adultrated.

For this to be achiveded the following are some basic policies to follow:

- Policy of password for the general user.
- Personal Identification and confidential data such as health state Information Policy.
- There must be protocol that must be followed when responding to security breaches on any Identifying Information.
- Policy of Management of Incident.
- Policy of the Management of Vulnerability.
- Electronic Media Disposal Standards.
- Policy of Security Liason.

Sensitive information means all data both in original and copy and could be any of below:

- Personal Identification or Identifying Information can be ID Card of Tax Payments, Drivers Licence Number, Social Security Number, Passport Number, Credit Card Number , Debit Card Number, Banking Account Numbers, Digital Signature, Fingerprints, Biometric Data, Passwords, Nickname or any other form of identifying a person.
- Confidential Health Information protected according to local laws.
- Information about Customer's Records.
- Payment Card Holder Data.

Public Information: These are information that can go in and out of the Institution without endangering the functioning of the establishment.

Roles and Responsibilities:

There must be Roles and Responsibilities assigned to every type of user.

- **Information or Data Administrator:** This will be responsible for approving the creation of set of information or data of the primary user of the information or data.
- **Information or Data Keeper:** -This will be responsible for Information o Data storage and Processing on behalf of the Administrator.
- **Consumer / User:** The person authorized to work with data, that is read, enter, copy, query, and update all information.
- **User Administrator:** The person in charge of creating users and their access to different part of the network. This person will approve or reject all request to access different parts of the network. The person will also ensure that all security requirements are followed.
- **Information Security Liaison:** Each Business Unit of the Insititution must keep its services of information and must also appoint Infromation Security Liaison that will create and carry out security policies, procedures and controls.
- **Executive Director and Information Security Officer :** This will Develop Information Security Strategy and also maintain Security Program to provide services to:

  1. Network Security.

  2. Consulting on Information Security.

  3. Standard and Policy of Informaiton Security.

  4. Security Awareness Inititatives of the Enterprise Information.

  5. Design and Architecture of the Insititution Security.

  6. Definition of Information Security Requeirements.
- **Policy of Critical Resources:** There must be a strong policys as to who have acess to very crintial resources in the Insititutiton. Examples are payroll, banking accounts, the environment where servers are sroed, protection of the Data Centres and all computer controlled acess.

Proceedures:

Security must be maintained by certain procedures.

1. **There must be procedure for the creation, use, Maintainance and Transmission of Informations that are sensitive to the Institution.**

   A. **Sensitive Information Creation:** The Admisnitrator must adhere to the standard of the protection of Sentitive Information. No unauthorized access to it.

   B. **Transmission of Sensitive Infromation:**

- Any transmission done through email or other means must comply with strict security standard with special attention paid to the privacy of individuals a
- All informations that are sensitive must never be handled through instant messaging.
- When using shared spaces on a network for storage of data and information, strict Information Security Standard must be followed.
- Before transferring defective electronic devices especially that contain Information Storage for maitainance and repair , special agreement must be signed to protect the Institutions Data. In case the content are highly sensitive, the Insititution must provide a space withing the establishment for the rpairs and maitianance to prevent such devices taken out of the premises of the institution.

   C. **The Use and Maintenance of Sensitive Information:**

- The Sensitive Information Storage must follow strict Information Security Standard outlines beforehand.
- No Sensitive Information must be transported on mobile communications devices or any disposable media except in accordance with Information Security Standard.
- All computing devices like Server, Workstation must be placed in well secured locations and protected with password that is encrypted.
- There must be adequate Control Mechanism for example privacy screen when displaying sensitive information.
- Restoration o sensitive information from backups must follow real procesdure stated by security standard.
- There must be a procedure for the duplication and use of sensitive information.

D. Permanent Deletion and Destruction of Sensitive Infromation.

The destruction of Information that are very sensible must follow guidelines for such. Deletion means removal from any data storage while destruction is for printed hard copy.

In this case all CDRom and optical storage elements must all be destroyed.

All software acquired for business purpose or for the running of the administration of the Institution must comply with standards and protected from illegal use and installation.

2. Access Controls.

All access both electronically or physically to Sensitive Information must be controlled. Those accessing them must be authorized by password and authentication. Remote Access to the network and sensitive information must be restricted to very necessary few and they must access with encrypted username and password.

There should be mechanism for Control Access to all Sensitive parts of Information Networks, I propose the following few points¨

A. Authorization. There must be appropriate control through authorization according to standard to access sensitive information.

B. Identification/Authorization: User identification must be unique and there must be authentication for all access to every sensitive part of the Network. There must be a password policy for all where by access to every sector is approved or denied.

C. Remote Access: When access is allowed from remote location outside the premises of the establishment. There also must be strict password policy limited within time range.

D. Physical Access: The must be a Custodian of the Area of Sensitive Information and Access into its Area must be strictly controlled, Here, only authorized persons can be allowed in. Only authorized person must be in contact with all computing devices. Only authorized persons can be allowed to operate any computing device, only strictly controlled and authorized persons can manipulate any computing device for maintenance.

E. **Emergency Access to Mission-Critical Devices and Data:** There must be a protocol for movement and access to the critical section during emergency. It may include creating special emergency password for some works to be done in a psace of time after which the password will be blocked. There must be a written order to justify such security loophole.

F. **Audit Controls:** There must be a rule for audit logs of all electronic access to very sensitive information. Logs must be reviewed periodically and backuped.

3. **Data Transfer and Printing:** There must be a Technical Security Mechanism to protect against any access to Sensitive Information transmitted over the Network. There must be contracts and written authorization for all data transmitted into and out of the Area of Sensitive Information. Data Transmission include fax in and out.

   The printing of Sensitive Information must not be done without due authorization. Neither must it and copies be vulnerable to unauthorized persons.

4. **Storage of Sensitive Information on Other Media:** Spedial measures must be taken to protect the Physical Security of all the information that are stored in external media which could be diskettes, CD_Rom, Hards Disks etc. Skydrive, Google Drive or other clouding environment must not and never be used to store Sensitive Informations. Instead Replication Servers could be located in different places for storage of copies of sensistive information.

5. **Incident Management:** Big Establishments should split their Informaton Network in zone so that every zone will establish and maintain a plan for updating Incident Manangement which must be according to the Incident Management Policy.

6. **Vulnerability Management:** Each Zone in the case of Big Establishment that has resources for the management and storage of Sensitive Information must carry out monthly vulnerability scanning to detect any vulnerability and act in acrodance. This procedure must also be in ccordance with Vulnerability Policy.

7. **Backup & Recovery:** Protectors and those in custody of all Information/Data must periodically make backup of all information/data. For this there must be a backup policy that stipulates protocol for carrying out

backups. All backup media must be encrypted and protected according to Information Security Standard. If backups must be transmitted, it must be done in compliance with protocol and Policy of the protection of Transmtted data.

Chapter 3.

Data and Transmission Standards.

Data Communication is when two Digital Devices exchange information between them.

When various Digital Devices are connected for communications between all of them such that information is accessible from anyone at anytime and at any place, we call such configuration **Networking**.

Interoperability is the Capability of different computers of different configuration and trademarks to transmit and receive Data acceptable to the user.

For this to be possible, there are collection of rules and procedures to make communications possible, these rules are what we call Protocol.

Data transmission can be serial or parallel. Protocol includes bits of synchronism, start and stop. We have Asynchronous Transmission and Synchronous Transmission.

Data Transmission is the movements of trains of bits across the network to different destinations.

Parallel transmission was used for communication between two devices directly connected to each other but when the device are at a distance, parallel communication becomes too expensive and its quality reduced.

Serial communication comprises converting parallel data into serial bit and transmitted bit by bit. This system allows data to be transmitted to distant digital devices. The earliest were through Serial Port RS232 and later USB. Protocols were developed for serial communication through RS232.

The development of Network Interface lifted networking to a higher level . For this to happen, various protocols were designed for these interfaces to link the two

devices. The first type of networks for personal computers was the Token Ring by which all computers form a ring and when data is transmitted from one computer to another , it passes through all the network interface but it is only the identified computer that processes the data sent. Under this configuration, communication was very slow until the Ethernet was introduced applying serial configuration with higher speed.

Data Transmission can be in half Duplex whereby each device alternate to use the communication channel and full Duplex whereby both devices transmit and receive simultaneously.

Data Transmission Interfaces:

Upon recommendations of ITU-T, EIA and TIA , Data Transmission Interfaces are as follows:

ITU-T is International Telecommunications Union – Telecommunications.

EIA is Electronics Industries Association.

TIA is Telecommunications Industries Association.

ITU-T recommended V.10, V.11, V.24,V.35, V.36, and x.21

EIA and TIA recommended EIA/TIA 232E, EIA/TIA -232E Alt A, RS 422 A, RS 423 A, RS 366, RS 449, RS 488, ANSI/EIA-530, EIA/TIA-574, AND RJ-12

All the interfaces have to do with the way electric current is handled to interprete digital signals they interface.

Guided Transmission Media:

These are Cables, Coaxial, Wavwguide and Fiber Optics.

The Standards also stated the application of the differen types of guides:

Twisted-pair cable – Analog Transmission Signals:

- With this voice signals are able to travel as far a 6 kilometers without need for repeaters.
- It has a loss at voice level of 1 db/km.
- It is used to transmit analog signals between two points with a bandwidth up to 1.1 MHz.

Twisted-pair Cable – Digital signal Transmission:

- Data can be transmitted up to 4Mbps for digital transmission between tow devices depending on the distance between them.
- It is susceptible to noise and interference because electromagnetic loads can couple into it.
- It can easily be affected by noise. That is why it is not recommended to be laid parallel to power line.

Application: Twisted pair is widely used for transmission of analog and digital signals. They are used in Telephone backbone systems in the subscriber loops. The human voice has a frequency range between 20 Hz to 20KH , nevertheless the standards bandwidth for voice transmission ranges between 300 and 3400 Hz.

It is also used to transmit digital data through modems up to 28,8 Kbps.

Coaxial is built with two conductors; it has a cylindrical outer conductor with an inner wire. It is a waveguide. With coaxial cable, analog and digital signal can be transmitted through very long distance. Signal up to 800 Mbps can be transmitted through it.

Waveguide: Waveguides are pipe-shaped structures that can be rectangular or circular and elliptic-sectioned through which electromagnetic energy is guided and bound within its limits.

Fiber Optics: Fiber optics are mediums made on glass or plastic and thin and flexible form with the capacity to carry optical beam. It is cylindrical with three concentric sections which are the core, the cladding and the jacket.

Fiber optics provided medium by which multiple communication channels could be made over very long distance. Fiber-optics allowed mono-mode and multimode propagations.

Non-Guided Media: These include Microwaves on ground and satellites, and Radio. In this case the bandwidth can be higher and digital transmission is faster. In the case of Radio the frequencies are low , thus it allows omnidirectional transmission. But when the frequency increases to microwave, transmission are directional that is the antennae of both side of transmission points to each other because the signal must be focused.

Broadcast: Radio waves are omnidirectional are are used in broadcasting omnidirectional and it is usually outwards or inwards but not in both simultaneously. Data broadcasting is done in very low speed in this type of data transmission.

Satellite: Satellites are Microwave repeater stations stationed I the sky. They link different transmitters and receivers in different parts of the earth. Satellite have reduced the cost of transmission of data. This provided a boom in telephony, data, internet, video and television transmission.

Chapter 4.

Electronic Funds Transfer (EFT).

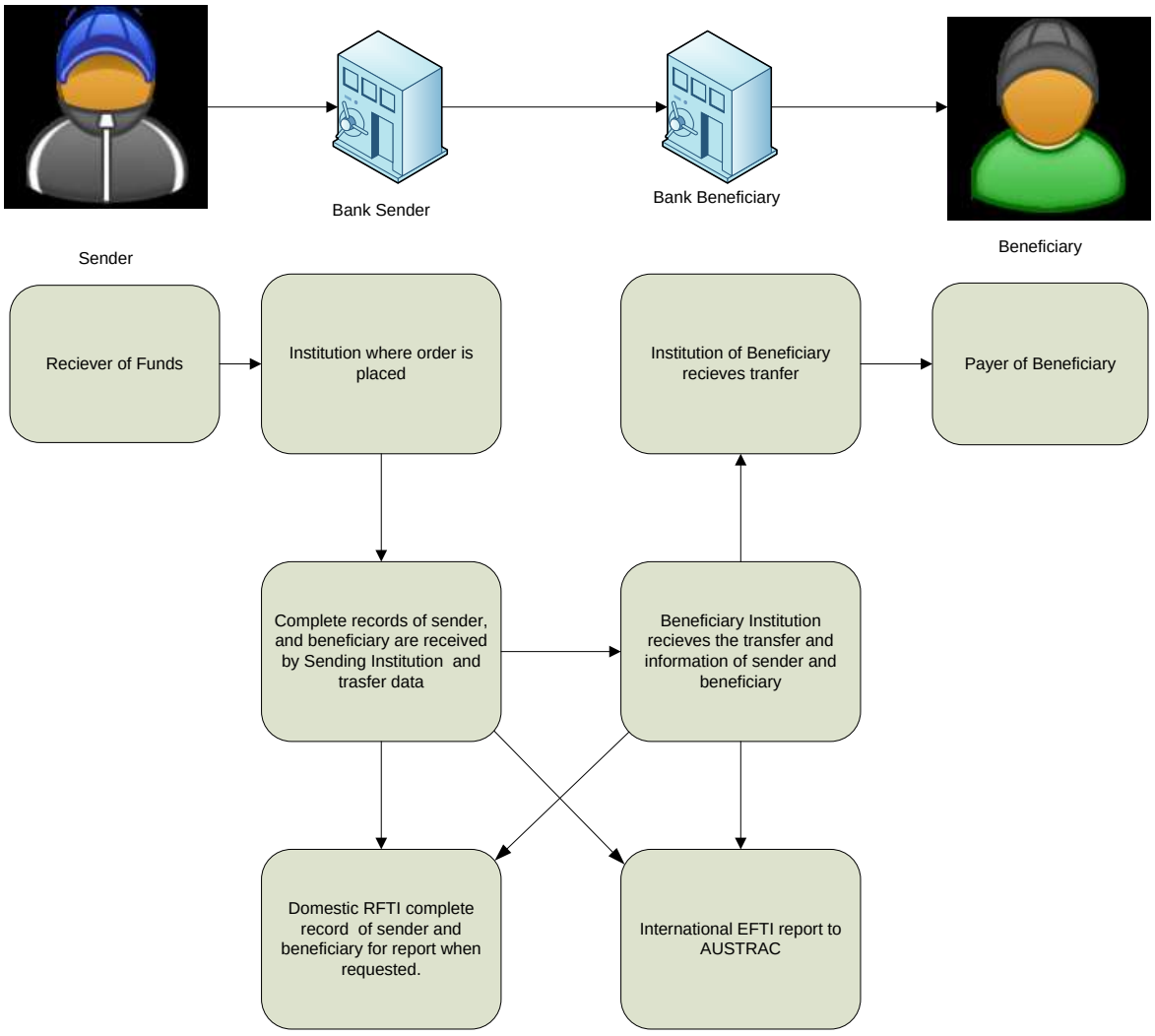
EFT is a processes of transferring funds from one institution to anther through computers. The institutions can belong to the same organization or different.entitiess. It is also a means of Financial Transaction through the Internet. These transactions include:

- Cardholder starting transaction through payment by Credit Card or Debit Card.
- Direct Deposit made by payers through machines such as Automatic Teller Machine.
- Electronic Benefit Transfer.
- Electronic Bill Payment.
- Electronic Payment in online banking.

The growth in IT and international conventions has made Electronic Fund Transfer possible bridging nations and villages around the world. It has made many emigrants transfer money to relatives in the remotest part of the world.

Every country has its own legislation that is complemented with international convention as to rate and taxes imposed on sender and receiver.

Simple Trasfer proceedure from Sender to Beneficiary



Since computers an IT is involved, EFT is not immune from fraud and dishonesty from employee of the Financial Institution. These case fall into the scope of Cybercrime.

Chapter 5.

International Standard for IT Governance.

IT Governance is a process by which efficient and effective use of IT can be ensured to enable an organization to achieve its goal. By saying “an organization” we mean that each organization can execute its iT Governance to suit its goal. We

only can give basic ideas on how to, but the final procedure depends on the interest of each Establishment or Organization.

Each organization must evaluate its risk and gain for the rules it sets out for IT Governance. It Govnernance does focus mainly on the Infromation Tehcnology System in the organization to make sure its management is easy and free of risks.

IT Govenrance creates strategy and rules to protect the information system from failure and cybercriminals.

There must be rules as to whose responsibility is the IT Governance but in many organization it is the responsibility of the Board of Directors and Executives of the Organization.

There must be a structure of relationship and process for the direct control of the organzaiton for it to achieve its goal. There msut be specification for the decision rights and the framework must be accountable to promote behaviours that are desirable in the use of IT.

IT Governance is used to define the set of people that are trusted with the Governance of the IT System by supervising, control monitoring and direct the entity.

IT Governance became necessary due to cybercrimes and and irregularities discovered in the use of IT Sytems in many organization such as spying for competitiors.

The following factors are borne in mind for successful IT Governance:

- High-level framework. This means defining roles in the use of IT System.
- Independent assurance: There must be internal and external auditing on the system that will report on the effectiveness or failure in the IT System.
- Resource Management to make sure competent resources of standard are employed.
- Risk Managemnet Team that monitor for risks to the IT System.
- Strategy alignment. Different parts of the organization can share understanding on how to improve the IT System.
- Performance Management Report must be periodically made.

ISO/IEC 38500:

The International Standard recommended for IT Governance s the ISO/IEC 38500.

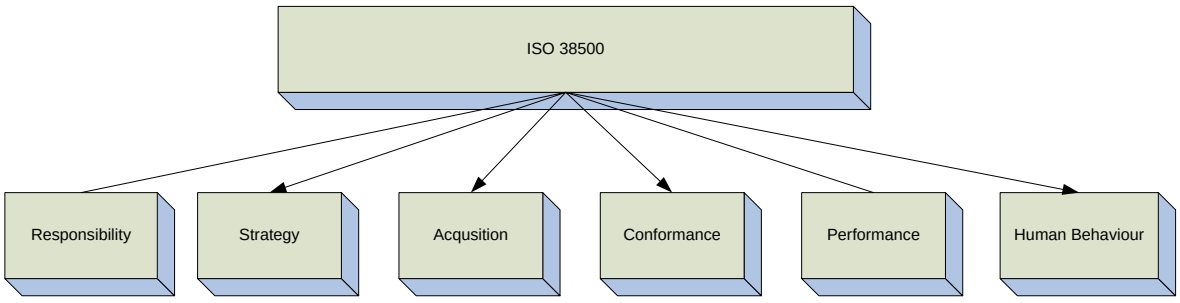
ISO means International Standard Organization.

IEC means International Electromechanical Commission.

This Standard ISO/IEC recommend a framework for IT Governance effectively by those in the highest level of great Corporations and Organizations to fulfill and understand their legal, ethical and regulatory obligation in their use of IT. This standard set guidance for directors of organizations to use Information Technology (IT) within their Establishment in a very effective, acceptable and efficient form. There are three prime sections to which the the standard divides its recommendations:

- Scope.
- Framework.
- Guidance.

The Framework is composed of definition, principles and model. The isx basic principles recommended for all types of organizations of all sizes are shown in the following block diagram:



Chapter 6

Data Protection Legislation.

Data legislation varies from jurisdiction to jurisdiction because it depends on the local interest. Although Europe , The Americas and Oceania have a lot of values to share, yet there are differences likewise their legislation.

The difficulty will be what data must be protected. To help on this Dataprotection.org promotes Data Protection Act that could be used for legislation. I have askd lawyers in Argentina about computer laws and data proteccion. They have come out lightly about ot. Which shows that already exisiting legislations on other matters can be applicable to data proteccion. For example the law protecting personal property, intellectual property can be applicable because a law centered on data protection alone may not stand the test of time.

Dataprotecion.org defined personal data in Data Protection Act as “data which has to do with an identifiable person which is confidential to the person and in the possession of another be it authority or third party”.

It stated eight points to protect data called Data Protection Principles. These are:

- Data must be fairly and Lawfully processed.
- The purpose of obtaining data must be lawful and specified.
- It should not be excessive and must be adequate and relevant.
- It must be accurate and update.
- It must b¡not be kept for a time longer than necessary.
- The individual’s right must be the determinant of its use that is according to the individual.
- It must be kept securely.
- Befroe being set to any other country, it must be provided adequate proteccion.

They also recommend that there be process for defining, Collecting, Handling and accessing data.

The complexity of data protection legislation must bare in mind “The freedom of speech” and “The right to be forgotten”. It is thus impossible to have a globally accepted data protection legislation because of the differences in many countries ruled bi differing ideological base.

Chapter 7:

Policing in Cyberspace.

The Cyberspace has become a ground prepared for warfare and also criminals that are faceless. Policing the cyberspace is and will always be a difficult task. More so that even governments are involved in activities that could become criminal. The intelligent organization employ illegal means to obtained results, China has thousands of gangs spying on the industries in the West , The West too spy on China. Any policing on the Internet will also affect them but that could create international crisis.

There is an ONG based in Canada by name The Society or the Policing of Cyberspace (POLCYB) WHOSE GOAL IS TO ENH

Chapter 8:

Legal and Policy Framework for addressing cybercrimes.

The internet has become a very powerful tool to potentiate economic growth and human development for developing countries all around the world. Based on this criminals have also used this communication system to increase their criminal power by which they continuously commit frauds worldwide at very low cost.

In order to contribute positively to economic growth and development, the Internet must be trustworthy. For this to be, there is need to create effective public policy based on mix-laws for the internet. For trust and security , there is need for criminal laws, laws to defend privacy, laws for the protection of the consumes and law that requires that Industries must build very reliable, trustworthy and secure system.

The Framework for Security and Trust could have at least four components:

- **Cybercrime:** The must be laws in every country against any criminal attack on Computer Systems.
- **There must be Standards to define and limit the access of government to stored data and communications:** Individual privacy must be protected to personal and there must be standard that allows Government agencies access to personal data especially in case of national security of any country.

- **Consumer Protection:** There must be rules that guide the easy use of Credit and Debit Cars in all transaction especially online business.
- **Security of Computers and Networks:** There must be laws that make computer networks very secure. For this , manufacturers of computers and Operating Systems must make sure their system are more secure and must provide tools fro adjusting the security of the computers in the system.

Legislation on Cybercrime:

Basic provision for cybercrime: Every nation should have basic laws against criminal activities using information systems and confidentiality, integrity or data stored in the computer.

- **Interception of Data:** Any data form non-public transmission must not intentionally be intercepted without rights of proprietors having been obtained. Permission.
- **Interference of Data:** Any damage, degrading , alteration, suppression and elimination of data from the computer of anyone without permission should be a crime.
- **Interference of System:** Any intentional disturbance of the function of a computer system but adding, removing, transmitting, damaging altering and deleting and suppression od data form a Computer System must be criminalized.
- **Illegal Access:** Anny access to a computer of another intentionally without permission must be criminalized.

Apart from these nations must consider basic concept of common interest in defining what can be termed cybercrime.

Convention on Crimes of the Council of Europe: There is a convention that was drafted by the Council of Europe in 2005 which has been ratified by some countries. This convention is very broad and far reaching beyond computer crime. The convention is composed of three sets:

- **Substantive computer crimes.** This is has to do with criminalization of hacking, cyber attacks, virus spreading against other's computer systems.
- **Government Access to Communications and Computer Data.** Here the right to privacy is must be protected against even the government.
- **Transcoder cooperation.** Here cooperation should be signed between countries by which computers can be seized after a search and protocols set to disciple the content of computers.

Surveillance standards and protection of privacy: There must be standards set for by which surveillance should be made without violating the basic human rights to privacy.

Any standard set must :

- Respect the right of privacy and protection of Identity on the Network world.
- Respect the right of privacy and the right of identity in this epoca of ubiquitous computing.
- Take the best measure to prevent technology from terminating privacy.
- Regulate Electronic Survelillance of all public gathering to make sure the individual human rights to participate is respected.
- Regulate all Telecommunication Interception to prevent broadcasting data obtained from publication.
- Protect right of individuals, the family and the public interest.
- Make sure children privacy is protected.

Chapter 9.

Interception:

Interception is one act that I believe is a threat to the internet though it has to do with national security. Interception has interest groups which I will split into four.

1. **Individuals** that just for experimental purpose develop software that can intercept routers and copy data illegally form those transmitted through the networks. They steal information and are capable of selling the information they have and make illegal use of them
2. **Corporate** that create interception equipment. They create spyware and make a lot of money from it from dictators. Even Democratic Governments in the Western World employ these Internet mercenaries. They manufacture equipment that relays communications codes and use that means to spy on journalists. Some of them create Hacking Team to intercept data in many corporations or State organs illegally.
3. **States** that are enemies of each other. They intercept information to and from any of them. This is possible because communications have protocols and all States participate in the design of protocols. States also use

interception to check the activites of Activists , it is all over the world. No country on earth is absolutely free from this idea to silence some who they feel is a threat.

4. **Cyber-Censorship** depends on every nation and the press is usually the worst victim.

Telecommunications Carriers' Forum published some guidelines for International Capability. That is the capacity to be able to intercept Telecommunications. Many countries if not all countries have legislation obliging all Network Operators and Providers of Services to make sure that all public Telecommunications Networks and Services have capacity to be intercepted and thus there is what is called Interception Act.

The guidelines elucidate all provision of Telecommunication Interception Capability Act. For all Networks Operators and Providers of Services.

It provides Standards that are relevant and overall solution architectures.

It provides for mediation and also Interception Technology.

It also provides for Agency Technology.

The guidelines also provide assistance to all Operators to comply with the TICA in a very efficient and cost effective and timely manner.

For TICA to be implemented, it requires legislation to regularize its implementation. Europe has and International standards called European Telecommunications Standards Institute which is focused on lawful implementation.

Risk Management and e-governance: One of the opposition methods to Cybercrime is Risk Management and e-governance.

Risk Management depends on the target to be applied to. It is about managing IT Risk in any organization. It includes Methodology of Risk Management, Risk Assessment, Mitigation, Communications, Monitoring and evaluation.

There are International Standard Organization recommendations for Risk Methodology. One of them is ISO/IEC 27005 .

The National Institute of Standards and Technology in 2002 published

Computer Security in which details are made on Risk Management. It states the process of managing risks which include Identification, Assessment, and steps to reduce Risk at a level acceptable to all. Risk is the most negative impact on networks and depends on the vulnerability of the system and the probability of the occurrence of danger to the networks. It allows IT managers to evaluate the balance of cost of operation of all protective measures and the gains for the establishment being protected.

Risk management stipulates roles and responsibilities for all managers of the security system of the Networks of any Organization.

Risk Management also include controls over all hardware and software failure, human errors, spam, virus and other kinds of malicious attack.

E-Governance has to do with governance driven by technology, especially IT. It is all running of business or administration using IT and the control for the effective

Ethical Hacking:

With advancement of IT and its overwhelm embrace of the planet building bridges accroos the nations converting the whole world into a glbal village, new concern have arisen. We are all interconnected both the good, the innocent and the evil.

Just as Govenrments, compaies ,Businesses , Corporations are all in the cyberspace, so also are criminals that use the crberspace for crimes. The criminal attack Netwroks from anywhere to anywhere.

The criminal spread evil data like virus , spyware , spybots to do harm to networks. Computers have gone to various homes and so also criminals have been able to reach home spreading pornographic matierials and unwanted mails that consume network bandwidth just to harm people. Hackers are inturduers who enter networks to steal infromations or alter informations form others.

Mnay companies use the internet for publicicty of their business , thse has increased electronic commerce and many are afraid of being hacked and need to protect their interests.

Mnay companies now hire independent Computer Security Professionals to attempt to break into their computer system as a way of evaluating intruder threat and the degree of the security their system. These professional would use the same tools and techniques that intruders and hackers used but they do no damage to their customer's systems. These Professionals at the end present their rports to the customers who gave them the employment. These are called **Ethic Hackers**.

Ethic hackers protect the information of their customer and prevent them from being publicized. Thye are not usually allowed into all the netweorks but a separate section for testing.

The basic things ethical hackers do are:

- Finding out what intruders can do to target system.
- Finding out what intruders or hackers can do with the information they get form the system.
- Finding out if anyone in the target system notice when there is or was intrusion into the system.

Intruders usually take week of reiteration before breaking into some systems and Ethic hackers can find residuals of their attempt or attacks..

Chapter 10.

Conclusion.

Since the IT is new, criminal investigation into IT is also new. For ages mankind had made laws to check crimes as different types of crimes appear. Usually crimes vary from society to society.

IT turned the world into a global village and as technology grows so also crimes grows because crime climbed unto the cyberspace and its effect is the same everywhere and no society is immune from it.

In this essay we made brief description of cybercrimes (brief because there are as many crimes as societies). We also made brief on IT Governance. Then we stated security policies and procedures.

For deeper understanding we stated some standards for Data and Transmission.

There was a brief on Electronic Funds Transfer which include banking over the Cyberspace.

It could also be seen that there are International Standards like the International Standard Organization which is very helpful when set security for networks.

Brenner Susan W. Criminal (2010) Threats from Cyberspace.

Etter Barbara The Challenges of Policing Cyberspace Retrieved from https://www.cs.auckland.ac.nz/~john/NetSafe/Etter.pdf .

Calder Alan, Watkins Steve IT Governace.

Center for Democracy and Technology (2011) Cybercrime. Retrieved from https://cdt.org/insight/cybercrime/ .

Kovacs Anja, Hawtin Dixie (2012) Cyber Security, Cyber Surveillance and Online Human Rights . Retrieved from http://www.gp-digital.org/wp-content/uploads/pubs/Cyber-Security-Cyber-Surveillance-and-Online-Human-Rights-Kovacs-Hawtin.pdf .

Reporters Without Borders (2013) Enemies of the Internet https://www.reporter-ohne-grenzen.de/fileadmin/docs/enemies_of_the_internet_2013_01.pdf

C.C. Palmer (2001) Ethical Hacking retrieved from http://pdf.textfiles.com/security/palmer.pdf

Introduction to Ethical Hacking retrieved from http://media.techtarget.com/searchNetworking/downloads/hacking_for_dummies.pdf .

Gary Stoneburner, Alice Goguen, and Alexis Feringa (2002) Risk Managmement Guide for Infromation Technology Systems retrieved from http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Woulds John (2004) A practical Guide to the Data Protecction Act. Retrieved from http://www.ucl.ac.uk/spp/publications/unit-publications/118.pdfhttp://www.ucl.ac.uk/spp/publications/unit-publications/118.pdf

Handbook on european Data Protection (2014) retrieved from http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf

The Guide to Data Protection. Retrieved ffrom https://ico.org.uk/Global/~/media/documents/library/Data_Protection/Practical_application/THE_GUIDE_TO_DATA_PROTECTION.ashx .

United Nations Office on Drugs and Crime (2013) Comprehensive Study of Cybercrime Retrieved from http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf .

Telecommunication Carriers Forum (2009) Guidelines for Intercpetion Capability Retrieved from http://www.tcf.org.nz/library/cc58568d-2100-46a8-9cfc-982c3d0679d8.cmr .

Global Internet Policy Initiative (2005) Trust and Security in Cyberspace: The legal and Policy Frameworks dor Addresing Cybercrime Retrieved from http://www.internetpolicy.net/cybercrime/20050900cybercrime.pdf .

Benites Manuel (2011) Communications and Data Transmission Networks Retrieved from http://www1.lima.icao.int/reddig/archivos/meetings/2010/REDDIGRTO2010/05%2006.%20Data%20transmssion%20interfaces%20data%20transmission%20means.pdf .

Dhupar K.K. Data Communication Retrieved from http://www.di.unipi.it/~bonucce/11-Datacommunication.pdf .

Blackboud Inc. (2009) Electronic Fund Transfer Guide https://www.blackbaud.com/files/support/guides/re7/eft.pdf