CPM 2006 WEST (May 23-25,2006) , Mirage Hotel, Las Vegas, NV, USA:

Electronic Fraud & Information Security

Timothy Asiedu, PhD – TIM Technology Services Ltd, Accra, Ghana.

E-mail: tasiedu@ieee.org

Introduction: Electronic Fraud and Information Security

- We find ourselves in a digital age with the world becoming a small place to live in. You can live in Ghana and can easily communicate with someone in the USA. Unfortunately, there is a price to pay for the Information Superhighway. We find ourselves with all sorts of scam spreading because the perpetrators are taking advantage of the situation.
- The current situation must be of grave concern to all of us, as depicted by the following statistics:
- According to the FBI, approximately 10,000 cyber crime complaints were filed in 2000 alone.

Introduction cont'd:

- Of the 10,000 filed, 4,000 were serious enough to be referred to law enforcement agencies and 273 of the compromised organization submitted financial loss numbers totalling $265,589,940.
- The other day there was an issue at a client's premises, where a top-ranking official of the organization was unable to use his PC for about three days. A spyware similar to the virus attacked his machine, which rendered his only mail system, Yahoo, useless. Anytime he goes into the Yahoo mail box, he is immediately thrown to a default site. The spyware normally comes to your PC unknowingly through downloaded files from certain Internet sites and can steal vital information about you.

Introduction cont'd:

- Many cases go unreported or unnoticed. Some of the reported cases are becoming complicated to the extent that not only should information officers be in the know, but also PC users. In most cases serious attacks are blocked with no investigation.
- By the end of the program through your cooperation you will be able to cover the following.
- - Electronic Fraud
- - What is Information Security ?
- - Basic Information Security Concepts.
- - Developing Corporate Information Protection Policies

Introduction cont'd.:

- Data Access Control (Physical & Logical)
- Data Security Audit
- Data Recovery Techniques
- Network Management
- Anti-Virus Techniques

Electronic Fraud (e-Fraud)

Simply put electronic fraud is the piracy of information for pecuniary and other benefits. Thus any act carried out with criminal deception using information technology as a medium constitutes electronic fraud.

- Target of Electronic Frauds.
- The following are reasons why people commit electronic frauds:
- 1. Financial Benefit to Hacker
- 2. Business/Trade Information
-

Electronic Fraud cont'd:

3. Marketing Information
4. Customer/Client Information
5. Product/Services Information
6. Personnel Information
7. Policies and Procedures

Why Do People Commit Electronic Crime ?

- - For money (e.g. theft , settle debts, etc.)
- - For revenge (settle old scores – former employees, jailed criminals, etc.)
- - For thrill or fun.

Why Care About Electronic Fraud ?

- 1. Loss of Money
- 2. Decrease in Productivity
- 3. Loss of time
- 4. Loss of credibility or business opportunity
- 5. Inability to compete
- 6. Legal Liability
- 7. Loss of life

Types of Electronic Frauds

- Credit Card Fraud/Bank Fraud – Credit card fraud is a major concern for banking institutions and governments worldwide. Profit from this type of fraud is often ploughed into prostitution, drug rings and other criminal organizations.
- Statistics – about 5,000 British credit cards are stolen daily.
- The average loss per card stolen is $1,500.
- It is estimated four (4) cards are stolen per second in the UK.

Types of Electronic Frauds cont'd

- The only form of security on the credit card is a small hologram. It only has information like the name of the owner of the card but it hardly bears any other relation to the identity of the actual user. Recent studies conducted indicate that photo ID cards are capable of reducing fraud by 90%. Often a card is sent to the customer by post. A potential thief therefore has a high degree of access to a particular card.

Types of Electronic Frauds cont'd

- **Telemarketing** – In general telemarketing involves a situation in which companies call consumers to sell goods or services, or consumers call companies to make a purchase in response to mailings or other forms of advertising. Whereas there are legitimate companies that use the telephone for marketing, consumers lose an estimated $40 billion a year through receiving fraudulent telephone offers. The FBI estimates there are 14,000 illegal telephone sales operations costing consumers in the U.S. every day.

Types of Electronic Frauds cont'd

- **Internet Fraud**: Online service and access to the Internet provid consumers with a world of information and provide companies with a new way to promote their products or services. "Cyber shopping," "banking online" and other conveniences spur an increasing number of consumers to do business by computers. But crooks also recognize the potential of committing crime in th cyberspace. The same scams that have been conducted by mai or phone can now be found on the Internet and new technologie are resulting in new ways to commit crimes against business.
- **PBX Phone Fraud**: Your business receives a call from someone who asks the receptionist to dial 90# to test a problem with the phone line or to be connected with an outside line.

Types of Electronic Frauds cont'd

- If you have any PABX phone system, the caller can then dial a company and, with no authority, make long distance calls at your expense.

Ways to Penetrate Your Network

- **Default Account**: The use of a default account is an easy method to penetrate a system. Often these accounts are not password protected or the password is easy to guess (e.g. password same as the user ID).
- **Black Account**: These are normally accounts that do not have password. Most often administrators who do not see to it that the users have been provided with passwords create these problems.
- **Trust Relationships**: Trust relationships enable hackers to quickly own many servers in a network, not just a single system.

Ways to Penetrate your Network cont'd:

- In most cases trust relationships are used to simplify communication between systems. Instead of having to authenticate each system in order to gain access, all that is required is an account that is originating from a specific name system. What this means is, if one system is taken out by a hacker, there is the likelihood that the rest of the systems will also be broken into. It is always appropriate you do not have trust relationships. Just spend a few seconds to log in to each system to keep the integrity of your network strong.

Ways to Penetrate Your Network cont'd:

- **Application Vulnerabilities**: There are possibilities of holes in your software or programs running on your computer systems. There is a long list in this category, and for the sake of this workshop we shall limit ourselves to only two typical cases picked from Oracle and Peoplesoft application systems. It is realized that the applications themselves work very well and can be secured. However, we often find common passwords for both applications.

Ways to Penetrate Your Network cont'd.

- The Oracle system often will have an account say Oracle with several common passwords. Most often you will have Oracle and Ora732. Peoplesoft will also have an account "peoplesoft" and password "peoplesoft" or "psoft." If such an account is found in the database system, a person can easily get the root or administrator's access.
- 5. **War Dialing**: This is normally the dialing of your entire phone number range to identify the modem connected to your computer system. Modems are currently the largest remote external vulnerability to your organization. Modems are cheap, easy to install and can run on virtually any type of system or network device. A hacker who is smart can circumvent your firewall by finding a poorly secured modem and gaining direct access to the network. This doesn't imply that all modems are bad. Some are very good.

Ways to Penetrate Your Network cont'd:

- **Remote Access Software**: There is the need to be careful with remote access software that enables users to access the network from a remote personal computer or workstation.
- When used in a securely manner, this is fine. Otherwise it is a hacker's delight. Remote control software is becoming common-place for users who work at home or for the "road warriors" who travel the globe armed with their notebook computers.
- **7. Password Cracking**: Once the hacker gets on to the system, their first task is to get the password file. They will then try and crack into the root or the administrator's password. The root password is very critical and once one has access to, he/she can damage the system.

Ways to Penetrate Your Network; cont'd:

- There are password crackers for system programs and software packages. Once they have little time they will easily break into the system. For good password management, it is always advisable to change your password on monthly basis.
- **Poorly Secured Routers**: Routers are electronic devices that dire traffic to the correct location. This helps to make the transfer of information more efficient and also filters out some of the junk, suc as broadcast messages. In many cases, routers are used to segm portions of a network. If properly configured they work well. If improperly implemented they tend to create a false sense of secur Routers are the gateways to many networks. Most routers authenticate by asking for password only. This reduces the amoun of time to crack into the router susceptible to an attack. Some of th more advanced routers do prompt for user ID and password, however, there is the need to remember to change the vendor defaults. Once a hacker gets onto a router, they will have access t the entire network segment.

Other Means to Secure the System

- **Firewall:** Another useful system set-up between the company's network and the Internet is the firewall. This is the most relevant and widespread technique to secure a network. Firewalls are set up to examine data as it enters the network and it blocks the traffic that does not meet specified criteria.

Other Means to Secure the System cont'd:

- **Encryption**: A means to prevent unauthorized access to information by tendering the communications illegible to unintended viewers. This approach maintains the free and connected structure of networks and the Internet by allowing data to flow freely in a secret language known only by the sender and the receiver.
- **Intrusion Detection System (IDS**): These are applications that actively monitor operating systems and network traffic for attacks and breaches are considered IDS. Its goal is to provide a real-time view of what is happening on the network. Example is the Secure Software.

Fighting Electronic Fraud

- So what can be done to avoid putting yourself at risk of fraud? The main advice is:
- - Have excellent knowledge of your trading partner if you are thinking of buying or selling anything over the Internet.
- - It is always advisable to have excellent knowledge of the business you are buying from before you give credit card details.

Fighting Electronic Fraud cont'd:

- It is advisable to be careful about invitations to lauder money from abroad and do not give details of your bank accounts to third parties.
- Never open suspicious e-mails.
- **The major frauds to be wary of are**:
- Internet Auction Fraud: You should think long and hard about buying or selling at Internet auctions and under no circumstance send cash or goods to foreign countries when you only have limited knowledge of your trading partner.

Fighting Electronic Fraud cont'd

- **Credit Card Fraud**: Credit cards represent the safest method of conducting business over the Internet. However, it is advisable to be careful and learn about the business to whom you disclose card details. Check your statements thoroughly.
- **Investment Fraud**: Investing abroad routinely entails higher degrees of risk and doing so over the Internet increases the risk. You need to be wary.
- However, the major message to avoid being a victim of fraud is simply to not trust anyone while surfing the Web.

What is Information Security?

- **Information Security** is about the security of our documents, our computers and the information retained in them. I trust your companies rely on their computers and records in these computers for the continuation of their business. There is the need to protect ourselves from:
- **THEFT** of computer equipment and documented information, which could be useful to our competitors.
- **DAMAGE** to our computer equipment caused either by accident or carried out deliberately. The information contained in these computers could also be damaged through VIRUSES, which effects could be disastrous.
- **DISRUPTION** to the computer services that could halt the continuous use of the information either through access or by other means for business.

Information Security cont'd:

- **Loss** of documented information we need either through printed copies of files. Documents that although stored and cannot be readily found, are as good as lost.

Basic Information Security Concepts

- Information security policy normally deals with three main qualities of information, namely:
- **Confidentially** : the assurance that company information is no disclosed to unauthorized persons inside or outside the compa and that unauthorized release of information will cause a loss o business disadvantage.
- **Integrity :** the assurance that information accurately represent the authorized business activities of your company and is not corrupted or modified by unauthorized persons inside or outsid the company. Integrity is particularly important for critical safety and financial data used for activities such as electronic funds transfer, air traffic control and financial accounting.

Basic Information Security Concepts cont'd:

- **Availability**: The assurance that information and information systems will be available when required by your company's needs or to comply with regulatory or legal requirements for information disclosure.
- Procedures must be implemented and maintained to protect the confidentially, integrity and availability of your company's business information.
- It is every employee's duty to contribute to the protection of information.
- It is every manager's responsibility to ensure that the staff and agents of the company know what is expected of them and that they act in a secure way to protect the company's information base.

Basic Information Security Concepts cont'd:

- Measures to protect information is based on good risk management practice. This means that security measures will be in keeping with the value of information to the business, and a judgement of the risks of breach of confidentiality, integrity and availability.
- Access to corporate information must be controlled on the basis of the minimum exposure needed to perform business functions, while retaining sufficient open communications for effective business performance.
- Processes and systems for managing information security must be as unobstructive as possible and not unnecessarily interfere with the conduct of the business.

Basic Information Security Concepts cont'd …..

- A copy of the policy statement must be made available to employees and agents. Copies should be provided on demand for consultation. New employee induction programs should introduce and explain the policy document and related standards, procedures and instructions. Digests of the policy and instruction guides and rules should be provided for employees and agents.

Developing Corporate Information Policies.

- To embark on an information security program, there is the need first and foremost to have an Information security policy in place, which is intended to be to help users and providers of information technology services to understand what they need to know and do to make sure the Information System in your company stay secure. Standard procedures will have to be in place to serve as a guide. The objective of the information security policy document is as follows:

Developing Corporate Information Security Policies cont'd ….

- **Objective:**
- To provide the direction and support for information security management in all departments and branches
- Demonstration of management support and commitment for information security
- The need to provide common objectives and directions throughout your company and its subsidiary

Developing Corporate Information Security Policies cont'd:

- **Standards/ Procedures**:
- Every unit in your organization, including your branches should have a policy document for information security, which must address certain security needs relevant to your business. The documents should be clear and understood by your customers and service providers. This document must be updated from time to time. This local policy may include a copy of your company's policy.

Developing Corporate Information Security Policies cont'd:

- This local policy must define the following:
- - Entire objectives and scope for information security in your departments (business units) and branches.
- It must also spell out the gains in being able to share information with other units of your company or your external agencies, including customers, suppliers, business partners and authorities.

Developing Corporate Information Security Policies cont'd:

- This local policy must have in it a statement of management intention supporting the goals and principle of information security.
- The endorsement of the senior management of your company must be explicitly in the policy document. The policy document should be signed by the managing director.

Developing Corporate Information Security Policies cont'd:

- The policy document must cover the following issues:
- Security education, awareness and training
- Legal and contractual compliance
- Virus protection, prevention and detection
- Business continuity planning

Developing Corporate Information Security Policies cont'd:

- The policy document must define the accountability and general management responsibility. The responsibility must include the appointment of a local information security manager.
- This local policy must be published and the deserved promotion given so that it is well-known and respected in your various companies.
- The local information security manager, who should be given specific responsibilities for information security, must report to the managing director.

Developing Corporate Information Security Policies cont'd:

- Within the local policy and any supporting documents, there should be processes of reporting information security incidents. This should include reporting security incidents or concerns to the information security manager.
- The responsibilities and accountability of all personnel must be defined. This should include reference to potential sanctions under employment contracts or prevailing computer misuse legislation where appropriate.

Developing Corporate Information Security Policies cont'd:

- The policy owner or the information security manager must ensure that there is annual review processes defined for information security policy, which also involves confirming the fitness-for-purpose and relevance of the local information security policy.
- NB. The policy statement is the highest level of a series of documents that provide a common framework and define the minimum common practices for information security within your organization.

System (Data) Access Control

- Business requirements for system access documented access control policy:
- Objectives:
- To ensure that authority is established and implemented for allowing (and preventing) access to business information.
- Standards/Procedures:
- Information owners must provide clearly defined and documente access policy statements, defining access

System (Data) Access Control cont'd

- Rights and restrictions for users and group of users
- There should be a documented statement of control policy for all business applications.
- Rights for "need-to-know" must be applied for information disseminations and entitlements.
- Access control must deal with contractual regulatory and legal requirements to protect access to data services.

System (Data) Access Control cont'd:

- Access control policies must specify the authorized use of the data in keeping with data privacy and protection legislation (in the UK this is the Data Protection Act, 1984).
- There must be standard user access policy defined and used for common categories of job.

System Access Control – Privilege Management

- Objectives:
- The use of special privileges is to be restricted to the minimum necessary number of trusted personnel.
- The trust will be reinforced by supervisory controls.
- Standards/Procedures:
- The categories of staff that needs to enjoy certain privileges associated with each system feature

System Access Control – Privilege Management – cont'd

- (e.g. Operating System, Database Management System) should be identified and documented.

System Access Control – Privilege Management, cont'd:

- Certain privileges must only be allocated to individuals on a need-to-use basis and event-by-event basis.
- Procedures should be established for authorizing and recording all privileges allocated.
- Privileges should not be allocated until the authorization process is complete.

System Access Control – Privilege Management cont'd:

- Systems routines should be used whenever possible to avoid the need to grant privileges to users.
- A record should be kept of all privileged user activity.
- The use of privileged access authority must be supported by peer supervisory controls and supervisory review logs.

System Access Control – User Password Management

- **Objectives**:
- To ensure that the issue and acceptance of new passwords is controlled and that users can be shown to have been instructed in good password management practices.
- **Standards/ Procedures:**
- Users must sign an undertaking to keep personal passwords confidential and work group passwords (where these are necessary) solely within the members of the group.
- Users must be provided with a once-only temporary password when being initiated to the system or recovering from a lost password.

System Access Control – User Password Management cont'd:

- Conveyance of passwords through third parties or unprotected (clear text) electronic mail must be avoided.
- Users must acknowledge receipt of passwords.

System Access Control – User Registration

- Users must have the documented authorization from the information owner for the use of the service.
- Checks must be performed by the local information security manager on access requests to confirm they are appropriate for the business purpose and are consistent with the security policy.
- Users must be given the access rights.
- Users must be required to sign an undertaking to indicate that they accept the condition of access.

System Access Control:- User Registration cont'd

- Access to new users with changed rights must be denied by the information custodian until all authorization procedures have been completed.
- Records must be maintained by the information custodian of all person registered to use the service.
- Accounts must be removed or changed immediately for users who leave the company or change job internally.

System Access Control – User registration cont'd

- There must be a periodic (at least monthly) check for removal of redundant user IDs and accounts no longer required.
- Procedures must be established to ensure that redundant user IDs are not re-issued to other users.
- There must be established procedures to notify the information custodians of users who leave the company or change responsibility internally.

Unattended User Equipment:

- **Objectives**:
- To advise users of good practice in shutting down or otherwise disabling terminals, workstation or personal computers at the end of working sessions or temporarily left unattended.
- **Standards/Procedures**
- 1. Users must be instructed to terminate active sessions when finished.

Unattended User Equipment cont'd:

- Users must be instructed to log off from remote or host computers when each session is finished.
- Computer users must be instructed to make PCs (or terminals) secure by a physical lock or an equivalent control (e.g. power up password) when not in use.
- All users and contractors must be provided with the advise regarding unattended equipment as described in the points above.

Enforced Path

- **Objectives:-**
- To control, where feasible, the route from the user terminal to networked system and the service accessed.
- **Standards/Procedures**
- There should be controls to restrict the route between the user terminal and the computer services that the user is required to access.

Enforced Path cont'd:

- Dedicated lines and telephone numbers should be used whenever viable.
- There should be a practice of automatically connecting ports to specified applications systems or security gateways.
- Menus and sub-menus options should be customized for individual users.
- There should be measures to restrict or prevent network roaming and browsing.

Segregation in Networks

- **Objectives**:
- To create secure network domains to limit opportunity for “browsing” or other unauthorized access.
- To make use of gateways or firewalls to provide secure paths between the domains.
- **Standards/Procedures**
- Large networks should be divided into smaller domains to help keep security management administration and access control manageable.
- The use of domains, firewalls and gateways must be defined and supported by information security procedures.

Segregation of Networks cont'd:

- All domains must be covered by security procedures and security management.

Password Management System

- **Objectives:-**
- To ensure that passwords as the principle means of user authentication are not compromised.
- To provide an effective, interactive facility that ensures quality passwords.
- **Standards/Procedures**:
- All computer users must have their own unique ID and passwords.
- There must be no facility for “guest” passwords.

Password Management System cont'd:

- Users must be forced to change their passwords regularly, say on monthly basis, as per your password management system.
- The password management system must enforce reasonable format controls on user passwords to include minimum/maximum length, types of characters, alphabetic, numeric, punctuation, etc.
- System access must be refused to a user after three unsuccessful login attempt (user ID + passwd) until reset by an authorized system / security administrator.

Application Access control

- **Objectives:**
- To ensure the information access and owners' requirements are translated into logical controls within application to restrict access capabilities – read, write, delete, execute of users.
- **Standards / Procedures**
- There must be access policy for each application, authorized by application owners and compliant with the information security policy.

Application Access Control cont'd:

- Application access policies must be regularly reviewed (at least every six month) by the information owners and independent authorities. (e.g. internal audit).
- Menus should be used to control access to application system functions in accordance with application access policy.
- Each application access policy must specify the types of access allowed: e.g, read, write, delete, execute

Data Security Audits

- Information security standards for your company – The standard defines what is to be done in all the branches or subsidiary in your company and also the business units to protect business information and systems. Normally the information security policy is contained in the information security standards.
- **Compliance**: Information security standards provide the general managers with a mandate to take actions to protect information and information systems. An essential part of the action is the appointment or identification of local information security manager (LISM).

Data Security Audits cont'd:

- The LISM should use these standards and associated self-assessment materials to help assess levels of compliance with the standards, and to conduct security improvement and maintenance programmes to achieve and sustain compliance.
- The information security standards will be used as the framework for audit by LISM. In addition a regular self-assessment will be conducted every six months. These audits will be carried out to continuously improve the existing system.
- Continuous audits will be carried out every month to assess the adequacy of the system.

Data Security Audits – Self-Assessment Process

- Objective of self-assessment:
- To enable business units or department assess the adequacy of their control environment.
- To enable local and regional management to measure compliance with the information security standards.

Data Security Audits cont'd

- To provide local management with a comparison of their own security environment against those of their business units in the region.
- To provide regional management with a measure of the overall progress made in improving the level of security in their region.

Data Security Review – Scope of the Review

- - Local security policies and management
- - Operating system security
- - Telecommunications and network security
- - Database security
- - Computer operations
- - Personal computer security

Data Security Review – Scope of the Review cont'd:

- Application-level security
- Program change control
- Physical computer security

Data Security Review Results and Implementation Status

- **Common Findings:**
- Technical controls
- Data and programs not properly protected
- Inappropriate access right granted
- Procedure/organizational controls
- Lack of documented procedures, e.g., system administration task

Data Security Review Results and Implementation Status cont'd:

- Lack of formalized monitoring procedure
- Lack of formalized "ownership" of data and applications
- No data classification
- Disaster recovery/business continuity planning
- Lack of a plan and formalized recovery arrangements

Security Incidents Identified

- Type of incident reported
- Unauthorized access attempts from other sites, other branches, or countries
- Unauthorized access attempts by external personnel
- Unauthorized login account established with supervisor rights
- Virus incidents

Security Incidents Identified cont'd

- Theft of PCs or components
- Pornographic material downloaded from the Internet
- "Chain letters" circulating on e-mail systems
- Use of company's computer resources for personal work
- Deliberate deletion of company data
- Power failure and water damage

IS Audit Questions

- Has LISM been appointed for your center?
- Do you have information security policy in place?
- Do you have anti-virus software installed on your system?
- How often do you embark on information security audits?
- Do you have IT contingency planning in place?
- When was last time you carried out a self-assessment process at this data center?

Causes of Security Failures

- Over-reliance on key staff
- Staff dissatisfaction
- Inadequate documentation – in development and in maintenance
- Unauthorized program changes
- No record of program/ master file amendments
- Inadequate program backup

Causes of Security Failures cont'd.

- Inadequate user control
- Bad physical security

Anti-Virus Techniques

- What is a virus?
- - A destructive program written to cause chaos on the system.
- Security Measures:
- Anti-virus measures
- Preparation.
- Prevention from
- Recovery

Detecting and Preventing Viruses

- **Objectives**:-
- The principle objectives of a reasonable balance from, early detection of and recovery from computer virus.
- The basis of protection against viruses should be founded on good security awareness, appropriate access controls and specific guidelines for system “hygiene” . virus detection and repair.

Standards/Procedures

- A formal policy must be established by the country or business units to ensure compliance with software licenses and prohibit the use of unauthorized software. This policy should cover unlicensed commercial software “freeware,” “shareware” and software made available through bulletin boards and other information sources.
- PC and workstation users must be informed of their responsibilities , liabilities and good practice for virus prevention They must be informed of the following:
- - Do not leave floppy disk in drive A after switching off the PC
- - Do not boot the PC from drive A except with a known “clean” (virus free) write–protected system disk.

Detecting and Preventing Viruses cont'd: ….

- - Do not use software "pulled down" from bulletin boards, or magazine cover disks.
- - Do not use "freeware," "shareware" or public domain software.
- - Use software from reputable manufacturers.
- - It must be ensured that PC and workstations are equipped with power-on passwords to ensure that the principle information custodians can control the use of the equipment.
- - All PCs must have the company's approved PC anti-virus tool installed and enabled.
- The following are some of the approved anti-virus tools.

Detecting and Preventing Virus cont'd:

- - - VirusScan, McAfee Associates Inc.
- - - Dr. Solomon's Anti-Virus Toolkit for Windows, S&S Software International
- - - Regular updates from the PC anti-virus tool supplier must be purchased and installed on all PCs.
- - For each different type of PC, a "clean" (virus free) write-protected floppy disk must be created with all system and device files necessary to boot the PC.
- - Virus "repair" software may be used with caution, only in cases where the virus characteristics are fully understood and fully trained personnel are certain of correct repair.
- - Procedures and responsibilities must be established for reporting and recovering from virus incidents.

Network Management

- **LAN** – Local Area Network, the network existing at a single location (typically one building or a campus of several buildings). LANs connect computer systems and peripherals (disk drives, tape backup units, etc) to a data and peripherals sharing group. LANs are distinguished by their high data transfer rates, low error rates and inexpensive media. Most LANs are privately owned and maintained.
- **WAN** – Wide Area Network spread over a wide area, such as across states or countries. Communication over WANs can take place via telephone lines, satellites.

Network Management cont'd:

- Compared to LANs and MANs, most existing WANs are slower and more error prone.
- MAN – Metropolitan Area Network

Network Security Control

- Preventing security breaches through networks
- The objective of the network security controls are as follows:
- - To ensure the protection of information in networks and safeguarding of the supporting infrastructure
- To ensure very good security management of networks which span organizational boundaries
- - To give assurances to the security of data on public networks

Network Security Controls cont'd:

- Access to the public networks must be controlled by a group of professionals in the network setup. Access to the network could be through SITA, BT, Ghana Telecom and other service providers. Local connections required to all public networks and services will have to be approved by the group of professionals before implementation. These includes services like the Internet and EDI. Each request must be submitted in writing and accompanied by business justification and a security risk assessment.

Network Security Control cont'd:

- Computer and network management must be sufficiently coordinated so the security measures are consistently applied across the IT infrastructure.
- Regarding the login access between countries across the WAN, there must be a limitation and stringently controlled and also comply with system access control.
- Precaution must be taken to prevent and detect the introduction of malicious software like viruses into your company via EDI link.

Disaster Recovery Techniques/ Planning

- **Objectives**:
- - Business continuity planning
- - To enable recovery from major failures or disasters
- Setting up a process for developing and maintaining continuity plans

Data Recovery Techniques cont'd:

- - Backups
- - UPS
- - Generator sets
- - Security safes
- - Insurance coverage
- - Fire extinguishers
- - Fire escapes

Recovery Plan Development

- Data center and network recovery plan
- - Emergency response
- - Damage assessment
- - Notification and activation
- - Recovery teams tasks and responsibilities
- - Site restoration teams, tasks and responsibilities
- -

Develop Recovery Strategy

- Compile resource requirements – functions/systems/ recovery timeframes
- - Facilities – centralized/distributed
- - Computer – hardware/data storage
- - Communications – voice/data
- - People

Evaluate Risk Management Practices.

- A) Identify and analyze threat
- B) Evaluate countermeasures
- - Off-site storage program
- - Insurance coverage
- - Operational control measures
- C) Document strenghts and weaknesses
- -

Perform Business Impact Analysis

- - Develop disaster scenarios
- - Document critical functions and systems
- ********** END **********