**Security, Integrity and Control**

**Introduction**

This chapter highlights the importance of protecting the data against any risks, threats and vulnerabilities,

**Terminology**

**Security:** protection of data from accidental or deliberate threats, which might cause unauthorized modification disclosure or destruction of data and the protection of the Information System from the degradation of non-availability of services.

**Data integrity:** Applies when data are the same as in source documents and have not been accidentally

or intentionally altered, destroyed or disclosed.

**System Integrity:** Refers to the system operation conforming to the design specifications despite attempts to make it behave incorrectly

**Risks:** Various dangers to information systems, the people, hardware, software, data and other assets with which they are associated.

**Threats:** Refer to people, actions, events or other situations that could trigger losses, they are potential causes of loss

**Vulnerabilities:** Flaws, problems or other conditions that make a system open/prone to threats.

**Controls:** Are counter measures to threats. They are tools that are used to counter risks from the variety of people, actions, events or situations that can threaten an IS. Are used to identify risk, prevent risk, reduce risks and recover from actual losses.

**Common Threats**

**i. Natural disasters**

E.g. five, floods, water damage, earthquakes, tornadoes, hurricanes, mud slides, wind and storm damage

Security planning should consider

 Disaster prevention

 Disaster containment

 Disaster recovery

e.g. **Prevention**: Use of backup power supplies or special building materials, locations, drainage system or structural modifications to avoid damage during floods, storms fires and earthquakes.

**Containment:** Consider sprinkler systems, halon gas fire

**Suppression:** System or watertight ceilings to contain water damage from fire hoses.

**Recovery:** developing contingency plans for use of computer facilities of vendors or non-

Competitors with similar computer systems

**ii. Employee errors**

Ordinary carelessness or poor employee training e.g. formatting the hard disk rather than drive A, keying incorrect data.

**iii. Computer crime, fraud and abuse**

Computer crime: stealing data, damaging or vandalizing hard ware, software or data or using computer software illegally or committing fraud.

**iv. Industrial espionage**

It’s the theft of original data by competitors. Also called economic espionage

**v. Hacking**

Also known as cracking. It’s the unauthorized entry by a person into a computer

system or network.

Hackers are people who illegally gain access to the computer systems of others.

They can insert viruses onto networks, steal data and software, damage data or vandalize a system.

**vi. Toll Fraud**

Swindling companies and organizations e.g. through telephone bills through false pretences – e.g. use of slugs instead of real coins

Toll hackers use maintenance ports, modem pools, voice mail systems, automated attendants or other facilities of PBX, the private branch exchanges that are the computerized telephone switches at customer sites.

Signs of frauds:

1. Numerous short calls

2. Simultaneous use of one telephone access mode

3. Numerous calls after business hours

4. Large increases in direct inward system access dialing or

DISA

**vii. Data diddling**

Use of a computer system by employees to forge documents or change data in records for gain.

**viii. Trojan horses and salami slicing**

This is a change in code that is made to a program without authorization.

It appears to be performing a proper task but may actually perform a variety of mischievous or criminal activities e.g. printing paychecks to employees or vendors who don’t exist.

**ix. Trap doors**

These are procedures or code that allows a person to avoid the usual security procedures for use of or access to a system or data.

**x. Computer viruses**

A computer virus is a hidden program that inserts itself into your computer system and forces the system to clone the virus (i.e. it replicates itself.)

They may cause serious damage by modifying data, erasing files or formatting disks.

e.g. cruise or stealth virus might lie dormant until it can capture financial information and transmit the data to thieves

Antivirus programs or vaccination products can be used. Antivirus programs help in:

Preventing the virus program inserting itself in your system

 Detecting a virus program so you can take emergency action

 Controlling the damage virus can do once they have been detected.

Hardware theft and vandalism

**Software privacy** – any reproduction or a copyright program is theft.

**Security policy and contingency plans**

A security policy will include the following: Identification of risks, Qualification of risks, Identification of counter-measures, Costing of counter-measures, selection of counter-measures, implementation of counter-measures, drawing up of a contingency plan. Risk Analysis.

A contingency can be defined as 'an unscheduled interruption of computing services that requires measures outside the day-to-day routine operating procedures.



A contingency plan must therefore provide for standby procedures so that operations can be performed while normal services are disrupted, recovery procedures, personnel management policies.

**Security measures (controls)**

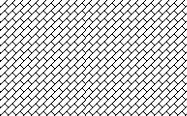
The nucleus of security lies in the design of the computer system and its programs. However design of a tightly controlled it’s not by itself. A layer of other controls must surround it. Therefore we can view security of the database as a group of layers of protection.

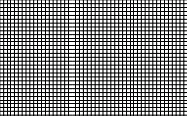
Database controls

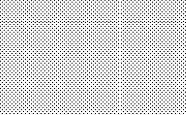
Accees controls

Physical security











Administrative control

Legal protection

**Administrative Controls**

These are the controls by non-computer based measures. They include:

 Personnel controls e.g. selection of personnel and division of responsibility.

 Secure positioning of equipment

 Physical access controls

 Building controls

 Contingency plans

**P C Controls**

They include the following:

 Keyboard lock

 Password

 Locking disks

 Training

 Virus scanning

 Policies and procedures on software copying

**Database Controls**

*A number of controls are embedded into DBMS, these includes:*

 granting of privileges and ownership, authentication

 Views

 Backup and Recovery

Checkpoints - the point of synchronization between database and transactions log file. All buffers are force written to storage

Integrity checks e.g. relationships, lookup tables, and validations.

Encryption - coding of data by special algorithm that renders them unreadable without decryption key

 Journaling - maintaining log file of all changes made

 Database Repair

**Development Controls**

*When a database system is developed, there should be controls over the design, development and testing e.g.*

Testing e.g. program testing, system testing and user department's acceptance testing

 Formal Technical Review

Controls over changes by use configuration management

 Controls over file conversion

**Document Standards**

They include the following:

 Standards are required for the documentation such as:

 Requirement Specification

 Program Specification

 Operations Manual

 *User Manual*

**Legal Issues**

They include the following:

 Escrow Agreements - legal contracts concerning s/w

 Maintenance Agreements

 Copyrights

 Licenses

 Privacy (Data Protection Act)

**Other Controls**

They include controls such as:Hardware Controls e.g. device interlocks which prevent input or output of data from being interrupted or terminated, once begun

Data Communication Controls e.g. error detection and correction.