Security Management in Organisations

- SM Highlights
  - Administrative and organizational security
  - Personnel security
  - Physical and environmental security
  - Operations security
  - Hardware security
  - Software security

Administrative and Organisational Security

- Administrative & Organisational security
  - Overview
    - The need to establish security functions organisations
    - The development and implementation of security policies and procedures
    - The determination of organisational needs and security threats

Administrative and Organisational Security

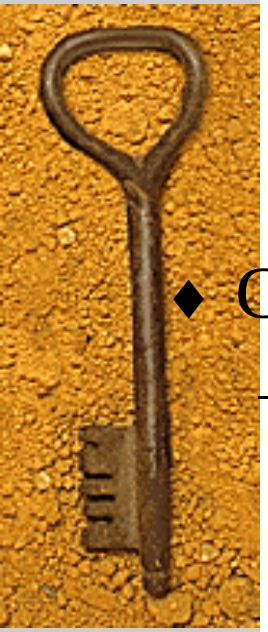
- Appointment and Responsibility
  - Companies must appoint responsible security officers
  - Functional and reporting requirement should be set out in the policy
- Organisational Requirements
  - Assignment of duties
  - Segregation of responsibilities
  - Job description
  - security officer responsible to senior Policies
  - Trained designates
  - Security audit
  - Reference materials/awareness
  - Organisation's acceptable use policy

Administrative and Organisational Security

- Information Security
  - Review of information holdings
  - Classification and designation of information
  - Relationship to privacy collection of personnel information
  - Information technology assets:
    - Inventories of sensitive IT assets
    - assign accountability
    - Conduct threats and risk assessments
- Managing security risks
  - Process to minimize risks to property, and employees
  - Risk Policies process help to
    - reduce, avoid, contain or accept risk
  - Conduct threat & risk assessment
  - Fill out statement of sensitivity

Administrative and Organisational Security

- Statement of Sensitivity
  - Outline
    - Confidentiality concerns
    - Integrity concerns
    - Availability concerns
- Contracting
  - Define security requirement in all contracts
  - Perform security clearance based on levels
  - Provision for employee's security obligations
  - Ensure security if work conducted on-site or off-site



Administrative and Organisational Security

- Contracting
  - All contract involving sensitive IT activity or assets including
    - programming
    - hardware, software
    - maintenance, suppliers and consultants
    - guards services, cleaners
    - off-site storage , contingency plans
    - contractors
      - Should be reviewed in line with the company's security policies
- Access control and authorization
  - Based on need to know
  - For information technology, you must determine needs for :
    - system users, including Policies
    - operations personnel
    - maintenance and support personnel
    - system analyst and programming staff

Administrative and Organisational Security

- Inspection & Investigation
  - Should be of normal administrative function
  - Normal random and routine in nature
  - Based on policy and procedures
  - Determine how to deal with breaches of security
  - Criminal offences, evidence, cooperation with police will be necessary
- Inspection & investigation
  - For IT security, surveillance and audit of
    - system logs and records
    - system security incidents
    - review of investigations
  - Audit of computer security should be an ongoing function and must be performed at least once a year.

Personnel Security

- Personnel screening process
  - develop and implement policies and procedures to confirm:
    - identification
    - loyalty
    - reliability of personnel
  - goals of protecting sensitive information and assets
  - screening process for :
    - organisation's employees
    - contract personnel
- Personnel screening for IT
  - IT employees must be security screened according to highest level of information and assets accessed
  - IT contractors must be screened to highest level also
  - managers responsibility to determine level required should be appointed

Personnel Security

- Primary checks to conduct include:
  - Verify personnel data (date of birth , address, NSITF number if applicable)
  - Verify relevant educational and professional qualifications
  - Verify employment data
  - assess reliability by checking with previous employment via identified references
- Other checks to conduct include:
  - character reference
  - personnel background
  - criminal records
  - finger print checks
  - intelligence services checks
  - credit history (potential effects on job reliability)

Personnel Security

- Other hiring considerations:
  - character (honesty, emotional stability)
  - financial situation
  - citizenship
  - personal belief s and associations

- Personnel screening for private sector contracts
  - 1.Security screening must be conducted before access to sensitive information or assets
    - try to use screened contractors
    - have contractor provide list of screened personnel

Personnel Security

- Personnel screening for private sector contracts
  - 2. Security screen must be conducted before access to designated information or assets
    - special circumstance can waive prior screening if clause in contract e.g screening requirement will be met within six months of contract awards

- Identification of personnel
  - 1.Approved ID cards should contain :
    - Name of card holder
    - Name of employer
    - photo (3/4 frontal)
    - signature of card holder
    - signature of issuing authority
    - Card controlled serially
    - Expiry date (max. 3 years)
  - 2.Should issue ID cards to all in organisation, especially if visit other facilities is necessary

Personnel Security

- Identification of personnel
- 3.Should document and implement for regular review and update of ID cards /access badges:
  - verification / withdrawal for any cause
  - Replacement/report loss and theft /replacement
  - expired cards (internal / disposal)
  - significant facial changes (e.g. Beards)

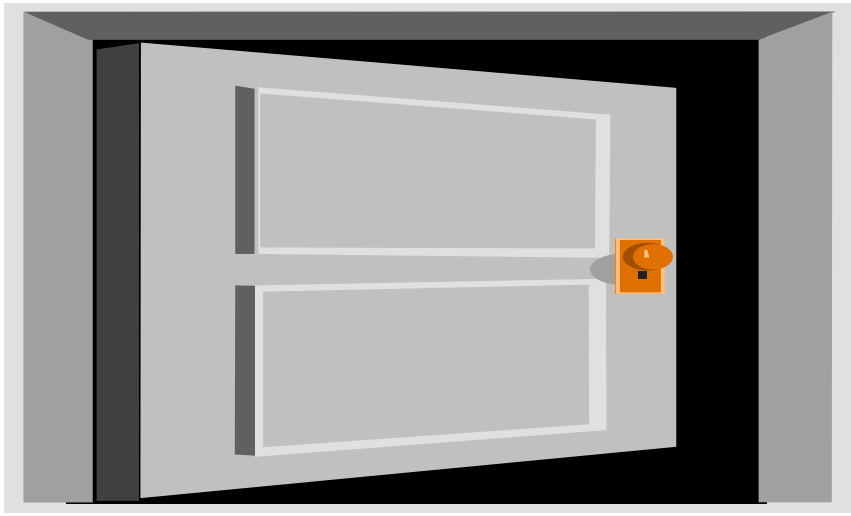
Personnel Security

- Security Orientation and Awareness
  - document and implement programs
  - ensure all IT employees are
    - shown security films / videos
    - familiar with security pamphlets /posters
    - aware of local local procedures
    - given formal security briefing s
    - notified of security violations
    - advice on other security issues specific to work-site

- Most Common Vulnerabilities
- program not developed or implemented
- employees not aware of all security requirements for IT equipment & information accessed by them

Physical and Environmental Security

- Physical and environmental security



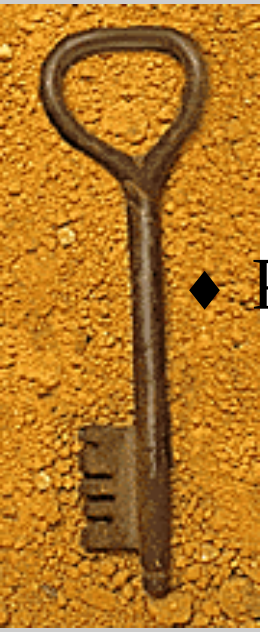
- Definition
  - the physical protection of assets against accidental and deliberate:
    - obstruction
    - removal or loss
    - corruption or modification
    - disclosure
    - Interruption of computing resources (*data*, *programs*, *accessories*, *network nods*, *devices*, *etc)*

Physical and Environmental Security

- Overview
  - physical security is the first line of data center defense
  - provide a protective environment for power, humidity and temperature
  - should be incorporated in the design phase of construction.
  - Based on regulation and codes
  - should be evaluated periodically against TRA (Treats Risks Assessments)
- IT Physical Security
  - common vulnerability is lack of control over physical access to sensitive information received by fax devices and computer terminals
  - limit access to computing & telecommunications equipment where possible, especially after working hours
  - establish secure zones

Physical and Environmental Security

- Data Center Construction
  - resist access using layered design technique
  - provide a safe haven for information processing using the following techniques :
    - control environment
    - disaster prevention
    - disaster containment
    - disaster recovery
- Physical Security Main Points
  - location & construction
    - IT site / facility
    - IT Equipment / Storage Areas
  - access control:
    - restricted zones, public zones
    - Control, authorize and monitor access
      - personal recognition (guards), identification (cards), electronic access control , intrusion detection, etc.



Physical and Environmental Security

♦ Physical Security Main Points.

- Evacuation Procedures in cases of disaster
  - Documentation to ensure:
    - Ensure personal safety
    - maintain security of sensitive information / assets
  - Include...
    - facilities, names, duties of personnel
    - Test regularly, distribute information
    - Ensure procedures are adequate & security maintained at all times

♦ Business Risks

- risks associated with breach of physical security include:
  - impediments to normal operations
  - excessive downtime, unauthorized access
  - bankruptcy, excessive preventable cost
  - Inability to process data
  - loss or injury of key employees
  - loss of critical data files
  - poor service levels

Hardware Security

- Overview
  - need to safeguard IT equipment and its functional environment
  - hardware security helps to ensure information is not accidentally lost or altered within the hardware devices
  - hardware security helps to ensure availability of service that could be lost due to electromagnetic emanations
- Common vulnerability
  - Inadequate policies and procedures for controlling changes to IT systems for normal operations and for maintenance
  - creates significant security risk but cost of minimizing risk is low

Hardware Security

- Hardware policies and procedures
  - should include:
    - placement of hardware to reduce effects of electromagnetic emanations
    - maintenance of hardware inventory and configuration chart
    - identification and use of security features implemented within the hardware
    - authorization, documentation and control changes to hardware

- Hardware policies and procedures
  - should include:
    - Identification of support facilities including air conditioning and power
    - provision of UPS
    - maintenance of IT equipment and services

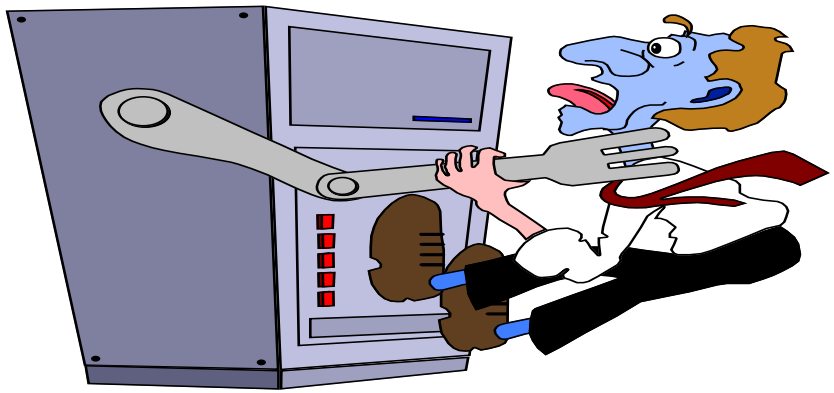
Hardware Security

- Hardware Maintenance Contracts should provide for:
  - supervision of service personnel
  - equipment exchange procedures
  - remote link-up procedures reporting policy
  - maintenance records, etc.
- Change control
  - retention of documentation for:
    - maintenance
    - configuration control
    - Modification procedures

- Hardware security conclusions:
  - ensure policies and procedures for controlling changes to IT are established
  - establish clauses in maintenance contracts
  - make sure change control process is in place for hardware
  - write procedures for erasure and disposal of media

Operations Security

- Operations security



Operations Security

- Operations security
- Overview
  - Operations procedures should ensure :
    - consistency and accountability in applying security policies
    - events related to security can be audited and traced to assets in taking corrective action
- System Access Authorization
  - control logical access:
    - user name password
    - banner
    - rules and regulations
  - limit privileges for job functions
  - policy & procedures for issue and control of access material

Operations Security

- Separation of Duties
  - define responsibilities
  - control physical access to IT resources and other related facilities
- Procedures and controls
  - normal operation procedures (server and user equipment):
    - commands
    - responses to applications
    - virus detection
    - e.t.c.
  - Procedures for transfer of operational control to prevent compromise
  - see list of procedures on next slides

Security Policies in Organisations

- Procedures and control
  - power up / power down sequence
  - start up / shut down of the systems (Incl. OS and applications)
  - equipment operation
  - trouble reporting
  - security incident handling
  - staff performed maintenance
  - response to network and applications program-generated messages
- Procedures and controls
  - network administration commands
  - start and stop communications
  - backup and restore
  - sanitizing erasable media
  - disposal of unserviceable erasable media
  - emergency situations
  - recovery and restart
  - handling of classified / designated materials

Operations Security

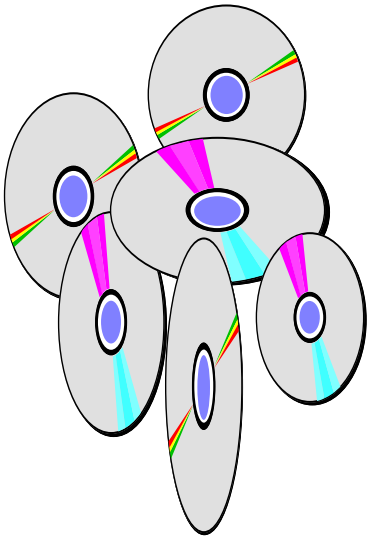
- Procedures and controls
  - environmental support equipment
  - setting and resetting of the server clock
  - virus scanning
- Media
  - Define:
    - media access controls
    - inventory requirements
    - control of media for re-issue
    - media erasure and disposal

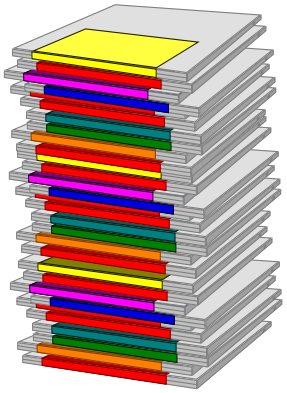
Security Policies in Organisations

- Detection and surveillance
  - definition of what constitutes security incident
  - methods to verify only authorized work in progress
  - consider third party software
- Contingency Measures
  - current copies of data and critical resources available
  - availability of software and documentation
  - index of resources on-site /off-site
  - telephone numbers
  - practice / testing

Software Security

- Software Security
  - “If something you can really care about (such as lives, money, resources, just plain data or even the survival of the world) is to be entrusted to a computer system, you should all be very suspicious “says Peter Neumann, He suggested that in fact when the real risk becomes to great, we had better rethink the use of computers in those applications”





Software Security

♦ Overview: Software Security

- must ensure security of all classes of software
- Software is regarded as a safeguard, as an asset and as a threat
- policies and procedures must be created for software security
- systems development life cycle (sdlc) standards must be adhered to
- program change controls are extremely important in application development

♦ Classes of software

- a brief review
  - operating system software (DOS, Macintosh, Windows NT ,UNIX, Novel Netware , Windows 95-2000)
  - Application software (word processors, accounting system etc)
  - customized software (development of a particular environment)
  - programming languages (C-BASIC etc) micro codes BIOS, source codes executable codes

Software Security

- Software as a safeguard
  - provides:
    - access control (via p/w, user-IDs, etc)
    - Encryption mechanisms
    - network Policies
    - audit control
    - log in identification
    - labeling
    - isolation of IT peripherals, LAN segments
    - System recovery
    - integrity verification techniques

- Software as an Asset
  - expensive to acquire, develop, maintain and replace
  - critical resources thus:necessary to maintain availability and integrity of system
    - deficiency in software will reduce validly of underlying hardware
    - problems can void the integrity of applications and data

Software Security

- Software as a Threat
  - certain software is capable of overriding, bypassing and altering controls (the case of a disgruntled employee(s)
  - can be used to gain access to sensitive application and data(the case of mischievous operations)
  - can be used to take control of system resources and prohibit authorization(the case of an overzealous student)

- Software policies and procedures
- administrative controls:
  - segregation of duties of IT staff
  - inventory
  - reviewing security
- configuration Policies
- control access to software and establish resources limits
- use surveillance and detection mechanisms
- identification and authentication

Software Security

- Policies and Procedures
  - audit controls and surveillance
  - system development life cycle standards :
    - design, development, test standards
    - control of change
    - problem solution
  - encryption
  - quality assurance
  - virus scanning

- Separation of duties
  - assign the following responsibilities to individual with separate areas:
    - system programming and services
    - application programming and design
    - software librarian and services
    - quality assurance and acceptance testing
    - network administration
    - database administration
    - security administration

Software Security

- Software Inventory
  - formally assign responsibility for maintenance of inventory records
  - reasons for maintaining a complete and accurate inventory:
    - accountability
    - business resumption planning
    - maintenance considerations
    - centralized source of documentation
- Software Configuration
  - parameter and options required to startup and customize the operation of :
    - system software
    - database Policies systems
    - application software
  - must be established and documented
  - customized data affects configuration performance and behaviour

Software Security

- Access control
  - control and monitor access to systems and data resources
  - access to resources based on user identity and pre-defined authorization
  - pass application access request to the access control facility
- Surveillance
  - 1. Monitor and review available logs and records
    - console logs
    - system logs
    - database journals and transaction logs
    - communication logs
    - security logs

Software Security

- System Development Life Cycle
  - 2.Establishes a framework for how an organisation's development projects will be run
  - 3.Ensures consistency of approach among various system of development projects
- Software Library Control
  - assign responsibilities for software librarian services, Including:
    - custody
    - access control for production, audit and change control purpose
    - adequacy of on-site backup procedures
    - maintenance of the records of access and changes
  - software Policies and distribution procedures for distribution and remote systems

Software Security

- Quality Assurance Testing
  - assign responsibilities for quality assurance functions, Including:
    - development and implementation of test standards and criteria
    - performance of quality assurance testing
    - reviewing and reporting on quality assurance test results
    - conduct testing in an environment separate from the production system

- Application Change Control
  - 1.formally assign responsibilities for maintaining change control records
  - 2.Document change control procedures for :
    - the mechanism for requesting changes
    - recording and tracking outstanding requests
    - approval of requests
    - testing and documenting changes
    - implementing changes

Software Security

- Application change Control
  - 3.Accept changes to production software after extensive testing and following compilation procedures
  - 4.Common short-comings of program change control include:
    - most organisation give change control "lip service" only
    - "too much paperwork"
    - they just resent control
    - they do not realize the risks

Software Security

- Application Change Risk
  - risks associated with application changes:
    - unauthorized changes can be induced with authorized changes
    - unauthorized changes to production programs
    - unauthorized access to program files
    - incorrect processing result from :
      - program error
      - fraud
      - incorrect formula
      - whimsical priorities

Software Security

- Application Change Risk
  - most auditor fail to audit object programs:
    - object program are compiled source programs (COBOL FORTAAN) in machine language
    - object programs can be changed without changing source programs using emergency fixes (super zap)
  - to audit object programs:
    - recompile production version of source code
      - create new object program use compare utility to compare to production object
      - there should difference in times of compile, ate of compile, version number

Software Security

- Desired Application Controls
  - document initiation of changes:
    - origination
    - users(modification)
    - operations(problems)
    - systems(efficiency)
  - reason for change:
    - legal/contractual
    - modifications
    - marketing
    - information-based

- Desired Application Controls
  - separation of duties :
    - programmers should never have access to production programmes
  - peer review
    - ensures efficiency
  - testing:
    - programmer unit test
    - managers system test
    - users stress test

Software Security

- Desired Application Controls
  - formal transfer procedures
  - use of library Policy package:
    - code compare
    - listing of changes and data
    - protection of data sets
    - archiving
    - ability to backup changes
  - Policies approval

- Desired Application Control
  - cost/benefit analysis
  - prioritization
  - staffing scheduling
  - safe custody
  - formal change control procedures: written requests
  - Policies approvals
  - change logs etc.

Software Security

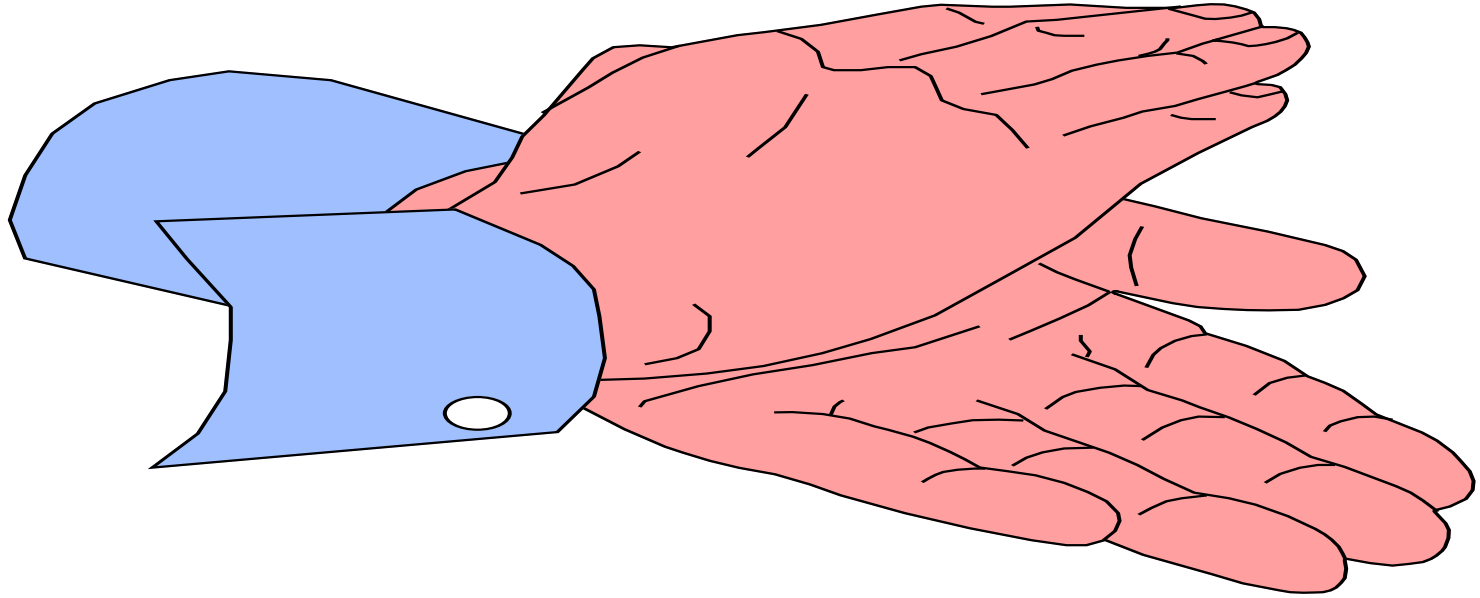
- Detecting Unauthorized Changes
  - if library package is in use
    - use package report writer
    - list all programs changed in (n) months
    - compare listing to unauthorized change in change log(differences represent unauthorized changes)
  - if library package is not in use
    - obtain a copy of all production programmes
    - wait a few months (four to six) and take a surprise copy of program you wish to test
    - use compare utility to compare both copies (differences represent unauthorized changes)

- Detecting Unauthorized Changes
  - conversely to check if a change is incorporated:
    - select change from the change control log
    - list data of changes to the program
    - list actual lines of code
    - compare program before change to after change

Software Security

- Software Security Conclusions
  - security of all classes of software is necessary
  - software can be regarded as a safeguard, as an asset and as a threat
  - policies and procedures must created for software security
  - system developments life cycle standards must be adhered to
  - program change control are extremely important application development

Managing IT Security in Organisations



THANK YOU ALL