Computer Centre Management

Computer Centre Management (CCM) Overview

Various Names of Computer Centre

All computer Centres are responsible for virtually similar tasks in all organizations, however, their focuses may not be the same. Using a certain name would identify its focused responsibilities, and the following are examples of such naming convention

1.	**Data Processing Centre**: To process business data (Sales, Accounts Deposit/Withdrawal, Airline Ticketing, Student Registration, etc.) and produce summary report or other business documents
2.	**MIS Centre**: To provide information for managers and executives for making timely and quality decisions (usually continuing the work of data processing.
3.	**Data Centre**: To provide data for use by all departments (e.g. Centre to provide criminal records, population records (Khonthai.com), etc.)
4.	**Office Automation and Internet Centre**: To provide services to all departments with office automation and communication systems.
5.	**Computing Service Centre** (or **Computer Centre** or **IT Service Centre**): Basically, to provide services of all types related to business data processing, business applications, and maintenance services to all departments in the organization.

Services Provided by Computer Centre

1.	To provide computer-related services to personnel and customers
2.	To provide advice and consultancy for users
3.	To provide systems development services to users
4.	To provide data entry services for users
5.	To create and maintain IT standards and procedures
6.	To provide IT acquisition services to users
7.	To keep and protect IT and data assets
8.	To ensure that the organization has adequate/advanced IT progress, which is in line with the organization's vision
9.	To ensure that services provided meet with users' requirements

CC Growth Stages

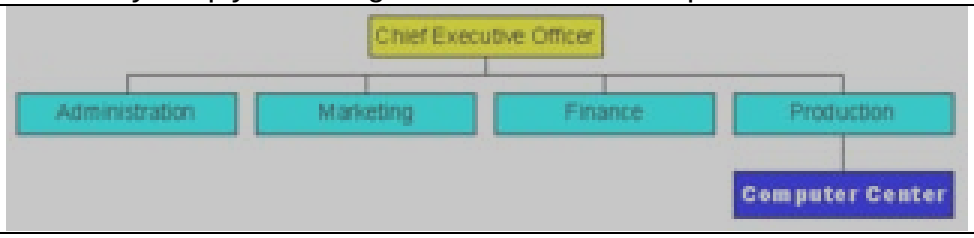
Richardson Nolan's Six Stages of Growth in CC

Initial Stage	At this stage, personnel has never used computer before. They have just start using computer with not much knowledge about it. This stage can take place in any department in the organization.
Contagion Stage	There is growth in expenditure for acquisition of computers as most departments seem to need computers for their task at all levels. Needs for computer in normal operations become stronger, and widespread throughout the organization.
Control Stage	The organization starts to take filtering and controlling actions on

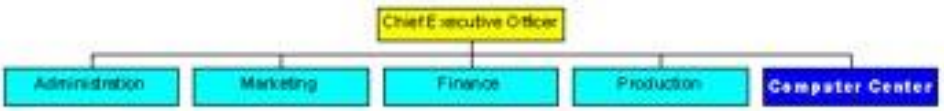
	acquisition of computers with references to expected results. Costs/Benefits consideration is made on each and every acquisition against expected business results or contributions by those departments to orgnization as a whole.
Integration Stage	Realized that there are increasing unnecessary repetition of data capturing, and processing throughout the orgnaization, thus, it starts to integrate all of them together to reduce repetition and redundant efforts. An improvement toward more productivity and better efficiency in managing data.
Data Admin Stage	The stage with active Data Sharing and Data Protection. Network(Internet) and Database has started being used at this stage.
Maturity Stage	The concept of Total Quality Management (TQM) is implemented, at this stage, the Computer Centre is capable of handling changes in people and technology quite well, it can manage to adapt and change in accordance with environmental changes.

Computer Centre and Its Presence in Organization

- A Computer Centre may simply be a single unit within each department.



- A Computer Centre may be, instead, a separated unit under Chief Executive Officer at the same level of authority as other functional departments
  - Computer Centre can provide services to other department as a company's Centre of a function --- computer-related .function.



EFFECTIVE COMPUTERIZATION (EC)

Meaning Of Computerization

This is the conversion of a manual-based process to a computer-based alternative

EC has to do with computerizing such that the envisaged aims and objectives of the computerization effort are adequately realized by the organisation .

Effective Computerization demands

- Inclusive practical systems analysis and design
- A user friendly SW development or SW acquisition, which ever method is used to procure the SW

- Carefully planned SW maintenance activity
- Provision of HW that will accomplish the goal of Centre
- Effective HW maintenance to guarantee high availability and low-down time
- High calibre, qualify and experienced staff.

Pre-requisite to EC

a. There must be a need for computers in the organisation. This implies the computer should not be bought merely for prestige sake.

b. The manual process must have failed to deliver the required result, and increasing workforce may result to men and materials getting on each others way, making the system muscle-bound

c. There is no manual way to get the job done and so the use of computer is compulsory

d. The organisation is determine to see her computerization process to a successful end and is willing to provide the right calibre of staff and equipment.

e. There must be in place operational standards, policies and guidelines

Every stage of software development requires a std doc. In which the correct way of performing what is required ateach stage is clearly specified.
Once the standard document for a given stage is in place, there must be a related quality control function with the responsibility to ensure that the stds are maintained in the environment.
Where sw devt is being contracted out, it is important to discuss stds before the contract is signed. If possible cause the contractor to adopt your own stds. At the minimum, let your quality control group examine the std docs of the contractor to ensure that you can live with it. This is in the case of a contractor who insists on following his own stds.

Where there no standard

1. Everyone works with his own style
2. Proper documentation of SDC is hard to come by
3. Difficulty to continue with someone s else job when he is absent
4. Deadlines are difficult to meet
5. Cost over-runs becomes a common feature and project may be abandoned
6. SW integration is very hard if not impossible.
7. It is difficult to allocate resources
8. Difficult to blend modules developed by different perso

What are Policies, Standards, Guidelines and Procedures?

In order to protect information, businesses need to implement rules and controls around the protection of information and the systems that store and process this information. This is commonly achieved through the implementation of information security policies, standards, guidelines and procedures. However, what exactly are these? There some confusion in the usage of the three concept which do not recognise the differences between each and how they fit together to form an information security policy framework.

Policies

An information security policy consists of high level statements relating to the protection of information across the business and should be produced by senior management.
The policy outlines security roles and responsibilities, defines the scope of information to be protected, and provides a high level description of the controls that must be in place to protect information. In addition, it should make references to the standards and guidelines that support it.

Businesses may have a single encompassing policy, or several specific policies that target different areas, such as an email policy or acceptable use policy. From a legal and compliance perspective, an information security policy is often viewed as a commitment from senior management to protect information.
A documented policy is frequently a requirement to satisfy regulations or laws, such as those relating to privacy and finance. It should be viewed as a business mandate and must be driven from the top (i.e. senior management) downwards in order to be effective.

Standards
Standards consist of specific low level mandatory controls that help enforce and support the information security policy.
Standards help to ensure security consistency across the business and usually contain security controls relating to the implementation of specific technology, hardware or software. For example, a password standard may set out rules for password complexity and a Windows standard may set out the rules for hardening Windows clients.

Guidelines
consist of recommended, non-mandatory controls that help support standards or serve as a reference when no applicable standard is in place.
Guidelines should
be viewed as best practices that are not usually requirements, but are strongly recommended.
consist of additional recommended controls that support a standard, or help fill in the gaps where no specific standard applies.
For example1:
a standard may require passwords to be 8 characters or more and a supporting guideline may state that it is best practice to also ensure the password expires after 30 days.
Example2:
a standard may require specific technical controls for accessing the internet securely and a separate guideline may outline the best practices for using the internet and managing your online presence.

Procedures
Procedures consist of step by step instructions to assist workers in implementing the various policies, standards and guidelines.
Whilst the policies, standards and guidelines consist of the controls that should be in place, a procedure gets down to specifics, explaining how to implement these controls in a step by step fashion.
For example, a procedure could be written to explain how to install Windows securely, detailing each step that needs to be taken to harden/secure the operating system so that it satisfies the applicable policy, standards and guidelines.

In order to help cement this concept, let’ s use an example to illustrate how all of these different framework pieces fit together.
A policy may state all business information that must be adequately protected when being transferred.
A supporting data transfer standard builds upon this, requiring that all sensitive information be encrypted using a specific encryption type and that all transfers are logged.
A supporting guideline explains the best practices for recording sensitive data transfers and provides templates for the logging of these transfers.
A procedure provides step by step instructions for performing encrypted data transfers and ensures compliance with the associated policy, standards and guidelines.

The Information Security Policy Templates
Acceptable Encryption Policy

Acceptable Use Policy
Clean Desk Policy
Disaster Recovery Plan Policy
Digital Signature Acceptance Policy
Email Policy
Ethics Policy
Pandemic Response Planning Policy
Password Construction Guidelines
Password Protection Policy
Security Response Plan Policy
End User Encryption Key Protection Policy

Acceptable Encryption Policy - Outlines the requirement around which encryption algorithms (e.g. received substantial public review and have been proven to work effectively) are acceptable for use within the enterprise.
Acceptable Use Policy - Defines acceptable use of equipment and computing services, and the appropriate employee security measures to protect the organization's corporate resources and proprietary information.
Clean Desk Policy - Defines the minimum requirements for maintaining a clean desk where sensitive/critical information about employees, intellectual property, customers and vendors is secure in locked areas and out of site.
Disaster Recovery Plan Policy - Defines the requirement for a baseline disaster recovery plan to be developed and implemented by the company, which describes the process to recover IT Systems, Applications and Data from any type of disaster that causes a major outage.
Digital Signature Acceptance Policy - Defines the requirements for when a digital signature is considered an accepted means of validating the identity of a signer in electronic documents and correspondence, and thus a substitute for traditional âwetâ signatures, within the organization.
Email Policy - Defines the requirements for proper use of the company email system and make users aware of what is considered acceptable and unacceptable use of its email system.
Ethics Policy - Defines the guidelines and expectations of individuals within the company to demonstrate fair business practices and encourage a culture of openness and trust.
Pandemic Response Planning Policy - Defines the requirements for planning, preparation and performing exercises for pandemic disease outbreak over and above the normal business continuity and disaster recovery planning process.
Password Construction Guidelines - Defines the guidelines and best practices for the creation of strong passwords.
Password Protection Policy - Defines the standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.
Security Response Plan Policy - Defines the requirement for business units supported by the Infosec Team to develop and maintain a security response plan.
End User Encryption Key Protection Policy - Defines the requirements for protecting encryption keys that are under the control of end users.

Password Protection Policy

Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of Company's resources. All users, including contractors and vendors with access to company systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any company facility, has access to the Company network, or stores any non-public company information.

Password Creation

All user-level and system-level passwords must conform to the *Password Construction Guidelines*.

Users must not use the same password for Company accounts as for other non-Company access (for example, personal ISP account, option trading, benefits, and so on). Where possible, users must not use the same password for various company access needs.

User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user to access system-level privileges.
Where Simple Network Management Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of public, private, and system and must be different from the passwords used to login interactively. SNMP community strings must meet password construction guidelines.

Password Change

All system-level passwords (for example, root, enable, NT admin, application administration accounts, and so on) must be changed on at least a quarterly basis.
All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least every six months. The recommended change interval is every four months.

Password cracking or guessing may be performed on a periodic or random basis by the Infosec Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.

Password Protection

Passwords must not be shared with anyone. All passwords are to be treated as sensitive, Confidential company information. Corporate Information Security recognizes that legacy applications do not support proxy systems in place.

Passwords must not be inserted into email messages, or other forms of electronic communication.

Passwords must not be revealed over the phone to anyone.

Do not reveal a password on questionnaires or security forms.

Do not hint at the format of a password (for example, "my family name").

Do not share Company passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.

Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.

Do not use the "Remember Password" feature of applications (for example, web browsers).

Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

For Application Development

Application developers must ensure that their programs contain the following security precautions:
Applications must support authentication of individual users, not groups.
Applications must not store passwords in clear text or in any easily reversible form.
Applications must not transmit passwords in clear text over the network.
Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

Use of Passwords and Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

Policy Compliance

Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Physical Computer Centre Setup

1. Site Selection
2. Designing office and rooms
3. Designing the whole Centre
4. Detailing the facilities
   - . Raised floor: let the wind blow under the floor

- False ceiling
- Air conditioner
- Smoke and heat detectors
- Rooms to be designed
- Machine room
- Operator working area
- Storage for paper, tapes, disks and outputs
- Customer engineer working area
- Technician area
- System development areas: for system analysts and programmers
- Library: for storing books, journals and software
- Conference and meeting rooms
- Training rooms
- Director rooms
- Secretary rooms
- Operator and guest areas
- Canteen
- Toilet
- Rest rooms
- Areas for storing power units and air conditioners: such areas are needed to be designed so that there will be no harm in case of power supply shortage

CARE Of CC

We have to be careful about small things such as:

- Dust
- Pest
- Transportation to the site
- Transportation for the staffs
- Bedrooms for night shift operators
- Burglar

Computer Centre Operations

Computer Centre will need to provide IT-related services to other department in the organization, the following are points to be discussed related to its services, which are:

- Management of Services on Daily Operations
- Kinds of Services by Computer Centre
- Managing End-User Computing
- Types of Users
- Phases of End-User Computing

Management of Services on Daily Operations

- Service Planning: know our customers and their expectation
- Define service level: Determine what can be done for customers. Manager need to understand what is expected by customers and draft out Service Level Agreement for further discussion with customers
- Make agreement with customers: tell customers the truth regarding what computer Centre can deliver
- Provide services to customers:
  - Organize staffs to provide agreed services
  - Prepare people and resources for such services
  - Assist customers when system is down, i.e. to recover the system within the pre-agreed period

- Collect information about the services provided, e.g. usage period, usage information, etc.
- Measure provided services: Analysis of services provided
- Improve services to bette satisfy customer's needs

What must be done at the beginning are:

- Be sure to develop a good organization structure
- Announce service policy - Need to ensure agreement among all parties
- Be sure that users understand Service Level Agreement (SLA)
- Set up Key Performance Index (KPI), which is normally used as Measurement of Service Level Achievement, for example:
  - System is up at 95% of the time
  - Systems of a certain number (as pre-agreed) will be developed in a certain year (as previously agreed)
  - Response time will be less than 2 seconds
  - Crashed system will be replaced within 2 hours
- Develop forms for users to submit requests and for collecting performance data
- Appoint a Computer Centre Steering Committee to help oversee the operations: Normally, VP in Administration should be the Chairman for his comments and ideas on operations
- Analyze perfomance data and improve the services
- Prepare reports for senior management

Managing End-User Computing

AS the number of users increases, it is not possible to maintain good services and users may not be happy. They may want to develop some systems and the Centre cannot produce for them in time. So users want to develop systems by themselves sometimes, and users then buy their own PCs for use and to develop their own systems. Such situation may be dangerous because users may not follow the good methodology and may not follow regulations. As a result, the whole systems may be subject to security problems.

User Computing - Technique that will allow Computer Centre Manager to manage users' own development well.

- Develop policy on user purchase - create standard specifications for hardware and software to be purchased
- Develop help desk function - have a group of computer staffs to help solve problems for users
- Communicate Standards throughout organization - such standards as: data standards, standard codes, naming convention, standard data backup practices, etc.
- Create regulations to protect users work and system security

Types of Users

Category	Description
Indirect End-Users	Use information generated from the Information Systems but do not directly interact with systems
Nonprogramming End-Users	Interact with systems by entering data and getting results from production systems
Direct End-Users	Do their own programming and data analysis on the computer systems using specially designed programming tools

Information System	They are experts in system analysis, design and

Professionals	programming. This typical users should be considered a type of **Specialist**s rather than a type of end-users, and in this table, most computer staffs can be considered as this typical user type

Risks Assessment

Basically, there are 2 types of risks, which are: Natural and Man-made Disasters. By nature/design computer cban operate large number of transactions within a very short period, thus, an exposure to risks may cause a very costly losses within a short period, too.

Major Categories of Exposures	
Exposure	**Discussion**
Destruction of Assets	Broad category that involves all of the physical facilities associated with computing
Loss or Alteration of Data	The most important asset of data processing is the corporate data. Its loss could ruin the company.
Faulty Software	This category most likely cause problems involving security and integrity
Inappropriate Use of Facilities	Its difficult to detect and apprehend individuals involved in these activities

Managing Risksy

It's very risky to simply have major concerns on replacing personnel within the system just to reduce labour costs, and by mistakes, concentrate duties, which will automatically concentrate the knowledge of the system among a certain group of person, thus, encourage fraud or error. It is recommended to segregate duties into separated parts in order to prevent from being reliable to only one group of personnel by concentrating duties . The following are example in segregation of duties which will help prevent and detect fraud or error.

Duty	Discussion
Authorization of Transactions	Some instances may dictate multiple authorizations. Forinstance in paying employees, this would involve more than one person signing the paychecks..
Custody of Assets	This not only involves physical custody of asset but also the ability to have the asset moved. A foreman in a warehouse may never touch the inventory but can have subordinates relocate the inventory.
Recording Transaction	This involves the records that are used to control and verify the validity of the transaction.
Verifying Correctness	This occurs after the transaction is concluded to control the operations through acknowledgements.

An example in banking business is that a bank may separate its risks by letting 2 VPs to hold 2 sets of numbers to be used for PIN Code generation.

DATA CENTRE

A **data Centre** (or **datacentre**) is a facility used to house computer systems and associated components, such as telecommunications and storage systems. It generally includes redundant: backup power supplies, data communications connections, environmental controls (e.g., air conditioning, fire protection) and security devices.

History

Data Centres have their roots in the huge computer rooms of the early ages of the computing industry. Early computer systems were complex to operate and maintain, and required a special environment in which to operate. Many cables were necessary to connect all the components and methods to accommodate and organize these were devised, such as standard racks to mount equipment, elevated floors, and cable trays (installed overhead or under the elevated floor). Also, old computers required a great deal of power, and had to be cooled to avoid overheating. Security was important – computers were expensive, and were often used for military purposes. Basic design guidelines for controlling access to the computer room were therefore devised.

During the boom of the microcomputer industry, and especially during the 1980s, computers started to be deployed everywhere, in many cases with little or no care about operating requirements. However, as information technology (IT) operations started to grow in complexity, companies grew aware of the need to control IT resources. With the advent of client-server computing, during the 1990s, microcomputers (now called "servers") started to find their places in the old computer rooms. The availability of inexpensive networking equipment, coupled with new standards for network cabling, made it possible to use a hierarchical design that put the servers in a specific room inside the company. The use of the term "data Centre," as applied to specially designed computer rooms, started to gain popular recognition about this time.

The boom of data Centres came during the dot-com bubble. Companies needed fast Internet connectivity and nonstop operation to deploy systems and establish a presence on the Internet. Installing such equipment was not viable for many smaller companies. Many companies started building very large facilities, called Internet data Centres (IDCs), which provide businesses with a range of solutions for systems deployment and operation. New technologies and practices were designed to handle the scale and the operational requirements of such large-scale operations. These practices eventually migrated toward the private data Centres, and were adopted largely because of their practical results.

As of 2007, data Centre design, construction, and operation became well-known discipline. Standard documents from accredited professional groups, such as the Telecommunications Industry Association, specify the requirements for data Centre design. Well-known operational metrics for data Centre availability can be used to evaluate the business impact of a disruption. There is still a lot of development being done in operation practice, and also in environmentally-friendly data Centre design. Data Centres are typically very expensive to build and maintain. For instance, Amazon.com's new 116,000 sq ft data Centre in Oregon is expected to cost up to $100 million.[1]

IT operations are a crucial aspect of most organizational operations. One of the main concerns is **business continuity**; companies rely on their information systems to run their operations. If a system becomes unavailable, company operations may be impaired or stopped completely. It is necessary to provide a reliable infrastructure for IT operations, in order to minimize any chance of disruption. Information security is also a concern, and for this reason a data Centre has to offer a secure environment which minimizes the chances of a security breach. A data Centre must therefore keep high standards for assuring the integrity and functionality of its hosted computer environment.

This is accomplished through redundancy of both fiber optic cables and power, which includes emergency backup power generation.

Telcordia GR-3160, *NEBS Requirements for Telecommunications Data Centre Equipment and Spaces*, provides guidelines for data Centre spaces within telecommunications networks, and environmental requirements for the equipment intended for installation in those spaces. These criteria were developed jointly by Telcordia and industry representatives. They may be applied to data Centre spaces housing data processing or Information Technology (IT) equipment. The equipment may be used to:

- Operate and manage a carrier' s telecommunication network
- Provide data Centre based applications directly to the carrier' s customers
- Provide hosted applications for a third party to provide services to their customers
- Provide a combination of these and similar data Centre applications.

Effective data Centre operation requires a balanced investment in both the facility and the housed equipment. The first step is to establish a baseline facility environment suitable for equipment installation. Standardization and modularity can yield savings and efficiencies in the design and construction of telecommunications data Centres.

Standardization means integrated building and equipment engineering. Modularity has the benefits of scalability and easier growth, even when planning forecasts are less than optimal. For these reasons, telecommunications data Centres should be planned in repetitive building blocks of equipment, and associated power and support (conditioning) equipment when practical. The use of dedicated centralized systems requires more accurate forecasts of future needs to prevent expensive over construction, or perhaps worse —under construction that fails to meet future needs.

Data Centre classification

The *TIA-942:Data Centre Standards Overview* describes the requirements for the data centre infrastructure. The simplest is a Tier 1 data Centre, which is basically a server room, following basic guidelines for the installation of computer systems. The most stringent level is a Tier 4 data Centre, which is designed to host mission critical computer systems, with fully redundant subsystems and compartmentalized security zones controlled by biometric access controls methods. Another consideration is the placement of the data Centre in a subterranean context, for data security as well as environmental considerations such as cooling requirements.[2]

The four levels are defined, the levels describe the availability of data from the hardware at a location. The higher the tier, the greater the accessibility. The levels are:

Tier Level	Requirements
1	▪ Single non-redundant distribution path serving the IT equipment ▪ Non-redundant capacity components

	▪ Basic site infrastructure guaranteeing 99.671% availability
2	▪ Fulfils all Tier 1 requirements ▪ Redundant site infrastructure capacity components guaranteeing 99.741% availability
3	▪ Fulfils all Tier 1 & Tier 2 requirements ▪ Multiple independent distribution paths serving the IT equipment ▪ All IT equipment must be dual-powered and fully compatible with the topology of a site's architecture ▪ Concurrently maintainable site infrastructure guaranteeing 99.982% availability
4	▪ Fulfils all Tier 1, Tier 2 and Tier 3 requirements ▪ All cooling equipment is independently dual-powered, including chillers and Heating, Ventilating and Air Conditioning (HVAC) systems ▪ Fault tolerant site infrastructure with electrical power storage and distribution facilities guaranteeing 99.995% availability

Physical layout

A data Centre can occupy one room of a building, one or more floors, or an entire building. Most of the equipment is often in the form of servers mounted in 19 inch rack cabinets, which are usually placed in single rows forming corridors between them. This allows people access to the front and rear of each cabinet. Servers differ greatly in size from 1U servers to large freestanding storage silos which occupy many tiles on the floor. Some equipment such as mainframe computers and storage devices are often as big as the racks themselves, and are placed alongside them. Very large data Centres may use shipping containers packed with 1,000 or more servers each· when repairs or upgrades are needed, whole containers are replaced (rather than repairing individual servers).

The physical environment of a data Centre is rigorously controlled:

- Air conditioning is used to control the temperature and humidity in the data Centre. ASHRAE's "Thermal Guidelines for Data Processing Environments"[8] recommends a temperature range of 16–24 °C (61–75 °F) and humidity range of 40–55% with a maximum dew point of 15°C as optimal for data Centre conditions.[9] The temperature in a data Centre will naturally rise because the electrical power used heats the air. Unless the heat is removed, the ambient temperature will rise, resulting in electronic equipment malfunction. By controlling the air temperature, the server components at the board level are kept within the manufacturer's specified temperature/humidity range. Air conditioning systems help control humidity by cooling the return space air below the dew point. Too much humidity, and water may begin to condense on internal components. In case of a dry atmosphere, ancillary humidification systems may add water vapor if the humidity is too low, which can result in static electricity discharge problems which may damage components.

Subterranean data Centres may keep computer equipment cool while expending less energy than conventional designs.

- Modern data Centres try to use economizer cooling, where they use outside air to keep the data Centre cool. Washington State now has a few data Centres that cool all of the servers using outside air 11 months out of the year. They do not use chillers/air conditioners, which creates potential energy savings in the millions.[10].
- Backup power consists of one or more uninterruptible power supplies and/or diesel generators.
- To prevent single points of failure, all elements of the electrical systems, including backup systems, are typically fully duplicated, and critical servers are connected to both the "A-side" and "B-side" power feeds. This arrangement is often made to achieve N+1 Redundancy in the systems. Static switches are sometimes used to ensure instantaneous switchover from one supply to the other in the event of a power failure.
- Data Centres typically have raised flooring made up of 60 cm (2 ft) removable square tiles. The trend is towards 80–100 cm (31–39 in) void to cater for better and uniform air distribution. These provide a plenum for air to circulate below the floor, as part of the air conditioning system, as well as providing space for power cabling.

Telcordia GR-2930, *NEBS: Raised Floor Generic Requirements for Network and Data Centres*, presents generic engineering requirements for raised floors that fall within the strict NEBS guidelines.

There are many types of commercially available floors that offer a wide range of structural strength and loading capabilities, depending on component construction and the materials used. The general types of raised floors include **stringerless, stringered, and structural** platforms, all of which are discussed in detail in GR-2930 and summarized below.

Stringerless Raised Floors - One non-earthquake type of raised floor generally consists of an array of pedestals that provide the necessary height for routing cables and also serve to support each corner of the floor panels. With this type of floor, there may or may not be provisioning to mechanically fasten the floor panels to the pedestals. This stringerless type of system (having no mechanical attachments between the pedestal heads) provides maximum accessibility to the space under the floor. However, stringerless floors are significantly weaker than stringered raised floors in supporting lateral loads and are not recommended.

There are two construction types of floors for network and data Centre equipment. Following are generic descriptions of these types of floors.

Stringered Raised Floors - This type of raised floor generally consists of a vertical array of steel pedestal assemblies (each assembly is made up of a steel base plate, tubular upright, and a head) uniformly spaced on two-foot Centres and mechanically fastened to the concrete floor. The steel pedestal head has a stud that is inserted into the pedestal upright and the overall height is adjustable with a leveling nut on the welded stud of the pedestal head.

Structural Platforms - One type of structural platform consists of members constructed of steel angles or channels that are welded or bolted together to form an integrated platform for supporting equipment. This design permits equipment to be fastened directly to the platform

without the need for toggle bars or supplemental bracing. Structural platforms may or may not contain panels or stringers.

Data cabling is typically routed through overhead cable trays in modern data Centres. But some are still recommending under raised floor cabling for security reasons and to consider the addition of cooling systems above the racks in case this enhancement is necessary. Smaller/less expensive data Centres without raised flooring may use anti-static tiles for a flooring surface. Computer cabinets are often organized into a hot aisle arrangement to maximize airflow efficiency.

DC Fire Protection Strategies

- Data Centres feature fire protection systems, including passive and active design elements, as well as implementation of fire prevention programs in operations. Smoke detectors are usually installed to provide early warning of a developing fire by detecting particles generated by smoldering components prior to the development of flame. This allows investigation, interruption of power, and manual fire suppression using hand held fire extinguishers before the fire grows to a large size. A fire sprinkler system is often provided to control a full scale fire if it develops. Fire sprinklers require 18 in (46 cm) of clearance (free of cable trays, etc.) below the sprinklers. Clean agent fire suppression gaseous systems are sometimes installed to suppress a fire earlier than the fire sprinkler system. Passive fire protection elements include the installation of fire walls around the data Centre, so that fire can be restricted to a portion of the facility for a limited time in the event of the failure of the active fire protection systems, or if they are not installed. For critical facilities these firewalls are often insufficient to protect heat-sensitive electronic equipment, however, because conventional firewall construction is only rated for flame penetration time, not heat penetration. There are also deficiencies in the protection of vulnerable entry points into the server room, such as cable penetrations, coolant line penetrations and air ducts. For mission critical data Centres fireproof vaults with a Class 125 rating are necessary to meet NFPA 75[11] standards.

Physical security also plays a large role with data Centres. Physical access to the site is usually restricted to selected personnel, with controls including bollards and mantraps.[12]Video camera surveillance and permanent security guards are almost always present if the data Centre is large or contains sensitive information on any of the systems within. The use of finger print recognition man traps is starting to be commonplace.

Energy efficiency

The most commonly used metric to determine the energy efficiency of a data Centre is power usage effectiveness, or PUE. This simple ratio is the total power entering the data Centre divided by the power used by the IT equipment.

Power used by support equipment, often referred to as overhead load, mainly consists of cooling systems, power delivery, and other facility infrastructure like lighting. The average data Centre in the US has a PUE of 2.0[23], meaning that the facility uses one Watt of overhead

power for every Watt delivered to IT equipment. State-of-the-art data Centre energy efficiency is estimated to be roughly 1.2.[24] Some large data Centre operators like Microsoft and Yahoo! have published projections of PUE for facilities in development; Google publishes quarterly actual efficiency performance from data Centres in operation.[25]

The U.S. Environmental Protection Agency has an Energy Star rating for standalone or large data Centres. To qualify for the ecolabel, a data Centre must be within the top quartile of energy efficiency of all reported facilities.

Network infrastructure

Communications in data Centres today are most often based on networks running the IP protocol suite.

Data Centres contain a set of routersand switches that transport traffic between the servers and to the outside world. Redundancy of the Internet connection is often provided by using two or more upstream service providers.

Some of the servers at the data Centre are used for running the basic Internet and intranet services needed by internal users in the organization, e.g., e-mail servers, proxy servers, and DNS servers.

Network security elements are also usually deployed: firewalls, VPN gateways, intrusion detection systems, etc. Also common are monitoring systems for the network and some of the applications. Additional off site monitoring systems are also typical, in case of a failure of communications inside the data Centre.

DC Applications/Uses

The main purpose of a data Centre is running the applications that handle the core business and operational data of the organization. Such systems may be proprietary and developed internally by the organization, or bought from enterprise software vendors. Such common applications are ERP and CRM systems.

A data Centre may be concerned with just operations architecture or it may provide other services as well. Often these applications will be composed of multiple hosts, each running a single component. Common components of such applications are databases, file servers, application qservers, middleware, and various others.

Data Centres are also used for off site backups. Companies may subscribe to backup services provided by a data Centre. This is often used in conjunction with backup tapes. Backups can be taken of servers locally on to tapes., however tapes stored on site pose a security threat and are also susceptible to fire and flooding. Larger companies may also send their backups off site for added security. This can be done by backing up to a data Centre. Encrypted backups can be sent over the Internet to another data Centre where they can be stored securely.

For disaster recovery, several large hardware vendors have developed mobile solutions that can be installed and made operational in very short time. Vendors such as Cisco Systems, Sun Microsystems, IBM and HP have developed systems that could be used for this purpose.

Design and Organization Considerations

The design and organization of your company's data center has a direct impact on its day-to-day operations. The following are just some of the considerations involved:

- *Capacity*. Your data center's capacity needs to be optimized in order to ensure that it can handle its workload. In this regard, there are three common approaches to capacity planning
  - Start with the most economical size then expand it, careful not to increase capacity beyond actual need.
  - Start with the size that best will be able to handle the projected initial capacity, then expand it as need increases.
  - Start the data center with a size that will handle the highest possible load that could conceivably be initially placed on it, and expand vigorously to keep ahead of load.

- *Expandability*. The data center should be scaleable so that if you choose to increase capacity, you will be able to do so without having to redesign the entire data center.

- *Uptime*. You will need to determine what level reliability you will need. A data center that is designed for 99.99999% reliability (3 seconds of outage per year), for example, will require extremely careful planning, as well as a commitment of resources that would not be necessary if you only are aiming for 99.99% reliability (52 minutes of outage per year), and yet even a 99.99999% reliable system may not be adequate for a life safety application, where a fraction of a second of outage could cause a severe risk of harm. It is important to keep the reliability requirement in mind during the planning and design of your data center.
- *Length of outages*. Closely related to uptime, you will need to determine the maximum acceptable length of outages. For an E911 service, for example, 1 second of outage would be 1 second too many; for a business-critical service, you typically will perform a cost-benefit analysis. Length of outages is *typically* quantified as mean time to repair. **(MTTR)** is the average time that a device will take to recover from any failure. Examples of such devices range from self-resetting fuses (where the MTTR would be very short, probably seconds), up to whole systems which have to be repaired or replaced.

The MTTR would usually be part of a maintenance contract, where the user would pay more for a system whose MTTR was 24 hours, than for one of, say, 7 days. This does not mean the supplier is guaranteeing to have the system up and running again within 24 hours (or 7 days) of being notified of the failure. It does mean the average repair time will tend towards 24 hours (or 7 days). A more useful maintenance contract measure is the maximum time to recovery which can be easily measured and the supplier held accountable.

Note that some suppliers will interpret MTTR to mean 'mean time to respond', and others will take it to mean 'mean time to replace/repair/recover/resolve'. The former indicates that the supplier will acknowledge a problem and initiate mitigation within a certain timeframe. Some systems may have an MTTR of zero, which means that they have redundant components which can take over the instant the primary one fails. That said however, the failed device involved in this redundant configuration still needs to be returned to service and hence the device itself has a non-zero MTTR even if the system as a whole (through redundancy) has an MTTR of zero. But, as long as service is maintained, this is a minor issue.

- *Investment*. How is the data center financed? How much money is available? How is it best spent?

- *Location*. Will the data center be located at your corporate headquarters, or off-site? Will you rent or own the location? Will the data center be co-located, for example, in a telephone-company central office or a carrier hotel? You will need to think about considerations as diverse as the cost of communications network connections, the cost of providing benefits to any employees that may work in the data center, and the legal environment.

The need to deliberately design and organize of DC

To maximize uptime, minimize length of outages, and optimize capacity subject to resource constraints, one should deliberately design and organize the data center. The following considerations merely highlight the importance of careful planning:

- *Large investment*. When you consider the costs of network connections, power and utilities, and rented or purchased space--to name only a few things--you can see the cost of starting a data center is more than the cost of computers and network equipment alone. After you start the data center, there are still the costs of operating it: the *annual* operating costs of a data center can easily reach into the tens of millions of dollars. It is important to optimize the allocation of resources to get the maximum "bang for the buck."
- *Hard to change*. Once a data center is up and running, it is very hard to change its design without bringing the entire data center down.
- *Hard to fix*. Generally, design problems are expensive to fix after the design has already been implemented. Thus, if your customers experience a problem that is inherent to the design of your data center, the cost of repair may be prohibitive.

Location Issues

Three Options: Own, Lease, or Co-locate
Own
Lease
Co-locate

- telephone company central offices
- carrier hotels

Considerations:
Cost
Shop around to compare prices. Many co-location centers give initially inflated prices.
Taxes
Suitability
Expandability
Convenience
Transportation

- Proximity to public transportation
- Proximity to highways

Capability
Loading Dock availability
Safety
Availability of emergency services

- fire insurance category

Safety from water damage
HVAC can fail in such a way that water comes out. Look out for pipes, vents, and ducts above your equipment. Air conditioners can freeze up and then thaw, water heaters can fail, ventilation ducts can pack with snow, toilets can overflow, etc. The building may be in a flood zone - does the insurance cover the damage? How long will it take to file the claim? Document who you must contact before the disaster happens.
Natural and manmade hazards

Natural hazards

- Wildfires
- Hurricanes
- Tornados
- Earthquake
- Mudslide
- Tsunami
- etc.

Manmade hazards

- Proximity of pollution sources
- Transportation-related risks
- Risk of crime, violence, terrorism, etc.

Legal environment

Electrical

Uninteruptable Power Supplies

Absolutely necessary

Types

Central UPS: All equipment stays up for same length of time.

Rack-mounted UPS: Put batteries where they are needed most. Easy redundancy with dual power supply computers.

Brick UPS: Good for smaller installations. Easy redundancy with dual power supply computers.

Sizing

Loads that cannot tolerate any outage shall be placed on UPS power. Critical systems, such as the air conditioning cannot tolerate a brief outage, so they should be supported from generator power. Battery run time for UPS loads are dependent upon the budget and level of reliability required. With a well designed backup generation system, UPS runtime may be minimized since the gensets will be online in 8 to 20 seconds.

Power Interruption

Plan for unattended shutdown and restart whenever possible.
Consider remote alert of power interruption.
Make sure the KVM is also on UPS.
Make sure you have emergency lights and flashlights for working in the dark.
Estimating remaining run time
Restart of UPS after full drain

Redundant UPS systems

Rack-mounted - side to side redundancy.
Central UPS - need two of them with separate breaker poxes/PDUs and color coded system.

Generators

Determine your local outage characteristics for your power supplier. Do they tend to be infrequent, but long? Common, but short?
On-site vs delivery contract
On site minimizes need for large UPSes
Environmental issues and permit requirements for fuel storage

Layout and Redundancy

Look for computers with dual power supplies, or, less preferably, make sure you have redundant boxes per function. This allows for rearranging power cables and moving a box from one area to another without turning it off.
Maintain side-to-side redundancy by placing power strips on separate breakers or UPSes.

Remote Power Control

Remote power on and off
Resetting stuck machines and routers
Power on sequencing

Air Conditioning

Sizing

Air conditioners are rated by tonnage. One ton equals 12,000 BTU per hour.
Equipment heat output is rated in BTUs.
Conversion rates and guides can be found in the appendix.
Use this to size the cooling load!

Redundancy issues

Your air conditioner will fail. It is only a matter of when and whether you have one to back it up.
Emergency Fan ventilation: Can you ventilate into the building or the outside? What is the outside summer temperature?

Multiple air conditioners

Spare
Over-sized
Mov-n-cools
Alarm fail over
Thermostatic fail over
Differential temperature settings
Layout your air conditioners to minimize temperature variation across the room.

Humidity Control

Found in larger systems
Eliminates static problems
Requires addition of plumbing

Power and Air conditioning issues

Emergency shut off for power and air conditioning Very Important stuff.

Security Systems Reasoning

More difficult entry
Selective access
Entry evident
Traceable access

Design

Determine who should have access to what
How many layers of access will there be
Consider using locking cabinets but not using computer locks
Consider locks on interior doors and fire cabinets.
Physical keys vs. card pass system

Key Management

Centralized keybox for computer keys
Room keys may need to be given to CEO, landlord, and fire department for placement in Knox box.

Pass Card Systems

For card pass system, make sure entries are logged.
Avoid double-door magnet systems for passcard entry.
Proximity or RFID cards are harder to forge and easier to use

Security Systems

Use a combination of motion detectors and door sensors. This does several things:

- Door sensors are good to minimize air movement alarms.
- Reminds personnel to shut off the alarm system upon entry.
- The door chime announces entry when there is no line of sight to the door.

Security systems are cheap compared to your other expenses. Splurge on the goodies, such as alarm pads with full English displays.

Also consider having security system monitor the power, temperature, and fire with remote callout alerts.

Visitors and Contractors
Use sign-in book for contractors and record name, company, identification number, date of entry, phone number, and purpose of visit so that problems can be traced.
I question the usefulness of having all visitors in a tour sign in.
Make sure all visitors are escorted by qualified personnel.

Layout Considerations

Space for wiring
Determine use of raised floor and/or overhead cable trays.
Some rack-to-rack cable organization will be necessary.
Rack Layout
It is crucial to lay out your racks, shelving, and stand-alone systems with accuracy of a few inches when considering location over raised floor access ports.
You should have a minimum of three feet between rack front and back to allow for opening of doors.
A 6' rack spacing interval is recommended as floor tiles come in 2'x2'.
The location of the wheels and/or feet at the bottom of a rack are critical to being able to lift floor panels.

Space for other necessities
You will absolutely have to have space for at least one desk with monitor and storage units for copious documentation and spare parts.
Phones and switches
Place light, power, and fire switches in an easy to reach place
Make sure phone is in easy reach of fire suppression cut off switch, NOT the other way around.
Mechanicals
Consider putting "non-computer" assets in separate rooms. You can contain leaks easier, as well as keep service technicians away from servers, increasing security, and reducing the need for supervision.

Contractors

Finding possible contractors
Landlord may do some physical work. Remember to deal with lease issues.
Look for contractors experienced in data center construction.
Get references, check them using a reference call checklist

Getting quality quotes
Get a minimum of three quotes. Some will completely ignore what you say is important.
Write up quote specifications in detail, this allows you to send the same information to multiple vendors, and compare the quotes fairly, as well as hold vendors to what you want done in the future.
Suggested quote requirements and specifications:

- Break down costs into line items which allows for easier cost analysis and comparison between quotes.
- Three similar project references.
- Completion dates based on date of signed PO.
- Level of documentation to be delivered.
- A thorough cleaning. You don't want dust in your computers and causing false fire alarms.
- Commentary and explanation on why their solution is the best solution.

Under Floor Organization
Place your major power lines in metal conduit.
Put all under-floor fiber connections in plenum-certified conduit, such as the orange crinkle tube.

If using electrical whips underneath floors, make sure the socket boxes are physically restrained in place and marked with the location on both ends.
Run all conduits and wires square to the floor panels to allow for easier under-floor organization.
When placing electrical power whips underneath the floor, take the time to make sure they are cut very close to length, as extra loops of this cable can take up a lot of space under the floor.

Rack to Rack Connections
Consider whether you want to use network switches and hubs in each rack and connect those to a central location, or use patch panels that go from rack to rack.
Use patch panels and other techniques to minimize how often you have to go into the floor. You should not need to lift floor panels to install a new computer.

Keyboard Video Mouse Switches
Consider using your KVM connections sparingly, using only one or two per rack and moving them when necessary for maintenance.
Buy a high-quality KVM, as quality counts, and go with an on-screen menu that allows you to label the computers.
Make sure your KVM allows for keyboard switching.
Compare against serial terminal servers if you have Unix boxes.
Use true KVM cables. Cables that you zip-tie together are harder to remove later. Also, the video connection that uses screws is shorter than the PS/2 connections, to reduce cable pull out.

Cable Management
Many products for rack cable management.
Velcro zipties are reusable.
Use Ethernet cables of many color and lengths. Consider color coding by length. Use only booted cables as they won't get caught up when being moved around.
Consider putting a unique serial number on both ends of every single cable going into your data center.
Use the shortest power cables possible. Put serial numbers on the power cables and consider using black and beige colored cables to show side-to-side redundancy.

Pre-plan location of power outlets on rack systems.

Planning for Expansion

Plan for extra analog phone jacks during construction, as they are often used for modems on equipment. Consider making them 56K leased-line capable.

Outfitting

Furniture

Put EVERYTHING on wheels
- Computer Desk
- Rolling Chairs
- General storage - shelving, cabinets, or bookcases
- Key box

Labeling

Neatness begets neatness.

Use a label maker. It means your labels look neat, uniform, and are easy to read.

Label front and back of machine with name, IP address, & MAC Address. This means you are less likely to pull the wrong cable or shut down the wrong machine.

Label multiple NICS on a single machine.

Document VLANs on switches to allow installation without a network engineer.

Security

The aim of all security installations is not just for computer systems, but to provide a balance of electronic, personnel and physical security that bests meet the threat within the budget.

Computer fraud, simply defined, is the misuse of the computer to satisfy selfish ends. This crime extends to payroll applications where ghost workers receive salaries and wages, in financial institutions such as banks where illegal transfers of huge sums of money are carried everyday.

These embezzlers use the computer to steal funds materials and trade secrets. Evidence shows that the problems of these fraudulent loses occur with the computer users.

An analysis of these computer frauds show that people with computer skills are in the minority of cases. The majority of cases come from people who use it for purposes management had not intended. There is also the cases related to data entry operators who are the normal day-to-day users of the system.

These problems arise because often, people are not taught through all the security consequences of introducing a computer system, and as a result, there are gaps in the controls.

Preserving the security of data (e.g. payroll file) necessarily requires consideration of the security of the entire computing systems including, its programs, internal data and hardware and firmware facilities.

Example: It is impossible to protect just data if the programs that access and potentially modify that data have been corrupted.

Data security is typically defined in terms of three properties:

i. Confidentially – i.e. assurance that data, programs and other systems resources are protected against disclosures to unauthorized persons, programs or systems.
ii. Integrity – assurance that data programs and other system resources are protected against malicious or inadvertent modification or destruction by unauthorized persons, programs or systems.
iii. Availability – assurance that use of data, programs and other system resources will not be denied to authorized persons, programs or systems.

Security can also be defined in terms of the properties of authentication (that persons, programs or systems are accurately identified by a computing system) and non-repudiation (communications received from persons, programs or systems can be assured to have been sent by their apparent senders.

A flaw in security therefore results from the lack, breach, or failure of confidentiality, integrity or availability. This flaw can arise from a variety of causes including human, mechanical, and environmental faults as well as problems internal to the computing system.

Computer security embraces many aspects of a computing system, including hardware design, operating systems, networks, database management systems. Vulnerability is a threat that could affect a system adversely, vulnerabilities of computer systems range from the possibility of a trusted employee's selling (or being forced to reveal) secrets to a competitor, disk failures that render an entire volume of data unreadable, unauthorized operating system penetration, loss of data because of flood or fire, acquisition of data through wiretapping or sensing the emanations of electronic equipment or denying access to computing resources by flooding the system with other requests for service.

Protection control can be effectuated through software, hardware, physical and procedural means and all these combine to provide appropriate coverage against vulnerabilities. Example, creating backup copies of important data combined with the physical measure of locking the door to the computer room ensures against loss of data. Hardware features and software controls all combine to confine the accesses of each system user.

Computer security has always been considered a technical problem. The threats against computers and their weaknesses and vulnerabilities, have been the result of the computer staff. The computer security remedies have therefore naturally evolved along technical lines.

Software securities, hardware modifications, encryption, networking facilities have all dominated computer security for many years.

There three basic elements that are vital to preventing loss of or damage or alternation to electronic data and these are – Personel, physical and document security.

Personnel Security

This is the most important of all the security measures because without a sound, enforceable and viable personnel security policy all other security measures will be fatally flawed. Example, if a caretaker is not to be relied upon, then the locks are of little use. If your personnel cannot be trusted, then technical and other defences can be circumvented. No matter what security resources are deployed to protect your computing function, ultimately you will have to trust your staff and it is this trust they can betray to your great cost.
Computer security is essentially a human problem. Computers do not commit crime people do. Computer disasters and security breaches are almost invariably the result of some human act or omission.

The insiders factor

The survey over the past years has shown that the greatest threat to computers is to be found from the simple error, omission or malicious action of an employee. Most computer system users will have only limited access and privilege. These users may have terminals on their desk simply for input purposes or simple retrieval of records. These people may often be unsupervised, untrained and possibly poorly motivated and poorly paid. There is also the danger posed by support and development staff, computer operators and system programmers, all with their greater knowledge and expertise. Many supervisors and managers still do not understand computers, so that their specialist staff can act unhindered and unchecked by the normal supervisory mechanisms.

Any computer crime committed against an organization is rarely without the influence of an insider. Most of these crimes are perpetrated by an insider either by abusing the simplest of procedures or capitalizing on the carelessness of others. The evidence available shows that most losses occur as a result of those with authorized access to computer engaging in unauthorized activities. It is also observed that these staff never intended to embark on a life of crime but rather fell into it in response to some pressure, financial or personal.

The Motivation for Crime

No matter how honest and trustworthy we like to think we are, we can all come under pressure to follow courses of action we would not normally consider. Given the " big chance" on the spur of the moment, we could all be tempted into dishonesty. Also when faced with blackmail, we could be forced into actions against our will. Low morale, lack of pride and self esteem or poor promotion prospects all make it seem more justifiable to deceive an employer especially when he/she feels is not getting adequate remuneration. When employees are badly treated, hen it becomes more likely that they will take advantage of a system or security weakness.

Given the opportunity, a reasonable chance of getting away with it and sufficient reward, even the steadiest individual can succumb to temptation especially, if the crime is easy to commit.
Example: A clerk was given to opportunity not only to input receipt of material but also to authorize payments through her terminal. Even though she was an honest and reliable employee, one day she made a simple mistake by inputting some incorrect details and noticed that payments were made in due course. Her colleagues and supervisors didn' t notice the error, so she was suddenly faced with opportunity and motivation. She created fictitious suppliers, allocated orders and deliveries to them and subsequently authorized payments to a number of false bank account. She later removed all traces of the false entries. This fraud continued for some time and she later resigned leaving no for marching address.

The main aim of any personnel security policy are:

i. To restrict access to those staff who can be trusted, to those physical and logical areas within the computer system.
ii. To educate staff about the dangers to electronic data and the counter-measures they can employ to improve the safety and security of the computer and network system.

iii. To supervise staff in order to identify those who no longer remain trustworthy and thus remove them from temptation and the potential to do damages.

To achieve these, certain principles were embarked namely:

a. The Need to Know Principle - Adequate clearance must be possessed before any access to information. Also an individual status within an organization must not be allowed to override this principle.

b. Dual Control: Certain functions which are so important to the safety and security of the electronic data contained within the computer system or network must be performed by at least two competent individuals, one checking the actions of the other to ensure no mistakes are made or unauthorized acts committed.

c. Rotation of Duties: - It is also important to ensure that collusion between two staff members with vital tasks being done by them is not possible. This then makes it reasonable to rotate staff duties so that different personnel carry out the checking of each other. Any corrupt activities will be revealed if the regular staffs are replaced even temporarily. It is therefore important to identify the staff members that hold the most sensitive appointments, or have access to the most valuable information or have greatest influence over computer operations. For these people efforts must be made on screening, vetting, training, and supervision of such personnel.

Physical Security

This is most effective and cost efficient when it has been incorporated in the initial design. It is here that all the conflicting requirements of the safety policy and safety requirements are resolved. The design takes into account what the building is made of, its location, its access and safety requirements. The sensitive areas can be located away from all types of threats such as being over-looked, overhead, flooded, subject to interference, physical and chemical attack.

1 Access Control : - This is the process of ensuring that systems are only accessed by those authorized to do so and only in a manner for which they have been authorized.

Therefore, access to all parts of the system must be controlled in any computing system include I/O devices, memory storage media, files and communication paths.

To enforce this authorized access, two things are necessary:

a. A reliable structure is needed under which authorization to use resources are revoked;

b. A reliable mechanism must exist to verify the authorization each time an access is attempted.

These things can be achieved by the following ways:

i. Use of Passwords – Controls access to a computer

ii. Locks – used to " lock out" a program or prevent sensitive data (passwords) should be avoided.

2. Communication Lines: - Eavesdropping or even connecting in an unauthorized terminal is difficult to guard against when lines pass through public areas. In this country, all such lines must use the post office lines and the relative merits of " public" or " private" lines must be weighed in relation to anticipated risk. For high security, the only effective protection against Eavesdropping is encryption of all messages.

3. File Encryption: - This is necessary for his security system and the costs are those of extra storage for the encryption key and of processing time for the encryption and de-encryption processes.

Encryption is a reversible process which can be used to transform information e.g. a message or data in a file into a representation which hides the meaning from an enemy. Usually, a key known as the " cryptographic key" is employed in the transformation and this key should be essential in order to interpret the encrypted data.

Files, in general are shared by more than one user each of which must have access to the encryption key. Files are usually large in volume so as enemy has more data to help him " break the code" , but in a longer period of time. As long as the file exists, the key has not be retained. Changing the key increases the security of the file, but costly for frequent re-organisation of very large files.

Encryption of files defends against accidental revelation due to hardware or software error or theft. This is because the person to whom revelation is made is unlikely to attempt to make sense of what appears to him gibberish. Defence against loss of information by theft depends on security of the files and key. Ideally, the file and key should be kept separately. If the key is shorter, it may be kept be the user and only loaded at his satellite computer where he requires access to his file which is held at the main centre. If this kind of arrangement is not possible because of many users, then there is the combined security of the file and the key.

File encryption is of most advantageous where transmission are encrypted and the application allows this data to be put straight into the file. In this case, the key will be help at the remote station. Note that certain parts of the transmission, message control characters will need to be interpretable by the main centre.

We can not but mention data compaction. For the purpose of reducing file storage, information is sometimes represented by special codes, use of bit fields, single character codes for commonly occurring character groups etc. Though this was not primarily designed to protect the data, considerable security against accidental revelation is provided and a little security against deliberate theft.
Note: File encryption is only worthwhile for high security.

How to build physical Security into a data centre

There are plenty of complicated documents that can guide companies through the process of designing a secure data center—from the gold-standard specs used by the federal government to build sensitive facilities like embassies, to infrastructure standards published by industry groups like the Telecommunications Industry Association, to safety requirements from the likes of the National Fire Protection Association. But what should be the CSO's high-level goals for making sure that security for the new data center is built into the designs, instead of being an expensive or ineffectual afterthought?

1. Build on the right spot. Be sure the building is some distance from headquarters (20 miles is typical) and at least 100 feet from the main road. Bad neighbors: airports, chemical facilities, power plants. Bad news: earthquake fault lines and (as we've seen all too clearly this year) areas prone to hurricanes and floods. And scrap the "data center" sign.
2. Have redundant utilities. Data centers need two sources for utilities, such as electricity, water, voice and data. Trace electricity sources back to two separate substations and water back to two different main lines. Lines should be underground and should come into different areas of the building, with water separate from other utilities. Use the data center's anticipated power usage as leverage for getting the electric company to accommodate the building's special needs.
3. Pay attention to walls. Foot-thick concrete is a cheap and effective barrier against the elements and explosive devices. For extra security, use walls lined with Kevlar.

Data centre physical security

4. Avoid windows. Think warehouse, not office building. If you must have windows, limit them to the break room or administrative area, and use bomb-resistant laminated glass.

5. Use landscaping for protection. Trees, boulders and gulleys can hide the building from passing cars, obscure security devices (like fences), and also help keep vehicles from getting too close.
6. Keep a 100-foot buffer zone around the site. Where landscaping does not protect the building from vehicles, use crash-proof barriers instead. Bollard planters are less conspicuous and more attractive than other devices. Or you could do as Apple and Google have done in hiring security guards.
7. Use retractable crash barriers at vehicle entry points. Control access to the parking lot and loading dock with a staffed guard station that operates the retractable bollards. Use a raised gate and a green light as visual cues that the bollards are down and the driver can go forward. In situations when extra security is needed, have the barriers left up by default, and lowered only when someone has permission to pass through.
8. Plan for bomb detection. For data centers that are especially sensitive or likely targets, have guards use mirrors to check underneath vehicles for explosives, or provide portable bomb-sniffing devices. You can respond to a raised threat by increasing the number of vehicles you checkperhaps by checking employee vehicles as well as visitors and delivery trucks.
9. Limit entry points. Control access to the building by establishing one main entrance, plus a back one for the loading dock. This keeps costs down too.
10. Make fire doors exit only. For exits required by fire codes, install doors that don't have handles on the outside. When any of these doors is opened, a loud alarm should sound and trigger a response from the security command center.
11. Use plenty of cameras. Surveillance cameras should be installed around the perimeter of the building, at all entrances and exits, and at every access point throughout the building. A combination of motion-detection devices, low-light cameras, pan-tilt-zoom cameras and standard fixed cameras is ideal. Footage should be digitally recorded and stored offsite.
12. Protect the building's machinery. Keep the mechanical area of the building, which houses environmental systems and uninterruptible power supplies, strictly off limits. If generators are outside, use concrete walls to secure the area. For both areas, make sure all contractors and repair crews are accompanied by an employee at all times.

13. Plan for secure air handling. Make sure the heating, ventilating and air-conditioning systems can be set to recirculate air rather than drawing in air from the outside. This could help protect people and equipment if there were some kind of biological or chemical attack or heavy smoke spreading from a nearby fire. For added security, put devices in place to monitor the air for chemical, biological or radiological contaminant.
14. Ensure nothing can hide in the walls and ceilings. In secure areas of the data center, make sure internal walls run from the slab ceiling all the way to subflooring where wiring is typically housed. Also make sure drop-down ceilings don't provide hidden access points.
15. Use two-factor authentication. Biometric identification is becoming standard for access to sensitive areas of data centers, with hand geometry or fingerprint scanners usually considered less invasive than retinal scanning. In other areas, you may be able to get away with less-expensive access cards.
16. Harden the core with security layers. Anyone entering the most secure part of the data center will have been authenticated at least three times, including:
    a. At the outer door. Don't forget you'll need a way for visitors to buzz the front desk.
    b. At the inner door. Separates visitor area from general employee area.
    c. At the entrance to the "data" part of the data center. Typically, this is the layer that has the strictest "positive control," meaning no piggybacking allowed. For implementation, you have two options:
    1. A floor-to-ceiling turnstile. If someone tries to sneak in behind an authenticated user, the door gently revolves in the reverse direction. (In case of a fire, the walls of the turnstile flatten to allow quick egress.)
    2. A "mantrap." Provides alternate access for equipment and for persons with disabilities. This consists of two separate doors with an airlock in between. Only one door can be opened at a time, and authentication is needed for both doors.
    d. At the door to an individual computer processing room. This is for the room where actual servers, mainframes or other critical IT equipment is located. Provide access only on an as-needed basis, and segment these rooms as much as possible in order to control and track access.
17. Watch the exits too. Monitor entrance and exit—not only for the main facility but for more sensitive areas of the facility as well. It'll help you keep track of who was where when. It also helps with building evacuation if there's a fire.
18. Prohibit food in the computer rooms. Provide a common area where people can eat without getting food on computer equipment.
19. Install visitor rest rooms. Make sure to include bathrooms for use by visitors and delivery people who don't have access to the secure parts of the building.

Computer Performance:

This is a critical evaluation of the system i.e. how well it is meeting the organisation' s objectives. Computer system performance is actually a key criterion in determining the usefulness and cost effectiveness of any computer system.

Throughput: amount of useful work that a computer can handle in a specific period of time.

Turnaround time: this is usually the most important yardstick for measuring how well a computer system performs its intended functions. This is the elapsed or clock time it takes for a computer system to complete a job. This time is measured in different ways.

Example:

If an end user submits a job to a computer, the turnaround time is the time that elapses between the submission of the job to the computer room and the result being returned to the end user. For an interactive system, it is the time it takes the system to respond to a request.

Performance Measurement

Several specific quantitative measurements are used to evaluate the productivity and performance of computer system.

1. Productivity and Production Time

Productivity – refers to useful or productive work accomplished by the computer system. This can be achieved by measurement of throughput.

Production time – This is the elapsed time that the system is available for actual processing activities which produces useful output from the system.

2. Non-production Time – This occurs during

(a) maintenance of the system; (b) make-up time – processing operations are repeated to compensate for problems or errors. (c) Test time

3. Setup and take down times:
Setup time – time it takes to prepare a device, computer system or other system to get ready to handle a job.
Take down time – involves clearing up after a job – removing tapes or disks collecting printed forms reports or documents etc.
4. Idle time – refers to periods of time when the computer is available for use but it is not being used.
5. Make up time – elapsed time that is used to re-run computer processing jobs.
6. Mean time between Failures (MTBF) – average period of time that a device is expected to perform without a malfunction or other type of failure. This is measured only while the device is in operation not while it is turned off. This is measured in hours and is widely used as a measurement of the reliability of a particular make or model of device.

Operational Problem

The management of computer services being that of material and human resources demands alertness, responsiveness and accuracy of a high degree in order to ensure that the business objectives of the establishment are attended to at all times. This then covers the overall environment in the computer room, the professional output and manpower availability of the right quality and number to meet up the varying and continuous needs of the computer industry.

There are some problems which face the management of computer centres in our country Nigeria and these also affect the performance of the organization. Some of these problems are listed below.

1 Lack of Manpower - Even though our universities are producing hundreds of computer science graduates every year, the computer industry still complains of lack of manpower in computer profession. The problem here is quality. A good computer centre will not only need a good overall manager/director but also a set of effective line managers who should attend to the various functional areas demanding specific specialization and at the same time offering training to trainees.

Since the 1980s, the banks and the industries offer attractive salaries to computer professionals. This makes it difficult for computer centres in the government establishments to attract and retain good computer professionals. This definitely affects their services and operation

.2 Power Supply - It has been found in practice that even if we have adequate quality of manpower, there is yet another area which forms a stumbling block in the effective running of a computer centre. We are all aware of the damages done to our domestic applications by the fluctuation and outages of our National electricity supply system. Such appliances as TV sets, refrigerator units, stereo sets etc have been damaged because of high sparks of electricity emanating from our National Electric power grid. The use of stabilizers has not saved the situation since they themselves have been blown up by the raw nature of our electricity supply.

When this problem is carried to the computer equipment which is made up of highly sensitive and micro-electronic devices, it becomes more unacceptable. The voltage and current requirements of the internal circuits of the computer sometimes run in mili-amperes and mili-volts. Because of the design tolerances placed on these internal devices, fluctuations of voltages in the range of 2 to 5 volts can do a lot of damage to the equipment. If an outage of electric power occurs during processing at the point of transfer of data from one device to another, such information can be corrupted.

This problem therefore dictates that the environment of the computer must be properly secured. This has led to the use of UPS (Uninterruptible Power Supply). This will help to monitor the power supply from the mains and if the level of power supply is unhealthy which means either too low or too high, it will regulate the supply through its internal mechanics and feed a healthy electricity to the computer. Also, if the main supply has completely cut off the UPS will borrow its power from a bank of batteries and ensure by that means to keep the computer system operational. While the UPS is using the power from the batteries to keep the computer running, it will through its own internal circuit turn on a standby generator which is disposed to take over the electricity supply requirements of the computer as soon as it has reached its operating level. By this means the UPS has become a major requirement in the computer centre in Nigeria today. Its availability and maintainability have also become equally as important as the computer itself and therefore should be given very high priority in considering the security of computer systems

Reporting CC activities

A Typical CC Work/Report Format is shown below.

SN	Task	Assign To Group/Individual	Time/ Duration	Priority	Required by	Comments
1						
…						

Task – Lists Work activities to be accomplished

Assign To – Specifies the group or person(s) to under take the task.

Time/Duration – specifies the expected start and duration in hours/days, week, etc.

Priority – specifies the urgency attached to the tasks to guide the executors.

Required by – specifies who makes use of the outcome/service of the task.

Comments – provide salient remarks of a particular task.

Administration of a Computer Center

Computer and Information Systems Managers

Significant Point

- Employment of computer and information systems managers is expected to grow faster than the average for all occupations through the year 2016.
- Many managers possess advanced technical knowledge gained from working in a computer occupation.
- Job opportunities will be best for applicants with a strong understanding of business and good communication skills.

Nature of the Work

In the modern workplace, it is imperative that technology works both effectively and reliably. Computer and information systems managers CISM play a vital role in the implementation of technology within their organizations. They do everything from helping to construct a business plan to overseeing network security to directing Internet operations

They plan, coordinate, and direct research and facilitate the computer-related activities of firms. They help determine both technical and business goals in consultation with top management and make detailed plans for the accomplishment of these goals. This requires a strong understanding of both technology and business practices.

CIS managers direct the work of systems analysts, computer programmers, support specialists, and other computer-related workers.

They plan and coordinate activities such as installation and upgrading of hardware and software, programming and systems design, development of computer networks, and implementation of Internet and intranet sites.

They analyze the computer and information needs of their organizations from an operational and strategic perspective and determine immediate and long-range personnel and equipment requirements.

They assign and review the work of their subordinates and stay abreast of the latest technology to ensure the organization does not lag behind competitors.

The duties of CIS managers vary greatly.

Chief technology officers (CTOs), for example, evaluate the newest and most innovative technologies and determine how these can help their organizations.

The CTO often reports to the organization' s chief information officer, manages and plans technical standards, and tends to the daily information technology issues of the firm. Because of the rapid pace of technological change, they must constantly be on the lookout for developments that could benefit their organizations. Once a useful tool has been identified, the CTO must determine an implementation strategy and sell that strategy to management.

Management information systems (MIS) directors or information technology (IT) directors manage computing resources for their organizations. They often work under the chief information officer and plan and direct the work of subordinate information technology employees. These managers ensure the availability, continuity, and security of data and information technology services in their organizations. In this capacity, they oversee a variety of user services such as an organization' s help desk, which employees can call with questions or problems. MIS directors also may make hardware and software upgrade recommendations based on their experience with an organization' s technology.

Project managers develop requirements, budgets, and schedules for their firms' information technology projects. They coordinate such projects from development through implementation, working with internal and external clients, vendors, consultants, and computer specialists. These managers are increasingly involved in projects that upgrade the information security of an organization.

Work environment.

Computer and information systems managers spend most of their time in offices. Most work at least 40 hours a week and some may have to work evenings and weekends to meet deadlines or solve unexpected problems. Some computer and information systems managers may experience considerable pressure in meeting technical goals with short deadlines or tight budgets. As networks continue to expand and more work is done remotely, computer and information systems managers have to communicate with and oversee offsite employees using modems, laptops, e-mail, and the Internet.

Like other workers who spend most of their time using computers, computer and information systems managers are susceptible to eyestrain, back discomfort, and hand and wrist problems such as carpal tunnel syndrome.

Training, Other Qualifications, and Advancement

Computer and information systems managers are generally experienced workers who have both technical expertise and an understanding of business and management principles. A strong educational background and experience in a variety of technical fields is needed.

Education and training.

A bachelor' s degree usually is required for management positions, although employers often prefer a graduate degree, especially an MBA with technology as a core component. This degree differs from a traditional MBA in that there is a heavy emphasis on information technology in addition to the standard business curriculum. This preparation is becoming important because more computer and

information systems managers are making important technology decisions as well as business decisions for their organizations.

Some universities offer degrees in management information systems. These degrees blend technical subjects with business, accounting, and communications courses. A few computer and information systems managers attain their positions with only an associate or trade school degree, but they must have sufficient experience and must have acquired additional skills on the job. To aid their professional advancement, many managers with an associate degree eventually earn a bachelor's or master's degree while working.

Certification and other qualifications. Computer and information systems managers need a broad range of skills. Employers look for managers who have experience with the specific software or technology used on the job, as well as a background in either consulting or business management. The expansion of electronic commerce has elevated the importance of business insight and, consequently, many computer and information systems managers are called on to make important business decisions. Managers need a keen understanding of people, management processes, and customers' needs.

Advanced technical knowledge is essential for computer and information systems managers, who must understand and guide the work of their subordinates yet also explain the work in nontechnical terms to senior managers and potential customers. Therefore, many computer and information systems managers have worked as a systems analyst, for example, or as a computer support specialist, programmer, or other information technology professional.

Although **certification** is not necessarily required for most computer and information systems manager positions, there is a wide variety of certifications available that may be helpful in getting a job. These certifications are often product-specific, and are generally administered by software or hardware companies rather than independent organizations.

As computer systems become more closely connected with day-to-day operations of businesses, computer and information systems managers are also expected to be aware of business practices. They must possess strong interpersonal, communication, and leadership skills because they are required to interact not only with staff members, but also with other people inside and outside their organizations. They must possess team skills to work on group projects and other collaborative efforts. They also must have an understanding of how a business functions, how it earns revenue, and how technology relates to the core competencies of the business. As a result, many firpppprefer to give these positions to people who have spent time outside purely technical fields.

Advancement. Computer and information systems managers may advance to progressively higher leadership positions in the information technology department. A project manager might, for instance, move up to the chief technology officer position and then to chief information officer. On occasion, some may become managers in non-technical areas such as marketing, human resources, or sales because in high technology firms an understanding of technical issues is helpful in those areas.

Related Occupations

The work of computer and information systems managers is closely related to that of computer programmers, computer software engineers, computer systems analysts, computer scientists and database administrators, and computer support specialists and systems administrators. Computer and information systems managers also have some high-level responsibilities similar to those of top executives.

Computer Programmers

Nature of the Work

Computer programmers write, test, and maintain the detailed instructions, called programs, that computers follow to perform their functions. Programmers also conceive, design, and test logical structures for solving problems by computer. With the help of other computer specialists, they figure out which instructions to use to make computers do specific tasks. Many technical innovations in programming—advanced computing technologies and sophisticated new languages and programming tools, for example—have redefined the role of a programmer and elevated much of the programming work done today.

Job titles and descriptions may vary, depending on the organization, but computer programmers are individuals whose main job function is programming. Programmers usually write programs according to the specifications given by computer software engineers and systems analysts. (Sections on computer software engineers and on computer systems analysts appear elsewhere in the Handbook.) After engineers and analysts design software—describing how it will work—the programmer converts that design into a logical series of instructions that the computer can follow. The programmer codes these instructions in a conventional programming language such as COBOL; an artificial intelligence language such as Prolog; or one of the more advanced object-oriented languages, such as Java, C++, or ACTOR.

Different programming languages are used depending on the purpose of the program. Programmers generally know more than one programming language, and because many languages are similar, they often can learn new languages relatively easily. In practice, programmers often are referred to by the language they know, such as Java programmers, or by the type of function they perform or environment in which they work—for example, database programmers, mainframe programmers, or Web programmers.

Programmers also update, repair, modify, and expand existing programs. Some, especially those working on large projects that involve many programmers, use computer-assisted software engineering (CASE) tools to automate much of the coding process. These tools enable a programmer to concentrate on writing the unique parts of a program. Programmers working on smaller projects often use " programmer environments," applications that increase productivity by combining compiling, code walk through, code generation, test data generation, and debugging functions. Programmers also use libraries of basic code that can be modified or customized for a specific application. This approach yields more reliable and consistent programs and increases programmers' productivity by eliminating some routine steps.

Programs vary widely depending on the type of information they will access or generate. For example, the instructions involved in updating financial records are very different from those required to simulate flight for pilot training. Simple programs can be written in a few hours, but some programs draw data from many existing systems or use complex mathematical formulas. These programs may take more than a year to create. In most cases, several programmers work together as a team under a senior programmer' s supervision.

Programmers test a program by running it to ensure that the instructions are correct and that the program produces the desired outcome. If errors do occur, the programmer must make the appropriate change and recheck the program until it produces the correct results. This process is called testing and debugging. Programmers may continue to fix problems for as long as a program is used.

Programmers working on a mainframe, a large centralized computer, may prepare instructions for a computer operator who will run the program. (A section on computer operators appears elsewhere in the Handbook.) Programmers also may contribute to the instruction manual for a program.

Programmers in software development companies may work directly with experts from various fields to create specialized software—either programs designed for specific clients or packaged software for

general use—ranging from games and educational software to programs for desktop publishing and financial planning. Programming of packaged software constitutes one of the most rapidly growing segments of the computer services industry.

Increasingly, advanced software platforms are bridging the gap between computer programmers and computer users. New platforms, such as spreadsheet, accounting, and enterprise resource planning applications, have created demand for computer specialists who have first-hand knowledge of a user-base. These workers use such platforms to develop programs that meet the specific needs of this base. Computer programmers often are responsible for creating the software platform, and then fine-tuning the final program after it has been made.

Computer programmers often are grouped into two broad types—applications programmers and systems programmers. Applications programmers write programs to handle a specific job, such as a program to track inventory within an organization. They also may revise existing packaged software or customize generic applications purchased from vendors. Systems programmers, in contrast, write programs to maintain and control computer systems software for operating systems, networked systems, and database systems. These workers make changes in the instructions that determine how the network, workstations, and central processing unit of a system handle the various jobs they have been given, and how they communicate with peripheral equipment such as terminals, printers, and disk drives. Because of their knowledge of the entire computer system, systems programmers often help applications programmers determine the source of problems that may occur with their programs.

In some organizations, workers known as programmer-analysts are responsible for both the systems analysis and programming. (A more detailed description of the work of programmer-analysts is presented in the section on computer systems analysts elsewhere in the Handbook.)

Work environment. Programmers spend the majority of their time in front of a computer terminal, and work in clean, comfortable offices. Telecommuting is becoming more common, however, as technological advances allow more work to be done from remote locations.

Most computer programmers work about 40 hours per week. Long hours or weekend work may be required, however, to meet deadlines or fix unexpected technical problems. About four percent work part-time, compared with about 15 percent for all occupations.

Like other workers who spend long periods in front of a computer terminal typing at a keyboard, programmers are susceptible to eyestrain, back discomfort, and hand and wrist problems such as carpal tunnel syndrome.

Training, Other Qualifications, and Advancement

Employers favor applicants who already have relevant programming skills and experience. Skilled workers who keep up to date with the latest technology usually have good opportunities for advancement.

Education and training. Most programmers have a bachelor's degree, but a two-year degree or certificate may be adequate for some jobs. Some computer programmers hold a college degree in computer science, mathematics, or information systems, whereas others have taken special courses in computer programming to supplement their degree in a field such as accounting, finance, or another area of business. In 2006, more than 68 percent of computer programmers had a bachelor's degree or higher, but as the level of education and training required by employers continues to rise, this proportion is expected to increase.

Employers who use computers for scientific or engineering applications usually prefer college graduates who have a degree in computer or information science, mathematics, engineering, or the physical sciences. Employers who use computers for business applications prefer to hire people who

have had college courses in management information systems and business, and who possess strong programming skills. A graduate degree in a related field is required for some jobs.

Most systems programmers hold a four-year degree in computer science. Extensive knowledge of a variety of operating systems is essential for such workers. This includes being able to configure an operating system to work with different types of hardware and being able to adapt the operating system to best meet the needs of a particular organization. Systems programmers also must be able to work with database systems, such as DB2, Oracle, or Sybase.

In addition to educational attainment, employers highly value relevant programming skills, as well as experience. Although knowledge of traditional programming languages still is important, employers are placing an emphasis on newer, object-oriented languages and tools such as C++ and Java. Additionally, employers seek people familiar with fourth- and fifth-generation languages that involve graphic user interface and systems programming. In the absence of a degree, substantial specialized experience or expertise may be needed.

Entry-level or junior programmers may work alone on simple assignments after some initial instruction, or they may be assigned to work on a team with more experienced programmers. Either way, beginning programmers generally must work under close supervision.

Because technology changes so rapidly, programmers must continuously update their knowledge and skills by taking courses sponsored by their employer or by software vendors, or offered through local community colleges and universities.

Certification and other qualifications. When hiring programmers, employers look for people with the necessary programming skills who can think logically and pay close attention to detail. Programming calls for patience, persistence, and the ability to perform exacting analytical work, especially under pressure. Ingenuity and creativity are particularly important when programmers design solutions and test their work for potential failures. The ability to work with abstract concepts and to do technical analysis is especially important for systems programmers because they work with the software that controls the computer' s operation.

Because programmers are expected to work in teams and interact directly with users, employers want programmers who are able to communicate with non-technical personnel. Business skills are also important, especially for those wishing to advance to managerial positions.

Certification is a way to demonstrate a level of competence and may provide a jobseeker with a competitive advantage. In addition to language-specific certificates, product vendors or software firms also offer certification and may require professionals who work with their products to be certified. Voluntary certification also is available through various other organizations.

Advancement. For skilled workers who keep up to date with the latest technology, prospects for advancement are good. In large organizations, programmers may be promoted to lead programmer and be given supervisory responsibilities. Some applications programmers may move into systems programming after they gain experience and take courses in systems software. With general business experience, programmers may become programmer-analysts or systems analysts, or may be promoted to managerial positions. Programmers with specialized knowledge and experience with a language or operating system may work in research and development and may even become computer software engineers. As employers increasingly contract with outside firms to do programming jobs, more opportunities should arise for experienced programmers with expertise in a specific area to work as consultants.

Computer Software Engineers

Nature of the Work

Computer software engineers apply the principles of computer science and mathematical analysis to the design, development, testing, and evaluation of the software and systems that make computers work. The tasks performed by these workers evolve quickly, reflecting new areas of specialization or changes in technology, as well as the preferences and practices of employers. (A separate section on computer hardware engineers appears in the engineers section of the Handbook.)

Software engineers can be involved in the design and development of many types of software, including computer games, word processing and business applications, operating systems and network distribution, and compilers, which convert programs to machine language for execution on a computer.

Computer software engineers begin by analyzing users' needs, and then design, test, and develop software to meet those needs. During this process they create the detailed sets of instructions, called algorithms, that tell the computer what to do. They also may be responsible for converting these instructions into a computer language, a process called programming or coding, but this usually is the responsibility of computer programmers. (A separate section on computer programmers appears elsewhere in the Handbook.) Computer software engineers must be experts in operating systems and middleware to ensure that the underlying systems will work properly.

Computer applications software engineers analyze users' needs and design, construct, and maintain general computer applications software or specialized utility programs. These workers use different programming languages, depending on the purpose of the program. The programming languages most often used are C, C++, and Java, with Fortran and COBOL used less commonly. Some software engineers develop both packaged systems and systems software or create customized applications.

Computer systems software engineers coordinate the construction, maintenance, and expansion of an organization's computer systems. Working with the organization, they coordinate each department's computer needs—ordering, inventory, billing, and payroll recordkeeping, for example—and make suggestions about its technical direction. They also might set up the organization's intranets—networks that link computers within the organization and ease communication among various departments.

Systems software engineers also work for companies that configure, implement, and install the computer systems of other organizations. These workers may be members of the marketing or sales staff, serving as the primary technical resource for sales workers. They also may help with sales and provide customers with technical support. Since the selling of complex computer systems often requires substantial customization to meet the needs of the purchaser, software engineers help to identify and explain needed changes. In addition, systems software engineers are responsible for ensuring security across the systems they are configuring.

Computer software engineers often work as part of a team that designs new hardware, software, and systems. A core team may comprise engineering, marketing, manufacturing, and design people, who work together to release a product.

Work environment. Computer software engineers normally work in clean, comfortable offices or in laboratories in which computer equipment is located. Software engineers who work for software vendors and consulting firms frequently travel overnight to meet with customers. Telecommuting is also becoming more common, allowing workers to do their jobs from remote locations.

Most software engineers work at least 40 hours a week, but about 17 percent work more than 50 hours a week. Software engineers also may have to work evenings or weekends to meet deadlines or solve unexpected technical problems.

Like other workers who spend long hours typing at a computer, software engineers are susceptible to eyestrain, back discomfort, and hand and wrist problems such as carpal tunnel syndrome.

Training, Other Qualifications, and Advancement

Most employers prefer applicants who have at least a bachelor's degree and experience with a variety of computer systems and technologies. In order to remain competitive, computer software engineers must continually strive to acquire the latest technical skills. Advancement opportunities are good for those with relevant experience.

Education and training. Most employers prefer applicants who have at least a bachelor's degree and broad knowledge of, and experience with, a variety of computer systems and technologies. The usual college major for applications software engineers is computer science or software engineering. Systems software engineers often study computer science or computer information systems. Graduate degrees are preferred for some of the more complex jobs. In 2006, about 80 percent of workers had a bachelor's degree or higher.

Academic programs in software engineering may offer the program as a degree option or in conjunction with computer science degrees. Because of increasing emphasis on computer security, software engineers with advanced degrees in areas such as mathematics and systems design will be sought after by software developers, government agencies, and consulting firms.

Students seeking software engineering jobs enhance their employment opportunities by participating in internships or co-ops. These experiences provide students with broad knowledge and experience, making them more attractive to employers. Inexperienced college graduates may be hired by large computer and consulting firms that train new employees in intensive, company-based programs.

Certification and other qualifications. Systems software vendors offer certification and training programs, but most training authorities say that program certification alone is not sufficient for the majority of software engineering jobs.

People interested in jobs as computer software engineers must have strong problem-solving and analytical skills. They also must be able to communicate effectively with team members, other staff, and the customers they meet. Because they often deal with a number of tasks simultaneously, they must be able to concentrate and pay close attention to detail.

As technology advances, employers will need workers with the latest skills. Computer software engineers must continually strive to acquire new skills if they wish to remain in this dynamic field. To help keep up with changing technology, workers may take continuing education and professional development seminars offered by employers, software vendors, colleges and universities, private training institutions, and professional computing societies. Computer software engineers also need skills related to the industry in which they work. Engineers working for a bank, for example, should have some expertise in finance so that they understand banks' computer needs.

Advancement. As with most occupations, advancement opportunities for computer software engineers increase with experience. Entry-level computer software engineers are likely to test designs. As they become more experienced, engineers may begin helping to design and develop software. Eventually, they may advance to become a project manager, manager of information systems, or chief information officer, especially if they have business skills and training. Some computer software engineers with several years of experience or expertise find lucrative opportunities working as systems designers or independent consultants.

Computer Support Specialists and Systems Administrators

Nature of the Work

In the last decade, computers have become an integral part of everyday life at home, work, school, and nearly everywhere else. Of course, almost every computer user encounters a problem occasionally, whether it is the annoyance of a forgotten password or the disaster of a crashing hard drive. The explosive use of computers has created demand for specialists who provide advice to users, as well as for the day-to-day administration, maintenance, and support of computer systems and networks.

Computer support specialists provide technical assistance, support, and advice to customers and other users. This occupational group includes technical support specialists and help-desk technicians. These troubleshooters interpret problems and provide technical support for hardware, software, and systems. They answer telephone calls, analyze problems by using automated diagnostic programs, and resolve recurring difficulties. Support specialists work either within a company that uses computer systems or directly for a computer hardware or software vendor. Increasingly, these specialists work for help-desk or support services firms, for which they provide computer support to clients on a contract basis.

Technical support specialists respond to inquiries from their organizations' computer users and may run automatic diagnostics programs to resolve problems. They also install, modify, clean, and repair computer hardware and software. In addition, they may write training manuals and train computer users in how to use new computer hardware and software. These workers also oversee the daily performance of their company' s computer systems and evaluate how useful software programs are.

Help-desk technicians respond to telephone calls and e-mail messages from customers looking for help with computer problems. In responding to these inquiries, help-desk technicians must listen carefully to the customer, ask questions to diagnose the nature of the problem, and then patiently walk the customer through the problem-solving steps.

Help-desk technicians deal directly with customer issues and companies value them as a source of feedback on their products. They are consulted for information about what gives customers the most trouble, as well as other customer concerns. Most computer support specialists start out at the help desk.

Network and computer systems administrators design, install, and support an organization' s computer systems. They are responsible for local-area networks (LAN), wide-area networks (WAN), network segments, and Internet and intranet systems. They work in a variety of environments, including professional offices, small businesses, government organizations, and large corporations. They maintain network hardware and software, analyze problems, and monitor networks to ensure their availability to system users. These workers gather data to identify customer needs and then use the information to identify, interpret, and evaluate system and network requirements. Administrators also may plan, coordinate, and implement network security measures.

Systems administrators are responsible for maintaining network efficiency. They ensure that the design of an organization' s computer system allows all of the components, including computers, the network, and software, to work properly together. Furthermore, they monitor and adjust the performance of existing networks and continually survey the current computer site to determine future network needs. Administrators also troubleshoot problems reported by users and by automated network monitoring systems and make recommendations for future system upgrades.

In some organizations, computer security specialists may plan, coordinate, and implement the organization' s information security. These workers educate users about computer security, install security software, monitor networks for security breaches, respond to cyber attacks, and, in some cases, gather data and evidence to be used in prosecuting cyber crime. The responsibilities of computer security specialists have increased in recent years as cyber attacks have become more common. This and other growing specialty occupations reflect an increasing emphasis on client-server applications, the expansion of Internet and intranet applications, and the demand for more end-user support.

Work environment. Computer support specialists and systems administrators normally work in well-lighted, comfortable offices or computer laboratories. They usually work about 40 hours a week, but if their employer requires computer support over extended hours, they may be " on call" for rotating evening or weekend work. Overtime may be necessary when unexpected technical problems arise. Like other workers who type on a keyboard for long periods, computer support specialists and systems administrators are susceptible to eyestrain, back discomfort, and hand and wrist problems such as carpal tunnel syndrome.

Computer support specialists and systems administrators constantly interact with customers and fellow employees as they answer questions and give advice. Those who work as consultants are away from their offices much of the time, sometimes spending months working in a client' s office.

As computer networks expand, more computer support specialists and systems administrators may be able to provide technical support from remote locations. This capability would reduce or eliminate travel to the customer' s workplace. Systems administrators also can administer and configure networks and servers remotely, although this practice is not as common as it is among computer support specialists.

Training, Other Qualifications, and Advancement

A college degree is required for some computer support specialist positions, but certification and relevant experience may be sufficient for others. A bachelor' s degree is required for many network and computer systems administrator positions. For both occupations, strong analytical and communication skills are essential.

Education and training. Due to the wide range of skills required, there are many paths of entry to a job as a computer support specialist or systems administrator. Training requirements for computer support specialist positions vary, but many employers prefer to hire applicants with some formal college education. A bachelor' s degree in computer science or information systems is a prerequisite for some jobs; other jobs, however, may require only a computer-related associate degree. And for some jobs, relevant computer experience and certifications may substitute for formal education. For systems administrator jobs, many employers seek applicants with bachelor' s degrees, although not necessarily in a computer-related field.

A number of companies are becoming more flexible about requiring a college degree for support positions. In the absence of a degree, however, certification and practical experience are essential. Certification training programs, offered by a variety of vendors and product makers, may help some people to qualify for entry-level positions.

Other qualifications. People interested in becoming a computer support specialist or systems administrator must have strong problem-solving, analytical, and communication skills because troubleshooting and helping others are vital parts of the job. The constant interaction with other computer personnel, customers, and employees requires computer support specialists and systems administrators to communicate effectively on paper, via e-mail, over the phone, or in person. Strong writing skills are useful in preparing manuals for employees and customers.

Advancement. Beginning computer support specialists usually work for organizations that deal directly with customers or in-house users. Support specialists may advance into positions in which they use what they have learned from customers to improve the design and efficiency of future products. Job promotions usually depend more on performance than on formal education. Eventually, some computer support specialists become software engineers, designing products rather than assisting users. Computer support specialists in hardware and software companies often enjoy great upward mobility; advancement sometimes comes within months of becoming employed.

Entry-level network and computer systems administrators are involved in routine maintenance and monitoring of computer systems, typically working behind the scenes in an organization. After gaining

experience and expertise, they often are able to advance to more senior-level positions. For example, senior network and computer systems administrators may make presentations to executives and managers on the security of the company computer network. They also may translate the needs of an organization into a set of technical requirements based on the available technology. As with support specialists, administrators may become software engineers involved in system and network design.

As technology continues to improve, computer support specialists and systems administrators must strive to acquire new skills. Many continuing education programs are provided by employers, hardware and software vendors, colleges and universities, and private training institutions. Professional development seminars offered by computing services firms also can enhance skills and advancement opportunities.

Computer Systems Analysts

Nature of the Work

All organizations rely on computer and information technology to conduct business and operate efficiently. Computer systems analysts help organizations to use technology effectively and to incorporate rapidly changing technologies into their existing systems. The work of computer systems analysts evolves rapidly, reflecting new areas of specialization and changes in technology.

Computer systems analysts solve computer problems and use computer technology to meet the needs of an organization. They may design and develop new computer systems by choosing and configuring hardware and software. They may also devise ways to apply existing systems' resources to additional tasks. Most systems analysts work with specific types of computer systems—for example, business, accounting, or financial systems or scientific and engineering systems—that vary with the kind of organization. Analysts who specialize in helping an organization select the proper system software and infrastructure are often called system architects. Analysts who specialize in developing and fine-tuning systems often are known as systems designers.

To begin an assignment, systems analysts consult managers and users to define the goals of the system. Analysts then design a system to meet those goals. They specify the inputs that the system will access, decide how the inputs will be processed, and format the output to meet users' needs. Analysts use techniques such as structured analysis, data modeling, information engineering, mathematical model building, sampling, and cost accounting to make sure their plans are efficient and complete. They also may prepare cost-benefit and return-on-investment analyses to help management decide whether implementing the proposed technology would be financially feasible.

When a system is approved, systems analysts determine what computer hardware and software will be needed to set it up. They coordinate tests and observe the initial use of the system to ensure that it performs as planned. They prepare specifications, flow charts, and process diagrams for computer programmers to follow; then they work with programmers to " debug," or eliminate errors, from the system. Systems analysts who do more in-depth testing may be called software quality assurance analysts. In addition to running tests, these workers diagnose problems, recommend solutions, and determine whether program requirements have been met.

In some organizations, programmer-analysts design and update the software that runs a computer. They also create custom applications tailored to their organization' s tasks. Because they are responsible for both programming and systems analysis, these workers must be proficient in both areas. As this dual proficiency becomes more common, analysts are increasingly working with databases, object-oriented programming languages, client– server applications, and multimedia and Internet technology.

One challenge created by expanding computer use is the need for different computer systems to communicate with each other. Systems analysts work to make the computer systems within an

organization, or across organizations, compatible so that information can be shared. Many systems analysts are involved with these " networking" tasks, connecting all the computers internally, in an individual office, department, or establishment, or externally, as when setting up e-commerce networks to facilitate business among companies.

Work environment. Computer systems analysts work in offices or laboratories in comfortable surroundings. They usually work about 40 hours a week—about the same as many other professional or office workers. Evening or weekend work may be necessary, however, to meet deadlines or solve specific problems. Many analysts telecommute, using computers to work from remote locations.

Like other workers who spend long periods typing on a computer, computer systems analysts are susceptible to eyestrain, back discomfort, and hand and wrist problems such as carpal tunnel syndrome or cumulative trauma disorder.

Training, Other Qualifications, and Advancement

Training requirements for computer systems analysts vary depending on the job, but many employers prefer applicants who have a bachelor' s degree. Relevant work experience also is very important. Advancement opportunities are good for those with the necessary skills and experience.

Education and training. When hiring computer systems analysts, employers usually prefer applicants who have at least a bachelor' s degree. For more technically complex jobs, people with graduate degrees are preferred.

The level and type of education that employers require reflects changes in technology. Employers often scramble to find workers capable of implementing the newest technologies. Workers with formal education or experience in information security, for example, are currently in demand because of the growing use of computer networks, which must be protected from threats.

For jobs in a technical or scientific environment, employers often seek applicants who have at least a bachelor' s degree in a technical field, such as computer science, information science, applied mathematics, engineering, or the physical sciences. For jobs in a business environment, employers often seek applicants with at least a bachelor' s degree in a business-related field such as management information systems (MIS). Increasingly, employers are seeking individuals who have a master' s degree in business administration (MBA) with a concentration in information systems.

Despite the preference for technical degrees, however, people who have degrees in other majors may find employment as systems analysts if they also have technical skills. Courses in computer science or related subjects combined with practical experience can qualify people for some jobs in the occupation.

Employers generally look for people with expertise relevant to the job. For example, systems analysts who wish to work for a bank should have some expertise in finance, and systems analysts who wish to work for a hospital should have some knowledge of health management.

Technological advances come so rapidly in the computer field that continuous study is necessary to remain competitive. Employers, hardware and software vendors, colleges and universities, and private training institutions offer continuing education to help workers attain the latest skills. Additional training may come from professional development seminars offered by professional computing societies.

Other qualifications. Employers usually look for people who have broad knowledge and experience related to computer systems and technologies, strong problem-solving and analytical skills, and the ability to think logically. In addition, because they often deal with a number of tasks simultaneously, the ability to concentrate and pay close attention to detail is important. Although these workers sometimes work independently, they frequently work in teams on large projects. Therefore, they must

have good interpersonal skills and be able to communicate effectively with computer personnel, users, and other staff who may have no technical background.

Advancement. With experience, systems analysts may be promoted to senior or lead systems analyst. Those who possess leadership ability and good business skills also can become computer and information systems managers or can advance into other management positions such as manager of information systems or chief information officer. Those with work experience and considerable expertise in a particular subject or application may find lucrative opportunities as independent consultants, or may choose to start their own computer consulting firms.