CHAPTER – 6

MANAGING IT SYSTEM

INTRODUCTION:

The management of IT system mean providing an environment of stability without stagnation (blockage) and change, without chaos for information, information technology and knowledge workers. Managing an IT system is a very delicate balancing act. We have to sustain current IT system components, while adjusting them to the forces of change and simultaneously protecting IT system from harm, both internal and external.

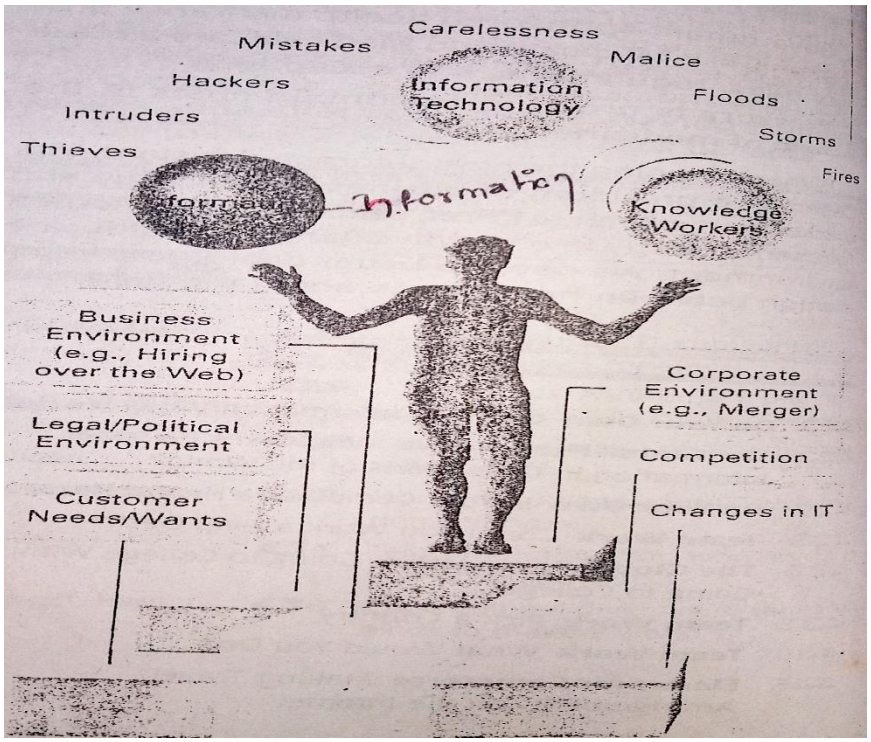
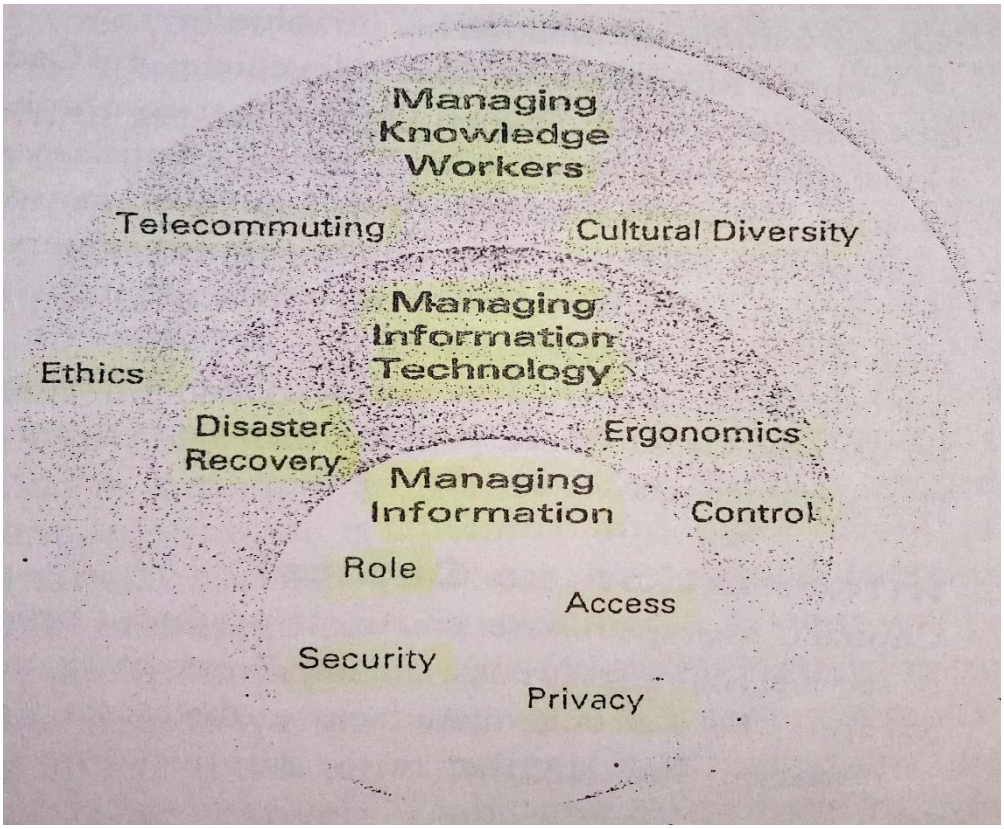


Fig: Managing IT Systems Is a Balancing Act

A stable IT system provides consistency and predictability, which are vital for the effective functioning of an organization. In a business environment continuous improvement is a vehicle that advances the ability to deliver valuable services to customer. In the current dynamic environment of IT. It's a challenge to maintain a balance.

IT systems are composed of knowledge workers who use information technology to generate access information. Therefore, managing IT systems involves:



1. Managing Information:

The four key aspects of managing the information are:

i. Role:

Nothing else is as universal or as versatile as information. The unique resource "Information" has two functions in an organization:

a. Information as Raw Material:

Raw materials are the components from which a product is made. These days information is just like a raw material for any organization because IT systems capture, process and deliver information. An organization cannot operate and sustain without information.

b. Information as Capital:

Capital is the type of asset we use to produce a product or service like building, machinery, truck, etc. Information can also be thought of as capital as it is used by companies to produce a product to enhance the customer value. Information capital is one of the most important and universal type of capital in an organization.

ii. Access to Information:

Right Information:

Managing information means providing an organization with the most effective means to access the right information, at the right time, in the right form. Information is useless if

it is not relevant to the organization or customer. Information must be accurate. Inaccurate information is useless for its users.

Right Time:

Information is worthless, if it is not available when we need it. Knowledge workers should be able to access complete information at every point of contact. They should have access to internal as well as external information as they need.

Right Form:

Information should be available in a form that is understandable consistent, logical and easy to manipulate. It should be produced in the form like text, tables, graphs, audio, video, etc. which is most appropriate for its users. Presenting information in a familiar format help to increase its usefulness.

iii. Security:

Information is of vital important for any organization so, we must provide proper security mechanism to protect the valuable information from different kinds of problems like hard disk crash, computer failure, unauthorized access by hackers, viruses and the access through the internet. To provide security we can use various mechanism like:

Backup:

The easiest and most basic way to prevent loos of information is to maintain continuous backups, so that we can recover the original information in case of any type of system failure or natural disaster. Traditionally backup was maintain in physical storage devices like floppy disk, magnetic tape, CD, DVD, etc. but these days, we prefer to remote backup using the internet and special service known as cloud computing.

Cryptography:

Encryption and decryption is one of the important mechanism to protect the confidential data while transmitting over the insecure communication channel like the internet or even while storing in a computer.

Anti-Virus:

A computer virus is a program developed by someone with malicious intent to harm an IT system. To protect the system and information from such virus, we must use anti-virus software.

Firewall:

While connecting a personal computer or private network to the public network like the internet the unauthorized persons (hackers) can gain access to the system. To protect a system from external users we can use firewall. A firewall is a barrier that is placed in between internal network and the public internet so that we can prevent outsiders from accessing the internal system.

iv. Privacy:

The issue of privacy while using an IT system especially the internet is an important fact to concern. Personal information about consumer's employees and even organization must not be distributed publically without permission. There are two conflicting goals as:

a. The right of employees to privacy
b. The needs of companies to have such information.

A company must maintain balance in between these two goals.

2. Managing Information Technology:

Managing IT means management of hardware, software and networking components of IT. It mainly includes:

a. Having control over IT components.
b. Arranging IT component to preserve the health of knowledge workers.
c. Taking steps to guarantee that a sudden disaster does not affect the information flow and shut down the IT system

i. Control:

Advances and breakthrough are occurring daily in IT industry. Better, faster, easier to use hardware and software with new approaches to generate and deliver information appear constantly. Having control means:

Interoperability:

It means the extent to which IT equipment and software component are compatible. Interoperability is the goal of IT system where all the existing component and newly adopted IT component should be compatible with each other.

Cost Control:

Another challenge while managing IT system is the cost of IT component because the investment on IT is challenging task. The IT systems are changing constantly due to this the huge investment on IT system as a long term investment may be risky.

ii. Ergonomics:

Ergonomics is the study of how to design and arrange our workplace so that we can achieve maximum productivity and reduce discomfort and adverse health effects. Ergonomics actually involves much more than having a good chair. It deals with all types of work areas and machinery.

Improperly arranged computer components can cause physical injuries. Repetitive Strain Injury (RSI), also referred to as Cumulative Trauma Disorder (CTD), is characterized by headache, neckache, eyestrain, wrist pain, fatigue and stress caused by repetitive actions. RSI known as "the industrial disease of the information age" is the leading cause of injury, productivity loss and financial strain on small business costing hundreds of thousands of

dollars a year in work related injuries. Some victims even become disabled, temporarily or permanently.

The U.S. Bureau of Labor Statistics says that, nationwide, the number of RSI-related illnesses and injuries was 22600 in 1982 and 332000 in 1994. An estimated 4.4 million people in the United States suffer from various computer related disorders. When an employee is out with an injury the company may have to pay overtime for workers to assume the job of the absentee and perhaps, train someone else.

So, how can we as a knowledge worker or a manager of IT systems avoid becoming part of the RSI statistics? Basically, our computer system should be an extension of our body as we perform any task. The posture of the person, the keyboard and mouse should be positioned to keep the arms parallel to the floor.

iii. Disaster Recovery:

Any kind of disaster like fire, flood, earthquake or terrorist may destroy entire IT system for any organization. To handle this case we have to develop a disaster recovery plan. It is a plan of how we will carry own business if a major disaster occur or destroy IT system. A well-managed DRP (Disaster Recovery Plan) focuses on business recovery and on computer operations as a necessary part of getting business going again.

A good disaster recovery plan will take the following into consideration:

Customer:

Customers should be aware about the situation and the organization must assure them that they will provide operation to customer vary soon. In case of large customer base an organization may use radio, TV or newspaper advertisement to notify them about the current situation, alternative arrangement and when an organization expect to back in operations.

Facilities:

One of the best option is hot site, which is a separate fully equipped facility on which a business can move immediately after the disaster and resume business. Another alternative is cold site, which does not have computer equipment installed but has backup systems, security systems and other facilities to protect the IT facilities.

Knowledge Workers:

Knowledge workers must know when and where to return to work after a disaster strikes. They will be under increased stress, especially if the disaster affect their personal life as well. The mental stress on knowledge workers should be managed properly.

Business Information:

The most effective action is to take backup of information as a part of normal business process that means knowledge workers are responsible for protecting organization information and it should not be assumed the responsibility of IT specialist only. Backup operations must be considered as business process not as an IT process.

Computer Equipment:

A big problem for firms with complex networks is that disaster recovery companies providing hot site services may have difficulties in providing client server facilities because most of the networks are unique and multi-venders array of systems and software.

Communication Infrastructure:

Loss of communication is one of the biggest problem during a disaster and due to this an organization may loss huge revenue so, restore of communication must be in higher priority.

3. Managing Knowledge Workers:

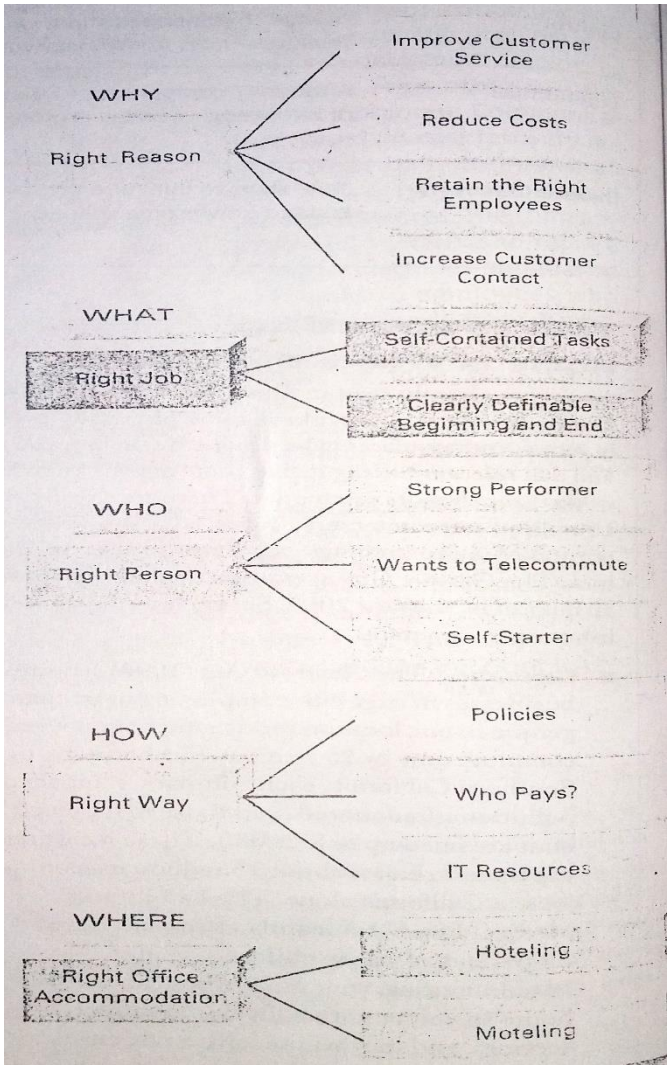
Most of the information are stored in databases and data warehouses. However, a considerable amount of valuable information is stored in the brain of employees. A good manager knows that human brain power resides at all levels employee, not just as management level. The management of knowledge workers is challenging task for manager. Management of knowledge worker can be discussed in three aspects:

i. Telecommuting:

Telecommuting means knowledge workers do not have to be physically present in corporate offices to do their task. They can work from anywhere like from home, on the road, park and even during the travelling. This freedom of working location that means telecommuting makers some knowledge workers more productive. This concept is in growing rate and several incentives contributing this trend are:

- Productivity
- Knowledge workers located in other state
- Knowledge workers located in other country
- Legislative

Telecommuting programs are offering various advantages but managing telecommuting requires skill and careful thought. We must clear on why? What? Who? How? And where? Before we begin telecommuting.



ii. Cultural Diversity:

Continuous improvement in telecommunication and transportation and the need to expand markets are forcing companies to become transnational. So, a company have to manage knowledge worker from different country, different region having different culture.

Culture is the collective personality of a nation or society including language traditions, currency, religion, history, music and acceptable behavior among other things. The most significant powerful factor of expanding transnational firm's IT system is not the hardware and software but the effect of cross-cultural diversity, that means the difference in behavior and attitude among people from different part of world. IT specialist and knowledge worker are often the employees to be send abroad when a company expand. In that case it may be difficult for the knowledge workers to work in an environment that is culturally entirely different.

A term cultural shock is used for disorientation and confusion that a knowledge worker experience in a new work place.

iii. Ethics:

Ethics is the set of principle or standard that help to guide behavior, actions and choices. It is the effort we make ta act reasonably. Ethics are the moral dimension determining behavior of individual users. In this society or age of IT, it is difficult to determine and manage the ethical behavior of knowledge workers. Three stages of ethical development are:

a. **Preadolescent Stage:** In this stage we keep the rules due to the fear of punishment and in the hope of rewards.
b. **Adolescent Stage:** In this stage we do the right things because of pressure and what people will think about us.
c. **Adult Stage:** In this stage, we do the right things because it is the right thing and we recognize that if the majority of people in a society do not support reasonable action, our society will suffer.

As a manager of IT system we must enforce an ethical working atmosphere by setting an example and formulating policies to guide knowledge workers in ethical behavior.