UNIT II

PEOPLE MANAGEMENT-HUMAN RESOURCE SECURITY

People management and security risk management

Good people management could be described as getting the best results from an employee in a healthy and safe way. People are our most valuable resource and if we believe happy, secure and motivated employees are more likely to be engaged, committed and productive, it makes good business sense to support employees well and to provide them with a healthy and safe working environment.

People management is a broad and complex subject that carries legal and ethical responsibilities for an organisation to ensure the physical and psychological health of an employee before, during and after the period of employment. Organisations have many legal and ethical ‘duty of care’ obligations and are expected to go above and beyond the legal minimum when working in high-risk environments.

Those in leadership positions – trustees, directors and managers – must invest time and resources in people management practices, and ensure technical specialists within human resources and security provide the necessary advice at the right time and in the right way.

People and security risk management – why should you care?

People management has a direct impact on security risk management, for example:

1. Recruitment – employing the wrong people can create security risks. A lack of skills and competencies can lead to poor performance and decisionmaking; poor behaviours can lead to personal and programme risks; and failure to consider the implications of the ethnic mix in some regions can create issues between staff and negative perceptions in the local community.
2. Induction – preparing people appropriately has a direct impact on how well and quickly staff settle into their new role, team life and the environment, thereby reducing the risk of security incidents.
3. Office closure and contract termination – a clear and transparent process on office closure and when contracts come to an end should be implemented some time before the notice period begins. Failure to do so can have serious security implications.
4. Stress management – risky and high-pressured situations are more likely to lead to a highly stressed workforce, which can impact behaviours, relationships and the ability to make good security- related decisions.

5. Employment policy and practice – employees are more likely to feel valued and protected when employment policies (e.g. reward, performance and conduct) are clear and consistently applied. Disgruntled and dissatisfied staff are a source of security threats to the organisation, staff and programmes.

Human Resource Management (HRM) is an operation in companies designed to maximize employee performance in order to meet the employer's strategic goals and objectives. More precisely, HRM focuses on management of people within companies, emphasizing on policies and systems.

In short, HRM is the process of recruiting, selecting employees, providing proper orientation and induction, imparting proper training and developing skills.

Features of HRM

Human Resource Management as a discipline includes the following features −

- It is pervasive in nature, as it is present in all industries.
- It focuses on outcomes and not on rules.
- It helps employees develop and groom their potential completely.
- It motivates employees to give their best to the company.
- It is all about people at work, as individuals as well as in groups.
- It tries to put people on assigned tasks in order to have good production or results.
- It helps a company achieve its goals in the future by facilitating work for competent and well-motivated employees.
- It approaches to build and maintain cordial relationship among people working at various levels in the company.

Integrating HR Strategy with Business Strategy

Today, human resource departments have a more precise, strategic role in companies, and an HR strategy affects the bottom line. Let us look into HR as part of a complete business strategy.

HR Strategy as Business Strategy

In real world, no margin in the sand is drawn between human resources strategy and business strategy. A successful business owner understands the strong connection between the two. Progressing human capital is essential to the longevity and success of a business.

Human resources strategy today includes executive leadership teams conferring with human resources experts to improvise complementary goals for human resources and the complete business.

HR Strategy and Business Productivity

The recruitment and selection process in human resources department is paramount to creating a productive workforce. Maintaining a workforce where employees enjoy high levels of job satisfaction and job security converts into a workforce that assists in achieving business goals.

Trends Affecting HR and Business Strategy

Presently, we can say that HR technologies have become an integrated engine in advancing the broader needs of businesses, supporting far more than the basic transactions, and advancing HR and business agenda for future.

Human resources information system (HRIS) is integral to the progress of performance management, recruitment, selection. It also plays a vital role in the rejection of candidates, their promotions and postings, etc.

Interaction among Executive Leadership

The best way to cultivate a relationship between HR and C-level executives is by demonstrating the return on investment (ROI) in human resources activities and practices. This may include explaining the link between reduction in employee turnover and improvement in job satisfaction that improves the bottom line.

Career Development

Career Development is the process by which employees improve through a series of stages, each associated with a different set of development tasks, activities and relationship.

It can also be defined as an ongoing formalized effort by an organization that aims at developing and enriching the organization's human resources in the light of both the employee and the organization's need.

The Need for Career Development

From a company's perspective, the failure to encourage employees to please their careers can result in ashortage of employees to fill open positions, lower employee commitment, and inappropriate use of money allocated for training and development program.

When a company helps employees in developing a career plan, the employees are less inclined to quit that company. Developing a career can boost the morale of the employee, enhance productivity andhelp the company become more efficient.

Career Development-Objectives

Career development has three major objectives −

- To meet the immediate and future human resource requirements of the company on a timely basis.
- To better update the company and the individual about potential career path within the company.
- To utilize existing human resource programs to the fullest by integrating activities and practices that select, assign, develop, and manage individual careers in alignment with the company's plan.

Probably, the most important objective of any career development program is to facilitate the tools andtechniques that will enable employees to gauge their potential for success in a career path.

Career development is also essential because career development can minimize unemployment and provide opportunity on the basis of performance & qualification. It tries to improve the overall personality of an individual solely as well as when in group.

HRM & Career Development Responsibilities

Career Development has its duties distributed at various levels and each level is answerable for their share of responsibilities. We have responsibilities assigned to the organization, employees as well as mangers.

Career development plays a crucial role in grooming an individual, group as well as the organization as a whole.

Organization’s Responsibilities

Organization’s responsibilities include instigation and ensuring in the first place that career development does take place. Specifically, organization’s responsibilities are to enhance career opportunities and improve interaction between employees.

The organization should promote the conditions and create a surrounding that will facilitate the development of individual career plans by the employees. Basically, the organization provides information regarding the mission and policies and helps employee prepare their career development plan and career path.

Employee’s Responsibilities

The only person who really knows what she or he needs is the individual and these desires differ from person to person. The duty of an employee varies with his/her designation.

While the individual is ultimately answerable for preparing his or her individual career plan, experiencehas shown that people make considerable progress only when they receive some motivation anddirection.

Manager’s Responsibilities

The manager should act as a catalyst and sounding board. The manager should show an employee how to go about a process and then help the employee understand what is required of him in the position.

The immediate manager facilitates guidance and encouragement. The manager typically verifies the employee’s readiness for **job mobility**. Moreover, managers are often the primary source of information about position openings, training courses, and other development options.

These are the major career development responsibilities an HRM needs to take care of in an organization.

Career Development Process

Career planning entails an individual and organizational requirements and options that can be matchedin a variety of ways. Thus, career planning is the process through which employees −

- Become aware of their interests, values, strengths and weakness.

- Collect information about job options within the company.
- Identify and choose career goals.
- Establish action plans to achieve those specific career goals and objectives.

Career development process may sound like just the qualifications that an individual gets throughout his/her educational field, but here we have unfolded a new side of it, as we see how an individual's career gets affected by the place where he/she works.

Career Planning System

Career planning system can be defined as a step by step process of improving as an individual; we canalso call it as a process of self-development.

This system consists of the following

four different stages −Evaluation

Process

The evaluation phase includes activities like self-assessment and assessment by the company. The
objective of having evaluation is to understand the employee's strengths and weaknesses.

Self-Assessment

Self-assessment assists employees in determining their career interest, values, aptitudes and behavioral tendencies. In order to do self-assessment, employees often take psychological tests and conduct self- directed searches.

Large amount of self-assessment materials is available over the internet and other commercial outlets. Tests also assist employees identify the relative value they place on work and leisure activities.

Career counselors are often used to help employees in the self-assessment process and translate the results of psychological tests into measurable goals and activities.

Assessment by the Organization

Organizations have several potential sources of information that also help for assessing employees. One of the most frequently used sources has been the performance appraisal process.

Direction Phase

The direction phase includes determining the career desired by the employee. What exactly interests theemployee? How can we match the employee's interest with the desirable job in the organization?

Thus, the steps that should be taken in order to realize their career objectives are −

- Evaluation Process
- Direction Phase
- Goal setting

- Action Planning

The description given above says it all about career planning system. As we can see, not a single stagecan be avoided, as all are interlinked and are crucial to career development.

Cyber Security Awareness

- Cyber Security Awareness" is the knowledge that VA (vetarans affairs) employees, contractors, and volunteers use to protect VA computer systems and data.
- It refers to the personal responsibility each of us assumes for ensuring:- the confidentiality, integrity, and appropriate availability of veterans' private data, timely and uninterrupted flow of information throughout the VA enterprise, and- VA information systems are protected from the potential of fraud, waste and abuse.
- Passwords
- Passwords are important tools protecting VA
- information systems. They ensure you have access to the information you need.
- Keep your password secret to protect yourself and your work. If you have several passwords, it is permissible to record and store them in a safe place, to which only you have access.
- Passwords can be easily stolen or duplicated if constructed poorly. Most password thefts occur as a result of poorly constructed passwords or social engineering.

Password Requirements:

Password must:

- Be constructed of at least eight characters (i.e.,Gabc123&).
- Use at least three of the following four kinds of characters:
    - { Upper case letters (ABC...)
    - { Lower-case letters (...xyz)
    - { Numbers (0123456789)
    - { Special characters," such as #, &, *, or @.
    - Be changed at least every 90 days.
    - Poor Password Construction ,Passwords that are not "strong," as explainedpreviously.
- Use of common words easily obtained from a dictionary.
- Passwords referring to your personal life (for example, names of family members or pets).
- Easily identifiable passwords are an open invitation to hackers.

Risk Awareness

- Username and password combinations, the primary method used by VA, provide a guarantee that you are who you say you are. Your username and password also limit you to only actions within your level of authorization.
- Once the details of your username and password have been shared with others, you have lost control over how they may be used or abused.
- It is worth noting that in most cases, usernames are very easy to get and tend to follow a pattern which relates directly to your own name. This is a necessary risk.
- Therefore, constructing strong passwords and maintaining their confidentiality is of great importance.

Secure information system development • Integrating security at the initial phase • Integrity security at the Development Phase • Integrity security at the Implementation Phase • Integrity security at the Maintenance Phase • Integrity security at the Disposal Phase

Types of Cyber Attacks

A cyber-attack is an exploitation of computer systems and networks. It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft.

We are living in a digital era. Now a day, most of the people use computer and internet. Due to the dependency on digital things, the illegal computer activity is growing and changing like any type of crime.

Cyber-attacks can be classified into the following categories:

Web-based attacks

System-based attacks

Classification of Cyber attacks

Web-based attacks

These are the attacks which occur on a website or web applications. Some of the important web-based attacks are as follows-

1. Injection attacks

It is the attack in which some data will be injected into a web application to manipulate the applicationand fetch the required information.

Example- SQL Injection, code Injection, log Injection, XML Injection etc.

2. DNS Spoofing

DNS Spoofing is a type of computer security hacking. Whereby a data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attacker?s computer or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.

3. Session Hijacking

It is a security attack on a user session over a protected network. Web applications create cookies to storethe state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.

4. Phishing

Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.

5. Brute force

It is a type of attack which uses a trial and error method. This attack generates a large number of guessesand validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security, analysts to test an organization'snetwork security.

6. Denial of Service

It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash. It usesthe single system and single internet connection to attack a server. It can be classified into the following-

Volume-based attacks- Its goal is to saturate the bandwidth of the attacked site, and is measured in bit per second.

Protocol attacks- It consumes actual server resources, and is measured in a packet.

Application layer attacks- Its goal is to crash the web server and is measured in request per second.

7. Dictionary attacks

This type of attack stored the list of a commonly used password and validated them to get original password.

8. URL Interpretation

It is a type of attack where we can change the certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.

9. File Inclusion attacks

It is a type of attack that allows an attacker to access unauthorized or essential files which is available onthe web server or to execute malicious files on the web server by making use of the include functionality.

10. Man in the middle attacks

It is a type of attack that allows an attacker to intercepts the connection between client and server and acts as a bridge between them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.

System-based attacks

These are the attacks which are intended to compromise a computer or a computer network. Some of theimportant system-based attacks are as follows-

1. Virus

It is a type of malicious software program that spread throughout the computer files without theknowledge of a user. It is a self-replicating malicious computer program that replicates by inserting copies of itself into other computer programs when executed. It can also execute instructions that cause harm to the system.

2. Worm

It is a type of malware whose primary function is to replicate itself to spread to uninfected computers. It works same as the computer virus. Worms often originate from email attachments that appear to be fromtrusted senders.

3. Trojan horse

It is a malicious program that occurs unexpected changes to computer setting and unusual activity, even when the computer should be idle. It misleads the user of its true intent. It appears to be a normal application but when opened/executed some malicious code will run in the background.

4. Backdoors

It is a method that bypasses the normal authentication process. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.

5. Bots

A bot (short for "robot") is an automated process that interacts with other network services. Some bots program run automatically, while others only execute commands when they receive specific input. Common examples of bots program are the crawler, chatroom bots, and malicious bots.