An Explication on Data & Information Security in Human Resource Management System

[*]Reena Singh, Dr. Trilochan Sharma

[*]*Research Scholar, Ch. Charan Singh University, Meerut*

**reena.mgmnt@gmail.com*

Received: *30.05.2020* ***Accepted:*** *26.07.2020*

ABSTRACT

This article totally emphasis on the security issues and challenges of data and information, which is related to human resource management system in an organization. Today's era is totally depends on information and the proper communication of information. The main focus of this research is concern about data security, security measures, security challenges, security issues which are faced during the implementation and use of human resource management system. This article also presents the security aspects that should be take care at the time of implementation of human resource management system in an organization. These security issues & challenges occur at each stage of the system whether they are related to human resource department or any other department. Thus, a complete work of Information Security professionals has now emerged that advises higher management persons and Human Resource Professionals on how to secure information data and secret data.

Keywords: - HRM, Data Security, Information Security, I.T. Industry.

1. INTRODUCTION

Proper Uses of information technology helps communication of reliable information in effective way. HRM functions are done more quickly and effectively with a set of software and hardware for employee and organizational development. Information security has an influence on all the practices of human resource management in terms of planning and management, recruitment, training and development and maintenance functions. Security is a fundamental concern in modern human resource management systems. The advancement in human resource management systems provides many benefits such as reducing work congestion and improving safety and efficiency via information technology (Wilton, 2016).

1.1 HUMAN RESOURCE MANAGEMENT (HRM) SYSTEM

Human resource management (HRM) is a combination of three words (Yee and Ali, 2011; Reena *et al.*, 2018, 2019):

Human: *Skilled workforce in an organization.*

Resource: *Limited availability or scarce.*

Management: *Meet the organization goals and objectives with the help of resources.*

Human Resource Management includes Manpower Planning, Recruitment, Selection, Training & Development, Analyzing the performance of employees, Providing compensation and recognition of the employees, Maintaining the relations with employees and their trade unions and ensuring employees health, welfare and safety schemes. The term *human resources* were first introduced in the 1960s, (Berman et al., 2015; Gamage, 2014; Gatewood et al., 2015; Jha, 2009)**.**

1.1.1 Human Resource Management Approaches (Sendogdu *et al.*, 2013; Silva and Shinyashiki, 2014)

- Strategic
- Commodity
- Management
- Reactive
- Proactive

1.1.2 Functions of Human Resource Management (Bloom and Reenen, 2009; Mathis *et al.*, 2016; Seliger and Stucki, 2014)

There are mainly two types of functions: -

1. Managerial Functions
2. Operative Functions

1. Managerial Functions (Shields *et al.*, 2015; PWC, 2012)**:**

- Planning
- Organizing
- Directing
- Controlling

2. Operative Function: (Chettinadtech, nd; Lussier and Hendon, 2015; Punia and Sharma, 2015)

- Recruitment & Selection
- Job Analysis
- Performance Appraisal
- Training & Development
- Salary & wages Administration
- Employee Welfare
- Labor Relations

2. RELATED LITERATURE

2.1 The 1960's

During the Cold War, lots of mainframe computers were brought through online medium to accomplish more sophisticated and complex tasks. It also became necessary to initiate these mainframes to communicate via a less heavy process than mailing magnetic tapes among the computer centres. In response to this need, the Department

of Defence's Advanced Research Project Agency (ARPA) began examining the feasibility of a redundant, networked communications system to support the military's exchange of information. The founder of the interne - Larry Roberts, started the project and developed —ARPANET—from its inception (Stone *et al.*, 2015)**.**

2.2 The 1970's and 80's

During the subsequent decade, ARPANET become more admired and broadly used, and the prospective for its exploitation grow rapidly. In December, 1973, Robert M. "Bob" Metcalfe, who is recognized with the maturity of Ethernet, one of the admirable networking protocols, identified essential trouble with ARPANET protection. Personal remote sites did not have adequate controls and safeguard to secure information from not authorized remote users. Other issue abounded: susceptibility of password formation and format; lack of security procedures for dial-up network connections; and imaginary user identification and authenticity to the existing system. Telephone numbers were broadly circulated and openly exposed on the parapet of any premises, giving hackers to painless access to ARPANET. Just Because of spectrum range and frequency of the computer, the privacy and security violation and the detonation in numbers of nodes and accessible users on ARPANET, Network security was referred to as network insecurity. In the year of 1978, a famous report published entitled "Protection Analysis: Final Report" (Parker, 1998; AlDosari, nd).

2.3 The 1990's

At the close of the twentieth century, networks of computers became more common, as did the need to connect these networks to each other. This gave sudden rise to Internet, became first global network of networks. The Internet was made available to the general public in the 1990s, having previously been the domain of government, academia, and dedicated industry professionals. The Internet bring connectivity to practically connect all computers that could achieve a telephone line or a connected Local Area Network (LAN). After commercialization of the Net, the technology became invasive, spreading almost every coordinate of the globe. Since its consideration as a tool for information or data sharing Defence Department information, the Internet has become an spine of millions of million network. Initially, these connections were based on de facto principles, because industry principles for connection of networks did not be present at that time. These standards did tiny to ensure the privacy and security of data though as these predecessor technologies were broadly adopted and became standard of industry, some level of privacy was introduce at that moment. However, In early era deployment of network treated protection as a low priority. 2000 to till today, the Internet bring millions of unsecured LANs into continuous transmission over and each other. The privacy of each node's stored data is now reliant on the level of security of every other system to which network it is communicated. Recent era have seen a growing consciousness of the necessity to improve data security, as well as a awareness that information privacy is more essential to national defence. The fast growing intimidation of cyber attacks has made organization and governments much aware of the need to defend the computer-controlled accessories. There is furthermore upward concern about nation-states engage in information conflict, and the prospect that business and individual information systems could grow to be wounded if they are vulnerable (KPMG, 2016; Punnet, 2015; Merriam-Webster; Silva, nd).

3. RELATED WORK

Several survey papers have been published covering various topics of the Data Security. The research paper, Maintaining Ethical Standards for a computer security by James Harris, convicted that one should evolve susceptible safety related details to function hands on networking tools. In 2018, 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications focus on bring collectively scientists and practitioners in the complete world working on fully trusted, computing and reliable communications, with regard to safety, protection, authenticity, trust, security, privacy, reliability, dependability, availability, and blemish forbearance aspect of computer technology and communication, and providing a common platform to present and consider rising ideas and trends in this highly challenging field (Reena *et al.*, 2018; Willis Ware). Wang and Lu (2013) mentioned the cyber-attacks on availability, integrity and confidentiality.

4. OBJECTIVE OF THE STUDY

- Understanding the roles of information security to fulfil the objectives of organization.
- Knowledge of expectations for managers and employees according to security concern of the work.
- Secure and Efficient communication between individuals and teams
- Identifying security measures in term of Authentication, Integrity, and Denial of Services.

5. INFORMATION SECURITY ANALYSIS

The Committee on National Security Systems (CNSS) defines information security as the safety of reliable information and its essential elements, including the computer and hardware that system use, storage, and transmission of that information. Information security includes the broad areas of information security management, computer and data security, and network security (Karnik, 2005; McCumber, 1991; Peter, 1998)

➢ **Significant Characteristics of Information are follows:**

- **Availability:**

Availability refers an authorized user— individual or computer system—to access information without intervention or obstacle and to receive it in the necessary format. Consider, for example, research labs that need identification before entry. Head of the lab protect the elements of the lab so that they are available only to authorized persons.

- **Accuracy:**

Accuracy means information have no error or mistake and have a significant value for end user. If information has been intentionally or unintentionally modified, it is no longer accurate. Consider, for example, a checking your personal bank account. You presume that the information contained in your bank account is an accurate as per your finances. Incorrect information in your checking account can result from external or internal errors. If any bank representative, for example, adds or subtracts from your account, the significance of the particular information is changed accordingly. Or, you may accidentally enter an incorrect amount into your account register. Either way, an inaccurate bank balance could cause you to make mistakes, such as bouncing a check.

- **Authenticity:**

Authenticity means the information should be original or authentic or the quality or state, rather than a replica. Any Information is authentic when it is in the exact state in which information was formed, placed, stored, or communicated.

- **Confidentiality:**

Confidentiality means any information is safe from the third party which is not involved in the communication of that particular information. Confidentiality ensures that only and only those have privileges to access information are able to do the same. If any unauthorized person or systems can view, edit or shuffle the information, confidentiality of the information is breached.

- **Integrity:**

Complete and uncorrupted information is maintaining the integrity of information. Integrity is in danger of extinction when the information is open to the elements to pursue any corruption, destroy, destruction, or other distraction on the state of information. When the information is being communicated or stored, any corruption can be occurring.

➢ **Network Security In this modern era:**

In the current era almost, every organization relies on computer networks to communicate information in the organization in a proficient and dynamic mode. Organizational computer networks are now becoming large and ubiquitous. It is mostly appropriate that stations may not be managed centrally, nor would they have outskirts safety. There exist huge numbers of vulnerabilities available in the connect network. Thus, during transmission, data is highly vulnerable to attacks. Security of Network is not the single concerned about the privacy security of the systems at every communication node; however, more or less its aim to make sure that the complete network is fully protected. Ensuring network security may appear to be very simple. But in reality, the mechanisms used to achieve these goals are highly complex. International Telecommunication Union (ITU), in its recommendation on security architecture X.800, has suggested some mechanisms:

- **En-Cipherment**

This process provides service for data confidentiality by converting data into different forms.

- **Digital Signature**

This mechanism is the electronic equivalent of ordinary signature in electronic data. It provides authenticity of data.

- **Access Control**

This mechanism is used to provide access control services. These mechanisms may use the identification and authentication of an entity.

6. DATA SECURITY

Data Security is a method of secure data, files, and databases over a network by following a set of rules, protocols, that recognize the importance of different datasets, their sensitivity, regulatory compliance requirements and then applying appropriate protections to secure those resources.

➢ **Data Security Elements**

The elements of data security are

- **Confidentiality** - Data can only accessed by authorized person.

- **Integrity** - Information is accurate as well as reliable.
- **Availability** - Data is available and accessible both to fulfil requirements.

Also known as **CIA triad**.

➢ **Data Security Technologies**

The following are data security technologies used to prevent breaches, reduce risk and sustain protections.

- **Data Auditing -** With proper data auditing solutions, IT administrators can gain the visibility necessary to *prevent* unauthorized changes and potential breaches.
- **Data Real-Time Alerts -** By monitoring data activity and suspicious behaviour in real-time, you can discover more quickly security breaches that lead to access personal data.
- **Data Risk Assessment -** Risk assessments summarize important findings, expose data vulnerabilities and provide a detailed explanation of each lacuna.
- **Data Minimization -** Today, data is a liability. The threat of a reputation-destroying data breach, loss in the millions or stiff regulatory fines all reinforce the thought that collecting anything beyond the minimum amount of sensitive data is extremely dangerous.
- **Purge Stale Data -** Data that is not on your network is data that can't be compromised. Put in systems that can track file access and automatically archive unused files.

➢ **Data Security Regulations**

Regulations such as HIPAA (healthcare), SOX (public companies) and GDPR (anyone who knows that the EU exists) are best considered from a data security perspective. From a data security perspective, regulations such as HIPAA, SOX, and GDPR require that organizations:

- Track what kinds of sensitive data they possess
- Be able to produce that data on demand
- Prove to auditors that they are taking appropriate steps to safeguard the data

I. HIPAA (Health Insurance Portability and Accountability Act)

HIPAA was legislation passed to regulate health insurance. From a data security point of view, here are a few areas you can focus on to meet HIPAA compliance:

- Continually Monitor File and Perimeter Activity
- Access Control
- Maintain a Written Record

II. SOX (Sarbanes-Oxley)

The "SOX" or "Sarbox," is requiring publicly traded companies. From a data security point of view, here are your focus points to meet SOX compliance:

- Auditing and Continuous Monitoring
- Access Control
- Reporting

III.GDPR (General Data Protection Regulation)

GDPR covers the protection of EU citizen personal data, like social security numbers, date of birth, emails, IP addresses, phone numbers, and account numbers. From a data security point of view, here's what you should focus on to meet GDPR compliance:

- Data Classification
- Continuous Monitoring
- Metadata
- Data Governance

7. SECURITY MEASURES FOR H.R. SYSTEM IMPLEMENTATION:

- Purchase Planning
- Check merchant Security Policies
- Restrict Access Based on Needs
- Keep all records Secure from Hackers
- Be Aware of Cyber Security
- Be careful for Phishing policies
- Create and Educate Employees on Security Protocols
- Keep Software Up To Date
- Enable Timeout Features
- Frequent Password Changes
- Prepare for the Worst
- Develop Password Priorities
- Provide Data Security Training
- Create Cyber Secure Policies
- Minimize Data Collection
- Have a Disaster Recovery Plan

8. CONCLUSION

In this paper, analysis has been done on the concept of Information security which determines the ways through which data cannot be affected by the hackers and also provides the solutions to protect the information from being leaked. Technology developed by computer scientists and engineers, which is designed for rigorous performance levels, makes information security a science as well as an art. Most scientists and researchers are agreed that specific circumstances cause all actions in computer. Almost each and every fault, security gap, and system's malfunctions are the outcomes of improper data security implementation in H.R.M. If the developers have proper knowledge and competency, definitely they can resolve and eliminate all the problems. There are many sources of recognized and approved security methods and techniques that provide sound technical security advice. The finest practices, standards and other solutions can reduce the level of estimation, required to secure data in an organisation.

I.T. helps the executive to get better the efficiency and effectiveness of their company, administrative decision making, and workgroup association, thus supporting the managers to strengthen the positions of their company in a rapidly changing environment. The outcome of this research, Human Resource and their team should work with

Information Technology, Marketing team and stakeholders to identify and set-up of a HR system to reduce the security risks. Workforce is imperfect, and mistakes will occur. To ensure the perfection of work in I.T. organization, every organization should take data security & protection on high priority.

9. REFERENCES

Berman, E. M., Bowman, J. S., West, J. P., & Van Wart, M. R. (2015). Human resource management in public service: Paradoxes, processes, and problems. Sage Publications.

Bloom N and Reenen J V (2009), Human Resource Management and Productivity, Retrieved from: http://eml.berkeley.edu/~cle/secnf/vanreenen_sl ides.pdf

Chettinadtech, (n.d), human resource management, unit 1, retrieved on: 19/03/2017; retrieved from: http://chettinadtech.ac.in/coursenotes/hrm_a%5 B1%5D.pdf

D. B. Parker. Fighting Computer Crime. 1998. New York: Wiley Publishing, 189.

Fahd AlDosari , Faculty of Computer and Information Systems, Umm AL-Qura University, Makkah, KSA.

Gamage A. S. (2014), "Recruitment and Selection Practices in Manufacturing SMEs in Japan: An analysis of the link with business performance", Ruhuna Journal of Management and Finance, Vol. 1, No. 1, pp. 37-52.

Gatewood, R., Feild, H. S., & Barrick, M. (2015). Human resource selection. Nelson Education.

Jha. R, (2009), Human Resources management, wordpress, 9, pp. 1-60.

Karnik . K. Nasscom, HR Challenges in the IT industry, Newsline, Issue.41, April 2005.

KPMG, (2016), Enterprise performance management in the telecoms industry, kpmg, UK, pp. 1-10.

Lussier, R. N., & Hendon, J. R. (2015). Human Resource Management: Functions, Applications, and Skill Development. SAGE Publications.

Mathis, R. L., Jackson, J. H., Valentine, S. R., & Meglich, P. (2016). Human resource management. Nelson Education.

McCumber, John. "Information Systems Security: A Comprehensive Model." Proceedings of the 14th National Computer Security Conference, National Institute of Standards and Technology, Baltimore, MD, October 1991.

Merriam-Webster. "security." Merriam-Webster Online. Accessed 8 February 2007.

Peter Salus. "Net Insecurity: Then and Now (1969–1998)." Sane '98 Online. 19 November 1998.

Punia. M and Sharma. B,(2015), A Comprehensive Review of Factors Influencing HRM Practices in Manufacturing Industries, Journal of Management Engineering and Information Technology (JMEIT), 2(2), pp. 1-9.

Punnett, B. J. (2015). International perspectives on organizational behavior and human resource management. Routledge.

PWC, (2012), enterprise performance management EPM, driving finance effectiveness, Indian chamber of commerce, pp. 1-28.

Reena Singh et al, "Employee's Performance Appraisal System: A Literature Review" Journal of Emerging Technologies and Innovative Research (JETIR) ISSN: 2349-5162, Vol. 6, Issue 5, May 2019, pp. 531-537.

Reena Singh et al, "Performance Management System and Its Impact on Performance of the Employees" International Journal of Institutional & Industrial Research ISSN: 2456-1274, Vol. 3, Issue 1, Jan-April 2018, pp. 118-121.

Reena Singh et al, "The Impact of HR Practices on Employee's Growth in the Sector of Information Technology" International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. 5, Issue 1, March 2018, pp. 494-497.

Seliger F and Stucki T (2014), The Relative Importance of Human Resource Management Practices for a Firms Innovation Performance, DRUID Society Conference, Copenhagen.

Sendogdu A. et al. (2013), "The relationship between human resource management practices and organizational commitment: A field study", Procedia - Social and Behavioral Sciences, Vol. 99, pp. 818 – 827.

Shields, J., Brown, M., Kaine, S., Dolle-Samuel, C., North-Samardzic, A., McLean, P. & Plimmer, G. (2015). Managing Employee Performance & Reward: Concepts, Practices, Strategies. Cambridge University Press.

Silva M P and Shinyashiki G T (2014), The Human Resource Management Can Reduce Turnover, Journal of Management Research, 6 (2), 39-52.

Silva S R (n.d), Human Resource Management, Industrial Relations And Achieving Management Objectives, International Labour Organization, Retrieved on 26 March 2017.

Stone, D. L., Deadrick, D. L., Lukaszewski, K. M., & Johnson, R. (2015). The influence of technology on the future of human resource management. Human Resource Management Review, 25(2), 216-231.

Willis Ware. "Security Controls for Computer Systems: Report of Defence Science Board Task Force on Computer Security."

Wilton, N. (2016). An introduction to human resource management. Sage Publication.

Yee K. V. and Ali J. (2011), "Relationship between business strategy and human resource management practices in private and public International Journal of Current Engineering and Scientific Research (IJCESR) ISSN (Print): 2393-8374, (Online): 2394-0697, Volume-4, Issue-8, 2017 36 Limited Companies In Malaysia", Journal Of Business Management And Accounting.