Descriptive Finding Regarding Factors Influencing Information Security Vulnerability: A Case Study in Electrical Company in Iran

Malahat Pouransafar, Nurazean Maarop[*], Ganthan Narayana Samy, Nurulhuda Firdaus Mohd Azmi

Advanced Informatics School, Universiti Teknologi Malaysia, Jalan Sultan Yahya Petra,, 54100 Kuala Lumpur, Malaysia.

Abstract

Implementing technology is important to enhance the enterprise information transaction but it is impossible to secure it without organizational and human supports. Information security is about confidentiality, integrity and availability of the data and due to complexity of human resources the users have always exposed the information security to the internal threat. This paper presents a descriptive result regarding the human factors of information security vulnerability in one electrical enterprise in Iran. The result is presented based on the continuation of the previous review work. The descriptive analysis was performed on twenty participants' response over qualitative investigation. Based on the descriptive scoring result, training, risk communication and emotional control are found to be the most significant factors influencing information security vulnerability. Surprisingly security culture and staff experience were not significantly influential in this study. In regard to future works, an in-depth thematic analysis will be performed in order to have an overall perspective regarding the factors of concern.

Keywords: Security issues; Information Security Vulnerability; Descriptive Study

1. Introduction

Several organizations fail to implement a secure information system because they have a very shallow insight into the potential threat of the staff. For example, in several cases it is found that some workforces prefer to avoid information security procedures for faster access to the organizational data [1]. In fact, human resources are internal threats of the companies and it is vital to concentrate on this significant factor in order to avoid information security breaches.

Usually, users of the information systems are not aware of consequences of security vulnerability. Due to the lack of knowledge, they usually do not care about formal security procedures, so the unintentional errors are usually accrued [2] [3].

Since, private information is recorded in databases the risk of information lost and unauthorized access is existed. In such organizations the staff should know about the consequences of the security breach. Nevertheless, demotivated and irresponsible work forces may simply contribute in sabotage. Furthermore, the initiation of the supportive programs to protect the information security systems via training and awareness sessions, award and penalty approaches, employee engagement and empowerment, are impossible without the ultimate support of top management and the maturity alignment between corporate and IT governances [4].

Information security is an emerging area of knowledge that assists the organizations to protect private information. Although there are several approaches to mitigate the risk of security breach among the enterprises, still those methods or technological solutions are not effectively organized

[*] Corresponding author. *E-mail address*: nurazean.kl@utm.my

and positioned within the companies. Furthermore, human factors are more significant than organizational and technological factors. Without having proper insight into the role of human resources, the enterprises may focus more on the technology rather than the human factors and it is the main reason of security breaches [5].

The human factors have a significant role in the design and implementation of the security systems. Also, the role of management is important to implement the information security system with a maximum attention to the human resources [6]. Based on our previous literature review regarding factors influencing information security vulnerability from human perspectives, eight deductive factors are found to be important in mitigating the information security vulnerability in organization and the summary of review is shown in Table 1.

Table 1: Summary of Deductive Factors Based on Related Literature

Factor	Related Studies
Training and Awareness	[4-5, [7]
Security Culture	[8-9]
Risk Communication	[8], [10]
Staff Experience	[7],[11]
Risk Perception	[12-13]
Staff Attitude	[14-16]
Team Working	[10],[17]
Emotional Control	[18]

A review of the conducted studies reveals that there are many security challenges related to the Human, Organizational and Technological factors as well as their interaction during implementation of information security systems in the organization [19]. According the study has been conducted by Botta , et al. [6], the human factor has a significant role in the design and implementation of the security systems. On the other hand the role of management is important to implement the information security system with a maximum contribution of the human resources. The risk management process and use of cultural theory is important to classify the different aspects of security risks related to human factor [20]. There is a lack of enough information about the impacts of organizational factors such as the size of the company, top management support, and type of industry. So a holistic framework is necessary to reveal the influences of those factors on the effectiveness of information security controls within organizations [21]. The purpose of this paper is to present the descriptive part of the overall study findings regarding the human factor that may influence information security vulnerability in organization.

2. Method

The single case study approach was chosen in this study to further investigate about the factors influencing the security vulnerability in one of the Iranian electrical company. This study was conducted based on descriptive approach and in regard to this paper, the count score analysis was performed on the qualitative data. According to Miles and Huberman [22] scoring on the excerpts can be regarded as an analysis technique in qualitative. Twenty-five participants from one enterprise electrical organization were invited and only twenty of them agreed to participate. In prior to data primary data collection, three experts in the respective organization reviewed the interviews survey instruments and corrected them accordingly. Participants were selected from Iranian electrical companies who are officially registered under the Iranian Electrical Industry Syndicate (IEIS). Purposive sampling involving IT departments of IEIS was applied resulted in twenty-one participants agreed to participate in the scoring survey.

3. Result and Discussion

In this section, we present the descriptive result of the information security vulnerability in electrical enterprise. The scoring of “Important” and “Most Important” was combined to represent the significant scoring.

a. Training

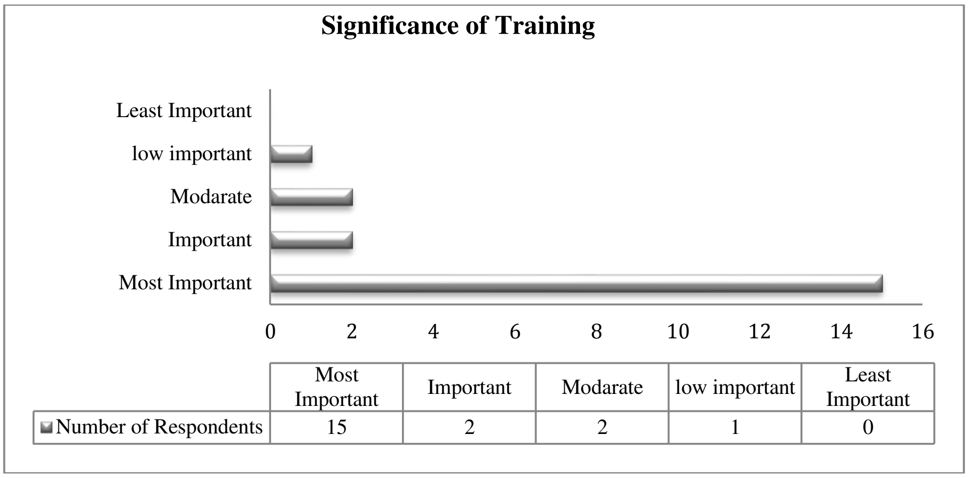
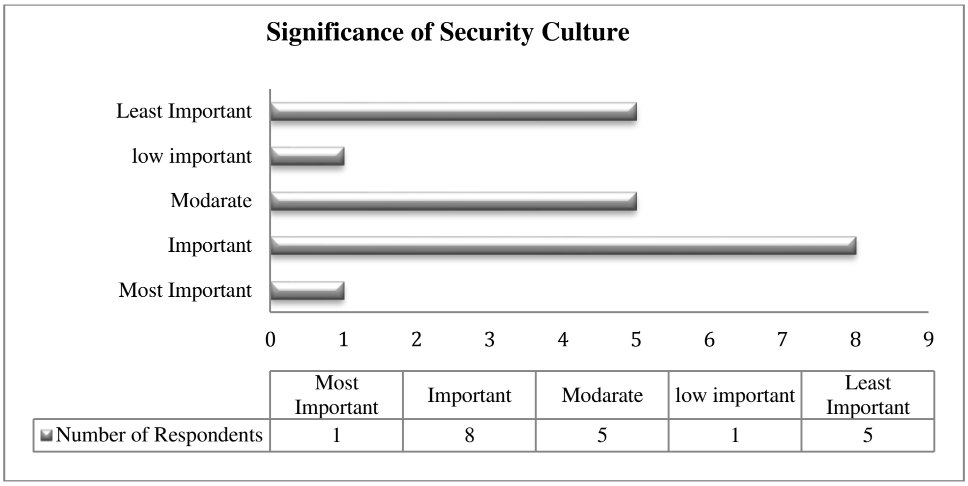


Figure 1: The result that shows the respondents agree that Training has a significant influence in preventing information security vulnerability in organization

The result shows that only 85% of the respondents agree that Training has a significant influence in preventing information security vulnerability in organization

b. Security Culture

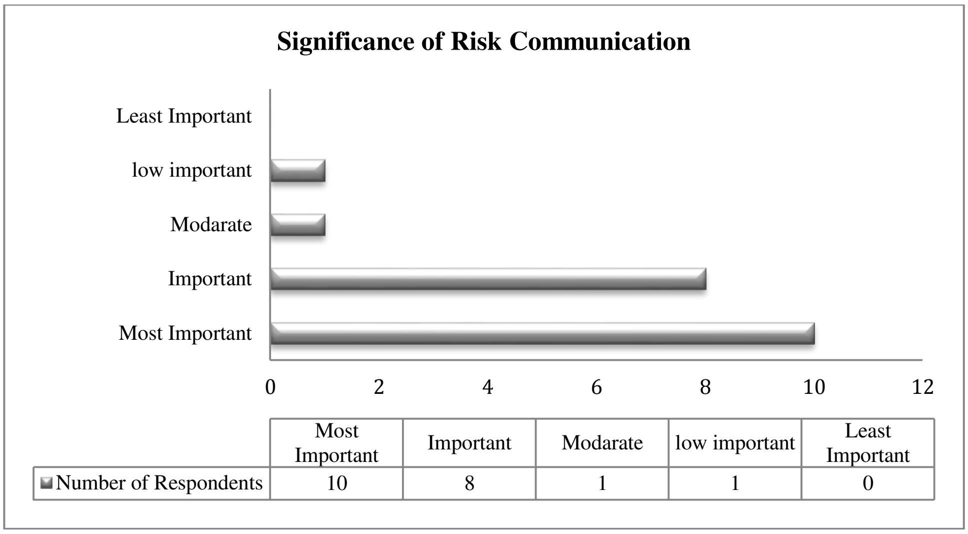


	Most Important	Important	Modarate	low important	Least Important
▪ Number of Respondents	1	8	5	1	5

Figure 2: The result that shows the respondents agree that Security Culture has a significant influence in preventing information security vulnerability in organization

The result shows that only 45% of the respondents agree that the Security Culture has a significant influence in preventing information security vulnerability in organization

c. Risk Communication

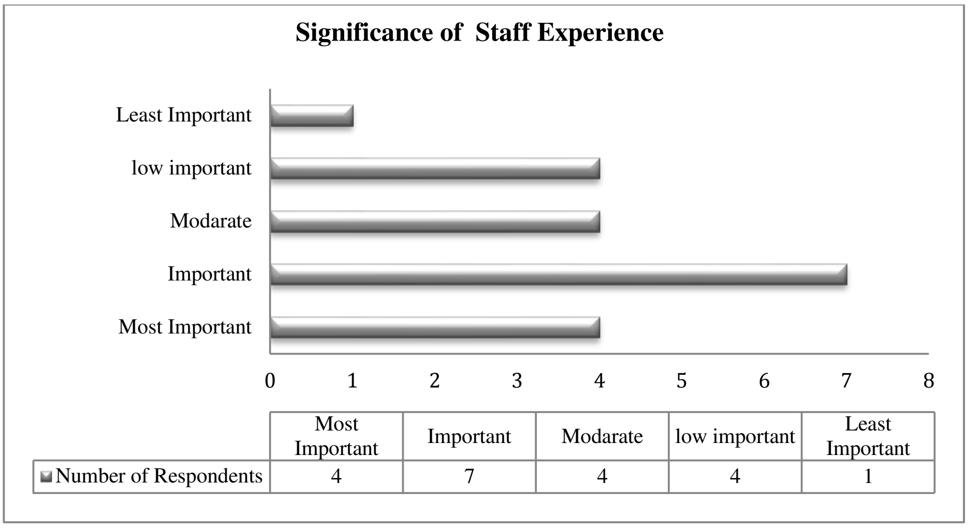


	Most Important	Important	Modarate	low important	Least Important
▪ Number of Respondents	10	8	1	1	0

Figure 3: The result that shows the respondents agree that Risk Communication has a significant influence in preventing information security vulnerability in organization

The result shows that 90% of the respondents believe that Risk Communication has a significant influence in preventing information security vulnerability in organization.

d. Staff Experience

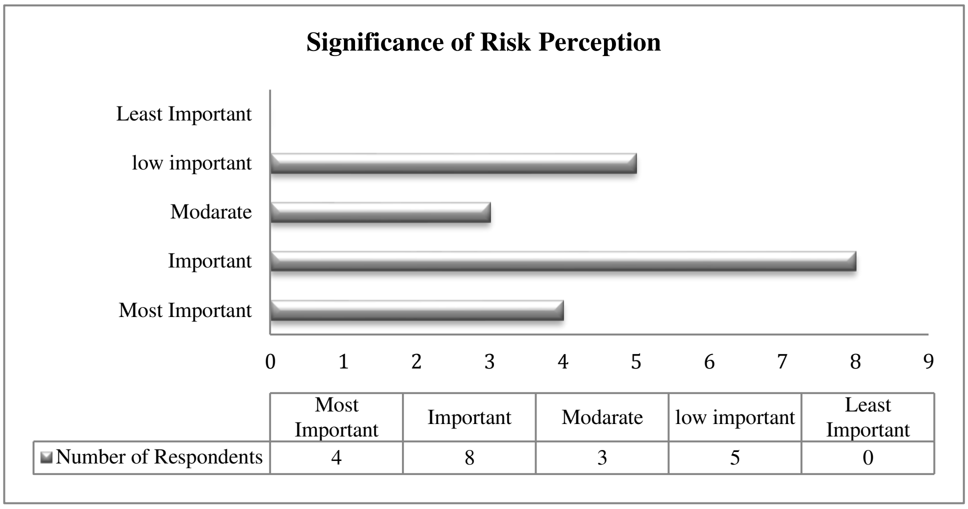


	Most Important	Important	Modarate	low important	Least Important
▪ Number of Respondents	4	7	4	4	1

Figure 4: The result that shows the respondents agree that Staff Experience has a significant influence in preventing information security vulnerability in organization

The result shows that 55% of the respondents believe that Staff Experience has a significant influence in preventing information security vulnerability in organization.

e. Risk Perception



	Most Important	Important	Modarate	low important	Least Important
▪ Number of Respondents	4	8	3	5	0

Figure 5: The result that shows the respondents agree that Perception of Risk has a significant influence in preventing information security vulnerability in organization

The result shows that 60% of the respondents believe that Perception of Risk has a significant influence in preventing information security vulnerability in organization.

f. Staff Attitude

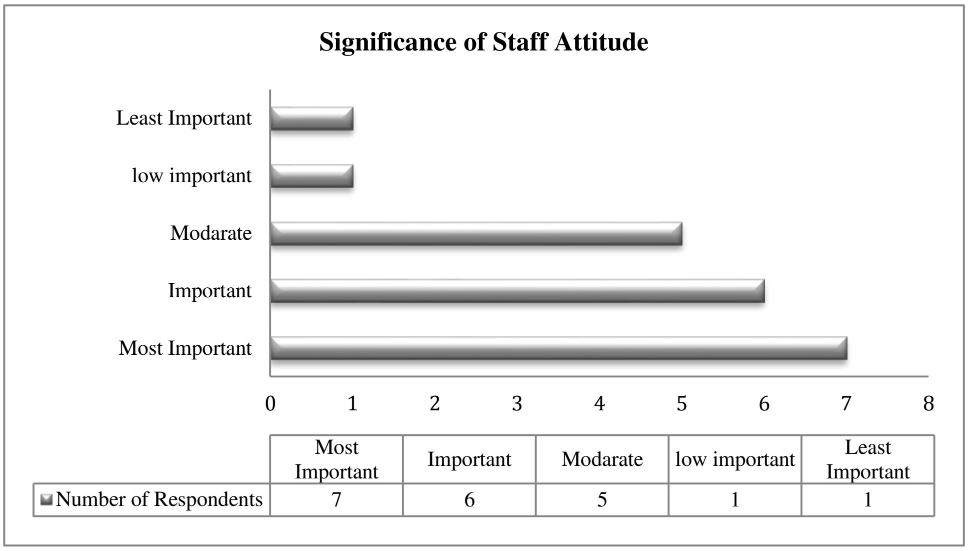


Figure 6: The result that shows the respondents agree that Staff Attitude has a significant influence in preventing information security vulnerability in organization

The result shows that 65% of the respondents believe that Staff Attitude has a significant influence in preventing information security vulnerability in organization.

g. Team Working

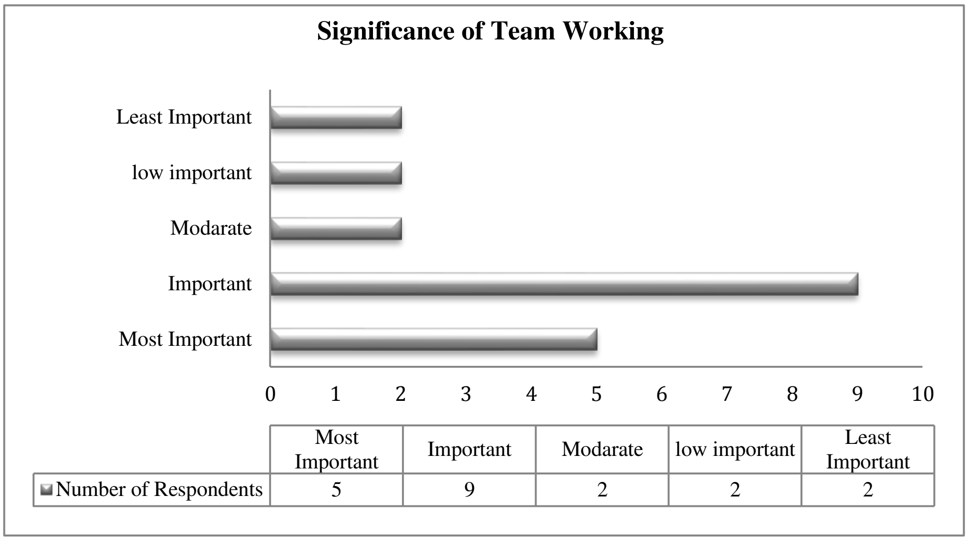
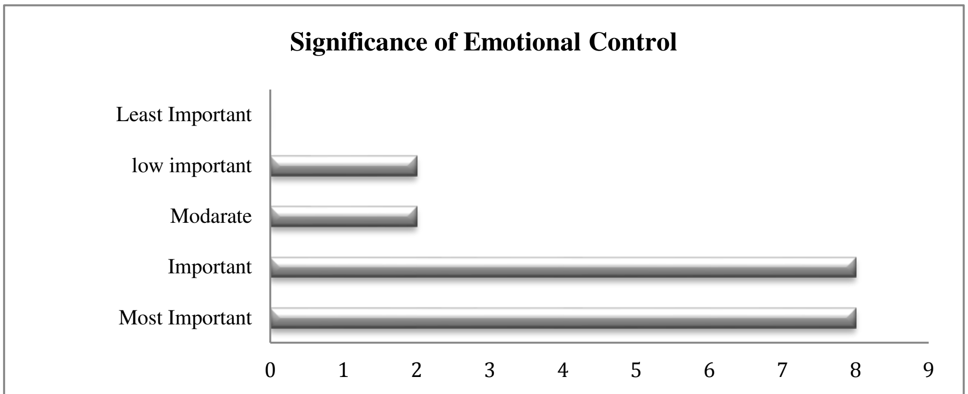


Figure 7: The result that shows the respondents agree that Team Working has a significant influence in preventing information security vulnerability in organization

The result shows that 70% of the respondents believe that Team Working has a significant influence in preventing information security vulnerability in organization.

h. Emotional Control



	Most Important	Important	Modarate	low important	Least Important
▪ Number of Respondents	8	8	2	2	0

Figure 8: The result that shows the respondents agree that Team Working has a significant influence in preventing information security vulnerability in organization

The result shows that 80% of the respondents believe that Team Working has a significant influence in preventing information security vulnerability in organization.

i. Overall Scoring

As can be seen risk communication, training and emotional control regarding information security were the most important factors in regard to information security vulnerability in this case study as the scoring is more than 80%. This result also revealed that, security culture and staff experience were regarded lesser important in the context of this study.

4. Discussion and Conclusion

The study revealed that proper training and awareness programs could provide a common understanding about the information security as well as the associated challenges among the human resources. Consistently, training is the main driver to engage the workforces in protecting enterprise data and enhances their contribution in information security placement [23]. Another factor namely Risk Communication was found very important in preventing information security vulnerability, hence the IT project managers and team leaders must be able to conduct and manage several meetings, communicate over the phone and build up a professional relationship with all staff to push everybody toward respecting IT governance. In regard to emotional control, the IT managers who have authority can initiative friendly environment to help control personal emotions and establish a strong level all potential energies of the workforces and drive everybody to respect and comply with information security objectives. There are number of limitations in this paper. The study was conducted using single case study. Hence, the result cannot be generalized to other type of enterprise organization. Furthermore, the result only exhibits the descriptive part of the study. Further enhanced work employing in-depth qualitative interviews should be conducted in order to present a better insight over preventing information security vulnerability issues in organization.

References

[1] P. Ifinedo, "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," Computers & Security, vol. 13, no. 1, pp. 83-95, February 2012.

[2] G. S. Alder, T. W. Noel and M. L. Ambrose, "Clarifying the effects of Internet monitoring on job attitudes:The mediating role of employee trust," Information & Management, no. 43, p. 894–903, 2006.

[3] C. Vroom and R. von Solms, "Towards information security behavioural," Computer & Security, no. 23, pp. 191-198, 2004.

[4] M. Kazemi, H. Khajouei and H. Nasrabadi, "Evaluation of information security management system success factors: Case study of Municipal organization," African Journal of Business Management, vol. 6, no. 14, pp. 4982-4989, 2012.

[5] M. Eminagaoglu, E. Ucar and S. Eren, "The positive outcomes of information security awareness training in companies - A case study," Information Security Technical Report, no. 4, pp. 223 - 229, 2009.

[6] D. Botta, R. Welinger, A. Gagne, K. Beznosov, L. Iverson, S. Fels and B. Fisher, "Towards Understanding IT Security Professionals and Their Tools," Symposium On Usable Privacy and Security, pp. 100-111, 2007.

[7] A. C. Maçada and E. M. Luciano, "The influence of human factors on vulnerability to information security breaches," in Americas Conference on Information Systems , Lima, 2010.

[8] D. Ashenden, "Information security management: a human Challenges?," Elsevier Information Security Technical Report, no. 13, pp. 195 - 201, 2008.

[9] H. A. Kruger, S. Flowerday, L. Drevin and T. Steyn, "An Assesment of the Role of Cultural Factors in Information Security Awareness," Potchefstroom, 2011.

[10] H. Tohidi, "Human resources management main role in information technology project management," Procedia Computer Science, vol. 3, pp. 925 - 929, 2011.

[11] S. Kraemer and P. Carayon, "Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists," Applied Ergonomics, vol. 38, no. 2, pp. 143-154, 2007.

[12] M. Kets de Vries, "The anarchist within clinical reflections on Russian character amd leadership style," Human Relations, vol. 54, no. 5, pp. 585-627, 2001.

[13] A. Tsohou, M. Karyda, S. Kokolakis and E. Kiountouzis, "Formulating information systems risk management strategies through cultural theory," Information Management & Computer Security, vol. 14, no. 3, pp. 198 - 217, 2006.

[14] A. Dutta and R. Roy, "Dynamics of organizational Information security, System Dynamics Review," WILEY, vol. 24, no. 3, pp. 349-375, 2008.

[15] K. Parsons, A. McCormac and M. Butavicius, Human Factors and Information Security: Individual, Culture and Security Environment, Edinburgh South Australia: Command, Control, Communications and Intelligence Division DSTO Defence Science and Technology Organisation, 2010 .

[16] S. Pahnila, M. Siponen and A. Mahmood, "Employees' Behavior towards IS Security Policy Compliance," in 40th Annual Hawaii International Conference on System Sciences (HICSS'07), 2007.

[17] S. Snedaker, Syngress IT Security Project Management Handbook, R. Rogers, Ed., Rockland: Syngress Publishing, Inc., 2006, pp. 95-116.

[18] B. G. Khosravi, M. Manafi, R. Hojabri, F. Farhadi and R. Gheshmi, "The Impact of Emotional Intelligence towards the Effectiveness of Delegation: A Study in Banking Industry in Malaysia," International Journal of Business and Social Science, vol. 2, no. 18, pp. 93 - 99, 2011.

[19] R. Werlinger, K. Hawkey and K. Beznosov, "Human, Organizational, and Technological Challenges of Implementing IT Security in Organizations," Information Management& Computer Security, vol. 17, no. 1, pp. 4- 19, 2009.

[20] R. B. Jr Vaughn Jr, Henning, R., & Fox, K. An empirical study of industrial securityengineering. The Journal of Systems and Software, 61(3), 225-232. 2001

[21]. Kankanhalli, A., Hock-Hai, T., Bernard, T., & Kwok-Kee, W. An Integrative Study of Information Systems Security Effectiveness. International Journal of Information Management. 2003

[22] M.B. Miles, A. M., Huberman, A.M., J. Saldana. Qualitative Data Analysis: A Methods Sourcebook Edition 3, Sage, Los Angeles. 2014

[23] D. Lacey. Managing the human factor in information security:how to win over staff and influence business managers. chichester: Jhon Whiley and Sons, Ltd. 2009