Review of Information Security Vulnerability: Human Perspective

Malahat Pouransafar, Nurazean Maroop, Zuraini Ismail, and Maral Cheperli
Advanced Informatics School
UniversitiTeknologi Malaysia, JalanSemarak, 54100 Kuala Lumpur, Malaysia
psmalahat2@live.utm.my , nurazean@ic.utm.my, zurainisma@ic.utm.my, and cmaral2@live.utm.my

ABSTRACT

Information security is about confidentiality, integrity and availability of the data and due to complexity of human resources the information security has always been exposed to the internal threat by the users. This study is an attempt to address the human factors of information security vulnerability which may present as an inter-organizational threat and contribute in information security breach. Based on the study, lack of training, lack of team working skill, having no control on emotions , having different risk perceptions, improper attitudes, improper security culture, improper risk communication, hiring inexperienced staff and having demotivated staff are found to be the significant factors of information security vulnerability from the human 's perspective.

KEYWORDS

Information security, security vulnerability, human factors, Security Behavior Human and Information System Interaction

1 INTRODUCTION

Nowadays, application of IT as a strong enabler that leverages enterprises and create sustainable advantage for the campanies is increased across the globe. In several organizations, information became an important source of analyzing the market situation, rivalry among competitors and several important data to gain competitive advantage. Several organizations are highly depended to the information system to conduct their business in a professional manner [1].

In order to keep the information confidential, correct and accessible with different access levels, the information security is practiced by the experts to mitigate the information security challenges within the organizations. Although several solutions were initiated to reduce the human, organizational and technical challenges of information security, but still many enterprises are struggling with information security breaches. On the one hand, having no information securty system is a big threat, on the other hand implementing information security is a costly process and cannot assure full protection of the information from unauthorized access [2].

There are several challenges and obstacles for implementing an information security system in organizations. The challenges are not only related to the technological factors, but also the influences of organizational and human elements are considerable [3]. Implementing technology is important to protect the enterprise information transaction but it is impossible to secure it without organizational and human supports. In other word, the attitude of the staff is always a critical to support the information security, but the inter-organizational processes and managerial commitments are also significant to align the human efforts with the objectives of information security systems [4].

Information security is all about protecting information from unauthorized accesses as well as to remain available for the authorized users upon their demand. In other word, the information security is about confidentiality, integrity and availability of the data (CIA). The confidentiality means that any unauthorized access should be banned. It is essential to specify a proper information security system to protect the private data [5]. The integrity means that the information should remain unchanged, unless by the authorized person. Finally, the availability of the data means that authorized users can access the information whenever needed [6].

Communicating both personal and organizational data over the net could be a challenging issue because of the high rate of data transaction as well as unpredictable behavior of humans. So, due to complexity of human resources, information system is always at risk [5].

Any kind of the weakness in an information security system including improper data transaction procedures, lack of control over unauthorized accesses or any kind of problem in operation or implementation of the system that make it fragile against the existed threats is considered information security vulnerability [7].

There is an interrelation between threat, vulnerability and risk. The risk is a result of vulnerability and threat. In fact, if the system is invulnerable then even with the existence of the threat, there is no risk at all. In another word, there are only two chances to mitigate the risks of the data transaction, either to decline the threats of the internal and external factors or to increase the strength of the information system. But, the hackers, attackers and unauthorized users always try to access and abuse the organizational data. In other word the threats are always existed, either actively or inactively (potentially). Information security managers should assure clean and authorized access of the users. Illegal accesses to the database must be banned using new tools and techniques. Companies should conduct intensive training and awareness programs to communicate the information security objectives and to teach human resources about the method of secure data transaction [8].

The main purpose of this study is to answer the question "what are the factors influencing information security vulnerability from human perspective?"

2 BACKGROUNDS

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 [9]. 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. Among information security vulnerabilities that made by human, just a few of them are generated intentionally or purposely. 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 [10] [11].

An academic case study that has been conducted about the information security success factors in Iranian public sectors, argues that the issue of information security is very sensitive in municipal organization. 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 [12].

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 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 [13].

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 [14].

According to the importance of the human role in implementing information security systems, as well as due to the insufficient studies about the human factors that may cause information security challenges, this research is an attempt to identify the main human factors in order to mitigate the information security vulnerability.

3 Method

Based on the outcomes of the critical literature review, nine major items realized as drivers of human security behavior. A combination of terms “Information Security Vulnerability” and “Human Factor” was used as the keywords combination.

Following strategies and criteria were considered in the review:

- Only manuscripts written in English are reviewed.
- The review only concentrates on identifying the human related factors only.
- The authors uses several keywords including “Information Security” + “Security Vulnerability” +“Security Behavior“ + “Human and Information System Interaction” , but the irrelevant manuscript were filtered properly.

4 RESULTS

In this part, the authors reflect the results of literature review in drivers of human security behavior toward information system.

4.1 Awareness and Training

Since human factors have a very high effect on the information system, this huge influence should be controlled by training and awareness programs. Based on the relevant practical methodologies and standards of information security, training programs are required to upgrade the level of knowledge among work forces. Training programs are not only about technical subjects but also it is necessary to communicate with all staff using simple words [13].

In order to engage the human resources to deploy information security systems, it is necessary to teach them about the importance of data protection [15]. Training is the main driver to engage workforces in protecting enterprise data [16].

Awareness of the human resources can significantly decline the rate of information security breaches [12].

Training and awareness programs must be boosted by using pictorial presentations, internal meetings and many other methods [17].

The critical point in training is the contents of the courses that should be related to the current practices and policies of the organizations [18].

The training might be needed at the different stages in order to upgrade the core competencies of the human resources. For instance, the basic training courses are usually necessary and the training contents should be identified carefully to meet the minimum requirements. But, the initial trainings are not enough to balance and harmonize the general perceptions of workforces. In fact, the continuing training programs are needed to develop the awareness level of the employee about the information security and associated risks [19].

Training programs without frequent checking and evaluation is not really effective. In order to maximize the efficiency of the trainings and facilitate the security management within the organizations, it is necessary to conduct several auditing and checking sessions [20].

4.2 Motivation

The best approach to enhance the level of the job performance as well as protect the organizational data, is creating the atmosphere of win-win situation between employees and the employer and assure the best appraisal based on the individual performance indicators [21].

According to the MARS model, the performance and organizational behavior of the employee is the outcome of the Motivation, Ability, Role Perception and the Situational factors. The individual characteristics such as emotions and attitudes, values, personality, perceptions, and stress are the primary drivers that affect the employee behavior and performance [22].

4.3 Risk Perception

There is strong relation between individual risk perception and personal culture. Based on the cross-cultural studies, workforces are not similar in dealing uncertainty. Some workforces are usually risk averse and avoid the risk, while others may accept the risk [23].

Risk perception, estimation, and evaluation depend on the personal point of view. Many factors that include level of knowledge about the source of hazard, can contribute to build up a particular risk perception [24].

4.4 Risk Communication

Communication is one of the most important issues of information technology projects. 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 and associated security issues. It needs technical ability, social and emotional intelligence to establish a kind of empathy with workforces for better risk communication. A good project champion should observe and control security behavior of with both technological and psychological abilities [25].

The improper communication within the organization can cause inconsistency or discrepancy of risk perceptions. As a result, each user may imagine some particular threats and defense against those specified threats only. The worst case is about conflict of risk perception among top managers and shareholders. In this case, decision making process is usually challenging. A common reason of this problem is limited power of the IT managers to define the security objectives of IT governance. In other word, IT managers are not usually empowered enough to orchestrate security objectives and align risk perceptions from the top of the hierarchy to the bottom [15].

There is a relationship between effective communication and culture of the organization as well as the culture of the individuals. A strong culture has a crucial impact on the effective communication among the staff [26].

4.5 Attitude

Employee attitude is always an important factor to protect information systems [4].On the other hand, according to the uncertainty of the employee behavior in different occasions, it is almost impossible to evaluate or forecast the impacts of human attitudes toward information security systems [27].

Attitude of individuals demonstrate their feelings about a specific object. This feeling could be either positive or negative. About the information security, human attitude demonstrates the internal feelings as well as willingness of workforces to obey or disobey information security objectives [28].

4.6 Security Culture

A legend cross-cultural study argues that there are five indexes to measure the cultural dimensions [29]. Also, the model of “Wheel of Culture” considered 18 cultural dimensions. Cultural differences are significant reasons of different perceptions, different values and dissimilar reactions toward uncertainties [23].

Cultural differences such as the mother tongue are important in information security awareness and it should be considered carefully to get better results [30]. The values and beliefs of the employee beside the organizational culture can cause a significant impact on information security success or failure [31].

Visible comportment of staff, attitude and norms of individuals are defined as different aspects of culture in an organization [15].

Culture is one of the important aspects of human resource management that can promote the manner and behavior of individuals. Also, strong culture has a crucial impact on the effective communication enhancement among the staff of IT department [26].

Strong culture is defined as a “values and norms shared among members of the organization”. Culture has a significant role in motivating staff for a better performance [32].

The influence of the national culture is greater than the organisation cultures in developing countries. In several developing countries, information security fails due to the improper security culture which is not tailored and custom-made particularly for the organizations. Nevertheless, it is always possible to improve information security culture by training and awareness programs. Furthermore, information security culture must be embedded into the body of corporate governance [33].

4.7 Experience

The working experience is considered as situational factor that usually contributes to the protection of the security systems [34].

A research that summarizes several studies about the human factors and information security vulnerability, has suggested an interactive model to illustrate the significant items that may positively or negatively influence on information security systems. Awareness of the users about information security policies can save information security and avoid security vulnerabilities. Some situational factors such as gender and working experience may contribute positively or negatively in information security protection. A positive organizational environment can increase the responsibility of the users. Responsibility of the workforces could be positively influenced by the level of awareness and familiarity with information security issues [17].

4.8 Team Working

Although team working is important in IT projects, organizing a team without capable and experienced people is useless. In other word, competent staff must support the objectives of the business while participating in team working activities as the leaders [19].

A practical solution for security risk identification and mitigation called “OCTAVE”. It means “Operationally Critical Threat, Asses and Vulnerability Evaluation”. This method emphasizes on close team working between IT practitioners and business staff. The OCTAVE approach suggests that the nominated team members identify risks together .Because the IT practitioners can simply deal with technical issues and identify the breaches of the information system. Also, business staff has deep insight into the corporate related issues, significance and level of privacy levels. The OCTAVE tries to introduce an applied system to engage both IT and business staff for a better risk identification, risk communication and risk mitigation. The advantage of OCTAVE is to reach a common perception about the risks of data communication/transaction in a particular business rather than implementing a general pattern for all types of the businesses [35]**.**

The most important step in managing information security projects is to build up a skillful team [25].

4.9 Emotional Control

Emotional intelligence is considered as a personal ability to control the emotions for a better performance. Social intelligence is all about the ability of managers to align the behavior of human resources with organizational objectives. IT managers who have a high level of emotional and social intelligence can control the emotions of the staff and establish a strong level of empathy to implement all potential energies and push everybody to comply with information security objectives. Since different staff may have different feelings and emotions about a certain object, managers must be intelligent enough to control their own emotions at first stage and then control the emotions of workforces. This can be done with the art of good listening, positive communication, and understanding needs, feelings and emotions of staff [36].

5 CONCLUSION

This study emphasizes the role of human factors as the major player in supporting information security systems. In order to manage the information security in an effective manner, it is necessary to concentrate more on the staff, because the human resources may contribute either in success or failure of the information security systems [37]. According to the outcomes of critical literature review, nine major drivers of human security behavior including training, team working ability, emotional control, perception, attitude, communication, motivation, culture and experience were considered as the baseline for literature review. Based on the review manuscripts, the role of the human is really significant in information security systems. Information security vulnerability could be caused by human, either intentionally or unintentionally. Although, there are several factors that may drive human behavior, but this study illustrates that there are nine major items that may significantly affect the human security behavior.

6 LIMITATION OF THE STUDY

The aim of this paper is to concentrate on human factor as the most significant reason of information security breaches, so organizational and technical issues are not considered in this research.

7 RECOMMENDATION

Scholars have conducted several studies about information security management and all associated risks and vulnerabilities. Human resource management science as an interdisciplinary area of knowledge has a strong linkage to information security management issues. Having more knowledge about proper human resource management and accompanying subjects such as training and awareness programs, attitude, motivation, team working ability, emotional control, perception, communication, culture and experience can help the information security champions within the organizations to mitigate risks of information breach.

This study helped to identify the major human factors that potentially mitigate information security vulnerability. Consequently, the main findings were described qualitatively. The key issues from the findings can be used to conceptualize teleconsultation utilization framework for future studies that can be further quantitatively validated.

8 REFERENCES

[1] J. Peppard and J. Ward, "Beyond strategic information systems: towards an IS capability," *Journal of Strategic Information Systems*, vol. 13, p. 167–194, 2004.

[2] K. Van der Leeden, "Security without risk?Investigating information security among Dutch universities," Unpublished MasterThesis, Enschede, 2010.

[3] 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.

[4] A. Dutta and R. Roy, "Dynamics of organizational

Information security, System Dynamics Review," *WILEY,* vol. 24, no. 3, pp. 349-375, 2008.

[5] H. Zafar, "Human resource information systems: Information security concerns for organizations," *Human Resource Management Review,* vol. 23, pp. 105 - 113, 2013.

[6] Government of the Hong Kong , "What is Information Security," 2002. [Online]. Available: http://www.infosec.gov.hk/english/information/what.html. [Accessed 11 Nov 2012].

[7] R. Kissel, Ed., Glossary of Key Information Security Terms, Diane Publishing, 2011.

[8] C. Benson, "Security Threats," 2013. [Online]. Available: http://technet.microsoft.com/en-us/library/cc723507.aspx. [Accessed 12 Feb 2013].

[9] 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.

[10] 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.

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

[12] 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.

[13] 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.

[14] 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.

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

[16] 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.

[17] 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.

[18] J. R. Vacca, Computer and information security handbook, J. R. Vacca, Ed., Boston, 2009.

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

[20] IT Governance Institute, "COBIT 4.1," 2007. [Online]. Available: http://www.isaca.org/Knowledge-Center/cobit/Documents/COBIT4.pdf. [Accessed 05 April 2013].

[21] D. Parker, "Organizing for Security," in *Fighting Computer Crime, A New Framework for Protecting Information,* D. Parker, Ed., John Wiley & Sons, 1998.

[22] S. L. McShane and M. A. Von Glinow, Organizational Behavior, Emerging Knowledge and Practice for the Real World, 5th Edition ed., Boston: McGraw-Hill, 2012.

[23] 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.

[24] 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.

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

[26] I. V. Koskosas and R. J. Paul, "The Interrelationship and Effect of Culture and Risk Communication in Setting Internet Banking Security Goals," in *6th international*

conference on Electronic commerce , New York, 2004.

[27] 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.

[28] 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.

[29] G. Hofstede, "Cultural Dimentions in Management and Planning," *Asian Pacific Journal of Management,* vol. 1, no. 2, pp. 81-89, 1984.

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

[31] L. Hassell and S. Wiedenbeck, "human factor and information security," Drexel University, Philadelphia, 2004.

[32] C. A. O' Reilly and J. A. Chatman, "Culture as a Social Control: Corporations, Culture and Commitment," *Research in Organizational Behaviour,* vol. 18, pp. 175 - 200, 1996.

[33] H. Shaaban and M. Conrad, "Democracy, culture and information security: a case study in Zanzibar," *Information Management & Computer Security,* vol. 21, no. 3, pp. 191-201, 2013.

[34] 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.

[35] . C. J. Alberts and A. J. Dorofee, Managing Information Security Risks The OCTAVE Approach, Boston: Pearson Education, Inc., 2003, pp. 13,25.

[36] 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.

[37] S. Bosworth, M. E. Kabay and E. Whyne, Computer Security Handbook, 5th ed., New Jersey: Wiley and Sons, Inc., 2009.