Behavioral Factors That Influence Employees to Comply With Information Security Policies

Golan Carmi, Dan Bouhnik
Jerusalem College of Technology, Israel

Abstract

In this paper we examine the awareness and behavior of employees with regard to information security procedures instituted within their organization. Moreover, the study focuses on employees' attitude toward compliance with information security policies, combined with various norms and personal abilities. 202 employees of a large financial institution fill out a self-reported questionnaire. Findings indicate that employees' attitudes, normative beliefs and personal capabilities, have positive effects on the organization's information security procedures compliance. Likewise, employees' general awareness of information security, as well as awareness to information security procedures within the organization, positively affects employees' information security procedures compliance.

1. Introduction

Information systems security includes actions aimed at protecting computer systems against threats, unauthorized access and use, disruption, distortion and destruction. In today's organizations, almost all of these actions are dependent upon technological tools [1]. Many databases serve individuals, companies, even countries, and these include both personal and business information; thus, the protection against penetration and damage becomes very critical [2]. Information security failures can lead to the disruption of business and to the violation of confidentiality and privacy, damaging the ongoing activity and reputation of the organization, as well as causing financial harm brought about by fines and regulation violations [3] [4].

Improper information security behavior can derive from several qualities of the individual: bitterness, malicious intent, lack of knowledge, negligence, indifference, etc. [5]. Some of these problems may be resolved by the creation of awareness. Employees who are aware of the devastating consequences information security deficiencies can cause can be less indifferent and more conscious of security breaches at their place of employment [6]. From a management point of view, organizations need to focus on two main elements: awareness, whose purpose is to arouse the workers, and teaching whose purpose is instilling the necessary expertise [7].

2. Literature Review

Studies have emphasized the importance of the human aspect of information security. Björck [8] claimed that proper management creates an atmosphere of information security in the corporation and that without clear guidelines the corporation would not succeed adequately in integrating information security procedures. Albrechtsen [9] argued that the quality of the management affects employees' awareness, motivation, and behavior, thus requiring the commitment of management levels to the maintenance of information security within the organization.

Herath and Rao [10] mentioned that management's approach toward the demand for proper information security behavior directly affects employees' attitude. Fagerström [5] recommended procedures for establishing such an environment. Wang, Cheng and Wang [11] also noted the improvement of social contacts via organizational bodies (commitment, involvement, norms) as an effective tool for preventing misuse of computers. The researchers Kotzias, Bilge, and Caballero [12] took a similar approach and emphasized the dangers stemming from the members of the corporation itself. These employees may comprise a threat as a consequence of authorizations they have received and procedures for which they are responsible, which they misuse, intentionally or otherwise.

In other study Herath and Rao [13] found that motivation for adhering to information security procedures is based on intimidation by punishment. The intimidation theory maintains that as the certainty of punishment rises, the level of the threats of the actual punitive measures rises. Pahnila, Siponen and Mahmood [14] also investigate motivational factors in order to explain employee compliance behavior. They found that sanctions and rewards did not influence the intention of employees to comply or actual compliance, and that information security may interfere with the primary goals of organizations. Accordingly, Tyler and Blader [15] claim punishments and rewards are external motivations, but it is well known that employee's intrinsic values provide internal motivation to follow regulations and procedures.

D'Arcy, Hovav and Galletta [16] reveal a positive effect of intimidation on information

 | DOI: 10.20533/jitst.2046.3723.2021.0087

security, but found that the certainty of punishment had no real effect, with the level of discouragement reliant upon the individuals' own ethical standards. Wang, Cheng and Wang [11] also speak of the "stick & carrot" method. They are of the opinion that in certain situations intimidation has a positive effect on compliance and at times rewards are more beneficial, depending on the general environment within the organization and the employees feeling of commitment.

Improper information security behavior can derive from several qualities of the individual: bitterness, malicious intent, lack of knowledge, negligence, indifference, etc. Some of these problems may be resolved by the creation of awareness. Employees who are aware of the devastating consequences information security deficiencies can cause can be less indifferent and more conscious of security breaches at their place of employment [17]. While formal information security procedures have a great effect on employee behavior, procedures which do not promote awareness have no impact on employee behavior. One of the effective ways to combat negligence and carelessness is the generation of awareness among the users. Establishing awareness of security threats will help the employees understand the gravity of the threats and improve their compliance to security procedures [18].

In light of this, in this study we attempt to understand the factors affecting employee compliance with information security demands is based on the theory of planned behavior (TPB) suggested by Fishbein and Ajzen [19] which sees behavioral intention as an indication of an individual's willingness to behave in a certain way. According this theory there are three major constructs: attitude, subjective norms, and the perception of behavior control in the context of precedents, which motivate the employees' intention to comply with information security policies. We also use cognitive beliefs as a part of the rational choice theory (RCT) as factors affecting attitudes [20]. Finally, we scrutinized the general awareness of the employees to the various security issues, employees' recognition of the importance of information security to the organization, and acquaintance with the organization's information security procedures.

3. Research Findings

Data was collected by a self-report questionnaire, distributed among employees of a large organization by the internal email system. Out of 275 distributed questionnaires, 202 were completed. Participants represented all positions in the organization, professional as well as administrative. Of the 202 participants, 54% were female; 62% between the ages of 26-45 (33% ages 26-35, 29% ages 36-45); 11% of the participants were employed by the organization for less than a year, 46% for 2-5 years, 31% for 6-10 years, and 12% for over 10 years. The participants' distribution among all the organization' departments reflects the relative size of the departments.

Nearly half (48%) of the participants reported their being very aware of general security issues, and 38% reported having extremely high awareness. Regarding awareness of security issues within the corporation, 42% reported that they very much understood the importance and the dangers relating to information security in the organization; 80% reported their having considerable understanding regarding information security policy, and 75% stated that they make an effort to comply with the information security policy related to their positions to a large extent, in order to protect the organization's information and technology; 76% reported that they protect information privacy to a very high extent.

The findings indicate a high level of compliance behavior and information security procedures compliance within the investigated organization. Also, a high level of awareness was found among the organization's employees regarding information security in general and specifically. Additionally, we found that attitude, beliefs and personal capabilities have a positive effect on employee ISP compliance. The results of the study indicate that the employees at all levels understand the immense importance of information security policy implementation at both the personal and organizational levels, and also have a conscious awareness and have adopted active behaviors regarding all that relates to the protection of the information resources and the security of the information itself.

Moreover, the research results indicate that conceptions and personal beliefs of the employees significantly affect behavior regarding all that relates to compliance with ISP. Similar to other studies [9] [8] our findings show a close association between ISP behavior and personal consequences-positive and negative-as an outcome of the actions which derive directly from the employees' manner of behavior. For instance, an anticipation of personal benefit increases the level of compliance, while imposing a personal cost as a result of non-compliance directly and positively affects compliance. In other words, the manner in which employees evaluate how compliance or non-compliance with IS procedures will affect the progress of his work assignments on the one hand and personal sanctions on the other hand, are parameters which greatly influence the level of actual compliance with the corporation's ISP. Appropriate awards may actually increase ISP compliance levels and cause employees who do not

 | DOI: 10.20533/jitst.2046.3723.2021.0087

recognize the importance of information security to comply with ISP.

4. Conclusion

The main conclusion of the study is that employee information security compliance level is a combined function of awareness and behavior. In order to achieve better information security results, organizations must invest resources on the development of information security awareness, as well as on information systems. In our opinion, information security awareness is a valuable preliminary conscious basis for understanding the importance of information security behavior and the organizational need for protection of information.

From this, we recommend that organizations strengthen their efforts to create awareness of information security among employees at all levels and positions, presenting the issue in seminars and training programs in order to teach them the importance of information security and the practical consequences of related behaviors. Moreover, various aspects of awareness may be more effective in modifying beliefs and behavior, depending on their hierarchic level and position. Therefore, the programs should be constructed keeping in mind the characteristics of the employee groups they are targeting.

5. References

[1] Carmi, G. and Bouhnik, D. (2016). 'Functional analysis of applications for data security and for surfing privacy protection in the Internet'. International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC), 4(7), 201-208.

[2] Herath, T. and Rao, H. R. (2009b). 'Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness'. Decision Support Systems, 47(2), 154–165.

[3] Itradat, A., Sultan, S., Al-Junaidi, M., Qaffaf, R. A., Mashal, F. A., and Daas, F. (2014). 'Developing an ISO27001 information security management system for an educational institute: Hashemite University as a case study'. Jordan Journal of Mechanical and Industrial Engineering, 8(2), 102-118.

[4] Talib, S., Clarke, N. L., and Furnell, S. M. (2010). 'An analysis of information security awareness in the home and work environments'. In proceedings of the 5th International Conference on Availability, Reliability, and Security, Krakow, Poland.

[5] Fagerström, A. (2013). Creating, maintaining and managing information security culture. Master's Thesis, Arcada University of Applied Sciences, Finland.

[6] Chen, H. and Li, W. (2018). 'Understanding commitment and apathy in is security extra-role behavior from a person-organization fit perspective'. Behaviour and Information Technology, 38(1), 1-15.

[7] Harris, M. A., Furnell, S., and Patten, K. (2014). 'Comparing the mobile device security behavior of college students and information technology professionals'. Journal of Information Privacy and Security, 10(4) 186-202.

[8] Björck, F. (2005). Discovering information security management. PhD Thesis, Stockholm University, Sweden.

[9] Albrechtsen, E. (2008). Friend or foe? Information security management of employees, PhD Thesis, Norwegian University of Science and Technology, Norway.

[[10] Herath, T. and Rao, H. R. (2009a). 'Protection motivation and deterrence: A framework for security policy compliance in organisations'. European Journal of Information Systems, 18(2), 106-125.

[11] Wang, L., Cheng, M.Y. and Wang, S. (2018). 'Carrot or stick? The role of in-group/out-group on the multilevel relationship between authoritarian and differential leadership and employee turnover intention'. Journal of Business Ethics, 152(4), 1069-1084.

[12] Kotzias, P., Bilge, L., and Caballero, J. (2016). 'Measuring PUP prevalence and PUP distribution through pay-per-install services'. In proceedings of the 25th USENIX Security Symposium (USENIX Security '16), Austin, TX.

[13] Herath, T. and Rao, H. R. (2009b). 'Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness'. Decision Support Systems, 47(2), 154–165.

[14] Pahnila, S., Siponen, M., and Mahmood, A. (2007). 'Employees' behavior towards IS security policy compliance'. In Proceedings of the 40th Hawaii International Conference on System Sciences (pp.156-166), Los Alamitos, CA: IEEE Computer Society Press.

[15] Tyler, T. R., and Blader, S. L. (2005). 'Can Businesses Effectively Regulate Employee Conduct? The Antecedents of Rule Following in Work Settings'. Academy of Management Journal, 48(6), 1143-1158.

[16] D'Arcy, J., Hovav, A., and Galletta, D. (2009). 'User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach'. Information Systems Research, 20(1), 79-98.

[17] Chen, H. and Li, W. (2018). 'Understanding commitment and apathy in is security extra-role behavior from a person-organization fit perspective'. Behaviour and Information Technology, 38(1), 1-15.

[18] Gundu, T. and Flowerday, S.V. (2013). 'Ignorance to awareness: Towards an information security awareness process. SAIEE Africa Research Journal, 104(2), 69-79.

 | DOI: 10.20533/jitst.2046.3723.2021.0087

[19] Fishbein, M. and Ajzen, I. (1975). Belief, attitude, intention and behavior: An introduction to theory and research, Addison-Wesley, Reading, MA.

[20] Scott, J. (2000). 'Rational choice theory'. In G. Browning, A. Halcli, and F. Webster (Eds.), Understanding Contemporary Society: Theories of the Present, SAGE Publications Ltd., Thousand Oaks, CA, 126-138.

 | DOI: 10.20533/jitst.2046.3723.2021.0087