



Organizational Behaviour

Elixir Org. Behaviour 83 (2015) 32989-32992

Elixir
ISSN: 2229-712X

Impact of Knowledge Management on Safety Culture in Iran Telecommunication Research Center

Abouzar Solat Rafiee¹, Akbar Alem Tabriz² and Mohammadreza Babaei³

¹Department of IT Management, Science and Research Branch, Islamic Azad University, Tehran, Iran.

²Department of Industrial Management, Shahid Beheshti University, Tehran, Iran.

³Department of Industrial Management, College of Management and Accounting, Yadegar - e- Imam Khomeini (RAH) Branch, Islamic Azad University, Tehran, Iran.

ARTICLE INFO

Article history:

Received: 13 April 2015;

Received in revised form:
25 May 2015;

Accepted: 4 June 2015;

Keywords

Knowledge Management,
Security Culture,
Security Behavior,
Iran Telecommunication Research
Center.

ABSTRACT

Human resources nowadays is one of the key factors in the issues raised from information security. Consequently, there has been a shift in information security from mere concentration on technology to human resources. An effective issue in this field is security culture which is influenced by several factors. The main purpose of the present study is to survey the relationship between knowledge management and security culture in Iran Telecommunication Center. Sample group size was determined using Morgan Jersey's Table (n = 114). Furthermore, a questionnaire was used for data gathering. Validity and reliability of the questionnaire was determined using content validity and Cronbach Alpha respectively. The relationship between security culture and knowledge management was examined by path analysis in AMOS. The results confirmed significant relationship among generation, utilization, and dissemination of knowledge and relationship between security behavior and information security culture.

© 2015 Elixir All rights reserved.

Introduction

Information technology (IT) can be considered as the biggest technological achievement of man throughout the history. Different fields of science have been connected to each other with the help of IT. By connecting all fields of science, the technology has brought the opportunity to researchers, businessman, producers, and different social groups to access needed information in shorted feasible time. It is not exaggeration to say that IT has removed the borders and created a global society (Mahmoudzadeh, 2006). Despite the undeniable role and effect of information in any organization, necessity of creating secure environment in organizations and related cultural matters have been neglected (Hassan et al., 2014). As recommended by the literature, many problems emerged regarding information security have been rooted in human factors, which are overshadowed by technological factors (Hassan et al., 2014). An important issue in this field of human force in organization is cultural matters (Saeed et al., 2010). One of the main features of the modern market is competition and change so that businesses and organization find nothing more reliable than human resources to survive in the market.

Businesses and organizations motivate their human resources to perceive, comprehend, and bring in knowledge and new ideas and put them into practice. Doing this needs developing organizational culture as the main element in personality of the organization that influence behavior of the employees. Such culture must support development of knowledge and knowledge-oriented activities (Sadeghi et al., 2010). Taking into account weight of cultural issues in management of the organization and in light of importance of information security matters in Iran Telecommunication Co., the present study is aimed at surveying the relationship between information security culture and knowledge management in the

company. A key variable in this regard is security behavior (Hassan et al., 2014)

Information Security Culture

Information technology is a serious matter for organizations; whoever, like any other technologies, it may be cause of good or bad consequences. Failing to take into account security concerns as to IT may results in a threat or a catastrophe. Ensuring information security entails protecting information and information system against possible attacks and several security services have been introduced to this end (Mahmoudzadeh, 2006). Lack of an effective security system might results in negative and unpredictable outcomes (Sakha Ravesh Co., 2003). Security means immunity to probable and actual threats that threaten existence and survival of a society, an individual, or an entity. In computer science, security is defined as minimizing the odds of information leak to unauthorized bodies (Kign and Asmaoqlu, 2001). Information security refers to a set of tools to prevent information leak, spying, crime, sabotaging. It also refers to the science of studying different methods for protecting data stored in computers or communication system against unauthorized modification or access (Hatef, 2009). A study by the Supervision Commission of the UK regarding abusing IT indicated that main reasons were rooted in the personal factors. Negligence of security by some of the users (e.g. security mistakes by users, recklessness, and so on) are to blame in many cases of security problems. Many organizations have realized necessity of launching campaigns to inform the users about security issues. Success of such campaigns is measurable by the extent of knowledge about security matters that the target group gains after the campaign. In the case of organizations, the employees need to obtain three levels of security risk awareness including knowledge, perception, and attitude/exhibited behavior/outcome (Kroger and Kearn 1, 2006). The role of culture have been emphasized by

Tele:

E-mail addresses: rafiee1358@gmail.com

© 2015 Elixir All rights reserved

many authors (Hassan et al., 2014); as it influences all aspects of the society and enables the organization to impact attitudes, motivations, occupation satisfaction, commitment, structure design, organization systems, setting goals and strategies, and implementing based on common beliefs and values (Robins, 2004). In the definition of this effective variable – culture – it is the relatively fixed beliefs, values, and common perceptions that are preserved by the members of the organization. Culture is a set of assumptions and values that is widely respected in the organization and leads to specific behavioral pattern (Donateh, 2010). Recent years have been featured with introduction of information safety culture as a new and critical issue in information security field. This is due to a shift in research trend from mere technological issues to human force issues (Hassan et al., 2014)

Knowledge Management

Knowledge is an intangible and invisible asset that is hardly measurable by traditional parameters (Al-Adialeh et al., 2011). Today, many find knowledge as intangible capital so that many organizations have realized necessity of knowledge management techniques (Saeed et al., 2014). In the turn of 21st century, considerable changes have taken place in technologies and complicity of the environment. It is not exaggerating to say that knowledge is the most valuable asset of organization in the modern age (Brito, 2010). Many studies on knowledge management consider knowledge as a considerable asset needed to gain competitive advantage and as a key factor in survival and success of an organization in the competitive environment (Zack et al., 2009). Fast development of new technologies and digital communication has led to more emphasis on knowledge management as a vital source of competitive advantage. Taking this into account, gaining strategic competitive advantage needs new type of organizations capable of creating qualitative knowledge (Rahnavard, 2009). To shed more light on this, Lopez stated that knowledge and organizational capabilities are specific sort of strategic assets that improve long-term goals of organization as to competitive and environmental necessities aspects. It is in the dynamic environments that knowledge finds strategy functions. To have knowledge management implemented successfully, it is essential to measure the effect of knowledge management; otherwise, development of knowledge capital is not easy (Anantamula, 2006). As recommended by literature, successful implementation of knowledge management entails support from the employees; Snonden wrote in this regard that knowledge management is recognition, optimization, and active management of intellectual assets; the knowledge can be explicit or implicit and possessed by the staff. Therefore, any measure that an organization takes toward implementation of knowledge management must be based on surveying and planning for acceptable performance beforehand. Finally, knowledge management is the process that helps the organization toward recognition, selection, organization, and transfer of valuable data and information (Seraj et al., 2013).

Security Culture and Knowledge Management

Knowledge management, has been one of the most challenging and intriguing topics of business management in the recent years (Seraj et al., 2013). It is a multi-aspect structure that represents different viewpoints. Still, three approaches/aspects are recognizable in the mainstream of studies; 1- generation of knowledge, 2-dissemination of knowledge, and 3- utilization of knowledge. Knowledge management applications in the organization depends on different prerequisites. One of the most important prerequisites of organizational culture is effective knowledge management (Saeed et al., 2010). It is noticeable that

an organization does not emerge in vacuum, but it rather is subject to cultural-social backgrounds (Hafsted, 2001). Still, importance of knowledge and management of this critical aspect of organization is a tough issue ahead of managers to implement knowledge management (Donate, 2010). Mosik (2013) introduced one of the most important challenges ahead of managers in implementing knowledge management among human forces. The challenge is more evident when it comes to cultural matters (Allame et al., 2011). Given that cultural issues and management is new area of challenge, it adds to complicity of creating effective and stable relationship between knowledge and organizational culture (Haloteske, 2013). The relationship is so important that without it Haloteske finds implementation of knowledge management impossible. Without this relationship, the process of knowledge management implementation encounters several problems in generating, storing, and transferring the knowledge. On the other hand, there is a trend of increasing usage of knowledge management in different organizations. In fact, one way to create information security and participating employees in creating a secure system in the organization is one of the ways of improving information security (Hassan et al., 2013). Creating proper grounds for implementation of secure system happens when the management focuses mainly on human resources (Saeed et al., 2014). There are studies on the causes of industrial accidents that confirmed role of human factors in the accidents (Hassan et al., 2014). In light of what mentioned thus far, three main aspects of knowledge management can be noted; generation, dissemination, and utilization of knowledge that eventually influence security culture of organization through security behaviors. The study was conducted based on the following hypotheses:

Hypothesis 1: knowledge management has significant effect on information security behavior.

Hypothesis 2: information security behavior has significant effect on security culture. Hypothesis 3: knowledge management has direct significant effect on security culture.

Hypothesis 4: knowledge management and security culture relationship is moderated by security behavior.

Methodology

The study was carried out as descriptive, correlative, and applied work. Study population was comprised of all managers and experts working in Tehran Telecommunication Research Center. To determine number of participants, Morgan Jersey's Table (1999) was used (n =114). Sampling was performed randomly and conceptual model is as pictured in Fig. 1.

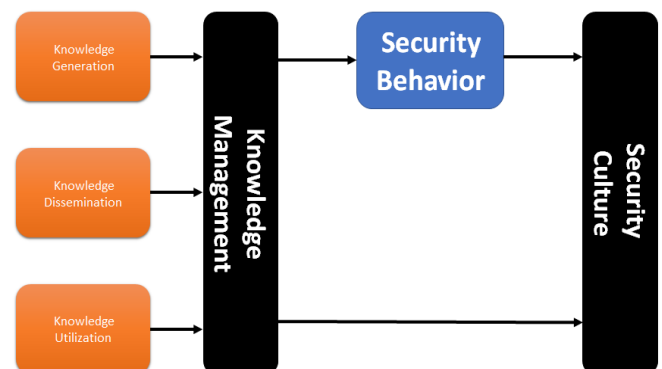


Figure 1. Conceptual model (ref. Hassan et al., 2014)

Research tools

A questionnaire designed based on Likert's five-point spectrum was used to collect the needed data. To check reliability of the questionnaire, Cronbach's alpha and extraction

variance mean were used. Features and reliability of the questionnaire are listed in Table 1.

Table 1- features of research tool

Variable	Number of questions	Cronbach alsp	EVA	CR	منبع
Knowledge management	15	0.745	0.54	0.87	Bukowitz, W. and Williams, R., (1999)
Security behavior	5	0.712	0.60	0.85	Furlell,S & Rajendran,A(2012)
Security culture	5	0.789	0.58	0.86	Furlell,S & Rajendran,A(2012)
Fitting indexes GFI=0.956 AGFI=0.923 RMSEA=0.074 Chi - square/df=2.65					

As listed in the Table above, Cronbach alpha of all the indices are above 0.7; which means high reliability of the questionnaire. Moreover, accumulated reliability of all indices is acceptable. In fact, reliability of all indices is higher than 0.8. Regarding extracted variance mean, it is higher than 0.5 for all variable. This value indicates high correlation of the research tool (Fornell & Larcker, 1981). General fitness of the model showed good fitness of the model as well.

The collected data were analyzed using descriptive and inferential statistics. Demographic information is listed in Table 3. The relationships were analyzed through structural equation modeling (SEM). Statistical specifications of the variables are listed in Table 4 and hypotheses tests are represented in Table 5 and figure 3.

Data analysis

Demographic feature of the study group including job title, main activity, and work experience are listed in Table 3.

Table 3. Demographical features

Demographical features	Group	Frequency (%)
Job title	Project expert	65
	Project manager	35
Main activity	Hardware	45
	Software	55
Work experience (years)	Less than 3	35
	4-6	30
	7-9	20
	More than 9	15

As listed in Table 3, project experts and project managers constitute 65 and 35% of the study group respectfully. In addition, 45% of the participants mainly work on hardware and the rest (55%) work on software. Regarding work experience, 35% have less than 3 years, 30% have between 4 to 6 years, 20% have between 7 to 10 years, and 15% have more than 9 years of experience.

The results regarding correlation between the variables, mean, and standard deviation are listed in Table 4.

Table 4- Specification of research variables

Structure	Mean	SD	1	2	3
Knowledge management (1)	3.70	1.40	1		
Security behavior (2)	4.99	1.08	.562**	1	
Security culture (3)	3.66	1.23	.481**	.444**	1

** Correlation at 0.01% level

Path Analysis and Hypotheses Test

Results of hypotheses tests and analyses are listed in Table 5 and pictured in figure 3. The hypotheses were examined in AMOS 22. As listed in the table, relationship among security behavior and knowledge management (4.77), Knowledge management and security culture (3.35), security behavioral and security culture (2.28), and indirect relationship between

security culture and knowledge management (4.85) were higher than 1.96- i.e. the hypotheses are supported. In addition, based on path coefficient, intensity of indirect relationship between security culture and knowledge management was higher than direct relationship between security culture and knowledge management. So the Hypothesis 4: knowledge management and security culture relationship is moderated by security behavior was supported.

Table 5. Hypotheses and path analysis

relationship	Independent variable	Dependent variable	t-value	Path coefficient	Sig.	Result
Direct	km	Security behavioral	4.77	0.23	***	Support ed
Direct	km	Security culture	3.35	0.29	0.04	Support ed
Direct	Security behavior	Security culture	2.28	0.39	0.02	Support ed
Indirect	km	Security culture	4.85	0.42	0.001	Support ed

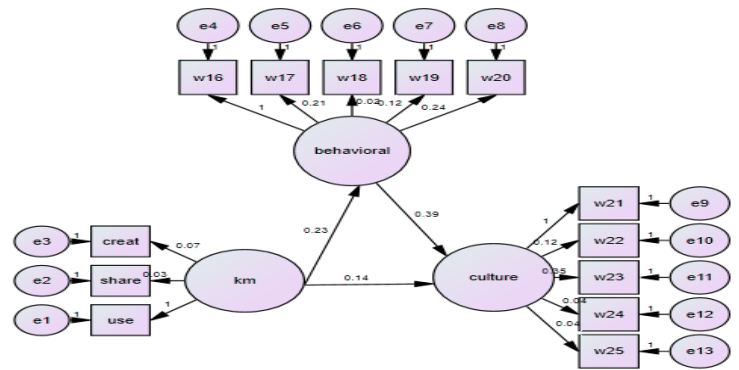


Figure 3. Results of Hypotheses Test

Conclusion and Recommendations

There are several studies conducted on the variables studied in this work. Many authors have argued for significant relationship between knowledge management and culture. The relationship between knowledge management and behavior of individual is also an ongoing debate as the both variables represent man's characteristics. People may have different behaviors, which in some cases is rooted in one' acquired knowledge. People make decision about their environment, which is saturated with knowledge and information, based on personal judgment. A set of continuous behavior of people forms culture of a society (Robins, 2007). Our results showed relationship between different aspects of knowledge management and security behavior of people. Furthermore, the results showed that safety behaviors are effective on security culture. The results are consistent with other studies including Hassan et al. (2014). Taking these into account, one may conclude that proper knowledge management throughout generation, recording, and dissemination using suitable software and hardware may result in improvement of security behaviors. On the other hand, empowerment of the employees regarding security behavior in organization guarantees general improvement of organization security. On the other hand, to reach desirable results from this culture, the employees and top managers in particular need to observe security behaviors and codes. This is also evident in Robins (2009) statement that top managers and founders' behavior is one of the main source of culture in an organization.

References

- Rahnavard F, Mohammad A (2009) *Identifying key elements of success of knowledge management in faculties and higher education centers of Tehran*; IT Management Journal, No. 1, series 1, 2009, 37-52
- Knowledge management of Sakha Ravesh Co. (2003) *Information security strategy in computer networks* (1st section, August 2004, <http://www.srco.ir>)
- Hafez M (2009), *Challenges and viewpoints of security in virtual space*, bimonthly of Human Development in Police Forces, 6th year, No. 22, 93-117
- Mahmoudzadeh A (2001), *Managing future by future technology*, Eaz Institute, Tehran, Iran
- Robins S (2004), *Foundation of organizational behavior*, Samt Publication, Tehran
- Donate, M (2010), The Effect of Organizational Culture on Knowledge Management Practices and Innovation, *Knowledge and Process Management*, Volume 17 Number 2, 82–94.
- Allameh, M., Zamani, M & Davoodi, M (2011), The Relationship between Organizational Culture and Knowledge Management, *Procedia Computer Science* 3 (2011), 1224–1236.
- Holowetzki, A (2013), The relationship between knowledge management and organizational culture: An examination of cultural factors that support the flow and management of knowledge within an organization, University of Oregon Applied Information Management Program.
- Kruger, H.A. and Kearney, W.D. (2006). A prototype for assessing information security awareness. *Computer & security*, 25, 289-296.
- Anantamula, Vittal S., and Shivraj Kanungo (2006), Structuring the underlying relations among the knowledge management outcomes. *Journal of knowledge management* 10 (44): 25-42.
- Al-Adaileh R and Al-Atawi M (2011), 'Organisational culture impact on knowledge exchange: Saudi Telecom context'. *Journal of Knowledge Management*, 15 (2): 212-230.
- Zack M, McKeen J and Singh S (2009), 'Knowledge management and organisational performance: an exploratory analysis'. *Journal of Knowledge Management*, 13 (6), 392-409.
- Hassan, N., Ismail, Z & Maarop, N (2014), Understanding Relationship Between Security Culture and Knowledge Management, *Knowledge Management in Organizations*, Volume 185, 2014, 397-402.
- Seraji, R., Ahadi Shoar, S & Abasi, A (2013), Study of the relationship between knowledge management and organizational culture Case study: agriculture organization of Qom, *International Research Journal of Applied and Basic Sciences*, ISSN 2251-838X / Vol, 4 (6), 1535-1542.
- Hassan, N.H. ; Adv. Inf. Sch., Univ. Teknol. Malaysia, Kuala Lumpur, Malaysia ; Ismail, Z. ; Maarop, N (2013), A conceptual model for knowledge sharing towards information security culture in healthcare organization, *Research and Innovation in Information Systems (ICRIIS)*, 2013 International Conference.
- Said, Abd Rahman, Abdullah, H & Abidin Mohamed, Z (2014), Relationship between Organizational Characteristics and Information Security Knowledge Management Implementation, *Social and Behavioral Sciences*, Volume 123, 20, 433–443.
- SAEED, T., TAYYAB, B., ANIS-UL-HAQUE, M., MUSHTAQ, A (2010), KNOWLEDGE MANAGEMENT PRACTICES: ROLE OF ORGANIZATIONAL CULTURE, ASBBS Annual Conference: Las Vegas.
- King, C., Osmanoglu, E & Dalton, C (2001), *Stock Image Security Architecture: Design, Deployment and Operations*, McGraw-Hill.