



The Role of Knowledge Management in Promoting Organizational Information Security

Babaei Mohammadreza¹, Abozar Solat Rafiei² and Hoda Takestani²

¹Department of Industrial Management, College of Management and Accounting, Yadegar - e- Imam Khomeini (RAH) Branch, Islamic Azad University, Tehran, Iran.

²Department of Information Technology Management, Islamic Azad University, Science and Research Branch, Tehran, Iran.

ARTICLE INFO

Article history:

Received: 1 February 2015;

Received in revised form:

28 February 2015;

Accepted: 16 March 2015;

Keywords

KM,
Information security,
Security factors of KM,
Present challenges in IS.

ABSTRACT

Considering the fact that approximately 80% of problems of organizational security have to do with negligence or lack of users' awareness of knowledge management (KM), the users' knowledge about information security has been identified to be one of the most fundamental issues in information security management. Accordingly, in the present study we analyzed different factors of knowledge management for recording, storage, sharing and dissemination of information security. The current paper is a type of descriptive-correlative in terms of collecting data and pragmatic in goal. The findings come from a field study on knowledge management experts at Iranian universities. Also, a questionnaire was the means for collecting the data. Finally, the data were analyzed using the partial least square and path analysis methods. The findings suggest that the information system users remarkably apply security factors of knowledge management. Furthermore, the authors realized that it is possible to use security factors of knowledge management by increasing the users' awareness in order to enhance informational security.

© 2015 Elixir All rights reserved.

Introduction

Not so long ago, competitive power and advantage of an organization or a human community was a parameter of extensive access to material resources (Ansari et al, 2012). However, presently transition from the Industrial Revolution and advent of the new millennium has essentially transformed circumstances, so that organizational development is not restricted to material resources and capital only. Yet, the most basic factor of comprehensive organizational and economic enterprises development in the contemporary world is "knowledge" (Davenport & Grover, 2001). Knowledge has changed to become one of the most critical strategic resources of organizations. Since then knowledge production stands to be crucial for gaining a competitive advantage and organizational success (Nonaka, 1995). Today, the most important competitive advantage of organizations is their ability in KM (Rahmanaiyousanlouee, 2011). Due to rapid pace of changes in IT technologies, new information threats have been generated. Thus, scholars have introduced new smart solutions of IS to decrease the risk of such threats. During the past decades, systems based on information security management systems (ISMS) like COBIT and ISO27001 have been created. That time onwards, an array of organizations adopted systems like ISMS. The KM is other management discipline aims to further reinforce effective management of knowledge (Walter S. L. Fung, Richard Y. K. Fung, 2008). There are occasions companies spend huge amount of money preparing Firewall, Proxy, Anti-Virus, intrusion detection mechanisms, digital signatures, network devices, protocols and so forth assuming technological solutions would be able to ensure information security. It is a common wrong belief since IS pertains to something beyond technological solution, and an end-to end management system indeed. Like any other comprehensive systems, this system consists of numerous components of the

public, policies, approaches, processes, standards and technology. Information may be stored in a server, personal computer, laptop, cell phone or any other device. Information may also be transferred place to place by some communication channels or they may be under processing by a program. Thus, IS could be overlooked in these situations. Being confidential, integrated and available are in fact three concerns in IS. All IS users function as entrance gates of a building. In each situation the user could be threatening for the IS of whole system. Reviewing different internal and external IS events, the researchers found that approximately 80% of the incidents occur as a result of internal staff negligence or due to disclosure of information and about 30% has happened because of hackers or other external causes (Yang yue jiang Yu yong xia, 2009). The second section of the present paper reviews the existing works and in the third section the research method to analyze the data will be introduced. Finally, we present the result in the section four and finish with providing the research model.

Related Works

Several different studies have examined KM. Gholi Zadeh (2004) states that there is a meaningful association between organizational culture and internalization and externalization of KM (Nikpour, & Salajagheh, 2010). Kangas (2006) worked on the relationship between organizational culture and KM innovations. The results indicate that in organizational culture KM may be an effectively strategic innovation and promotes long-time achievement, development of values and contribution to increased competitive advantage of organization (Rajaei pour, & Rahimi, 2008). Rouzdar (2002) understood that KM results in increased efficiency and so KM and performance positively correlate together. Marywood (2003) concluded that organizations with KM-based leadership and strong organizational culture perform much stronger in gaining knowledge, and analyzing complicated situations (Nazem et al,

Tele:

E-mail addresses: rafiei1358@gmail.com

© 2015 Elixir All rights reserved

2011). Martines et al believe that despite a majority of KM projects has initiated their activity providing a technological solution, organizational culture and leadership are two vital factors in KM programs success. The investigators also identified the factors affecting KM as organizational culture, motivation and skills, senior management, and structures, processes and IT (Abounouri et al , 2011).

Mathi (2004) considers culture, proper organizing of KM, strategy, system, IT infrastructures, measurement and effective and systematic processes as factors influencing KM. Holsappel and Joshi (2000) introduced the effective KM factors as technology, culture, management, organizational compliance, employees' motivation and external factors. In 1997, the researchers classified factors affecting the KM including: management of environmental factors and factors related to resources either human or material. Scream and Amidon (1997) identified seven key factors in implementation of KM as : strong commitment to business, knowledge leadership, architecture and vision, culture of generating and sharing knowledge, non-stop learning, organizational knowledge processes and developed technological infrastructures (Rahnavard & Mohammadi, 2009). Davenport et al (1998) performed an exploratory study on 31 KM projects in 24 companies. They extracted seven chief factors of success including the value of industry, multiple channels for knowledge transfer, shared language and purpose, flexible and standard structure of knowledge, knowledge – friendly culture, technical and organizational infrastructures, motivational activities, and supporting KM . Chourides and colleagues (2003) and Hasanpour et al (2010) worked on factors like culture, IT, management, organizational structure, strategy, training, human resources, and positive attitude towards changes, knowledge processes and motivational awards. They concluded that factors of leadership and manager support from KM implementation and proper sharing of knowledge among members show he highest significance. Considering the national modern economies are entirely dependent upon IT, today need for information and information system security seems inevitable. Meanwhile, the need for protection of information and reduced risk compared to earlier time is more critical (Schou & Trimmer, 2004). Various national studies have confirmed attacks to organizational informational resources (Bagchi, Udo 2003, Ammete, Gardner , Hochwarter , Ferris , 2002, CERT Statistics, 2004). On the other hand, by increasing development of IT and expansion of communication networks, vulnerability of the information exchange atmosphere has intensified and as a result more complicated threats have appeared .therefore, marinating the security atmosphere of information exchange is of imperative purposes of information and communication development (Veiga & Eloff,2010; Kruger& Kearnney,2006; Wilson &Hash, 2003).

One significant strategy for protecting and managing IS is increased awareness of IS users. In this regard, users will obtain required information relevant to their role and responsibility in improvement of IS in their own business (Von Solms & Von Solms, 2004). In fact, being acquainted with IS leads to some changes in users' behavior and consequently reinforcement of good security activities. It also allows the user to be responsible to IT security (Wilson &Hash, 2003) and gradually becomes an organizational culture (Kruger & Kearnney, 2006, Niekerk & Solms, 2009). Currently, a majority of studies have been conducted on information systems security (ISS) have investigated technical issues, so attitudes toward ISS as a technical problem

has a significant dominance over the ISS studies (Magklaras Furnell ,2002, Kathleen & Carley, 2000, Hinson, IsecT Ltd 2003, Gonzalez, & Sawicka 2002, Theoharidou, 2005, Hinson, IsecT 2003, Kotulic,& Clark, 2004). Another study tried to find out the effect organizational characteristics on information security knowledge management implementation. The result shown the positive relationship [Abd Rahman Said, Haslinda Abdullah, Jegak Uli, Zainal Abidin Mohamed, 2014]. However, no independent research has explored the impact of KM on IS so far. Few studies have been conducted on IS in which some models were tested experimentally and human factors and organizational and management structure have been used, but employees' behavior has been overlooked instead the behavioral consequences were considered (Basie von Solmsa, 2005).several scholars have attested lack of independent research on IS (Bagchi, & Udo ,2005, Bento & Bento ,2004, Basie von Solmsa, Rossouw von Solms ,2004).

Km Factors Affecting Organizational Information Security

For successful designing of factors of sharing KM, we need to apt a strategy. Hansen and colleagues have introduced two major strategies of KM.

- **Development:** development refers to a strategy peoples adopt for documents including internet loading, and database.
- **Customization:** customization is people to people strategy. It is used to connect individuals together and for growth of networks and communities utilize the strategy

Factors of KM are used for promotion of IS are as follows

- **Documentation:** advanced content management systems (CMSs) consist of facilities for secure explorations, writing patterns, maintaining integration of web pages links, periodical evaluation , archiving, meta-data, version control, configuration rules, indexing, audit, authorized access, management alarms and flexible use change for different operating systems and formats.
- **Classification:** excessive supply of information or “digital distribution” in internal networks has caused users inability to fid relevant information in a timely manner and so, numerous classification factors have been created. Classification must reflect needs, behaviors, duties and users' words and be able to provide different strategies and attitudes. Classification has to be easily used and users can understand and apply it effortlessly. This therefore helps users find their favorite knowledge of information security.
- **User Grouping:** Online communities are emerging as a powerful factor for sharing and preservation of knowledge. This is an important factor for sharing knowledge among coworkers as well as a substantial component for rapid distribution of IS data to other group like information about a new virus attack. Sharing an experience or an expertise is a useful strategy for connecting skilled workers in such communities. The on-line communities especially in field of security problems are effective to solve the existing problems.
- **E-Learning:** one astounding advance of KM is increasing convergence of attitudes among the KM community and the E-learning one. The KM and learning management are two supplementary disciplines are continuously getting closer together and as a result supporting innovative investments. In order to train new workers in IS and educating new security technologies, the e-learning could be highly influential.
- **Invention:** with new technologies and more efficient access to experts besides benefiting from old technologies, KM contributes to organizational productivity. Noble innovative ideas and IS solutions can use these systems and be developed.

In the present study five mentioned factors are examined as we believe that by increasing them for users, IS could be enhanced.

Research Method

In the present study the authors first prepared a list of IS benchmarks using the Internet and other available resources. Then, they explained the assessor group, all were computer experts working at the university units, a final checklist was prepared and the group agreed to collaborate to evaluate the IS status of university units. The benchmarks include:

- -fields relevant to management
- -fields relevant to training and informing
- -fields relevant to organization dependency to employees
- -fields relevant to access and access rights
- -fields relevant to organizational procedures
- -fields relevant to control
- -fields relevant to security policies
- -fields relevant to documents
- -fields relevant to software and hardware
- -fields relevant to network
- -fields relevant to users

During the assessment, the researchers applied three checklists according to Table 2 in 11 fields in each university unit. The status of system users based on the employment at four university units is as follows: In the current research, each item is scored 1 if the university has the standard criteria and otherwise it is scored 0 . Although, most of academic units have used the security software for years it seems that there is still an urgent need for identification of KM principles and basics in order to enhance IS. As Table 1 shows, identification and increase of security in technical problems is the central subject.

Research Model

Generation and use of knowledge has a long history, yet the role of KM in IS is a relatively new subject in Iran. There exists few studies on the role of successful KM in gaining IS at universities. So, organized investigations are rarely available. No independent research has considered the way KM can be used and the impact of successful implantation of KM in IS . The authors in the present research adopted factors were also used in (APQC:Wong, 2005; Awazu, 2006; Yeh et al, 2006) research models. Moreover, we tried to provide a wide range of the factors were previously examined in form of a new conceptual model after asking for the experts' opinions in Iran. Considering the conceptual model and the research goals, the following research hypotheses are addressed:

- **H1:** using KM positively associates with increased IS.
- **H2:** documentation positively associates with KM success.
- **H3:** Classification positively associates with KM success.
- **H4:** user grouping positively associates with KM success.
- **H5:** E-learning positively associates with KM success.
- **H6:** invention positively associates with KM success.

According to the research purposes , the conceptual model is as below:

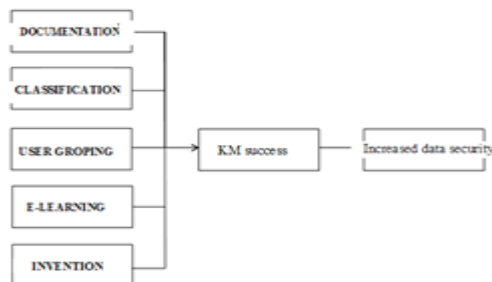


Fig 1. The Conceptual Model

Research Population And Sample

The research population for the present study consists of IT managers, and KM experts at universities. All managers and counselors of universities in Tehran form the population. But, because of limited number of experts at the universities, a referendum was conducted. Also, due to essential differences between the universities, we used multi-stage sampling method (Alerk,1995). Finally, items for measuring the research variables were designed after reviewing previously performed studies. Except for the demographical items, the authors adopted the Likert scale to grade the items. Furthermore, since the original list of standard items was in English, the researchers first translated them into Persian then the new questionnaire validity and reliability were measured. So, a pilot study was conducted and ambiguous and irrelevant items were identified and removed from the questionnaire. Then, the modified instrument was distributed among the participants. The Cronbach's alpha was a means to calculate the instrument reliability. The alpha value was equal to 0.76.

Findings

From total number of 90 distributed questionnaires, 62 complete questionnaires backed. Table 2 present the demographical results.

The investigaors applied the partial least square method to analyze the data . the advantage of this technique is possibility of component-based estimation of the variables impact on the model. The PLS has the lowest limimitation in terms of sample size, measurement scale, and distribution of residues (Chung Hung et al, 2005). Generally speaking, the PLS has a high potential in investigating the variables relationships in complex models. The data then were analyzed using the PLS Graph software. Fig.2 shows the PLS Graph and standard regression coefficient.

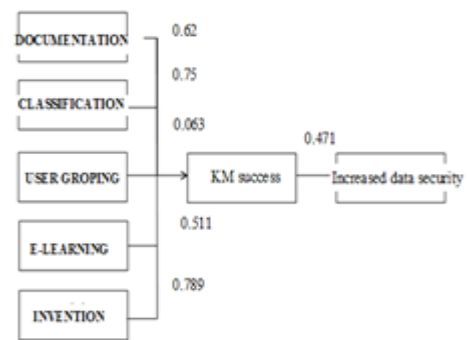


Fig 2. The Dependent Coefficients

After computation of the path coefficients indicating probability of each variable impact on the successful KM implementation, the researchers assessed the variables. The H2 to H6 measures the relationship between documentation, classification, user-grouping, E-learning, invention and KM implantation. Since the obtained path coefficients are positive for the variables, the hypotheses are confirmed. Fig. 3 illustrates the path coefficients for the variables.

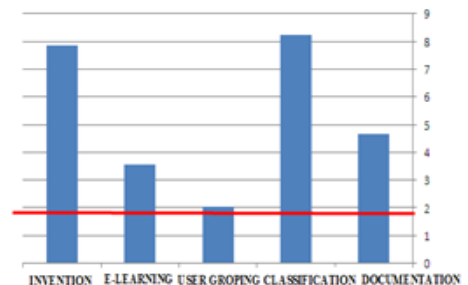


Fig 3. Standard Error of Measurement

Table 1. Universities Status in Terms of IS

	Security sections	Universities score				Number of checklist items	score
		U1	U2	U3	U4		
1	Security policy	0	0	0	0	4	4
2	Organizational security	1	1	1	1	15	15
3	Monitoring and classification of assets	1	0	1	1	4	4
4	Personnel security	1	1	1	1	13	13
5	Environmental and physical security	12	12	12	12	30	30
6	Operation and communication management	32	28	28	32	55	55
7	Access control	20	20	20	27	48	48
8	Maintenance and development of systems	14	14	14	14	32	32
9	Integrated information management	0	0	0	0	13	13
10	Confidentiality	1	1	1	1	16	16
11	router	36	37	37	37	53	53
12	Physical security checklist	2	2	2	2	24	24
	total	120	116	113	128	307	307

Table 2. A Summary of Questionnaires Data

Variable	Age (year)	gender	Education(year)	Job history	Working with KM (month)
Mean score	45	68% male	4.25	10.5	36

Table 3. Path Analysis Coefficient of Km Variables and IS

Variable	Path analysis	t-test
Information security	0.569	3.42

According to the H1, positive impact of successful implementation of KM has a positive impact o increased security. Since the path analysis value of the independent variable and ratio of estimation to standard deviation is higher than 1.96, the H6 is confirmed. Table 4 shows the path analysis.

Conclusion

It is important to ensure the success of KM in identification of effective factors on the KM success to implement the KM for increasing organizational information security and consequently useful adoption of limited organizational resources, decreased rate of employing human resources, materials and time and still expect to achieve favorite results. Since the present study investigated small and medium sized universities, reviewing factors influencing any decision on KM implementation would be essential. So, the current research investigated and compared factors affecting the KM success in several previously performed studies. Combining the factors, the authors designed a set of relevant factors to employment of KM in IS after asking for the experts’ opinions. The researchers extracted the factors of IS for universities on the basis of experts’ remarks. After conducting the survey, the results suggest that the independent variables could properly explain changes in the dependent variables. The correlation of determination of the KM success was equal to 0.569. This means that the independent variables could properly account for the KM success. Moreover, the coefficient of determination value for the increased IS variable shows that applying the KM system has a slight effect on increase of IS. This result therefore accords with the H1 result i.e. positive impact of employing the KM systems on the increase of IS. Considering the KM success factors, five independent parameters entered the conceptual model. The result indicates that all variables are statistically meaningful in successful implementation of the KM. also, significant decrease of the path analysis value for the user grouping variable could be because of emerging use of these system in organizations and overlooking the user grouping in implementation of new management systems. Thus, as these systems are gradually appearing in Iranian organization, public declaration about usage

of these systems firstly needs time. Secondly, adopting these systems must become an integral part of organizational strategies and employees are trained to use the systems. The coefficient of determination for the KM implementation is equal to 0.569.

Future Studies

We present the initial model of KM which makes contribution to organizational information security as follows. The model consists of three parts (Fig.1):

- **Collection:** in this section we stored knowledge relevant to IS.
 - Standards: information security standards
 - Best methods: selection of successful methods
 - Threats and solutions: whole threats and options we had.
- **Sharing and distribution of knowledge:** this section has to do with sharing knowledge among beholders, distribution of knowledge among relevant peoples and updating the IK library with new knowledge by users.
 - Domestic experts
 - Domestic users
 - Foreign users and experts
- **Implementation:** in this section we intend to see whether the model is operated in the organization and entire information management of knowledge security are effective.
 - implementation in the users’ section
 - Implementation in the experts’ section

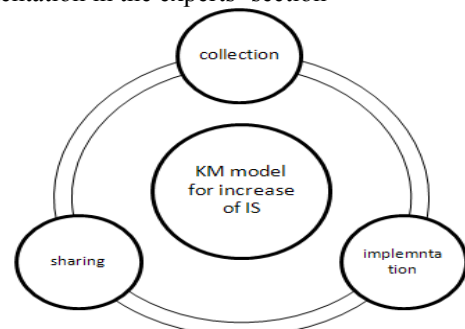


Fig 4. Increased is Model by KM

References

- Abd Rahman Said, Haslinda Abdullah, Jegak Uli, Zainal Abidin Mohamed. (2014) Relationship between Organizational Characteristics and Information Security Knowledge Management Implementation, *Procedia - Social and Behavioral Sciences* 123 (2014) 433 – 443
- Abounouri, E., Saeidi, P., Niaiz, I., and Zanganeh, M. (2011). An analysis on KM infrastructures at selected universities. *Journal of Educational Management*, 3(1), 93-113.
- Ammeter A, Douglas C, Gardner W, Hochwarter W, Ferris G. Toward a political theory of leadership. *The Leadership Quarterly*; 13:751-96, 2002.
- Ansari M. Rahmany Youshanlouei H. and Mood M. (2012). A conceptual model for success in implementing knowledge management: A case study in tehran municipality, *Journal of Service Science and Management*, 5(2), 212-222. doi: 10.4236/jssm.2012.52026.
- Bagchi, K. and G. Udo, An Analysis of the Growth of Computer and Internet Security Breaches. *Communications of the AIS*, 12(46): p. 684-700, 2003.
- Bagchi, K. and G. Udo, An Analysis of the Growth of Computer and Internet Security Breaches. *Communications of the AIS*, 2003. 12(46): p. 684-700, 2004.
- Basie von Solmsa, Rossouw von Solms, From information security to business security?, *Computers & Security*, 24, 271-273, 2005.
- Basie von Solmsa, Rossouw von Solms, The 10 deadly sins of information security management, *Computers & Security*, 23, 371-376, 2004.
- Bento, A. and R. Bento, Empirical Test of a Hacking Model: An Exploratory Study. *Communications of the AIS*, 14(32): p. 678-690, 2004.
- Chourides, P., Longbottom, D., Murphy, W. "Excellence in knowledge Management: an Empirical Study to Identify Critical Factors and Performance Measures", *Measuring Business Excellence*, Vol. 7. No. 2, pp. 29-45, 2003. Computer Emergency Response Team (CERT), CERT Statistics. 2004.
- Davenport T. & Grover V. (2001) .Knowledge management. *Journal of Management Information Systems*, 18(1), 3-4.
- Davenport, T., De Long, D. and Beers, M. "Successful Knowledge Management Projects", *Sloan Management Review*, Vol. 39, No. 2, pp.43-57, 1998.
- Gary Hinson, IsecT Ltd, Human factors in information security, Innovative information security awareness programs, NoticeBored, 2003.
- Gary Hinson, IsecT Ltd, Human factors in information security, Innovative information security awareness programs, NoticeBored, 2003.
- Hasan pour, H., Jahanshahi, H., and Ahmadi, M. (2012). Identification and analysis of effective factors on rate of universities readiness to successfully implement KM. *Journal of Parks and Development Centers*, 8(30), 43-50.
- Holsapple, C.W., Joshi, K.D. "An investigation of factors that influence the management of knowledge in organizations", *Journal of Strategic Information Systems*, No. 9, pp. 235-61, 2000.
- Jorma Kajava and Rauno Varonen, IT and the Human Body and Mind in the Information Security Perspective, European Intensive Programme on Information and Communication Technologies Security, IPICS'2002, 3rd Winter School. Oulu, Finland. April 2-9, 2002.
- Jose J Gonzalez, Agata Sawicka, A Framework for Human Factors in Information Security, Dept. of Information and Communication Technology, Agder University College, Presented at the 2002 WSEAS Int. Conf. on Information Security, Rio de Janeiro, 2002.
- Kathleen M. Carley, Information Security: The Human Perspective, Dept. of Social and Decision Sciences, Carnegie Mellon University, August 2000.
- Kotulic, A.G. and J.G. Clark, Why There Aren't More Information Security Research Studies. *Information & Management*, 41(5): p. 597-607, 2004.
- Kruger, H.A. and Kearney, W.D. (2006). A prototype for assessing information security awareness.
- Magklaras G, Furnell S. Insider threat prediction tool: evaluating the probability of IT misuse. *Computers and Security*; 21(1):62-73, 2002.
- Marianthi Theoharidou, Spyros Kokolakis, Maria Karyda, Evangelos Kiountouzis, The insider threat to information systems and the effectiveness of ISO17799, *Computers & Security*, 24, 472-484, 2005.
- Nazem, F., Karim zadeh, S., and Ghaderi, E. (2010). The relationship between KM, organizational health and employees' entrepreneurship in social welfare organization. *Journal of Social Research*, 3(9), 93-99.
- Nik pour, A., and Salajagheh, S. (2010). The relationship between KM and organizational culture from faculty members of Kerman university of Medicine, *Journal of Management*, 4(14), 9-10.
- Nikrerk J.F. and Solms, Van (2009). Information security culture: a management perspective.
- Nonaka I. & Takeuchi H. (1995). *The knowledge creating company*, Oxford university press Oxford, UK.
- Rahmaniyoushanlouei, H. (2011). Designing KM success model with multiple level approach. M.A. dissertation, MBA, University of Tehran.
- Rahnavard, F., and Mohammadi, A. (2009). Identification of key success factors of KM systems at universities of Tehran. *Journal of Management and IT*, 1(3), 37-52.
- Rajaeipour, S., and Rahimi, H. (2008). The relationship between transforming KM and performance of faculty members of Isfahan, 8(4), 65.
- Schou, C.D. and K.J. Trimmer, Information Assurance and Security. *Journal of Organizational and End User Computing*, 16(3): p. i-vii, 2004.
- Security Culture. *Computer & Security*, 29(2), 196-200. training program. National Institute of Standards and Technology, sp 800-50, 20-79.
- Veiga, A. Da., and Eloff, J.H.P. (2010). A Framework and Assessment Instrument for Information Von Solms, B. (2000). Information security - the third wave. *Computers & Security*, 19, PP. 15-19.
- Walter S. L. Fung, Richard Y. K. Fung, (2008), Knowledge-Centric Information Security, International Conference on Security Technology, IEEE Wilson, Mark, and Hash, Joan. (2003). Building an information technology security awareness Yang yue jiang Yu yong xia, (2009), Behavioral science-based information security research, First International Workshop on Education Technology and Computer Scition Technology and Computer Science IEEE.