J. Appl. Environ. Biol. Sci., 5(9S)428-438, 2015

ISSN: 2090-4274
Journal of Applied Environmental and Biological Sciences
www.textroad.com

An Evaluation of Impacts of Knowledge Management System and Management Information System in Increasing International Organizations' Information Security

[1]Abozar Solat Rafiee, [2]Mahsa Jadid Tavvaf, [3]Akbar Alem Tabriz, [4]Mohammadreza Babaei

[1,2] Department of IT Management, Science and Research branch, Islamic Azad University, Tehran, Iran
[3]Department of Industrial Management, Shahid Beheshti University, Tehran, Iran
[4]Department of Industrial Management, College of Management and Accounting, Yadegar - e- Imam Khomeini (RAH) Branch, Islamic Azad University, Tehran, Iran

Received: March 26, 2015
Accepted: May 17, 2015

ABSTRACT

Knowledge Management (KM) and knowledge-based activities are presently focused by all organizations and experts at different arenas of the society. A management information system is one which is able to provide information for activities performed by managers at an organization. Currently, this term is exclusively used for computer systems that are composed of hardware and software and save, process, and retrieve data. Large-scale volume of the information within the framework of plans, drawings, policies, bylaws, commercial letters, documents of research projects, etc., provokes us to take meticulous measures for retaining such data. Above-said information is the key to an organization's advancement and growth. If we fail to keep such data secured from strangers and other threats, we would be strongly damaged. Information security is a vital issue that had entangled worldwide organizations. This article is aimed at examining the direct impact of KM and management information systems in elevating the level of information security in international organizations at the International Diabetes Prevention and Control Association. According to the data obtained from hypothesis tests, there is a significant relationship between KM system and management information system, on the one hand, and elevating the level of information security, on the other. Moreover, there is a significant relationship among components of management information system, i.e., software, hardware, databases, human resources.
KEY WORDS: Knowledge management system; management information system; information security.

1. INTRODUCTION

Knowledge is, presently, regarded as an organization's investment, and managers have found that retention of such intellectual capitals is more important than ever. Due to their key role in achieving competitive advantage, intellectual capitals have been changed into strategic resources of organizations (Cech, P. and Bures, V., 2000). With the advent of information and communication technologies (ICT), there has been an improvement in both manners of traditional saving and transferring, and effectiveness and efficiency of general knowledge transference mechanisms (Lin, B. and Umoh, D., 2002). As the most valuable capitals of an organization, intelligent and knowledgeable workers, thanks to their creativity and innovation, are responsible for establishment of modern organizational processes, foundation of cutting-edge technologies, and development of new products and services aimed at achievement of stable competitive advantage. Innovative attempts are the fruits of purposeful investment in the process for knowledge management learning and improving. Management information systems are principal instruments for solving problems and making decisions, and a wrong application of them results in disqualification of decisions. Management information system provides the information required for strategic, tactical, and operative decisions as well as all subsystems within an organization. In the present-day commerce, information plays the role of an organization's *capital*, a retention of which constitutes one of the factors which help the organization keep breathing. Globalization of economy has provoked an intensification of competitions at global scales whereby many companies are inevitable to cooperate with others to prolong their presence at global scenes. Consequently, vital are categorization, evaluation, and maintenance of information resources for an organization. Increasing growth of information technologies and networks has, however, escalated vulnerability of information communication spaces, and addressing said threats is becoming more complex. Therefore, security of information communication spaces is one of the most important purposes held by the ICT (Veigaand Eloff, 2010).This article is aimed at measuring the direct impact of KM and management information systems in elevating the level of information security at the International Diabetes Prevention and Control Association.

* **Corresponding Author:** Abozar Solat Rafiee, MSc Student of IT Management in Azad University of Science and Research of Tehran

2. Knowledge Management System

Data is changed into information through summarizing, modifying, calculating, clustering, and documenting. Information, in its turn, is transformed into knowledge by means of comparison, investigation of peoples' interactions, consideration of repercussions, and making them practical. Knowledge Management (KM) is a type of managing by means of the processes whereby organizations make attempts to identify, utilize, develop, organize, and share knowledge (Hsia, T., Lin, L., et al, 2006). In fact, an effective and efficient management of knowledge requires a suitable combination of managerial, social, and organizational initiatives, as integrated by appropriate technologies (Selsky, D., B., Eisenberg, F., P., et.al, 2001). In the age of information, KM has been experienced as one of the most promising ways to achieve success and increase competitive capability (Marwick, A., D., 2001). KM is interpreted as increase of innovation and reactivity (Mohayidin, M., G., et al, 2007). This process can be pigeonholed into different sections: creation of internal knowledge, acquisition of external knowledge, storage of knowledge as documents instead of saving in routine work, updating knowledge, and sharing internal and external knowledge (Malone, D., 2002). KM includes all methods whereby an organization directs its knowledge assets: the manner to collect, save, utilize, update, and create knowledge. Through altering human capitals into organized intellectual assets, KM builds value for the organization. In the age of information, managers intend to make use of KM techniques and solutions at all organizational levels by understanding importance and value of knowledge in decision-making processes.

KM systems are a body of information systems to make use of organizational knowledge (Malone, D., 2002). IT-based systems are established to support and improve the processes for creation, storage, transference, and utilization of organizational knowledge (Newman, B., Conrad, K., W., 1999). Many KM initiatives refer to IT as an important infrastructure. IT process has, recently, provoked an increase in KM capabilities which were formerly improbable. For instance, finding an expert from registered source of knowledge using online encyclopedias and search databases, sharing knowledge through internet and intranet, getting access to previous information or projects, and learning about customers' needs by delving into the data at hand. As a matter of fact, many new IT applications are operated to support organizational KM and its duties (Barnes, S., 2002). At the present age of globalization, those organizations would be successful which could make effective use of all their personnel's knowledge reserves at all levels. Consideration should be given to such issues as content, connection, society, culture, cooperation, and investment aimed at achievement of successful KM processes. Following are some factors which play significant roles in successful KM processes at organizations:

1. Leadership and senior management (support);
2. Organizational culture;
3. Processes in the KM;
4. Controlling explicit knowledge;
5. Exploration of implicit knowledge;
6. Knowledge clubs;
7. Improvement of knowledge market;
8. Measurement methods;
9. Increase in number of people performing the duties and their skills;
10. Technological infrastructures.

KM systems provide with the organizations the structures required for establishment of KM processes. Accomplishment of KM systems, just like any other systems, depends on making effective uses by users. Therefore, getting insight into organizational needs and, thus, users' demands give a golden hand to admission of such systems and their successfulness. Depiction of a body of intra-organizational relationships which facilitate/obstruct knowledge creation and transference among users is a way to get insight into organization's and its users' demands. Cooperation, sharing, and transference of information and knowledge depend on anyone's relationships and his/her interest for making cooperation. Therefore, application of an organizational analysis method, which is able to contribute to understanding informal and cooperative intra-organizational networks, will allow system analysts to understand cooperative processes, knowledge-sharing flows, and intra-organizational information. This helps managers make decisions and offer proposals to improve cooperation, manage knowledge, and recognize the capabilities required for a KM system. Creating, sharing, coding, and applying knowledge are known as key processes for successfulness of knowledge-based organizations. On the other hand, in such organizations, activities are not repetitively and monotonously performed, and people seek knowledge-sharing for completing their tasks. Basically, KM contains two bases: KM activities and KM system functions.KM activities present a process perspective of knowledge management; while, KM system functions are to do with technological aspects and are defined as functions which facilitate/complement KM activities by means of certain applicable technologies and utilities.KM systems are classes of information systems which are used for managing organizational knowledge. They are IT-based systems which have been developed to support and improve organizational processes for creation, storage, retrieval, transference, and utilization of knowledge.

3. Management Information System

Management information systems (MIS) are composed of a mixture of computer-aided human attempts to collect, store, and retrieve information using communication systems to apply desired management on an organization's activities. MIS is an official system in an organization that provides required reports with the managers to enable them to make decisions at different levels of the organization (Schoderbek P.P., et.al, 1975). Official and unofficial systems provide old and present information and that relevant to future plans in oral and written forms as related to internal operations of the organization and its environment. Such information is used by managers, personnel, and key components of the organization in decision-making processes in an appropriate time framework. MIS is a sort of computer information system that is able to collect and process information from different sources and provide it for completing decision-making processes. Such information systems, in fact, process the information generated by Transaction Processing System (TPS) and present it to the manager as a report in a significant mold. To put it simply, MIS facilitates managers' responsibilities by means of generating summarized, structural reports on an orderly, repetitive basis. A MIS's output is, in addition, used to control, plan, and arrange an organization's activities. MIS offers a general framework, based on which to coordinate other information systems. Presently, MISs are regarded as a body of subsystems which are designed and operated as necessity arises. Therefore, an organization, aimed at meeting managerial needs at different levels in different modes, is able to have several related information systems rather than a single, general one. Experience shows that establishment of a wholly integrated system is very complicated and, even, impossible, since there are many factors which are to be considered both together and simultaneously (Davis, G.B., and Olson, M.H., 1985).

4. Physical Components of MIS

There are important factors in a MIS, including:

1. Hardware: technical equipment, hardware for information processing, storage, and retrieval;
2. Software: system software and utilities;
3. Database: non-redundancy, transparency of data, well-timed updating, compilation of standards, and policies for getting access to databases;
4. Human forces: programmers, IS managers, IT advisors, etc.

5. Information Security in Organizations

Organizations all around the globe confront a vital issue: information and information systems security. Three items are professed as the basics of information security:

- Reliability: making sure that information is accessible only for those who are authorized;
- Comprehensiveness (coherence): maintaining accuracy and completeness of information and processing methods; and,
- Accessibility: ensuring that users can get access to information as a need arises.

Gaining access to these factors is referred to as effectiveness of security in information systems.

Information security is observed from different aspects. Information systems security can be addressed from two sides: technology and people.

Gary Hinson asserts that information security includes both technology and individuals. But, most organizations regard technical solutions as the instant replies to their security issues, while there are many obstacles for a mere technical approach, including:

1. Technology is packable;
2. Quantitative organizations should well understand their security problems in a proper manner in order to make use of appropriate technical solutions thereof;
3. The term "technical solution" comes with a high expense;
4. Beside their effectiveness, security technologies can be improperly used or damaged by users, the process which will lead to effectiveness failures (Gary Hinson, 2003).

IBM suggests that there would be smaller and more clandestine attacks in 2006 on organizations' information systems, the attacks which are grounded upon users' nonchalance and oversimplification. David Mackey, director of security intelligence at IBM, in Armonk, N.Y, believes that *users* will be still abused as the most vulnerable elements in security models. Basie von Solmsa and Rossouw von Solms (2004) published their article entitled "Ten Fatal Mistakes in Managing Security of Information Systems," in which following ten mistakes were considered as ISS pernicious errors, indicating that if even one of such aspects is wholly or partially disregarded, serious problems would occur in an ISS program. A major part of such errors are based on human factors and issues thereof.

In 2006, moreover, "Information Security: Fourth Wave" addressed four waves of information security so far (Basie von Solms, 2006). First wave was technical, in which technical solutions were offered to security issues. Second wave indicated that information security has a powerful management dimension such as policies and managerial involvements which are important as much. Third wave contained the need for having

information security standards in companies and aspects such as best management practices, affirmation of a suitable culture for information security, and measurement and supervision over information security. Fourth wave was concerned about designation of categorical role of the manner whereby information security is administered. All above-mentioned factors should work together to ensure that reliability, comprehensiveness, and accessibility of a company's information assets are secured as at all times. Recently, a new pattern on information security is established that looks into the issue as a *human issue* and *organizational issue* (Knapp, K.J., et al., 2004).

Presently, accomplishment of information security seems to be largely dependent upon effective behaviors of its users. Constructive behaviors by users, system managers, and others can greatly elevate effectiveness of information security. Improper behaviors, on the contrary, can obstruct effectiveness. One of the important ways to sustain and manage information security is to improve users' awareness levels thereon. In this way, users would obtain required insights into their roles and responsibilities respecting the area of information security (Von Solms& Von Solms, 2004). Awareness of information security provokes users to change their behaviors and improve their good security practices, enabling them to be responsible for and concerned about IT security (Wilson & Hash, 2003). This will be gradually changed into a culture in different organizations (Kruger and Kearrney, 2006; Niekerk and Solms, 2009).

6. LITERATURE REVIEW

Ken McPhail (2009) addressed ethics in the age of knowledge. Although, since the present article is confined to ethical indices in KM dimensions, only ethical parameters related to KM dimensions are extracted, as delineated hereunder together with their relationships with each KM dimension a per the general KM paradigm: knowledge creation, organization, distribution, and utilization.

Azmi (2010) referred to such issues as ownership, accuracy, assistance, confidentiality, sincerity, and commitment in knowledge creation, organization, and utilization (Azmi, I.M., 2010). Wing et al. consider group confidence as effective in publication and distribution of knowledge (Wing S.C. and Chan, L.S., 2008). Chua (2002) regards personal reliance, assistance, and commitment as effective in knowledge creation (Chua, A., 2002). Hutchings and Michailova (2004) focus on the role of group reliance in distribution of knowledge (Hutchings, K. and Michailova, S., 2004). Huysman and Wit (2004) regard as effective helping others and conscience in distribution of knowledge (Huysman, M. and de Wit, D., 2004). Inkpen (2005) considered as important both group and personal reliance in distribution of knowledge (Inkpen, A.C. and Tsang, E.W.K., 2005). Lang (2004) emphasized on the role of ownership and loyalty in utilization and distribution of knowledge (Lang, J.C., 2004).

There are, in addition, studies carried out on the factors impacting on admission and development of KM systems (Chan, K. and Liebowitz, J., 2006), identification of indices formeasurement of KM system performance and the manner to improve quality of KM systems (Tseng, S.M., 2008), definition of qualitative dimensions of KM systems (Rao, L. and Osei-Bryson, K.M., 2007), and investigation of the factors influencing on establishment of KM systems and investigation of the relationship among such factors (O'Donovan, F., Heavin, C. and Butler, T., 2006). These studies have, in one kind or another, been conducted aimed at understanding the relationship between typical KM-related needs of organizations. To extract needs of KM system users, Ravishankar and Pan Shanmade attempts to identify socio-cultural backgrounds of organizations through conducting fifty face-to-face interviews and unofficial observations and documents. They, using such recognitions, presented some solutions to improve KM in organizations. In addition, Mugellesi et al. (2008) identified main branches of knowledge in an organization and weighted their importance in short-, medium-, and long-term through knowledge auditing. Then, they extracted KM needs for preservation, sharing, and improvement of identified knowledge, presenting suitable solutions in each area for eliminating identified gaps. This is used upon designation of a KM system in an organization. Wong and Aspinwall have explained in the framework of a case study the manner to develop KM and KM systems in an organization (Wong, K.Y. and Aspinwall, E., 2006). They, first of all, identified knowledge areas in an organization and, then, specified individuals' responsibilities in an organizational KM system. Finally, they re-categorized organizational knowledge information based on identified knowledge areas, developing manuals for each person.

Dave and Koskelaargued that a knowledge-type study is necessary to implement any sort of KM solution in an organization (Dave, B. and Koskela, L., 2009). Based on the categorization by Dawevport, they argued that the cooperative knowledge model is suitable for KM in the construction industry. Moreover, they, in their case study, identified KM-related problems of construction area and extracted users' needs through workshops and interviews to select a system enabled to support cooperative work. They selected a system which was able to respond to users' problems and needs. Based on theory of Task Technology Fit (TTF), Hahn and Wang argued that designation of diverse KM systems is different for every knowledge task (Hahn, J. and Wang, T.W., 2009). They demonstrated that the type of KM system appropriate for divergent knowledge issues that is able to

support production. On the contrary, for convergent problems, a KM system whose purpose is to select knowledge and supports knowledge analysis and transparency is more effective.

On information security, there are quantitative studies in which models are empirically tested and constraints and structures related to human factors and behaviors and/or organizational and managerial structures are used. Such little studies have focused on behavioral results rather than individuals' behaviors (Kotulic, A.G. and J.G. Clark, 2004; Basie von Solmsa, Rossouw von Solms, 2005; Jorma Kajava and Rauno Varonen, 2002).

Many information security scholars and experts have emphasized on shortage of empirical research in such aspects (Bagchi, K. and G. Udo, 2003; Bento, A. and R. Bento, 2004; Basie von Solmsa, Rossouw von Solms, 2004). Gonzalez introduced human factor as the Achilles' heel of information security (Jose J Gonzalez, Agata Sawicka, 2002). Chang and Whua (2005) addressed the factors which were of impact in implementation of information security management. Stressing on organizations' need to managerial structures for guarding their information assets, they considered such security structures as an effective weapon required to keep breathing in present-day competitions. Based on research findings, IT managers' abilities and lack of environmental certainty have left a positive impact on organizations' implementing their information security management and BS7799 standard.

In addition, findings showed that organizational factors including organization's size and type of industry greatly influence on application of information security management (Cheng, K., 2005). Mahabi (2010) investigated awareness of information security as viewed by system managers and end users in Florida State University. Results indicated that system managers emphasize more on external and technical threats than internal and non-technical ones ensuing from such different factors as resource accessibility, behavior to personnel, and satisfaction from technical instruments. Second part of the study, which was focused on final users, was indicative of necessity of paying attention to users' needs and improvement of their awareness levels to be equipped with guarding tools against security threats. Results were expressive of importance of human factors in information security (Mahabi and Victoria, 2010). Tintamusik (2010) investigated the relationship between an organization's systems and awareness of information security. This study focused on the vital relationship between organization's systems within the theory of organizational behavior and Information Security Awareness (ISA). Key in this study was lack of awareness by users of security issues as a deterrent factor for organizations in defending against cyber-attacks. According to the findings, there is a significant relationship between users' awareness of information security and official dimensions of the organization, aspects of organizational culture, and HR policies and methods (Tintamusik, Yanarong, 2010).

Wu (2008) used a combination of ANP and DEMATEL methods to appraise KM strategies (Wu, W. W., 2008). Also, Tseng (2011) used the same two approaches to evaluate KM environmental capabilities (Tseng, M. L., 2011). Maconacchy et al. (2001) addressed important aspects ofinformation security. According to main characteristics (accessibility, accuracy, and reliability), security initiatives (technology, policies, procedures, training, and awareness) and information status (data transference, storage, and processing), achievement of information security was investigated. In their study on awareness level of workers at international mines companies of information security, Kruger and Kearrney (2006) achieved significant results. They divided awareness into three levels: knowledge, attitude, and behavior. Areas to be addressed in these three levels were commitment to policies, generation of powerful passwords and keeping them safe, internet and emails, safety of mobile equipment in data transfers, reporting security events, and suitable actions and reactions. The researchers concluded that personnel's awareness levels are generally average and they need additional attentions and attempts at each knowledge area. In another study, Chang (2007) concluded that organizational culture had direct influence on establishment of information security culture. Organizational components contain cooperation, innovation, coordination, effectiveness, and efficiency on information security principles (privacy, availability, accuracy, and responsibility). Results showed that all organizational culture factors are of positive impact on information security components. In one of the principal studies, Choi et al. (2008) drew to the conclusion that increase in management awareness and users' knowledge of information security have direct impact on the manner managers perform and personnel express security-involved behaviors. This will result in an improvement of organization's performance.

Elsewhere, Veiga and Eloff (2010) provided a framework for establishment of information security culture. They grounded their model on the basis of the fact that some components such as leadership and governance in organization, change, security policies, procedures, and operations can lead to establishment of information security culture in an organization through impacting on personal, group, and organizational behaviors. In another study by Kruger, Drevin, and Steyn (2010) entitled "An Evaluation of Awareness of Information Security," level of knowledge and users' behaviors were appraised in a test. Researchers concluded that increase in personnel's awareness level of information security by means of vocabulary and comprehension tests is very productive and there is a specific relationship between information security learning and change in workers' security behaviors. Finally, following articles have addressed the issue of information security: Maisa

Mendonça Silva et al., 2014; Sean Allam et al., 2014; Mouna Jouini et al., 2014; Derek L. Nazareth, and Jae Choi, 2014.

7. Statistical Population

Statistical population of this study includes the workers at the International Diabetes Prevention and Control Association. It contains 150 people using the stratified cluster random sampling method.

8. Hypotheses

Major hypotheses:

- There is a significant relationship between KM system and increase in organizations' information security;
- There is a significant relationship between management information system and increase in organizations' information security;
- There is a significant relationship among KM system, management information system, and increase in organizations' information security.

Minor hypotheses:

- There is a significant relationship between hardware component of management information system and increase in organizations' information security;
- There is a significant relationship between software component of management information system and increase in organizations' information security;
- There is a significant relationship between database component of management information system and increase in organizations' information security;
- There is a significant relationship between HR component of management information system and increase in organizations' information security.

9. Conceptual Model of the Research

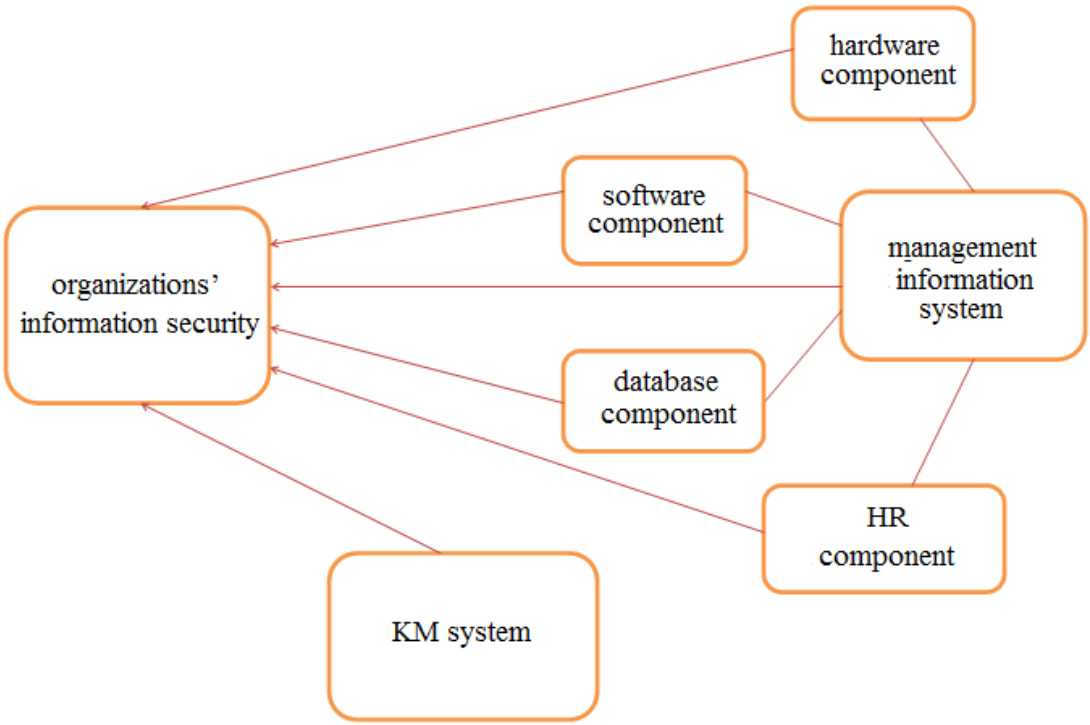

Fig. 1: Conceptual Model of the Research

10. Testing the Hypotheses

First major hypothesis: There is a significant relationship between KM system and increase in organizations' information security.

H_0: KM system has no direct relationship to increase in organizations' information security.

H_1:KM system has direct relationship to increase in organizations' information security.

Table 1: Correlation between KM system and increase in organizations' information security

Variable	Test	Increase in organizations' information security
KM system	Correlation coefficient	0.861
	Significance	0.002
	Number	150
	Average	-0.4125
	SD	0.2065
	T value	-10.431

According to above data, results show that level of significance of the test is lower than 1 percent. Therefore, $H_0$is rejected and this can be said that KM system has an impact on increase of organizations' information security at confidence level of 99 percent. In addition, paired correlation coefficient is equal to 0.861. According to significance level, this is safe to claim that there is there is a direct and significant between KM system and increase of organizations' information security (p<0/01).

Second major hypothesis: There is a significant relationship between management information system and increase in organizations' information security.

H_0: Management information system has no direct relationship to increase in organizations' information security.

H_1:Management information system has direct relationship to increase in organizations' information security.

Table 2: Correlation between management information system and increase in organizations' information security

Variable	Test	Increase in organizations' information security
Management information system	Correlation coefficient	0.793
	Significance	0.002
	Number	150
	Average	-0.4532
	SD	0.2163
	T value	-10.654

According to above data, results show that level of significance of the test is lower than 1 percent. Therefore, $H_0$is rejected and this can be said that management information system has an impact on increase of organizations' information security at confidence level of 99 percent. In addition, paired correlation coefficient is equal to 0.793. According to significance level, this is safe to claim that there is there is a direct and significant between management information system and increase of organizations' information security (p<0/01).

Third major hypothesis: There is a significant relationship among KM system, management information system, and increase in organizations' information security.

Table 3: variance analysis and regression indices for increase in organizations' information security to determine predictor variables

Stage	Model	Squared Squares	Degree of freedom	F	Significance	R	Squared R
1	Regression	36614.796	1	109.556	0.002	0.502	0.252
	Remnant	108952.717	148				
	Total	145567.512	149				

As illustrated for prediction of increase in organizations' information security, KM system, and management information system, variance analysis of regression model (p=0/002; F=109/556) is significant and the model can predict an increase of 25 percent variance in increase of organizations' information security.

Table 4: regression coefficients to predict increase of organizations' information security, KM system, and management information system

Variable	B	Standard error	Beta coefficient	T- coefficient	Significance
KM system and management information system	1.370	0.131	0.502	10.46	0.002

Results indicated above show that KM system and management information system have a positive and significant share in predicting increase of organizations' information security.

First minor hypothesis: There is a significant relationship between hardware component of management information system and increase in organizations' information security.

H_0: Hardware component of management information system has no direct relationship with increase in organizations' information security.

H_1: Hardware component of management information system has direct relationship with increase in organizations' information security.

Table 5: Correlation between hardware component of management information system and increase in organizations' information security

Variable	Test	Increase in organizations' information security
Hardware component of management information system	Correlation coefficient	0.714
	Significance	0.002
	Number	150
	Average	-0.5332
	SD	0.3163
	T value	-11.654

According to above data, results show that level of significance of the test is lower than 1 percent. Therefore, $H_0$is rejected and this can be said that hardware component of management information system has an impact on increase of organizations' information security at confidence level of 99 percent. In addition, paired correlation coefficient is equal to 0.714. According to significance level, this is safe to claim that there is there is a direct and significant between hardware component of management information system and increase of organizations' information security ($p<0/01$).

Second minor hypothesis: There is a significant relationship between software component of management information system and increase in organizations' information security.

H_0: Software component of management information system has no direct relationship with increase in organizations' information security.

H_1: Software component of management information system has direct relationship with increase in organizations' information security.

Table 6: Correlation between software component of management information system and increase in organizations' information security

Variable	Test	Increase in organizations' information security
Software component of management information system	Correlation coefficient	0.701
	Significance	0.002
	Number	150
	Average	-0.5754
	SD	0.3421
	T value	-11.698

According to above data, results show that level of significance of the test is lower than 1 percent. Therefore, $H_0$is rejected and this can be said that software component of management information system has an impact on increase of organizations' information security at confidence level of 99 percent. In addition, paired correlation coefficient is equal to 0.701. According to significance level, this is safe to claim that there is there is a direct and significant between software component of management information system andincrease of organizations' information security ($p<0/01$).

Third minor hypothesis: There is a significant relationship between database component of management information system and increase in organizations' information security.

H_0: Database component of management information system has no direct relationship with increase in organizations' information security.

H_1:Database component of management information system has direct relationship with increase in organizations' information security.

Table 7: Correlation between database component of management information system and increase in organizations' information security

Variable	Test	Increase in organizations' information security
Database component of management information system	Correlation coefficient	0.693
	Significance	0.002
	Number	150
	Average	-0.5129
	SD	0.3012
	T value	-10.798

According to above data, results show that level of significance of the test is lower than 1 percent. Therefore, $H_0$is rejected and this can be said that database component of management information system has an impact on increase of organizations' information security at confidence level of 99 percent. In addition, paired correlation coefficient is equal to 0.693. According to significance level, this is safe to claim that there is there is a direct and significant between database component of management information system and increase of organizations' information security (p<0/01).

Fourth minor hypothesis: There is a significant relationship between HR component of management information system and increase in organizations' information security.

H_0: HR component of management information system has no direct relationship with increase in organizations' information security.

H_1: HR component of management information system has direct relationship with increase in organizations' information security.

Table 8: Correlation between HR component of management information system and increase in organizations' information security

Variable	Test	Increase in organizations' information security
HR component of management information system	Correlation coefficient	0.684
	Significance	0.002
	Number	150
	Average	-0.6234
	SD	0.3986
	T value	-11.345

According to above data, results show that level of significance of the test is lower than 1 percent. Therefore, $H_0$is rejected and this can be said that HR component of management information system has an impact on increase of organizations' information security at confidence level of 99 percent. In addition, paired correlation coefficient is equal to 0.684. According to significance level, this is safe to claim that there is there is a direct and significant between HR component of management information system and increase of organizations' information security (p<0/01).

Conclusions

Knowledge constitutes the main instrument of competition for many organizations. Commercial and scientific societies believe that organizations can upkeep their competitive advantages by means of knowledge leverage. In order to stream knowledge aligned with organizational purposes and attain permanent competitive advantages, managers are bound to administrate their knowledge. They should uplift their abilities in this regard, get acquainted with KM strategies, and establish cultural, knowledge-based, and interactive environments among their workforces to easily share and manage information flows. Under these conditions, managers will be able to change existing knowledge into permanent competitive advantages. As a type of information system, management information system is developed to support managerial decisions. A management information system generates information which is able to procure many daily decision-making needs of managers and business experts. Information systems should be flexible enough to allow users at different levels to fulfill their demands. In this article, attempts were made to evaluate impact of KM system and management information system in increasing the international organizations' information security at the International Diabetes Prevention and Control Association. According to the results obtained from testing the hypothesis, there is significant relationship among KM system, management information system, and increase in information security. There is, additionally, significant relationship between components of management information system (hardware, software, database, and human resources) and increase in information security.

REFERENCES

1- Azmi, I.M., 2010, "Legal and ethical issues in knowledge management, in Malaysia", journal of Computer law & security review, 26, pp. 61-71.
2- 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.
3- Barnes, S., Knowledge Management Systems: Theory and Practice, Thomson Learning Press, 2002.
4- Basie von Solms, Information Security – The Fourth Wave, computers &security25, 165–168, 2006.
5- Basie von Solmsa, Rossouw von Solms, From information security to business security?, Computers & Security, 24, 271-273, 2005.
6- Basie von Solmsa, Rossouw von Solms, The 10 deadly sins of information security management, Computers & Security, 23, 371-376, 2004.

7- Bento, A. and R. Bento, Empirical Test of a Hacking Model: An Exploratory Study. Communications of the AIS, 14(32): p. 678-690, 2004.
8- Cech, P., Bures, V., Knowledge Management and Czech Universities, Information Technology and Management, 1, Czech Republic, 2000.
9- Chan, K. and Liebowitz, J., 2006, "The synergy of social network analysis and knowledge mapping: a case study", International Journal of Management and Decision-making, 7(1), pp. 19–35.
10- Chang, Ernest, Lin, Chin-Shien (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems, 107*, 1-10.
11- Cheng, K. (2005), "Surviving hacker attacks proves that every cloud has a silver lining", Computers in Libraries, Vol. 25 No. 3, pp. 6-8, 52-6.
12- Choi, Namjoo, Kim, Dan, and Goo, Jahyun (2008). Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action. *Information Management & Computer Security, 16*, 484-485.
13- Chua, A., 2002, "The influence of social interaction on knowledge creation", Journal of Intellectual Capital, 3(4), pp.375–392.
14- Dave, B. and Koskela, L., 2009, "Collaborative knowledge management—A construction case study", Automation in Construction, 18(7), pp. 894–902.
15- Davis, G.B., and Olson, M.H., Management Information system: Conceptual, foundations, structure, and development. 2nd ed. New York: McGraw-Hill, 1985.
16- Derek L. Nazareth, Jae Choi, "A System Dynamics Model for Information Security Management", Information & Management, In Press, Accepted Manuscript, Available online 4 November 2014.
17- Efthymia Metalidou, Catherine Marinagi, Panagiotis Trivellas, Niclas Eberhagen, Christos Skourlas, Georgios Giannakopoulos, "The Human Factor of Information Security: Unintentional Damage Perspective", Procedia - Social and Behavioral Sciences, Volume 147, 25 August 2014, Pages 424-428, 2014.
18- Gary Hinson, IsecT Ltd, Human factors in information security, Innovative information security awareness programs, Notice Bored, 2003.
19- Hahn, J. and Wang, T.W., 2009, "Knowledge Management Systems and Organizational Knowledge Processing Challenges: A Field Experiment", Decision Support Systems, 47(4), pp. 332-342.
20- Hsia, T., Lin, L., et al, A Framework for Designing Nursing Knowledge Management Systems, Interdisciplinary Journal of Information, Knowledge and management, Volume 1, Taiwan, 2006.
21- Hutchings, K. and Michailova, S., 2004, "Facilitating knowledge sharing in Russian and Chinese subsidiaries: the role of personal networks and group membership", Journal of Knowledge Management, 8(2), pp. 84–94.
22- Huysman, M. and de Wit, D., 2004, "Practices of managing knowledge sharing: towards a second wave of knowledge management", Knowledge and Process Management, 11(2), pp. 81–92.
23- Inkpen, A.C. and Tsang, E.W.K., 2005, "Social capital, networks, and knowledge transfer", Academy of Management Review, 30(1), pp. 146–165.
24- 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.
25- 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.
26- Knapp, K.J., et al., Top Ranked Information Security Issues: The 2004International Information Systems Security Certification Consortium (ISC) 2Survey Results, Auburn University: Alabama 2004.
27- Kotulic, A.G. and J.G. Clark, Why There Aren't More Information Security Research Studies. Information & Management, 41(5): p. 597-607, 2004.
28- Kruger, H.A. and Kearney, W.D. (2006). A prototype for assessing information security awareness. *Computer & security, 25*, 289-296.
29- Kruger, H.A., Drevin, L. and Steyn, T. (2010). A Vocabulary test to assess information. Information Management & Computer Security Journal,. 18(5), 316-19.
30- Lang, J.C., 2004, "Social context and social capital a senablers of knowledge integration", Journal of Knowledge Management, 8(3), pp. 89–105.
31- Lin, B., Umoh, D., E-Healthcare: A Vehicle of Change, American Business Review, 20 (2), 27-32, 2002.
32- Maconachy, W. V., Schou, C. D., Ragsdale, D., Welch, D. (2001). *A Model for Information Assurance-An Integrated Approach*. Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, June, 5-6.

33- Mahabi, Victoria (2010). Information Security Awareness: System Administrators and End-User Perspectives at Florida State University. Dissertation for the degree of Doctor of Philosophy in Library and Information Studies .the Florida State University.
34- Maisa Mendonça Silva, Ana Paula Henriques de Gusmão, Thiago Poleto, Lúcio Camara e Silva, Ana Paula Cabral Seixas Costa, " A multidimensional approach to information security risk management using FMEA and fuzzy theory", International Journal of Information Management, Volume 34, Issue 6, December 2014, Pages 733-740, 2014.
35- Malone, D., Knowledge Management: A Model for Organizational Learning, International Journal of Accounting, Information Systems, 3, 111-123, 2002.
36- Marwick, A., D., Knowledge Management Technology, IBM Systems Journal, 40 (4), 2001.
37- McPhail, Ken, 2009, "Where is the ethical knowledge in the knowledge economy? Power and potential in the emergence of ethical knowledge as a component of intellectual capital", Journal of Critical Perspectives on Accounting, 20, pp. 804–822.
38- Mohayidin, M., G., et al, The Application of Knowledge Management in Enhancing the Performance of Malaysian Universities, The Electronic Journal of Knowledge Management, Volume 5, Issue 3, pp 301-312, Malaysia, 2007.
39- Mouna Jouini, Latifa Ben Arfa Rabai, Anis Ben Aissa, "Classification of Security Threats in Information Systems", Procedia Computer Science, Volume 32, 2014, Pages 489-496, 2014.
40- Mugellesi Dowa, R., Pallaschkea, S., Merria, M., Montagnona, E., Schabea, M., Belingheria, M, Bucherc, M.and Astronautica, A., 2008, "Overview of the knowledge management system in ESA/ESOC", Acta Astronautica, 63(1), pp. 448 – 457.
41- Newman, B., Conrad, K., W., A Framework of Characterizing knowledge Management Methods, Practicesand Technologies, Washington University Course EMGT, 298. T1, Springer, 1999.
42- Nikrerk J.F. and Solms, Van (2009). Information security culture: a management perspective. *Computer & security, 5*, 142-144.
43- O'Donovan, F., Heavin, C. and Butler, T., 2006,"Towards a model for understanding the key factors in KMS implementation", 14th European Conference on Information Systems University of Göteborg, Sweden, pp. 1-12.
44- Rao, L. and Osei-Bryson, K.M., 2007, "Towards defining dimensions of knowledge systems quality", Expert Systems with Applications, 33(2), pp. 368–378.
45- Ravishankar, .M.N. and Pan Shan, L., 2008, "The influence of organizational identification on organizational knowledge management (KM)", Omega, 36(2), pp. 221-234.
46- Schoderbek P.P., Asterios G. Kefalas, and Charles C. Schoderbek, Management Systems: Conceptual Considerations, Dallas, Texas, 1975.
47- Sean Allam, Stephen V. Flowerday, Ethan Flowerday, "Smartphone information security awareness: A victim of operational pressures", Computers & Security, Volume 42, May 2014, Pages 56-65, 2014.
48- Selsky, D., B., Eisenberg, F., P., Hersh, W., Buitendijk, H., J., Knowledge Integration: Insight through the EPortal, Journal of Healthcare Information Management, 15(1), 13-24, 2001.
49- Tintamusik, Yanarong (2010). Examining the Relationship between Organization Systems and Information Security Awareness. Dissertation for the degree of Doctor of Business Administration. Northcentral University.
50- Tseng, M. L., (2011). Using a hybrid MCDM model to evaluate firm environmental knowledge management in uncertainty. Applied Soft Computing, 11, 1340–1352.
51- Tseng, S.M., 2008, "Knowledge management system performance measure index", Expert Systems with Applications, 34(1), pp. 734–745.
52- Veiga, A. Da., and Eloff, J.H.P. (2010). A Framework and Assessment Instrument for Information Security Culture. *Computer & Security, 29*(2), 196-200.
53- Von Solms R, Von Solms B. (2004). Information security management (1): Why information security is so important. Information Management and Computer Security, Vol. 6, PP. 174 -77.
54- Wilson, Mark, and Hash, Joan. (2003). Building an information technology security awareness and training program. *National Institute of Standards and Technology*, sp 800-50, 20-79.
55- Wing S.C. and Chan, L.S., 2008, "Social network, social trust and shared goals in organizational knowledge sharing Department of Finance and Decision Sciences, School of Business", Journal of Information & Management,45, pp.458–465.
56- Wong, K.Y. and Aspinwall, E., 2006, "Development of a knowledge management initiative and system: A case study", Expert Systems with Applications, 30(4), pp.633–641.
57- Wu, W. W. (2008). Choosing knowledge management strategies by using a combined ANP and DEMATEL approach. Expert Systems with Applications, 35, 828–835.