Information and Knowledge Management
ISSN 2224-5758 (Paper) ISSN 2224-896X (Online)
Vol.5, No.1, 2015
www.iiste.org

Impact of Knowledge Management on Security of Information and its Strategic Outcomes

Sayed Fayaz Ahmad (Corresponding author)
Center for Emerging Sciences, Engineering and Technology,Islamabad, pakistan
E-mail: fayazafghani@gmail.com

Muhammad Khalil Shahid
Center for Emerging Sciences, Engineering and Technology,Islamabad, pakistan
E-mail: khalildona@yahoo.com

Abstract
Security of Information plays an important role in the progress of any organization. This research finds out that Information Security can be achieved through proper Knowledge Management in organizations especially in Telecommunication Sector. Not only the literature supports the theme of the research but it was also proved by the analysis and results of the respondents responses. Knowledge Management was found to have positive and significant influence over Security of Information. A framework was also developed for studying the relationship among Knowledge Management, Security of Information, Information Governance, Information Risk Management and Safety to Organizational Knowledge; which was tested through correlation and regression. Though the research was carried out in Telecommunication Sector organizations, yet it is equally valuable for and implementable in any other sector.
Keywords: Knowledge Management (KM), Information Governance (IG), Information Risk Management (IRM), Safety to Organizational Knowledge (SOK).

1. Introduction

Information is the most precious asset of all organizations. All of the operations of any organization depend upon its information. All of the product specifications, records, process details etc comes under the heading of information. With out complete and appropriate information, organizations fail to run their operations of producing goods or services or both. The entire decisions made by management also depend upon the information available for these decisions.

Importance of information depends upon their type and need. For example security agency's information is more worthy than daily news information. This shows that information ranges from some what important to highly important information. As much as there is the need and importance of information, so much it needs to be managed and used effectively and carefully.

With the development of modern technology and the shape of modern market, there is always fear of information theft. Various elements which can be used for this purpose are humans, electronic devices, internet etc.

This research focuses on the problem of Information Security and tries to find out a way to make information secure through Knowledge Management. The research will also discuss the relationship of SI with some important elements like Information Governance, Information Risk Management and Safety to Organizational Knowledge. Though the research was conducted in Telecommunication Sector Organizations, it is equally applicable to all types of organizations and the author is confident for its valuable results.

2. Literature Review

2.1 Security of Information

Security of Information is one of the prime needs of organizations in modern days. Speed in communication, transmission and electronic devices have alarmed for SI every where. Electronic devices like mobile phone, computers, USB, memory cards are majorly used in modern day businesses. Information of an organization are exchanged, transmitted and shared through them which can cause severe damage to personal and organizational information [1].

As the medium through which information of an organization are made accessible, these information needs to be prevented from corruption, theft and changing and the process of doing so is known as SI [2]. It is a complicated process, affected by workers, their education, and technology. Therefore these factors need to be managed carefully.

SI is not only an organizational issue. Its failure can cause sever damage at higher level as well. Therefore policy and regulations has been developed for it nationally and internationally. Every employee and organization is bound to obey the laws and standards regarding information and its security [3].

Importance of SI depends upon the nature of organization and information. Due to this natural fact

almost every organization has different security policy and regulations for its SI. The strictness and rigidness of SI policy also differs from organization to organization and have a strong relationship with organizational goals and objective. Through SI policy firms secure its information by adopting rules, control tools, protection walls etc [4].

In order to make information secure, organizations have to evaluate security risks continuously and make every possible and necessary steps for its control [5]. In spite of it's solely importance usually organizations invests less amount than the required for its information security [6].

The above literature shows that SI is still a problem and a challenge for organizations. Modern market is more competitive that the past one. Theft and leakage of information from an organization not only eliminate its competitive advantage but also put down its life on stack. Therefore organizations should manage its information very carefully to get its strategically suitable goals and objectives. The following hypothesis has been assumed for research.

H (2.1): Knowledge Management has positive relationship with Security of Information.

Ho (2.1): KM has no relationship with SI

2.2 Safety to Organizational Knowledge (SOK)

Knowledge or information is one the most important assets of organization. The roles of information in organizations are increasing day by day in enhancing various operations. Information is used in formulating the organizational strategies and in the process of decision making. As much as the people know and recognize the value of information as much they try to make it secure because the value of information is directly proportional to its security abuses.

Evidence shows that due the lack of management attention to IS many cases of security abuses happened [7]. There are many other researches which show that many severe information losses occurred. The main reason of the security abuses are less security [8].

Information loss from an organization can cause severe economical loss, ruin competitive advantage and destroy other organizational capabilities. Most alarming factor is that the vulnerability of the firm is increasing with the development of modern technology and computer software [9]. There are evidences that management has less concern about the SI and the main reason for this is either they do not know about the benefits or have no knowledge to control the problem. It is important to take every possible step for making the organizational information safe and secure from the unauthorized access and use [10].

The present research is going to find out the relationship between SI and SOK. Security is the only source through which organization can make its information, corporate memory and other knowledge safe and secure from illegal use. Therefore, the author proposed the following hypothesis.

H (2.2): SI has positive impact on Safety to Organizational Knowledge.

Ho (2.2): SI has no impact on SOK.

2.3 Information Governance

Information is one of the core elements upon which all of the process, operations product specifications etc are dependent. The heading consists of two component, information and governance. Information covers every aspect of the organizational data. It may be financial, HRM related, product specification, marketing, policy, regulations, strategy, mission etc. it can be used as input in making decisions, formulating strategies, in the process of creating goods and services and in many other operations [11]. Therefore it is highly recommended that the information should be used and treated in an honest and organizational friendly manner. The process of finding, seeking, using and transferring of information etc all comes under the umbrella of the information governance or information control. It is defined as "the arrangements of privacy and security needed to information" [12].

The value of information is changing from one person or organization to another. Some information is more important and precious than others. It is very difficult to produce or create information for the first time but interestingly very cheap and easy to reproduce [13]. Therefore, for the one who creates information it is very necessary for to keep it under lock and key.

Some information is highly sensitive and some or less. It is due to its value which differs in satisfying human needs [14]. Governance of information is a method of managing records, regulations regarding information privacy and security, information exchange and transferring among individuals; and managing data life and cycle [15].

The environment inside and outside of an organization consists of many actors. These actors are constantly at interactions with each other. Due to their different role they have different interface with each other and are working in different relations. These actors lack knowledge to solve complex problems, and face the challenges of environment boldly. They need governance for controlling their relations, working and interconnections with each other. Coming back to the information governance, it is important and necessary to

exchange information under honest governance. There should be a continuous effort inside organization for understanding the nature and structure of various connections among individuals and events [16].

All of the information in an organization is important for one reason or another to one person or another. And the organization needs to govern its information according to the context. i.e. which means all the necessary factors effecting the relationship of an organization and information [17]. There should be some principles and policy for the creation, usage and exchange of information with in the organization. When the information flows from one actor to another, there should be an eye over it to make sure its honest and sincere use [18].

In this research we will find out the relationship between SI and IG. Our concept is new than the previous approaches who had studied IG. We are going to present an alternate approach for getting IG through SI. The following hypotheses are supposed to be checked.

H (2.3): Security of Information has positive relationship with Information Governance.

Ho (2.3): SI has no relationship with Information Governance.

2.4 Information Risk (IR)

As a matter of fact, information is the most precious assets of organization. With the use of this assets organization design the strategy for its operation, product specifications, processes etc for achieving its objectives. Information is used to formulate strategy and to make organizational short and long term decisions. Due to its high importance, there is always fear of information theft; and managing and controlling of information becomes the need of maintaining competitive advantage and strong market position.

Management usually identifies weaknesses and threats which can cause spoil to the information assets of the organization and makes counter measure for there reduction. This process is known as IRM. In other words it is the process of addressing and identifying the unauthorized use or damage of firm's information [19]. IRM is a continuous process inside organization. If organization's information is safe under today's condition it may not safe under the same measure tomorrow. Therefore continuous and updated measures are required for analyzing and identifying risks related to information. Once the risk is identified, it is easy to take some counter measure for its control and reduction.

IRM is not an easy task. Most of the time incidents related to information security occur from an unexpected and unpredictable side and are unique in its nature. This gives additional importance to IRM and gives organization a message to endlessly identifies and analyze all the expected and unexpected areas of risks [20]. It is important to note here that identification of all types of risks is impossible and the unaddressed risk is known as residual risk.

Human error, electronic device, designer etc are the most vulnerable points in information systems. Therefore it is highly recommended that these points must be under security measure always [21]. Management chooses the lowest acceptable risk when the occurrence of risk is unavoidable. Sometime risks are mitigated while sometime it may be transferred from one area to another but always the management prefers to get less loss [22].

The literature review clarifies that risk may occur any time any where and can cause more or less loss and damage to the organizational information. Therefore it is mandatory to continuously identifies and assess all of the vulnerable areas and points of information system. It is a fact that management cannot overcome the risk completely but they can minimize it to the acceptable level. The following hypotheses are assumed to be true.

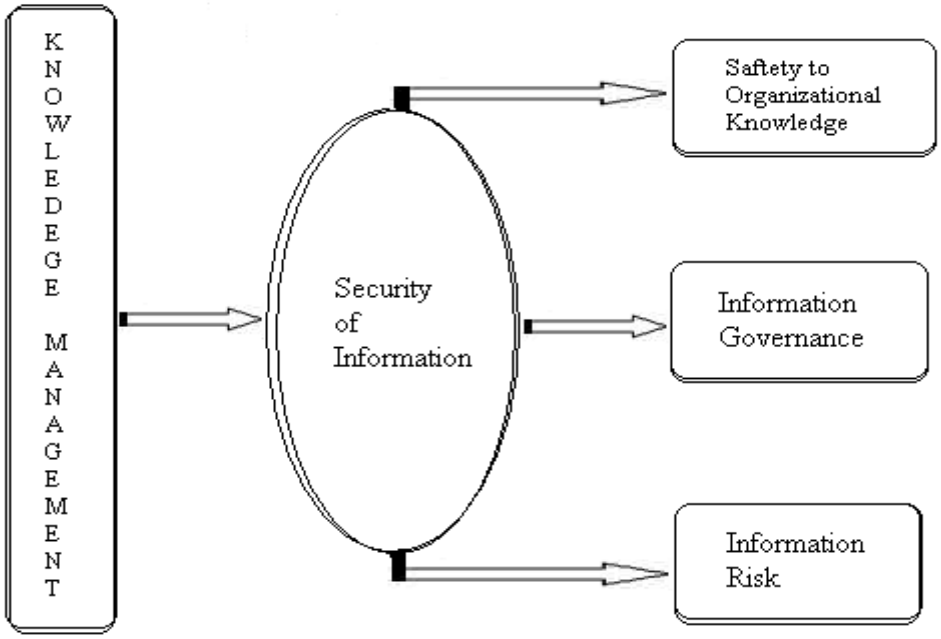
H (2.4): SI has positive relationship with Information Risk Management

Ho (2.4): SI has no relationship with IRM.

2.5 Proposed Structural Model

After reviewing literature about the above discussed variables, the author designs the following model for the proposed relationship. Like the previous model, the arrow's head shows the direction of relationship and goes from independent variable to dependent variable.

Figure 1: KM as a Tool for Achieving SI and its Strategic Important Outcomes



Model:

Knowledge Management as a Tool for Acheiving SI and its Strategic Outcomes

3. Methodology

The research is a part of PhD thesis and is based on questionnaire survey from the senior managers of various firms of Pakistan. The questionnaire was first timely created and tested for the study. Organizations which are selected for the survey are PTCL, Warid, Telenor, UFone, Mobilink and Zong. The data collected was analyzed through SPSS software and results were obtained through correlation and regression analysis.

4. Analysis and Results

4.1 Reliability Statistics

The newly designed questionnaire was checked for its reliability after collection. Cronbach's Alpha value for the data is 0.762, which means that the data is reliable and enough good for the research. After this test we became sure for our research data goodness and reliability.

4.2 Correlation Analysis

We have find out the relationship among different variable through correlation analysis at the significance level 0.05 and 0.01. Correlation analysis is used to find out weather there is relationship between variables of interests or not. Its starts from negative one (-1) to positive one (+1), when there is negative value, it means that the relationship is negative while positive value represents positive relationship. Zero value represents that there is no relationship at all. The correlation analysis of the data is given in the table below.

Hypothesis 1:

H (4.2.1): Knowledge Management has positive relationship with Security of Information

Ho (4.2.1): KM has no relationship with SI

The correlation matrix above shows that there are significant positive relationship between KM and SI. Values for this relationship is (0.664**, p = .000). The correlation values support our assumptions. In other words, there is strong positive relationship between KM and SI. If KM changes then obviously do the SI.

Table 1: Correlations						
		KM	SI	SOK	IG	IR
KM	Pearson Correlation	1				
	Sig. (2-tailed)					
	N	208				
SI	Pearson Correlation	.664**	1			
	Sig. (2-tailed)	.000				
	N	208	208			
SOK	Pearson Correlation	.725**	.540**	1		
	Sig. (2-tailed)	.000	.000			
	N	208	208	208		
IG	Pearson Correlation	.476**	.571**	.512**	1	
	Sig. (2-tailed)	.000	.000	.000		
	N	208	208	208	208	
IR	Pearson Correlation	.269**	.760**	.320**	.380**	1
	Sig. (2-tailed)	.000	.000	.000	.000	
	N	208	208	208	208	208
**. Correlation is significant at the 0.01 level (2-tailed).						

Hypothesis 2:

H (4.2.2): SI has positive impact on Safety to Organizational Knowledge

Ho (4.2.2): SI has no impact on SOK

We have assumed that SI has positive impact on SOK. The hypothesis was also validated through correlation analysis with the values (0.540** and p = .000). It shows that there are positive and significant relationship between SI and SOK and encourages our assumption.

Hypothesis 3:

H (4.2.3): SI has positive relationship with Information Governance

Ho (4.2.3): SI has no relationship with IG

The relationship between SI and IG was also measured through correlation analysis and it was find out that there is positive significant relationship between them. The value of correlation is 0.571** at the significance level p = .000.

Hypothesis 4:

H (4.2.4): SI has positive relationship with Information risk Management

H (4.2.4): SI has no relationship with IRM

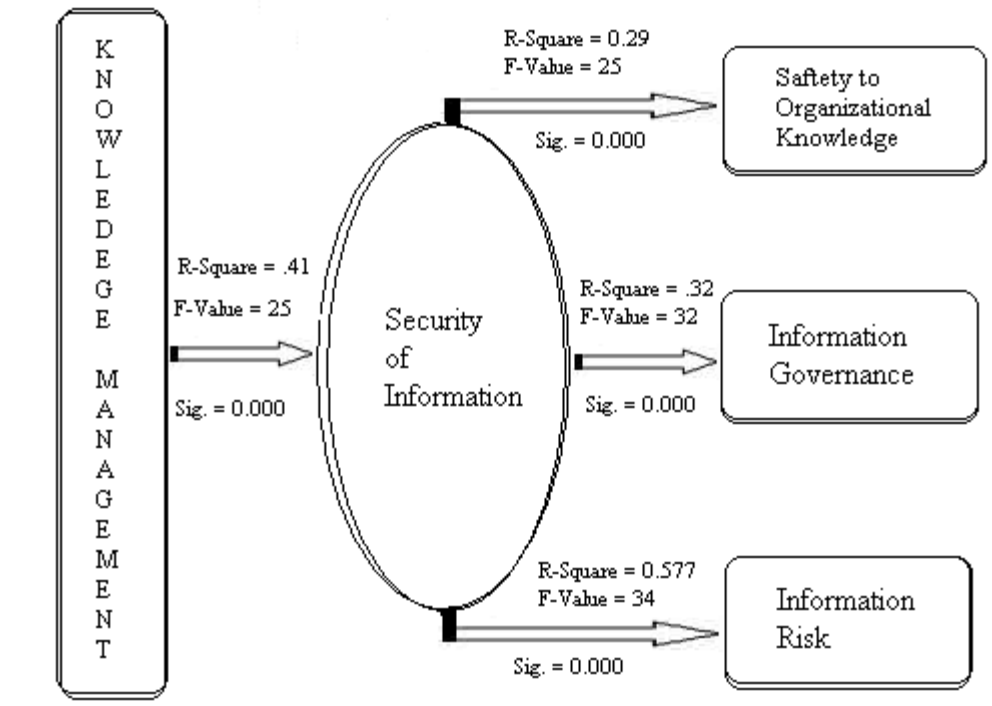
SI and IRM have also positive relationship with each other. We assumed their positive relationship in our hypothesis. The correlation matrix validated our assumption with the value 0.760** at the significance level p = 0.000.

4.3 Regression Analysis

1. Regression Analysis of KM and SI:

Regression analysis is used to find out weather one variable (the predictor) can predict the (dependent) other variable or not. It also gives us the extent to which one variable can be predicted. For this purpose we also run the data through regression analysis.

Figure 2: Tested Model for "KM as a Tool for Achieving SI and its Strategic Important Outcomes



Model:
Knowledge Management as a Tool for Acheiving SI and its Strategic Outcomes

As our model consists of five different variables, so we checked only the concerned relationship. The R-square value for the model between KM and SI is 0.414, for SI and IR is .577, for SI and IG is .326 and for SI and SOK is .291. The R-square value is used to predict the dependent variable. e.g. R-square value 0.414 means that KM can predict SI with the certainty of 41 percent and so on. The summary of the regression analysis for all the models are given below.

Table 2: Regression Analysis of KM and SI

		B	Std. Error	t-Stat	Sig.	R-Square	F-Stat	P-Value
1	(Constant)	1.089	.131	8.340	.000	.414	25.810	.000[a]
	KM	.391	.077	5.080	.000			
a. Predictor (Constant), KM b. Dependent Variable: SI								

2. Regression Analysis of SI and IR:

Table 3: Regression Analysis of SI and IR

		B	Std. Error	t-Stat	Sig.	R-Square	F-Stat	P-Value
1	(Constant)	1.173	.066	17.860	.000	.577	34.00	.000[a]
	SI	.215	.037	5.831	.000			
a. Predictors: (Constant), SI b. Dependent Variable: IR								

3. Regression analysis of SI and IG:

Table 4: Regression analysis of SI and IG

		B	Std. Error	t-Stat	Sig.	R-square	F-stat	P-Value
1	(Constant)	1.084	.113	9.636	.000	.32	32.9	.000[a]
	SI	.363	.063	5.738	.000			
a. Predictor (Constant), SI b. Dependent Variable: IG								

4. Regression Analysis of SI and SOK:

Table 5: Regression Analysis of SI and SOK

		B	Std. Error	t-Stat	Sig.	R-Square	F-Stat	P-value
1	(Constant)	1.225	.078	15.610	.000	.291	25.885	.000[a]
	SI	.224	.044	5.088	.000			
a. Predictors: (Constant), SI b. Dependent Variable: SOK								

5. Conclusion

Knowledge Management has tremendous importance and role in SI in telecommunication sector organizations in particular and all other organizations in general. The results show that through better KM organizations can get their information secure and safe. Through KM organizations can not only make their strategy secure but also their products and services.

Security of Information, which is an outcome of KM further gives many advantageous elements which are the need of modern day firms. The relationship and extant of dependence were checked and validated through correlation and regression. It was found that there are strong, positive and significant relationship of SI with IG, IRM and SOK. There fore it became crystal clear that SI not only gives us security to organizational memory or information but also enhances the capability of good information governance, increases the potential of Information Risk Management.

In other words we can say that organizations can make their information or knowledge secure through better KM. SI further gives IG, IRM and SOK. There fore if an organization wants to get better IG, reduce information risks and SOK, it should provide high security to its organization information.

5.1 Recommendations

The following recommendations are made after carrying out the research.

1. The importance of Knowledge Management becomes further clear for the Security of Information and it is recommended that organizations should manage their knowledge to get their strategic and all other type of information secured. As some information is less important than other so the information with high importance value should be manage with the most affordable and achievable level.
2. Use of information is another important element of success for organizations but the way they use and utilize this information is the most important. Most of the information or knowledge are department and individual specific and if they go to wrong place can make severe damage to the organization's success. Therefore knowledge and information should be managed in such a way to be governed effectively and efficiently.
3. To overcome and minimize the loss and improper use of information and knowledge, the practice of Knowledge Management should be used. Interestingly KM gives security to all of the organizational knowledge and security further reduces the risk of loss and illegal use.
4. Knowledge of an organization can be kept secure by providing proper lock and key system. This will make these information secure and will provide safety to the firm's knowledge. Therefore it is strongly recommended that organizations should grant and give security to their knowledge for keeping all of their organizational knowledge protected.
5. Lastly, it summarized that KM is the key source of achieving security of information. With out KM, SI can never be achieved in telecommunication sector especially and in other sector organizations generally. In addition, SI further gives effective and advantageous information governance, reduces information related risks and maximizes safety to organizational knowledge. Based on the above analysis and results the author proposed that IG, ISM and SOK are achieved by providing enough security to information; and SI can only be achieved through proper KM.

References

[1] Dodge, C.R., Carver, C., & Ferguson, J.A. (2007). Phishing for user security awareness. Computer &Science, 26(1), 73.
[2] Vural, Y.(2007). Kurumsal BilgiGüvenli˘gi veSızmaTestleri. Masterthesis,Science Institute ofGaziUniversity,40–42.
[3] Wood, C.C.(2005). Information securitypoliciesmadeeasy. USA:InformationShield Publications., pp.35–36.
[4] Kalman, S. (2003). Web security field guide. Networking technology. India: Cisco Press., pp. 36–37.
[5] Peltier, T.(2005). Information securityriskanalysis (2nd ed.).USA:AuerbachPubli- cations., pp.7–10.
[6] Deloitte (2006). IS Survey Report 2006, 41–63. http://www.deloitte.com/ dtt/cda/doc/content/us fsi 150606 global security survey(1).pdf
[7] Zviran, M., & Haga, W. (1999). Password security: An empirical study. Journal of Management Information Systems, 15(4), 161–185.
[8] Panettieri, J. C. (1995). Information week/ Ernst and Young security survey. Information week 555, 32–37.
[9] Dhillon, G., & Backhouse, J. (2000). Information system security management in the new millennium. Communications of the ACM, 43(7), 125–128.
[10] Straub, D. W. (1990). Effective IS security: An empirical study. Information Systems Research, 1(3), 255–276.
[11] Rafaeli, S.(2003).Experimental investigation of the subjective value of information intrading. Journal of the Association for Information Systems, 4, 119– 139.
[12] Donaldson, A.,&Walker,P.(2004).Information governance—A view from the NHS. International Journal of Medical Informatics, 73, 281–284.
[13] Shapiro, C.,& Varian, H. R.(1999). Information rules. Boston: Harvard Business School Press.
[14] Huizing, A.(2007).The value of arose: Rising above objectivism and subjectivism. In A. Huizing, & E. de Vries (Eds.), Information management: Setting the scene. London: Elsevier.
[15] Economist Intelligence Unit.(2008). The future of enterprise information governance. London: The Economist Intelligence Unit Limited.
[16] Klein, G., Moon, B.,& Hoffman. (2006). Making sense of sense making1: Alternative perspectives. IEEE Intelligent Systems, 21(4), 70–73.
[17] Davenport, T.H., & Prusak,L.(1997). Information ecology: Mastering the information and knowledge environment. New York: Oxford University Press.
[18] Huizing, A.,&Bouman,W.(2002).Knowledge and learning, markets and organizations: Managing the information transaction space. InC. W. Choo ,& N. Bontis (Eds.), The strategic management of intellectual capital and organizational knowledge (pp. 185–206).New York: Oxford University Press.
[19] ISACA (2006). *CISA Review Manual 2006*. Information Systems Audit and Control Association. p. 85. ISBN 1-933284-15-3.
[20] Spagnoletti, Paolo; Resca A. (2008). "The duality of Information Security Management: fighting against predictable and unpredictable threats". *Journal of Information System Security* 4 (3): 46–62.
[21] Kiountouzis, E.A.; Kokolakis, S.A. *Information systems security: facing the information society of the 21st century*. London: Chapman & Hall, Ltd. ISBN 0-412-78120-4.
[22] NIST SP 800-30 Risk Management Guide for Information Technology Systems

The IISTE is a pioneer in the Open-Access hosting service and academic event management. The aim of the firm is Accelerating Global Knowledge Sharing.

More information about the firm can be found on the homepage:
http://www.iiste.org

CALL FOR JOURNAL PAPERS

There are more than 30 peer-reviewed academic journals hosted under the hosting platform.

Prospective authors of journals can find the submission instruction on the following page: http://www.iiste.org/journals/ All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Paper version of the journals is also available upon request of readers and authors.

MORE RESOURCES

Book publication information: http://www.iiste.org/book/

Academic conference: http://www.iiste.org/conference/upcoming-conferences-call-for-paper/

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar