P: ISSN No. 0976-8602 RNI No.UPENG/2012/42622 VOL.-6, ISSUE-3, July - 2017

E: ISSN No. 2349-9443 Asian Resonance

Knowledge Management Effectiveness in Securing Information and Network Systems: A Study on Odisha

Sanjay Kumar Satapathy
Associate Professor,
Deptt.of Commerce
Ravenshaw University,
Cuttack,Odisha, India.

Chitta Ranjan Moharana
Research Scholar,
Deptt.of Commerce,
Ravenshaw University,
Cuttack,Odisha, India.

Abstract

You can't manage knowledge – nobody can. What you can do is to manage the environment in which knowledge can be created, discovered, captured, shared, distilled, validated, transferred, adopted, adapted and applied.

(Chris Collison and Geoff Parcel, Learning to Fly - Practical Knowledge Management from Leading and Learning Organizations (2005)

The extensive use of Information technology elevates the misuse of the information resources of the organizations. Online criminal activity to harm the information and network systems is called as Cybercrime. The criminals use the computers and computer networks as platform to attack the information system of the organizations. It is found that the employees of the organizations are mostly responsible for occurrence of such incidents. It is due to negligence or lack of sufficient awareness on secure practices. An effective knowledge management could be a reliable instrument for addressing the security issues. The objective of the article is to study the effectiveness of knowledge management practices adopted by organizations to strengthen their information systems. The study has been undertaken thirty organizations selected from various sectors in Odisha. Structured questionnaires are used to collect data from 50 Technical users and 150 End users. Both quantitative and qualitative methods have been used to analyze the collected data. It is found that, majority of organizations are lacking proper knowledge management policy and practices essential to secure their information systems. A model named as Competency, Reliability and Security (CRS) has been developed to suggest an advanced practice of knowledge management. This will help in creating a healthy environment protected from the internal and external attacks on information and network system in organizations.

Keywords: Information Security, Network Security, Knowledge Management, Cybercrime

Introduction

Information and Communication Technology (ICT) has become an important aspect of today's world of activities. Information and Network Security for various organizations have become a great challenge today. ICT is used broadly by the organizations for doing various activities, starting from their lower level or operational level to the higher level or Tactical level. The increasing need of keeping and sharing the information online increases the possibility of maltreating of the information.

Information Security

The term Information security describes the security concerns associated with the Information Systems and the computing environment. Information System can be broadly classified in to three parts, namely Software, Hardware and Communication paradigm. Information Security mainly focuses on securing the organization in three levels, namely organizational level, Physical level and Personal level. Information security policies are made to educate different type of users, like general users and Administrators about the secure way to interact with the Information system.

"The term "information security" means protecting information and information systems form unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide-

1. Integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
2. Confidentiality, which means preserving authorized restriction on access and disclosure, including means for protecting personal privacy and proprietary information; and
3. Availability, which means ensuring timely and reliable access to and use of information."

Managing the above three factors in Information System is known as Information System Management (Moharana, Pal, & Rout, 2012).

Network Security

Network security is safe-guarding the network components including data, media and infrastructure. Network security encompasses use of different measures to protect network components and resources from different threats. The threats include physical catastrophe like fire, natural disaster and sabotages and illegal use of resources.

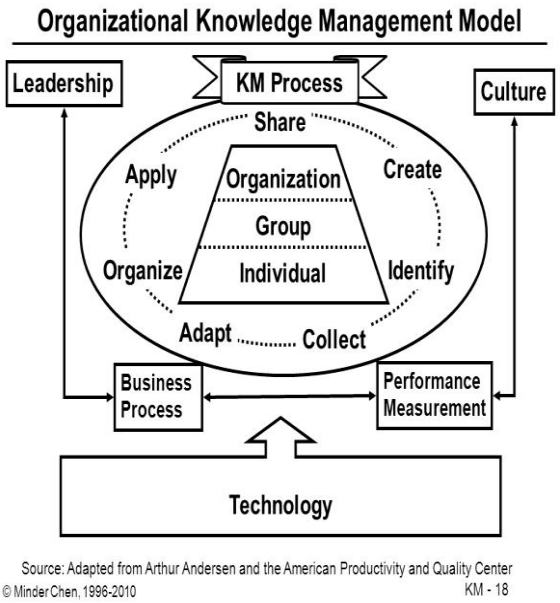
Network security management involves three components namely, accurate threat assessment, use of best cryptographic tool, and use of effective network access control products like firewalls. In order to secure the communication network, it is required to have a well devised corporate policy and proper authorization. The policy includes disaster recovery plan, data backup policy, assigning specific job roles or authorization to employees and providing access to information system accordingly, timely monitoring and testing of the security status and use of proper data encryption methods (Gallo & Hancock, 2005).

Network security comprises of some rules and regulations monitored and controlled by a network administrator. This is to check illegal access, misappropriation, alteration of data and rejection of request to a computer network. The purpose of network security is to safeguard privacy, to ensure reach to the required information, and preserve integrity.

There are many reasons for fall down of network performance.Security threats like viruses, denial of service, spywares, malwares, unrestrained access of internet, illegal use of network resources and unintentional removal of sensitive data become the origins of network security attacks. Loss of vital information is another threat to a network.Installation of unauthorized programs like songs, videos; games etc can become a reason for security attacks. Weakness includes faults in web server, and lack of proper mechanism to monitor and control the inputs to the server system could be reasons for security breaches (Ghansela S, 2013).

Knowledge Management

Knowledge is considered to be intellectual assets which are intangible in nature. This is used to achieve the competitive advantages of organizations. An effective knowledge management stresses upon creation, codification, sharing and utilization of knowledge. In this age of information technology, everybody is keen on the effective way of managing the knowledge assets.



The above diagram elaborates one of the idea knowledge management practices adopted by organizations where knowledge will built up the organizational culture and knowledge will sharpen security linked business process which is result in effectiveness of leadership.

Knowledge is considered as a primary resource in any organization. The organizations could be able to achieve many advantages in case they manage their knowledge resources effectively. The advantages could be in the form of enhancement of customer service, efficiency of the business, effectiveness and innovations. The culture of the organization has got a strong influence in knowledge management. The goal and job oriented culture impacts positively on employee intensions in knowledge management process. However, the strongly organized culture has got negative impacts. (Chang & Lin, 2015).

Effective knowledge management practices could help the organizations to keep their information and network security. Organizations require putting efforts to find out the possible causes of risk. Employees need to be trained properly in order to enhance their understanding in security management. Information related to security need to provision to reach at the employees to increase their level of awareness.

Review of Literature

The knowledge management process according to (Bhatt, 2001), classified in to creation, validation, presentation, distribution, and activity related to application of knowledge. It is required to balance the knowledge management activities in order to be benefited for any organization. The balancing activity requires significant changes in culture, technology and techniques for any organization. It is found that most of the organizations manage knowledge by focusing on people, technology or techniques exclusively. However, in order to manage knowledge effectively it is required to

focus on the interaction between people, technology or techniques. This will help the organizations to achieve competitive advantages over different dimensions of their business. The above insists on creation of an environment of nurturing and learning-by-doing procedure.

(McDermott & O'Dell, 2001), briefs that effective knowledge sharing mostly influenced by the culture of an organization. Through studies, it is found that many organizations did not make required changes in their culture in order to do proper knowledge management. Mostly, they focus on a knowledge management process which can fit into their organization culture. It is done through use shared knowledge for solving business problems, using shared knowledge to a readily available core value. They insist on developing a knowledge management system that matches with the organizations way of working. The information sharing by users is based on existing networking system. This restricted the proper utilization of knowledge management.

(Mats Edenius, 2003) explains that, the corporate managers are occupied by knowledge management processes in terms of identification, generation, transmission, storage and effective assimilation of knowledge. Therefore, they continuously look towards different knowledge management strategies for effective results. It has a link with various types of information technology tools like intranet. In knowledge management intranet is used as tool for both information and strategic management.

(Belsis, Kokolakis, & Kiountouzis, 2005), find that "Information systems security management is a knowledge-intensive activity that currently depends heavily on the experience of security experts. However, the knowledge dimension of IS security management has been neglected, both by research and industry. This paper aims to explore the sources of IS security knowledge and the potential role of an IS security knowledge management system. The results of this paper are based on field research involving five organizations (public and private) and five security experts and consultants. A model to illustrate the structure of IS security knowledge in an organization is then proposed". It is found that, "Successful security management largely depends on the involvement of users and other stakeholders in security analysis, design, and implementation, as well as in actively defending the IS. However, most stakeholders lack the required knowledge of IS security issues that would allow them to play an important role in IS security management."

(Randeree, 2006), finds that though there is an increased attention on knowledge management, the organizations missed to include the security dimension linked with it. Therefore, the author focuses to assess the security dimension associated with knowledge management. "This paper reviews security for data and information and explores the dimensions of secure knowledge systems. The emphasis is on knowledge security and the development of future knowledge management systems". It is found that, "there exists a general lack of focus on security in the knowledge management framework – both in a research setting and in practical applications. Knowledge is different from information and data and needs special consideration in firms".

(Ryan, 2006), focuses on security needs of knowledge management. The objective is to find out the way to manage conflict of interest between sharing and protection of knowledge. It is found that, "A particularly interesting challenge is the conflict of interest between individuals (including enterprises) and communities of practice. Innovation spurred through common interest can be dangerous for individuals in the short term, while beneficial to the community as a whole. Greater understanding of these tensions can assist managers in understanding how and when to apply protections in knowledge management.

(Roy & Saxena, 2010), brief, "User's knowledge of information security is one of the important factor in information security management as 70-80% security incidents occurred due to negligence or unawareness of users. In this paper we have analysed the utility of knowledge management tools to rapidly capture, store, share and disseminate the information security related knowledge with the view that it should be effectively applied by the information system users. We found that, the knowledge management tool can be used to enhance the information security".

(AlHogail & Berri, 2012), explains, "Security of Information Systems (IS) is a major concern for organizations nowadays as security related risks may affect the organization's information assets badly. Security systems in organizations can benefit a great deal from knowledge and experiences of security experts, practitioners and professionals if this knowledge is acquired, encoded into a knowledge management system and distilled appropriately to help decision making in IS security management".

According to (Massingham, 2014), knowledge resources could be managed by Knowledge management. The tools used for knowledge management are knowledge strategy and knowledge measurement. The knowledge management contributed a lot in finding out future capability requirements and sourcing. It is found that knowledge management helps in understanding the capacity of the organization and outcomes in actual.

(Saida, Abdullahb, Ulib, & Mohamed, 2014)"examine the effects of organizational characteristics and its dimensions, culture, top management support, reward and incentive, and organization structure as knowledge management success factor on information security knowledge management implementation. Using the quantitative analytical approach, the theoretical model and hypotheses in this study were fully tested based on the empirical data collected from 182 services sector in Malaysia. Data gathered from the survey questionnaires were then analysed using the correlation coefficients and multiple linear regression

analyses. The results showed that organizational characteristics made significant positive effects". This shows that the successful knowledge management tends to better information security of organizations.

Scope And Limitations

The present study is done to understand the effectiveness of knowledge management practices adopted by some organizations in Odisha. The result of the study is based on 30 organizations from six sectors. The study could be done further by considering organizations from each sector to have a broader understanding.

Back Ground of the Study

In Odisha, the organizations are more or less Information Technology Enabled, doing most of their work through internet and various tools of Information Technology. The advances in computers and telecommunications made most businesses and many individuals dependent on computer network systems to carry out their daily activities. This escalates the possibility of criminal activities to misuse the sensitive organizational information both online and offline. The online criminal activity is known as Cybercrime.

Cybercrime is a new genre of criminal activity, having its origin in the growing dependence of modern life on computer systems. This refers to all criminal activities performed using the medium of computers, the internet, cyberspace and the World Wide Web.

Cybercrime includes traditional activities such as fraud, theft or forgery of data, computer sabotage, unauthorized access and copy of computer programs. It also can be defined as the act of creating, distributing, altering, stealing, misusing or destroying information through the computer. This is without the use of physical force and against the will of the victim. This creates challenges in maintaining Information security.

New generations of cybercrime has evolved with the advent of internet. These includes computer hacking, phishing , software piracy, industrial espionage, password breaking, spoofing, email bombing, spamming, pornography, credit card fraud, cyber terrorism, cyber laundering and other telecommunication frauds. This creates challenges in maintaining Network security.

Odisha is one of the 29 states in India, ranked as 9th largest state in area and 11th largest by population. The major industries in Odisha are manufacturing, mining, gas, electricity, water supply and construction. Contribution of the Industrial sector to the Gross State Domestic Product (GSDP) was estimated at 33.45% and contribution of Service sector is estimated to 51% in 2014-15. In order to achieve Millennium Development Goals (MDG) and human development objective, there is a rapid growth of organizations in various sectors. (Odisha Economic Survey, 2014-15)

The mushroom growth of organizations causes substantial rise in possibility of Cybercrime in Odisha. The authors have chosen the Service sector, looking towards its major contribution to GSDP in Odisha. The study has included various subsectors like Education, Finance, Retail, Logistic, Automobile and BPO.

Objective of the Study

The organizations are badly suffering from the various threats to their information and network systems. One reason for this could be lack of proper use of their knowledge management practices and poor understanding in the policies made for the same. Objective of the study is therefore,

"To study the effectiveness of knowledge management practices adopted by organizations in order to strengthen their information and network systems".

Methodology

The primary data are collected from 30 organizations, belongs to various sectors e.g. Education, Finance, Retail, Automobile, BPO and Logistics. The data are collected from two types of users e.g. Technical users and End Users. The instrument used for data collection is structured questionnaire and interviews.Judgmental sampling has been used for selection of organizations for the study. Thirty organizations in and around Bhubaneswar have been taken for the study. Random sampling is used for selection of respondents from each organization. A total of 200 respondents are chosen for the study, out of which 50 are Technical users and 150 are End users or Key users. The researcher has used both qualitative and quantitative techniques for data analysis. Chi-square test has been used to test the association between the knowledge management strategies adopted by organizations in various sectors. The SPSS 20.0, the statistical software is used to conduct analysis. The outcomes of the analysis are then presented and interpreted.

Chi- square test = $$\sum\left(\frac{(Observed value - Expected\ value)^2}{Expected\ value}\right)$$

Hypothesis of the Study

"Organizations have proper knowledge management policy and practices to secure their IT infrastructure."

Analysis and Discussion

The study is done on the basis of the primary data collected from 200 respondents from 30 organizations selected from 6 sectors. Two different structured questionnaires were followed for data collection from the different types of users. The respondents are classified as per the following dimensions.

Category of Respondents According to Job role

The respondents are categorized based on their job role, as shown in the Table 7.1.

Table 7.1: Category of Respondents According to Job role

Types of Respondents	Nos. of Respondents	Percentage
Technical User	50	25%
Key User	150	75%

Interpretation

The Table 7.1 shows the percentage of total 200 respondents included in the study. Out of total 50 (25%) are Technical Users and 150 (75 %) are Key Users.

Category of Respondents According to Sector

The sector wise percentage of total 200 respondents is shown in the Table 7.2.

Table 7.2: Category of Respondents According to Sector

Sector	Key User	Technical User	Total Users	Percentage
Education	49	19	68	33 %
Finance	39	14	53	26 %
Retail	29	7	36	19 %
Logistic	12	4	16	8 %
Automobile	9	3	12	6 %
BPO	12	3	15	8 %

Interpretation

The Table 7.2 shows the sector wise category of the respondents. Out of the total respondents 68 (33%) respondents are from Education Sector, 53 (26%) are from Finance Sector, 36 (19%) are from Retail Sector, 16 (8%) are from Logistic, 12 (6%) are from Automobile, 15 (8%) are from BPO Sector.

Asset Management

The respondents' views are recorded on the information asset management strategy adopted their organizations. The responses are summarized in the Table 7.3.

Table 7.3: Asset Management

Asset Manage ment	Response Yes	Percen-tage Yes	Response No	Percen-tage No
Have full list of its assets	44	88%	6	12%
Have identified user for its assets	28	56%	22	44%
Have idea on usage of assets over time	28	56%	22	44%

Interpretation

The Table 7.3 indicates the responses of 50 Technical users. It is observed that, 44(88%) respondents claimed that their organization have got full list of their assets.

28(56%) of respondents claimed that their organization have identified users for its assets. Same percentage of respondents reported that they have idea on usage of assets over time.

Source of Security Awareness

The respondents' views are recorded on theirsource of knowledge update on security attacks. The responses are summarized in the Table 7.4.

Table 7.4: Source of Security Awareness

Source of Security awareness	Responses	Percentage
Conferences	13	6%
Cyber Security Forums	8	4%
Research Publications	6	3%
Vendors/ Business partners	4	2%
Consultants	30	15%
Websites and Blogs	29	14%
Don't update	122	61%

Interpretation

The Table 7.4 shows the responses of 200 respondents i.e. 50 Technical users and 150 End users. It is found that 122(61%) of the total respondents claimed that they don't update their knowledge on information and network security breaches.

Identification and Assessment of Risks

The respondents' views are recorded on identification and assessment done by their organization on possible risks to information and network system. The responses are summarized in the Table 7.5.

Table 7.5: Identification and Assessment of Risks

Identification and Assessment done	Responses	Percentage
Yes	15	30%
No	35	70%

Interpretation

The Table 7.5 shows the responses of 50 Technical users. Out of the total respondents 35(70%) responded that their organizations have not done any identification and assessment of risks to their information and network system.

Allotment of Budget for Knowledge Management

The respondents' views are recorded on budget allotment by their organizations for Knowledge management. The responses are summarized in the Table 7.6.

Table 7.6: Allotment of Budget for Knowledge Management

Budget Available	Responses	Percentage
Yes	12	24%
No	38	76%

Interpretation

The Table 7.6 shows the responses of 50 Technical users. Out of total, 38(76%) respondents

indicated that they don't have any budget allotted for Knowledge management.

Internal Audit of Knowledge and Information Functions in Last Two Years

The respondents' views are recorded about the internal audits done by their organization in last two years in connection with Knowledge and information functions. The responses are summarized in the Table 7.7.

Table 7.7: Internal Audit for Knowledge and Information Functions

Conduct of Internal audit	Responses	Percentage
Yes	12	24%
No	38	76%

Interpretation

The Table 7.7 shows the responses of 50 Technical users. Out of total, 38(76%) respondents conveyed that they don't have any internal audit for Knowledge and information functions of their organizations in last two years.

Record Management Policy

The respondents' views are recorded on the availability of record management policy in their organizations. The responses are summarized in the Table 7.8.

Table 7.8: Record Management Policy

Record Management Policy	Responses	Percentage
Paper records	15	30%
Paper and Electronic records	22	44%
Don't have	10	20%
Don't required	3	6%

Interpretation

The Table 7.8 shows the responses of 50 Technical users. Out of total, only 22(44%) responded on availability of the policy for both paper and electronic records. Only, 15(30%) respondents agreed upon availability of the policy for paper records only. However, it is found that 10(20%) said they don't have any such policy and 03(06%) respondents don't feel the requirement of such policy.

Frequency of Annual Security Awareness Programs

The respondents' views are recorded on the frequency of annual security awareness programs organized by their organization. The responses are summarized in the Table 7.9.

Table 7.9: Frequency of Annual Security Awareness Programs

Frequency	Responses	Percentage
1 – 2 times	9	5%
3 – 4 times	0	0%
More than 4 times	0	0%
Happens, but not in a fixed schedule	30	15%
Does not happen	161	80%

Interpretation

The Table 7.9 shows the responses of 200 respondents, i.e. 50 Technical users and 150 End users. Out of total, 161(80%) respondents admitted that their organization don't conduct any Security awareness programs.

Effectiveness of Security Awareness Programs

The respondents' views are recorded on the effectiveness of security awareness training programs conducted for the employees of their organization. The responses are summarized in the Table 7.10.

Table 7.10: Effectiveness of Security Awareness Programs

Measure of Effectiveness	Responses	Percentage
Strongly Agree	7	5%
Agree	18	12%
Neutral	34	22%
Disagree	27	18%
Strongly Disagree	64	43%

Interpretation

The Table 7.10 shows the responses of 150 End users. Out of total, 27(18%) respondents conveyed that they are disagree and 64(43%) reported that they are strongly disagree on the effectiveness of security awareness programs.

User Assessment and Feed backing on Security Awareness

The respondents' were asked about theirassessment and feed backing on information and network security awareness by their organizations. The responses are summarized in the Table 7.11.

Table 7.11: Assessment and Feed backing on Security Awareness

Have Assessment and Feed backing?	Responses	Percentage
Yes	9	6%
No	141	94%

Interpretation

The Table 7.11 shows the responses of 150 End users. Out of total, 141(94%) respondents agreed upon the fact that they have neither been assessed on their knowledge on information and network security nor got any feed backed on their present status.

User Access to Cyber Risk Related Information

The respondents' views were recorded on their access to cyber risk related information available with their organization. The responses are summarized in the Table 7.12.

Table 7.12: User access to Cyber Risk Related Information

User Access	Responses	Percentage
Yes	19	13%
No	131	87%

Interpretation

The Table 7.12 shows the responses of 150 End users. Out of total, 131(87%) respondents reported that they don't have any access to the information related to cyber risk available with their organization.

Chi Square Test

H_0 Null Hypothesis

Knowledge and information management strategy is independent of sectors.

H_1 Alternate Hypothesis

There is an associationinthe knowledge and information management strategies adopted in various sectors.

Table 7.1: Knowledge and Information Management Strategy

Sector		Knowledge and Information Management Strategy		Total
		Yes	No	
Education	O	6	62	68
	E	*20.4*	*47.6*	
	χ^2	-10.16	-4.36	
Finance	O	39	14	53
	E	*15.9*	*37.1*	
	χ^2	-33.56	-14.38	
Others	O	15	64	79
	E	*23.7*	*55.3*	
	χ^2	-3.19	-1.37	
Total		**60**	**140**	**200**

O-Observed value, E-Expected value

The hypothesis has been tested using Chi-square test to find the association between the various sectors in their knowledge and information management strategy. The findings are given below.

Calculated χ^2 = 67.027,
df = 2,
Tabulated χ^2 = 5.991,
P(χ^2 > 67.027) = 0.0000

At 5% level significance, it is found that calculated value of χ^2 (67.027) is greater than Tabulated value of Chi-square (5.991), i.e. χ^2cal (67.027)>χ^2tab (5.991). Also p-value is less than .05, hence the Null hypothesis is significant, i.e., rejected. This means, There is an association in the knowledge and information management strategies adopted in various sectors.

Discussion of Findings

The findings of the study is as per the followings,

1. Most of the organizations do focus on proper use of their assets. However, it is observed from 44% users that their organization don't have identifiers for their assets and they don't have an idea on the usage of assets over time. This indicates that there is ample scope of mishandling of information assets in the organization.
2. Most of the users are ignorant about the security breaches happening on day to day basis.
3. The majority of organizations don't do identification and assessment of risk to their information and network systems.
4. The majority of organizations don't keep any budget for the purpose of knowledge management.
5. Most of the organizations don't conduct any internal audit related to Knowledge and information functions.
6. About 56% of organizations don't have any policy for managing paper and electronic records. Therefore, these organizations are under serious security threats.
7. About 80% of organizations don't conduct any security awareness programs. Others are not conducting the programs in a fixed schedule and the frequency is very less.
8. The majority of respondents are not convinced with the effectiveness of security awareness training programs conducted by their organizations.
9. Most of organizations don't focus on assessment of the employee's knowledge on information and network security and to feedback them.
10. Majority of organizations don't stresses upon creating awareness among employees on the risks associated with information and network security.
11. There is an association in the knowledge and information management strategies adopted in various sectors.

Based on the above findings, it is seen that most of the organizations don't have proper knowledge management policy and practices to secure their IT infrastructure.

Conclusion

The finding of the study reveals that, most of the organizations have not taken the asset management practices religiously. The awareness level of users about the information and security is found to be very poor. Organizations don't take much initiative to enhance the user awareness about information and network security.Most of the employees are not given quality training programs, never been evaluated on their knowledge and never feed backed onthe improvements required. It is found that most of the organizations don't have any budget for knowledge management functions. They neither do risk management nor conduct audit for to assess the threats related to information and network security. This can have a serious impact on their security systems. Most of the organizations don't have any policy for management of paper and electronic documents. It can cause the theft of sensitive information of the organizations. The authors also found that the need andefficacy of knowledge and information management strategy adopted by organizations differs in various sectors. Therefore, it is concluded that most of the organization irrespective of the sectors they belongs to, are under severe threats of security breaches. They need to assess their strengths of existing knowledge management practices and take necessary steps as suggested below.

Suggestions

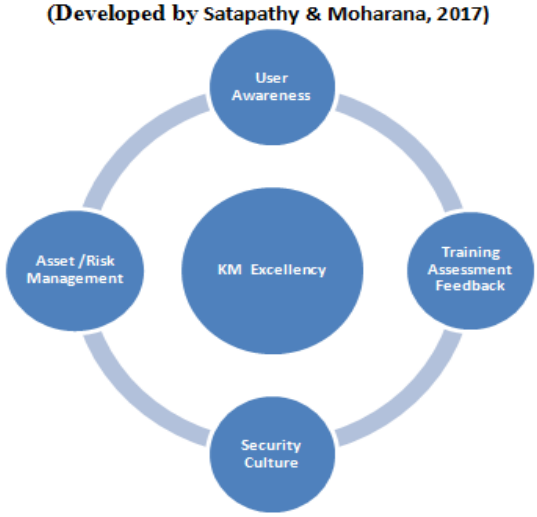
Based on the findings from the study the following suggestions would be helpful for organizations.

1. Organizations should proper management of their information assets. They should maintain a list of all information assets available with them. They must identify appropriate users for each asset and define the usage of assets over time.
2. Organizations must take initiative to enhance the information level of their employees in terms of information and network security. The

employees need to be given well devised training programs imposing the qualitative values. In certain intervals, the employees need to be assessed on their awareness level in security perspective and need to be given proper feedback individually for their improvement.

3. The organizations must fix some budget for information and knowledge management functions. This will facilitate different initiatives to protect the information and network system from various threats.
4. Organizations need to introduce well devised risk management practices to identify, assess and mitigate various possible threats to their information systems.
5. Organizations must do timely security audits to ensure a secure work environment.
6. Every organization must have a well thought policy for managing their paper as well as electronic records.

Competency, Reliability and Security (CRS) Model (Developed by Satapathy & Moharana, 2017)



The models pertaining to knowledge management came across the study seems incomplete without the security with human face. As man is precious of all the resources and simultaneously, man is danger of all resources; no technology, no system, no methods will lead to excellence unless there is a culture of **C**ompetency, **R**eliability and **S**ecurity (**CRS**).

References

AlHogail, A., & Berri, J. (2012). Enhancing IT security in organizations through knowledge management. 2012 International Conference on Information Technology and e-Services, (pp. pp. 1-6).

Belsis, P., Kokolakis, S., & Kiountouzis, E. (2005). Information systems security from a knowledge management perspective. Information Management & Computer Security, XIII(3), 189-202.

Bhatt, G. D. (2001). Knowledge management in organizations:examining the interaction between technologies,techniques, and people. Journal of Knowledge Management, V(1), 68-75.

Chang, C. L.-h., & Lin, T.-C. L. (2015). The role of organizational culture in the knowledge management process. Journal of Knowledge Management, XIX(3), 433-455.

Edenius, M., & Borgerson, J. (2003). To manage knowledge by intranet. Journal of Knowledge Management, VII(5), 124-136.

Gallo, M. A., & Hancock, W. M. (2005). Computer Communication and Network Technologies. Thomson.

Ghansela S. (2013). Network Security: Attacks, Tools and Techniques. International Journal of Advanced Research in Computer Science and Software Engineering, III(6).

Massingham, P. (2014). An evaluation of knowledge management tools: Part-I-managing knowledge resources. Journal of Knowledge Management, XVIII(6), 1075-1100.

McDermott, R., & O'Dell, C. (2001). Overcoming cultural barriers to sharing knowledge. Journal of Knowledge Management, VI(1), 76-85.

Moharana, C., Pal, M., & Rout, D. (2012). INFORMATION AND NETWORK SECURITY IN E-GOVERNANCE: PERSPECTIVE AND ISSUES. International Journal of Research in Engineering, IT and Social Sciences, II(11), 1-16.

Odisha, G. o. (2014-15). Odisha Economic Survey. Bhubaneswar, Odisha: Directorate of Economics and Statistics ,Government of Odisha.

Randeree, E. (2006). Knowledge management: securing the future. Journal of Knowledge Management, Volume 10(Issue 4), pp. 145-156.

Roy, S., & Saxena, M. (2010). Role of Knowledge Management in Enhancing Information Security. IJCSI International Journal of Computer Science Issues, Volume 7(Issue 6), pp. 320-324.

Ryan, J. J. (2006). Knowledge management needs security too. VINE Journal of Information and Knowledge Management Systems, Volume 36(1), pp. 45-48.

Saida, A. R., Abdullahb, H., Ulib, J., & Mohamed, Z.A. (2014). Relationship between Organizational Characteristics and Information Security Knowledge Management Implementation. Procedia- Social and Behavioral Sciences (pp. 433-443). ELSEVIER.

Wali, A. F. (2013). Information Technology Infrastructure and Customer Service Delivery. British Journal of Marketing Studies, I(2), 17-32.