A Knowledge Management Model to Improve Information Security

Yogesh Kumar Mittal[1], Dr Santanu Roy[2] and Dr. Manu Saxena[3]

[1] Ajay Kumar Garg Engineering College
Ghaziabad,Uttar Pradesh, India
Research Scholar, Singhania University
Jhunjhunu,Rajasthan,India

[2] Institute of Management Technology
Ghaziabad,Uttar Pradesh, India

[3] Human Resource Development Centre
Ghaziabad,Uttar Pradesh, India

Abstract

Information security is an important issue in today's world. Information security management can no more be done by merely a set of hardware and software, rather, it requires a complete end-to-end system. Such a system is called Information Security Management System. We have proposed a model to improve Information Security using knowledge management techniques. The model has three modules naming information security knowledge repository module, information security knowledge sharing and dissemination module and information security knowledge Implementation & effectiveness module, first module is to store the information security knowledge in a systematic and easy to use format, second module promote sharing and dissemination of knowledge, third module is responsible to monitor and measure effectiveness of total system respectively. We have allocated knowledge management tools to each module to achieve goals of each module, then we have analyzed relationship between these modules.

Keywords: *Information Security Management, Information Security, Knowledge Management, Information Security Knowledge Management*

1.0 Introduction

Managing the growing problem of computer frauds has led researchers and practitioners to emphasize the need to take into account the 'social' aspects of information security(IS). In addition, wider organizational issues such as lack of awareness have been associated with computer fraud. Inspecting the domestic and foreign each kind of information security event, it is discovered that behind information security events, those who play the decision role is the human, human's behavior and the information security is closely related, human's unsafe behavior causes accident's primary cause[1]. It requires

special focus and participation from all levels of employees with full commitments and responsibilities in establishing such a system and implementing it. In trying to minimize 'opportunities' for computer fraud, managers' awareness and knowledge of how an organization information security functions can significantly affect the effectiveness of management of information security. This is because managers can send 'cues' to other employees, which influence how the latter perceive and abide by information security and other policies and procedures in their daily activities [2]. When InfoSec meets Knowledge Management(KM) on process level, security knowledge can be helpful to enhance the effectiveness and maturity of InfoSec[3]. In managerial view, the security problems are invoked because of the short of knowledge to protecting the targets (systems)[4]. In this paper we are proposing an Information Security Knowledge(ISK) Management model.

2.0 Knowledge Management Model to Improve Information Security

The proposed model consists of three modules(refer fig. 1).

2.1 ISK Repository Module

In this module we will store knowledge related to IS. This will include:

(a) Standards: Information Security Management System(ISMS) standards like ISO 27001, COBIT and other standards may be stored.
(b) Best practices: Industry specific best practices are always evolving with experience. People like to contribute and refer to these practices.
(c) Threats and solutions: Information related to current threats and solutions should be stored, which can be easily referred by the users.

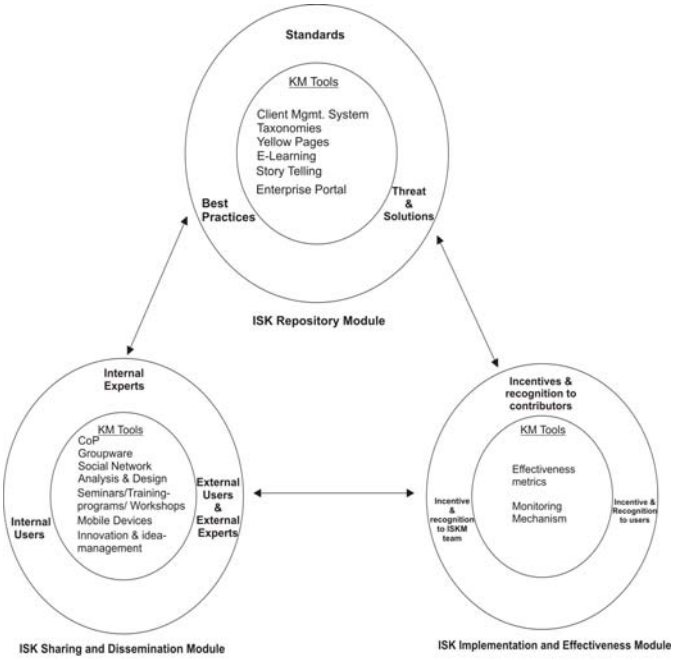

Fig 1 Knowledge Management Model to Improve Information Security

2.2 ISK Sharing and Dissemination Module

This module includes sharing ISK between stake holders, disseminate this knowledge to the concerned people and update the ISK repository with the new created knowledge by the users. This module will include:

(a)Internal experts: Internal information security experts are mainly responsible for any type of security breaches in the organization. They have to address security related issues of the organization and to ensure that the users are understanding and applying this information.

(b)Internal user : Internal users should keep themselves updated with IS related knowledge because they are on the edge of information system. Users may find new problems or ambiguous situation to be discussed with the experts.
(c)External users and external experts: Organizations are having extended networks in the form of suppliers and customers, they may also face IS problems. Company's authorized external experts may also take part in sharing the ISK. External experts are having links with the other companies and outer world also, so they can help in sharing. Knowledge regarding coming up IS threats and solutions.

2.3 ISK Implementation & Effectiveness Module

In this module we want to ensure that ISK is implemented and the whole exercise of information security knowledge management(ISKM) is effective. This module has three components:

(a)Incentives and recognition to contributors: One of the major problem in application of KM is that experts/knowledgeable persons don't want to share their knowledge, so here we emphasize that incentives recognition and incentives should be given to the contributors of Knowledge.

(b)Incentives and recognition to ISKM team: Overall IS effectiveness should be measured in terms of reduction in IS incidents and better awareness of employees. ISKM team's effort should be recognized and incentives should be given.

(c)Recognition to users: Users should also be recognized for their active participation, awareness and effectively applying the knowledge available through ISKM activities. Incentives should also be given to the users for their remarkable Knowledge application and contribution for ISKM activities.

Above described ISKM activities are to be implemented through the KM tools. Now we will analyse, role of KM tools.

3.0 KM Tools for ISKM Implementation

Following KM tools can be used to develop a well structured ISK repository.

3.1 KM Tools for ISK Repository Module

(a)Content management system: Content related to standards, best practices, new threats and solutions may be stored in a well structured manner using content management system.

(b)Taxonomies: Many times, it is difficult to understand the meaning of the technical terms by the common users. Taxonomies is the way of naming technical terms in a natural way or using metaphors and then grouping the information in a convenient way keeping user in view.

(c)Yellow pages: Yellow pages is like a directory of experts, In which one can search the experts in no. of ways. It may be on the basis of expertise, on the basis of location, on the basis of name of expert etc.

(d)E-Learning: E-Learning methods like interactive video lectures, quizzes etc can be used by the users sitting anywhere in the world to grasp the basic and advanced knowledge related to IS. This may include knowledge related to standards, best practices, new threats and solutions etc.

(e)Story telling and narrations: This KM technique can be used to explain concepts like social engineering, virus attacks, disaster and recovery activities etc.

(f)Enterprise portals: This tool can be used as a gateway for all type of information security knowledge and ISKM activities which can be accessed from any where in the world.

3.2 KM Tools for ISK Sharing and Dissemination Module:

Following KM tools can be used for ISK sharing and dissemination.

(a)Communities of practice(CoP): Online CoPs may be formed by stakeholders. Different type of CoPs may be formed on the basis of their expertise, interest and usage.

(b)Groupware: To disclose knowledge personnel affinity is very important. Group ware develops that affinity using the group dynamics. People become closer using these groups and knowledge sharing become easier.

(c) Social network analysis and design: People want to connect socially instead of professionally. Providing opportunities for social networking helps in making social relations. This helps in knowledge sharing. Social network analysis and design will help in designing social networks as per the need and social attributes of the people.

(d)Seminar/training programs/ workshops: Regular seminars/training programs and workshops can help the users and other stake holders to upgrade their knowledge and skills.

(e)Mobile devices : Mobile devices can be used to update the security related knowledge immediately and on the move and any where in the world. Like new virus attacks or any disaster condition can be informed immediately.

(f)Innovation and idea management: Through innovation and idea management system new ideas may be created, nurtured and perfected. The persons contributed that idea may be recognized and rewarded.

3.3 KM Tools for ISK Implementation & Effectiveness Module

Implementation of Information Security is the main aim of ISKM. Here we should have following tools.

(a)Effectiveness metrics: Effectiveness metrics should be engineered. Which may include points for user involvement and implementation, reduction in security incidence, contribution, KM team effectiveness etc. On the basis of this metrics rewards and recognition should be given to the contributors, users and ISKM team.

(b)Monitoring Mechanism: A monitoring mechanism is required to get the information about contributors, active users & over all information security performance. This can be done by preserving logs of knowledge sharing sessions, security incident logs, feedback from different stake holders.

4.0 Relationship between ISK Repository Module, ISK Sharing & Dissemination and ISK Implementation & Effectiveness Module:

All the three modules have to interact with each other and take help from each other to fulfill their objectives. ISK repository will store all types of knowledge available and

captured in second module. Second module will create new knowledge but may need to access already created knowledge from the first module whenever required. This way second module will enrich the knowledge repository of the first module. Third module is related to implementation and effectiveness, it will refer the captured knowledge for solving day today IS routine work, it will search solution of a particular problems in first module, it may refer second module for newer problems. Both first and second module will receive feed backs from the third module regarding effectiveness of the solutions available in first module and second module.

5.0 Conclusion

Proposed model uses KM techniques to effectively educate users regarding information security. This Model describes how different KM tools can be used for different functions of information security knowledge management. All the three modules of this model should be in sync for getting better results from ISKM efforts. This model can be applied for other areas where knowledge is changing with time and updating of stakeholders with that knowledge is important.

References

[1]Behavioral science-based information security research, Yang yue jiang Yu yong xia, 2009, First International Workshop on Education Technology and Computer Science IEEE

[2]Knowledge management within information security: the case of Barings Bank, Shalini Kesar, International Journal of Business Information Systems 2008 Vol. 3, No.6 pp. 652 - 667.

[3]Knowledge-Centric Information Security, Walter S. L. Fung, Richard Y. K. Fung, 2008 International Conference on Security Technology, IEEE

[4]Knowledge Management Tools & Techniques, Practitioners & Experts Evaluate KM Solutions, Madan Mohan Rao, 2005 Elsevier

[5]Knowledge Management in Theory and Practice, Kimiz Dalkir, ,2005, Elsevier Inc.

Yogesh Kumar Mittal did B.Tech. from Maulana Ajad College of Technology, Bhopal, India (Now MANIT, Bhopal) in 1987 than M.Tech. in Computer Science and Technology from University of Roorkee, Roorkee, India (Now IIT Roorkee) in 1989. He also did PGDBM from IMT, Ghaziabad, India in 1993. He qualified prestigious CISA (Certified Information System Auditor) exam in 2001. He has around 21 years of experience in industry and academia. He has worked as Consultant, Information System Auditor, General Manager and Chief Executive Officer before joining the teaching profession. He published 10 papers in National/International conferences/journals. His academic and research interest includes IT in Business, Knowledge management, Software Project Management, Enterprise Resource Planning, Software Engineering, Information security and Auditing, Social and Cultural issues.

Dr. Santanu Roy is currently serving as a Professor, Operations Management Area, at Institute of Management Technology (IMT), Ghaziabad, India. Dr. Roy had earlier served as a Senior Scientist (Scientist F) in National Institute of Science, Technology and Development Studies (NISTADS), New Delhi. Dr. Santanu Roy has done his Ph.D. in Industrial Engineering and Management from IIT Kharagpur, India and Integrated Master of Science (M.S.) from IIT Delhi. He has more than 26 years of experience in research, consultancy and teaching.

Dr. Manu Saxena did B. Sc. in 1977 from , Meerut University, India, M. Sc. in 1979 from University of Roorkee, Roorkee, India Ph. D. from University of Roorkee, Roorkee, India in Operational Research in 1988. He published 19 papers in national/international conferences and journals. He supervised 13 dissertations of post graduation level.