Role of Knowledge Management in Enhancing 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

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 analyzed 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.

***Keywords**: Knowledge Management, Information Security, Knowledge Management Tools, Information Security Challenges.*

1.0 Introduction

Due to fast pace of change in IT technology and its important applications, new security threats evolves around it. New and smart methods of information security are also devised by researchers to mitigate the risk occurred due to these threats. In the last decade process based information security management system(ISMS) such as ISO27001 and COBIT have emerged. Many organizations since then have adopted such ISMS. Knowledge Management(KM) is another management discipline enterprises employ, with aim to foster a more effective management of knowledge[1].

Organizations sometimes spend substantially on firewall, proxy, antivirus, intrusion detection mechanism, digital signatures, special network devices and protocols etc., assuming that security of information can somehow be ensured by procuring these technology solutions from the market. This is a wrong notion because security management is more of managing an end-to-end system rather than just installing technical solutions. As like any other full-fledged system, this has many components including people, policies, procedures, processes, standards and technology[2].

Information may be stored in a server, PC, Laptop, mobile phone or in any other device, it may be in transit from one place to another place through some communication channel, or may be under processing through a program, security of the information may be breached at any stage. Confidentiality, integrity and availability are the three major information security considerations. Protection of information is just not dependent on only information security people of the company but all the users. All the user of information system are like on the gates of a building and the gate opening by any of the employee may prove fatal for the safety of the whole information system. Inspect the domestic and foreign each type of information security event to discover that 70-80% are because the internal personnel negligence or intends to divulge creates, 20-30% are because the hacker invades or other external reasons creates[3].

2.0 Information Security Challenges

In general, the information security management of an organization broadly deals with the processes and procedures that the employee should adhere to in order to protect the confidentiality, integrity and availability of information and other valuable assets. The standard approach to managing information security involves conducting a risk analysis to identify risks to confidentiality, integrity, and availability of information systems, which is followed by risk management where safeguards are employed to mitigate those risks[4] .With this definition in mind, the main goals of information security within organizations are to reduce the risk of systems and organizations ceasing operations; maintain information confidentiality; ensure the integrity and reliability of data resources; ensure the uninterrupted availability of data resources and online operations; and ensure compliance with national security laws and privacy policies and laws. Thus, management of information security involves implementing and maintaining information security policies and procedures to minimize 'opportunities' for threats like computer fraud [12].

Knowledge of information security is essential for all the employees or users as per their requirements. Lot of information on information security is available through books, internet, journals etc., but people don't use this information because:

1. Getting particular useful information out of a glut of information is very difficult and time consuming.
2. Users may not aware about importance of information security, they feel that it is the work of information security staff or IT department.
3. Lack of motivation in getting Information security knowledge.
4. Information Security experts not willing to share the knowledge with the users.
5. Communication gap or social gap between users and experts.
6. Users may not know, who is the expert for particular security issue.
7. Users are very busy in their regular work.
8. Infrastructure not available to communicate.
9. Geographical distance between users and experts.
10. Lot of knowledge is experience based or in tacit form and need to be codified to be shared or require a proper platform to share.

So, there may be number of reasons of unawareness about security threats and remedies. But the result is really horrible in terms of security incidents which may lead to information leaks, non availability, compromise on integrity etc. and huge losses in terms of reputation, loss of customers and direct monitory loss[5].

3.0 Role of KM in Information Security

The role of Knowledge management is really important to manage the knowledge of information security as Knowledge Management has been defined as "the capability by which communities capture the knowledge that is critical to their success, constantly improve it, and make it available in the most effective manner to those who need it"[13]. According to Granneman [6] most people do not secure their computers or act in a secure manner. The main reason being that the average user just does not know what to do. This is alarming, considering that 65.9% of the Australian population are Internet users [7] and the success of the 2000 LOVELETTER virus and 2003 Blaster/SoBig worms were largely due to individuals uneducated in information security issues [8]. A holistic understanding of e-security and privacy issues is vital for the individual as well as for the society. Therefore key considerations and possible solutions include:

Education and Awareness – Education and awareness efforts targeting existing and emerging new threats, risks, vulnerabilities, countermeasures and safeguards are required.

Foster a security conscious culture – A security culture where compliant attitudes, behaviors and sensitivity to privacy and security become second nature and assumed throughout every day life[9].

Knowledge management is enabling and enhancing capabilities to perform such processes, including sourcing and deployment of the right knowledge assets, in order to achieve the desired results. Knowledge assets include embodied knowledge in people; embedded knowledge in technology, systems and processes; enculturated knowledge in work relationships, teams and networks; and actionable information and insights[10].

Three major phases of KM cycles are:

1. Knowledge capture and /or creations
2. Knowledge sharing and dissemination
3. Knowledge acquisition and application

Knowledge capture refers to the identification and subsequent codification of existing knowledge and know how with in organization and/or from the environment. Knowledge creation is the development of the new knowledge and know how or innovations that did not have previous existence with in the company like from experts, research papers etc.. Once it has been decided that the new or newly identified knowledge is of sufficient value, the next step is to contextualize this content. Contextualize means giving link to the contributors of that knowledge and tailoring it towards the target users. Then the knowledge is shared and disseminated. The knowledge is disseminated to the users using portals , emails and other KM tools. Users apply the knowledge and with their experience also new knowledge is generated and captured. Knowledge management advocates different type of recognitions and incentives for the people who are sharing their knowledge and the people who are actively using the knowledge to improve their knowledge and performance.

Knowledge management has multi dimensional benefits at different levels from individuals to organization such as for individuals, it helps people to do their job in an efficient way through better decision making and problem solving. Help people to keep up to date. On community level, promotes peer to peer knowledge sharing. At the organization level, diffuse best practices, builds organizational memory. In other words, knowledge of how an organization functions in the context of management of information security can significantly impact the effectiveness of procedures in minimizing 'opportunities' for computer fraud.

4.0 Application of KM Tools for Information Security:

In order to design successful tools for knowledge sharing, a strategy needs to be chosen. Hansen et al. distinguish two main knowledge management strategies: *codification and personalization. Codification* is the people-to documents strategy. Here the effort is to load intranets and databases with best practices, case studies and how-to guides to help people in their day-to-day work[11]. *Personalization* is the people-to-people strategy. Here the effort is to link people with other people and to grow networks and community of practices. Emphasis is on informal-knowledge sharing.

Following KM tools may be used for improving information security:

1. Content Management
2. Knowledge Taxonomies
3. Groupware
4. Online Communities of Practice
5. Enterprise Portal
6. Social Network Analysis and Design
7. E-learning
8. Storytelling and Narrations
9. Wireless tools for knowledge Mobilization
10. Innovation and idea management system
11. Tools for extending KM across organizational boundaries

4.1 Content Management :

A well designed content platform must be able to handle multiple content types, sources and access patterns. Theses content sources include security related libraries, activities and personnel directories. Content can be structured or unstructured. Some of it is generated online during various knowledge activities(e.g. on line brain storming).

Organizations may use content management system for information security best practices, lesson learned, security case studies etc.. Content teams, meta data, knowledge maps, and a workflow contextualization can ensure effective reuse of the content. Advanced content management system include features for seamless exploration, authoring templates, maintaining integrity of web pages and links, periodic review, archiving, meta-data, version control, rule setting, indexing, audits, authorized access, administration alerts, and flexible repurposing for multiple platforms and formats.

4.2 Knowledge Taxonomies**:**

Taxonomy is the practice and science of classification according to natural relationships.
The info-glut or "digital sprawl" on corporate intranets has led to users not being able to find relevant information in time and numerous taxonomy development tools are coming to the rescue. It must reflect the needs, behaviors, tasks and vocabulary of the users, and be able to provide multiple paths and points of view. Taxonomy should be easy to maintain and users should find it easy to understand, navigate and contribute. It will help the users to easily locate specific information security knowledge.

4.3 Groupware:

Desirable features for collaboration in the context of KM include affinity building, knowledge mapping, threading, polling, group document creation, rating, anonymity and access management. A notable trend in tools for collaboration between networked employees is the convergence between asynchronous (e.g. collaborative document management) and synchronous(e.g. instant messaging) service. It is an important tool for knowledge sharing among the peer groups. It is an important tool to disseminate information security information instantly to a group like information regarding new virus attacks.

4.4 Online Communities of Practice(CoP):

Online communities constitute a growing part of the organizational landscape of 21st century global players, but businesses are still at the early stages of individual and organizational optimization of web based communities. Online CoPs are emerging as powerful tool for knowledge exchange and retention. Participation levels in CoPs can be segmented into core, active, and peripheral. Success levels can be diagnosed via the application of knowledge., in the form of interviews anecdotes and employee survey. Expertise directories are a useful way for connecting knowledge worker in such forming communities, but they must connect people and not just resumes. CoPs are particularly useful in discussing current security related problems and come out with solutions.

4.5 Enterpriser Portal

Portals help create the “on demand” workplace, customized to individual employee needs. A well-designed portal can serve as a delivery channel for KM applications any time, any place, and on any device. Knowledge portals are the single point of interaction and coordination for collaboration. General user may reach the portal for getting their solutions of security related problems and current security scenario.

4.6 Social Network Analysis and Design

Social network analysis (SNA) is emerging as a powerful tool for mapping knowledge flows and identifying gaps. SNA can be used to reinforce existing flows and to improve knowledge integration after activities like mergers and acquisitions. Natural language techniques, visualization tools, and recommender systems can be harnessed here, leading to actions like identifying key individuals for retention or expended roles or creating teams for cross-organizational and cross-functional activities. Direct applications of SNA include security process redesign, role development, and improved collaboration between knowledge seekers and providers. SNA can help identify central people, connectivity levels of individual knowledge workers, diversity of subgroups, and level of organizational inter-connectivity. Getting things done often depends less on formal structure than on informal net-works of people. SNA can help improve general security environment by disseminating information security knowledge naturally and effortlessly.

4.7 E-learning

One interesting emerging development on the KM front is the growing convergence of viewpoints between the KM community and the e-learning community. The concept of KM can be united with the goals of e-learning to create the larger ideal of a learning organization-via blended learning, skills directories integrated with course delivery, and the interleaving of working and learning. KM and learning management are two complementary disciplines that are continuously growing closer and support an innovative and agile enterprise. For training of new recruits about information security and for training of new security technologies, e-learning may be very useful.

4.8 Storytelling Narratives

Personal storytelling builds community and can revitalize the way we do business. Non-traditional business communication techniques like art, theatrical tools and even a poetry can improve internal and interpersonal communication. Stories are good framework for sharing information, meaning and knowledge. Blogs encourage story-telling and foster understanding because they usually offer context. Social engineering type of attacks can be easily described using these techniques.

4.9 Wireless Tools for Knowledge Mobilization

One of the most notable emerging trends in workforce connectivity is the increasing use of mobile technologies to take “KM” to another dimension-“knowledge mobilization”-by bringing relevant knowledge directly to the fingertips of a company’s road warriors and field-workers via cell phones, PDAs, industry-specific handheld devices, Wireless Local Area Network (WLAN), and Radio Frequency Identification (RFID) tags. While personal computers (PCs) and workstations have come under some criticism for “tethering” knowledge workers to their desks, wireless technologies may be the perfect answer to “mobilizing” the workforce by letting them capture and harness key information and knowledge attributes wherever they are, whenever they want, and however they want. This tool enables information security knowledge to be disseminated for the people on the move and it is immediate.

4.10 Innovation and Idea Management Systems

Managing an innovation pipeline, promoting an “idea central” or ideas marketplace, and creating the “hundred headed brain” are some creative approaches being adopted by KM pioneers. KM also helps organizations increase the efficiency of innovation by improving access to experts and tapping into past innovations. New innovative ideas and information security solutions can be evolved using these systems.

4.11 Tools for Extending KM across Organizational Boundaries

Online services such as dial-up bulletin boards and web communities have actually helped network communities of interest across the globe for years. The world Bank has leveraged a strategy of "global knowledge, local adaptation" for brokering global knowledge exchanges. Information Security knowledge can be accessed from all over world to be applied in the company.

5.0 Conclusion:

We can see that to deal with the ever changing nature of information technology and the newer security threats coming up at a very fast pace, we need some technique to educate the users in an effective manner. KM tools can be used to evolve newer, economical and faster methods to deal with information security issues. KM tools like content management may be used to create content and update information security knowledge like information security standards and best practices, taxonomies to easily understand and locate the right and required information, CoPs for consulting with each other and giving a feeling of belongingness to share the knowledge. Enterprise portals can be used as a single point of contact for all the interested stakeholders. E-learning methods may be used to educate the new joiners and to train on the latest developments in the area. Storytelling is good for understanding point of view and social aspects. Wireless tools make the person free from a specific location and person on the move may get the latest knowledge. Innovation is the key for the new solutions. Lot of research and innovations are taking place in information security field. KM can encourage people to give new ideas and rewarding them accordingly. This way we can see that there is a lot of scope to improve information security using knowledge management techniques.

References:

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

[2]Information Security Management - A Practical Approach,2007,Manik Dey, , IEEE

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

[4]Knowledge Based Model for Holistic Information Security Risk Analysis,2008 Wen Huang, Yong-Sheng Ding, Zhi-Hua Hu, Jing-Wen Huang, 2008 International Symposium on Computer Science and Computational Technology, IEEE

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

[6] S. Granneman, "A Home User's Security Checklist for Windows,"SecurityFocus,2004. http://www.securityfocus.com/columnists/220

[7]Nielsen/NetRating, "Top Rankings," Netrating, Inc., 2004. http://www.nielsen-netratings.com/

[8]CERT/CC and Carnegie Mellon University, "CERT/CC Overview Incident and Vulnerability Trends," 2003. http://www.cert.org

[9]The Multifaceted and Ever-Changing Directions of Information Security – Australia Get Ready!, Leanne Ngo and Wanlei Zhou, 2005 Proceedings of the Third International Conference on Information Technology and Applications (ICITA'05) IEEE

[10]Knowledge Management in Asia: Experience and Lessons 2008,Report of the APO Survey on the Status of Knowledge Management in Member Countries.

[11] Collaboration and Knowledge Sharing Platform for supporting a Risk Management Network of Practice Katerina Papadaki, Despina Polemi, 2008, The Third International Conference on Internet and Web Applications and Services, IEEE

[12] BSI 2002

[13] Birkenkrahe, M. (2002). How large multi-nationals manage their knowledge. Business Review, 4(2), pp. 2-12.

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.