Volume 5, Issue 1, January 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Function of Knowledge Direction in Heightening Information Security

[1]Shreay Mehrotra, [2]Prof Vibhor Mehrota

[1]Student of B.tech Cs & Engg.

[2]Asstt Prof Deppt of Computer Science & Engg SSVIT Bareilly, India

Abstract: User's cognition of information protection is one of the crucial factors in data protection management as 70-80% protection commotions happened due to carelessness or unknowingness of exploiters. In this paper we have examined the utility of cognition management tools to quickly capture, store, share and circulate the information protection related cognition with the view that it should be effectively enforced by the data system users. We found that the cognition management tool can be used to heighten the information protection.

Keywords: Cognition Management, Information Protection, Cognition Management Tools, Information Protection Challenges.

I. INTRODUCTION

Due to fast stride of exchange in IT engineering and its significant applications, new protection menaces develops around it. New and smart procedures of information protection are also invented by investigators to extenuate the risk happened due to these menaces. In the last decade procedure based information protection management system (ISMS) such as ISO27001 and COBIT have emerged. Many establishments since then have assumed such ISMS. Knowledge Management (KM) is some other direction discipline endeavors employ, with aim to foster a more efficient direction of knowledge [1].

Organizations sometimes expend considerably on security system, proxy, antivirus, violation catching mechanics, digital signatures, particular network devices and protocols etc., assuming that protection of information can somehow be assured by procuring these technology solutions from the market. This is a wrong notion because security management is more of dealing an end-to-end system rather than just installing proficient solutions. As like any other fully fledged system, this has many elements admitting people, policies, processes, processes, standards and technology [2].

Information may be hived away in a waiter, PC, Laptop, mobile phone or in any other device, it may be in pass through from one place to another place through some communication channel, or may be below marching through a program, protection of the information may be gapped at any stage. Concealment, unity and availableness are the three major information protection circumstances. Protective cover of information is just not depending on only information protection people of the company but all the users. All the user of data system are like on the gates of a building and the gate opening by any of the employee may demonstrate fatal for the safety of the whole information system. Scrutinize the domestic and extraneous each type of data security event to discover that 70-80% is because the internal personnel department negligence or means to divulge creates; 20-30% is because the cyber-terrorist invades or other external reason creates [3].

II. INFORMATION PROTECTION DISPUTES

In general, the information protection management of a governing body generally deals with the procedures and procedures that the employee should bind to in order to defend the circumspection, wholeness and accessibility of information and other worthful assets. The standard approach to dealing information protection demands carrying on a risk analysis to distinguish risks to concealment, unity, and accessibility of information systems, which is complied by risk management where precautions are applied to extenuate those risks[4] .With this resolution in mind, the main goals of information protection within establishments are to cut down the risk of establishments and organizations ceasing operations; maintain information circumspection; ensure the integrity and dependability of data resources; ensure the continuous accessibility of data resources and online procedures; and ensure abidance with national protection laws and privacy policies and laws. Thus, management of information protection involves enforcing and maintaining selective information protection policies and processes to denigrate 'chances' for threats like computing machine fraud [12].

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

1. Getting especial useful data out of a glut of data is very unmanageable and time taking.
2. Users may not cognizant about grandness of data security; they feel that it is the work of data security staff or IT department.
3. Lack of motivation in acquiring Data protection cognition.

4. Information Protection individuals not willing to share the knowledge with the users.
5. Communication gap or social gap amongst users and experts.
6. Users may not know who the practiced for exceptional security issue is.
7. Users are very engaged in their unconstipated work.
8. Infrastructure not available to transmit.
9. Geographic distance between users and experts.
10. Lot of cognition is go through based or in tacit form and need to be statute to be shared or require a proper platform to share.

So, there may be number of concludes of unknowingness about protection threats and cures. But the consequence is really frightful in terms of protection commotions which may lead to data leaks, non availability, compromise on integrity etc. and huge losses in terms of repute, loss of clients and direct monitory loss [5].

III. FUNCTION OF KNOWLEDGE MANAGEMENT IN DATA SECURITY

The function of Knowledge management is really crucial to deal the cognition of data protection as Knowledge Management has been determined as “the capability by which communities catch the cognition that is vital to their achiever, invariably amend it, and make it usable in the best manner to those who need it”[13]. According to Granneman [6] most people do not ensure their computing machine or act in a secure manner. The main reason being that the average user just does not know what to do. This is alerting, conceiving that 65.9% of the Australian population is Internet users [7] and the success of the 2000 LOVELETTER virus and 2003 laster/So Big 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 cognizance efforts directing being and issuing new menaces, risks, exposures, measures and precautions are commanded.

Foster a protection witting culture – A protection culture where willing attitudes, conducts and predisposition to privacy and protection become use and acquired during every day living [9].

Knowledge management is changing and heightening capacities to execute such procedures, admitting obtaining and preparation of the right cognition assets, in order to accomplish the hoped results. Cognition assets admit corporal cognition in individuals; engrafted cognition in engineering, systems and marches; assimilated cognition in work human relationship, teams and meshes; and unjust data and brainwaves [10].

Three major phases of Knowledge Management cycles are:

1. Knowledge capture and /or foundations
2. Knowledge apportioning and dispersion
3. Knowledge attainment and coating

Knowledge captivate mentions to the recognition and accompanying codification of existent cognition and know how ith in establishment and/or from the surroundings. Cognition creation is the growth of the new cognition and knows how or introductions that did not have previous universe with in the party like from individuals, research papers etc. Once it has been determined that the new or freshly distinguished cognition is of enough value, the next step is to contextualize this content. Contextualize means yielding link to the readers of that knowledge and tailoring it toward the direct users. Then the cognition is shared and distributed. The cognition is broadcast to the users using portals, emails and other Knowledge Management tools. Users employ the cognition and with their go through also new cognition are generated and caught. Knowledge management recommends dissimilar type of credits and inducements for the people who are dealing their cognition and the people who are actively applying the knowledge to amend their cognition and functioning.

Knowledge management has multi dimensional gains at unlike levels from people to establishment such as for someone’s; it helps people to do their job in an effective way through better decision making and intellection. Help people to keep up to date. On community of interest’s level, encourages peer to peer cognition sharing. At the Establishment level, diffuse best exercises, constructs organizational remembering. In other words, cognition of how an establishment functions in the context of management of data security can importantly impact the effectuality of processes in downplaying ‘chances’ for computer fraud.

IV. APPLICATION OF KNOWLEDGE MANAGEMENT INSTRUMENTS FOR DATA PROTECTION

In order to intention fortunate instruments for cognition apportioning, a strategy demands to be chosen. Hansen et al. differentiate two main knowledge management schemes: *codification and personalization. Codification* is the people-to documents strategy. Here the cause is to load computer network 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 scheme. Here the attempt is to link people with other people and to develop electronic network and biotic community of practices. Emphasis is on Informal-cognition dealing.

Following Knowledge Management tools may be used for amending data protection:

1. Content Management
2. Cognition Classifications
3. Groupware
4. Online Communities of Exercise

5. Enterprise Portal
6. Social Electronic network Analysis and Design
7. E-learning
8. Storytelling and Narratives
9. Wireless instruments for cognition Mobilization
10. Invention and idea management organization
11. Instruments for leading KNOWLEDGE MANAGEMENT throughout organizational limits

4.1 Content Management

A good planned content program must be able to cover multiple content types, origins and access forms. These message origins admit protection concerned libraries, actions and personnel department directories. Content can be integrated or amorphous. Some of it is generated online during various cognition actions (e.g. on line brain storming).

Establishments may use content direction system for data protection best practices, lesson learned, protection case studies etc. Capacity teams, Meta data, cognition maps, and a work flow context can ensure effectual reuse of the capacity. Encouraged capacity management system admit features for unseamed exploration, writing templets, keeping unity of web pages and connects, occasional review, archiving, metadata, version control, rule setting, indexing, audits, empowered access, government alerts, and elastic repurposing for multiple platforms and formats.

4.2 Cognition Classifications:

Classification is the exercise and science of categorization consorting to natural relationships. The info-glut or “digital sprawl” on collective computer network has led to users not being able to find applicable information in time and legion taxonomy growth tools are coming to the deliverance. It must ponder the needs, demeanors, tasks and vocabulary of the exploiters, and be able to furnish multiple paths and points of view. Classification should be easy to assert and exploiters should find it easy to realize, navigate and lead. It wills assistance the users to easily locate particular data protection cognition.

4.3 Groupware:

Suitable characteristics for coaction in the circumstance of Knowledge Management admit affinity constructing, cognition mapping, meandering, canvassing, and group papers creation, and rating, anonymity and access direction. A famous trend in tools for collaboration between networked employees is the converging amongst asynchronous (e.g. collaborative document management) and synchronous (e.g. instant messaging) service. It is an significant tool for cognition sharing among the peer groups. It is an significant tool to circulate selective data protection data instantly to a group like data regarding new virus attacks.

4.4 Online Communities of Exercise (CoE):

Online communities establish a developing part of the organizational landscape of 21st century global players, but business organization is still at the early degrees of person and organizational optimization of web based communities. Online CoEs are issuing as powerful tool for cognition substitute and memory. Participation levels in CoEs can be sectioned into core, active, and peripheral. Success levels can be named via the application of knowledge in the form of consultations anecdotes and employee survey. Expertise directories are a useful way for connecting cognition worker in such forming communities, but they must connect individuals and not just resumes. CoEs are particularly useful in talking about current security related problems and come out with solutions.

4.5 Enterpriser Portal

Portals help produce the “on demand” workplace, customized to individual employee demands. A well-designed portal can serve as a deliverance channel for Knowledge Management applications any time, any place, and on any device. Knowledge portals are the single point of fundamental interaction and categorization for collaboration. Universal user may reach the portal for getting their results of security related problems and current security scenario.

4.6 Social Electronic network Analysis and Design

Social network analysis (SNA) is rising as a powerful tool for function cognition flows and identifying gaps. SNA can be used to reinforce existent flows and to amend cognition desegregation after actions like unifications 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 protection process redesign, role development, and bettered collaboration between cognition searchers and suppliers. SNA can help identify central people, property 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 circulating information security knowledge naturally and effortlessly.

4.7 E-learning

One interesting emerging development on the Knowledge Management front is the growing convergence of viewpoints between the Knowledge Management community and the e-learning community. The concept of Knowledge

Management 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. Knowledge Management 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 protection and for training of new security technologies, e-learning may be very useful.

4.8 Storytelling and Narratives

Personal storytelling builds up community and can regenerate the way we do business concern. Non-traditional business communicating proficiencies like art, theatrical tools and even poetry can amend internal and social communication. Stories are good framework for sharing information, meaning and knowledge. Blogs encourage Story-telling and foster understanding because they normally offer context. Social engineering type of attacks can be easily depicted using these proficiencies.

4.9 Wireless Instruments for Cognition Mobilization

One of the most famous emerging courses in workforce property is the altering use of cellular telephone technologies to take “KM” to another dimension-“knowledge mobilization”-by bringing relevant cognition directly to the fingertips of a company’s road warriors and fieldworkers via cell phones, PDAs, industry-specific handheld devices, Wireless Local Area Network (WLAN), and Radio Frequency Identification (RFID) tags. While personal computers (PCs) and digital computer have come under some criticism for “tethering” knowledge workers to their desks, wireless engineering may be the perfect answer to “mobilizing” the workforce by letting them catch and harness key information and knowledge attributes wherever they are, whenever they want, and however they want. This instrument changes data protection cognition to be circularized for the individuals on the move and it is contiguous.

4.10 Invention and Idea Management Organizations

Managing an invention pipeline, promoting an “idea central” or ideas market place, and producing the “hundred headed brain” are some originative approaches being assumed by Knowledge Management innovators. Knowledge Management also helps organizations increase the skillfulness of invention by improving access to experts and tapping into past innovations. New innovative ideas and information protection solutions can be evolved using these systems.

4.11 Instruments for Leading Knowledge Management throughout Organizational Limits

Online services such as dial-up bulletin boards and web communities have really assisted network communities of Interest across the globe for years. The World Bank has leveraged a strategy of “global knowledge, local adaptation” for negotiating global knowledge substitutes. Data Protection knowledge can be accessed from all over world to be applied in the company.

V. CONCLUSION

We can ensure that to carry on with the ever changing nature of information technology and the newer protection menaces arising at a very fast pace, we need some technique to formulate the users in an effective manner. KNOWLEDGE MANAGEMENT tools can be used to evolve newer, economical and faster methods to deal with information security issues. KNOWLEDGE MANAGEMENT tools like content management may be used to create content and update data protection knowledge like data protection measures and best practices, classifications 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 concerned stakeholders. E-learning methods may be used to train 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. Invention is the key for the new solutions. Lot of research and innovations are taking place in data protection field. KNOWLEDGE MANAGEMENT can promote individuals to give new ideas and rewarding them consequently. This way we can see that there is a lot of scope to improve information security using knowledge management proficiencies.

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.