Integrating IS Security with Knowledge Management: Are We Doing Enough To Thwart The Persistent Threat?

Murray Jennex
San Diego State University
mjennex@mail.sdsu.edu

Alexandra Durcikova
The University of Oklahoma
alex@ou.edu

Abstract

Knowledge management focuses on capturing and sharing knowledge. Because of this, KM researchers tend to focus on issues related to knowledge capture, storage, and sharing. However, because knowledge is valuable, it is a target needing to be protected. This paper posits that KM researchers and practitioners also need to think security and explores how important security skills are to KM practitioners and researchers. A literature review is performed to determine how much attention is paid by KM researchers to knowledge security. Additionally, 50 KM job postings are examined to determine if security skills are considered important by those hiring KM practitioners. Finally, a survey is prepared for exploring security attitudes of KM practitioners.

1. Introduction

Information System, IS, security is about protecting IS assets, networks, data, information, computers, and applications by restricting access to the assets and preventing unauthorized modification or destruction. Knowledge management, KM, is about sharing and transferring knowledge from knowledge sources to knowledge users. It is not intuitive that security and KM are related as KM is about sharing while IS Security is about restricting access. However, it is our position, and the position of this paper, that KM and IS Security are complementary. Knowledge has value and items of value are targets for theft or attack. This paper posits that KM does not have close enough links with IS Security. It is posited that this is evidenced by a lack of research literature addressing the integration of KM and IS Security and a lack of interest in integrating KM and IS Security by KM practitioners. To investigate the links between KM and IT Security this paper performs a review of the KM research literature with respect to IS Security. Additionally, to assess how KM practitioners value IS Security skills and capabilities 50 recent KM job postings are analyzed to determine what skills and capabilities are desired in new KM position hires. Finally, to explore KM practitioner attitudes with respect to the role of IT Security in KM an exploratory survey is generated and presented in this paper.

The value of this paper is in providing insight into perceptions and attitudes with respect to integrating IS Security into KM. The concern is that there is too little integration and that KM practitioners and researchers need to put more effort into creating secure KM. We believe this is necessary given the cyber threat environment. The cyber threat is growing. The Ponemon Cost of Cybercrime Report shows that the cost of data breeches has risen to an average cost of $8.9 million per breech in 2012, a 6% increase from 2011 (note that this is for the organizations in their survey) [32]. Additionally, there has been a 44% increase in the number of successful attacks, rising to 102 successful attacks a week [29]. What is taken in data breeches? Personal identification information, credit card numbers, and intellectual property are among the leading items taken with knowledge being a key component of intellectual property. Finally, how are cyber-attacks carried out? The most costly come from malicious insiders and web based attacks [31] with advanced persistent threats (APT) coming from state sponsored espionage [26] and sophisticated cybercriminal rings [29].

The last issue is the movement towards cloud and mobile technologies. The cloud is increasing the use of service based products such as Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS). Cloud services are providing cost savings to organizations but due to the lack of control by the organization over the service there is a security concern [21]. Mobile technologies are easy to use and are widely adopted. However, there are many attacks focused on these devices and bring your own device (BYOD) policies are increasing the risk to the organization [32].

Ultimately there are persistent threats that are risks to the knowledge relied upon by our organizations. We posit that it is a responsibility of KM researchers and practitioners to develop secure KM so that these

978-1-4799-2504-9/14 $31.00 © 2014 IEEE
DOI 10.1109/HICSS.2014.429

critical knowledge assets can be stored, accessed, and utilized.

2. Methodology

This is exploratory research focused on determining if KM and IS Security are integrated well enough to protect knowledge assets from the persistent threats of disclosure, modification, and destruction. Three data gathering methods are used. The first is a literature review of the research literature. Google Scholar and the AIS eLibrary were used to search for KM papers that also discuss security. Relevant papers were reviewed and the security aspects summarized. Conclusions were reached based on the numbers of relevant papers found and the security concepts discussed.

The second data gathering method was to find current KM job postings. Google was used to search job posting sites such as monster.com, carrerbuilder.com, and glassdoor.com as well as independent job postings found on the web. 50 job posting were found posted during the spring of 2013. The 50 job postings were divided into two groups, KM managers and KM technicians. Additionally the postings were grouped by those related to defense activities and those related to civilian business. Each of the two groups, KM management and KM technician, were analyzed by coding the job requirements into a set of overall job requirements ranked by how often each was mentioned.

The third data gathering method was to generate a survey for gathering opinion data on how important IS Security is to KM practitioners. The survey was generated based on general IS Security attitude surveys and included demographic items. The survey was demonstrated using the web and posting to KM practitioner groups and listserves. Survey results are analyzed using descriptive statistics.

3. Literature Review

The KM research literature was reviewed with respect to incorporating security into KM. Three types of papers were found: 1) KM papers that recognized the need for security for KM to be successful; 2) KM papers that applied specific IS Security technologies to solving specific KM issues; and 3) KM papers that incorporated risk management techniques. These are summarized below.

3.1. Security as Part of KM Success

How to be successful with KM? Initial research focused on the identification of critical success factors, CSFs, for initiating KM/KMS and the application of these CSFs into KM success models (Note: CSFs are areas in which satisfactory results ensure successful competitive performance and are the minimum key factors that an organization must have or do in order to achieve some goal [2]). Davenport, DeLong, and Beers [6] identify four objectives for knowledge-based projects: create knowledge repositories, improve knowledge access, enhance knowledge environments, and manage knowledge as an asset. KM projects are successful when there is a growth in resources attached to the project, a growth in knowledge content, a likelihood that a project would survive without the support of a particular individual or two, and some evidence of financial return. Jennex and Olfman [17] surveyed the literature on KM and KM project success to generate a list of KM CSFs. The following list of CSFs is ordered by the popularity of the CSF in the literature with the most commonly mentioned CSF listed first and the least mentioned CSF last:

- A Knowledge Strategy that identifies users, sources, processes, storage strategy, knowledge and links to knowledge for the KMS.
- Motivation and Commitment of users including incentives and training
- Integrated Technical Infrastructure including networks, databases/repositories, computers, software, KMS experts
- An organizational culture and structure that supports learning and the sharing and use of knowledge
- A common enterprise wide knowledge structure that is clearly articulated and easily understood
- Senior Management support including allocation of resources, leadership, and providing training
- Learning Organization
- There is a clear goal and purpose for the KMS
- Measures are established to assess the impacts of the KMS and the use of knowledge as well as verifying that the right knowledge is being captured
- The search, retrieval, and visualization functions of the KMS support easy knowledge use
- Work processes are designed that incorporate knowledge capture and use
- Security/protection of knowledge

The last CSF focuses on security and protection of knowledge. This has been incorporated into KM success models including Jennex and Olfman [18] who modified the DeLone and McLean's [8] IS Success Model to incorporate the KM CSFs listed above into a KM success model. Additionally, Lindsey [24]

proposed a KM effectiveness model based on combining Organizational Capability Perspective theory [10] and Contingency Perspective Theory [3] and included a protection construct.

In addition to the KM success models several other authors have identified security as a CSF. Holsapple and Joshi [11] identified control as an influence on KM success and included security as a part of the control construct. Security was defined as the administrative and technical controls used to prevent unauthorized disclosure, modification, or destruction/obsolescence of knowledge.

Malhotra [25] identified security and protection of knowledge in knowledge management systems, KMS, as an inhibitor to the sharing of knowledge and a cause for why KMS fail.

Alavi and Leidner [1] identified as a concern of managers when considering implementing a KMS, the protection of data on the web.

Kamphol [22] discussed the need for KMS to be compliant with IS Security policies and practices. This was considered necessary for organizations to be competitive on an international basis.

To summarize, there is a small but growing body of literature that recognizes that successful KM requires the integration of IS Security even though this integration may result in lesser knowledge usability, making it more difficult to transfer knowledge. Note that usability as used in this paper refers to ease of use construct as defined by Davis [7] in the Technology Acceptance Model, TAM This integration is best stated as KM being compliant with the security goals and policies of the organization and IS Security best practices and standards. The implication is that the design and implementation of KMS should include IS Security requirements but in a thoughtful and balanced approach that minimizes the impact of IS Security on usability of the KMS

3.2. Security as Reflected in Risk Management in KM

There is also a small body of literature that looks at the integration of KM and IS Security through the application of risk management to KM. KM has been described as a selective capture and use of knowledge [12] and KM success has been described as getting the right knowledge to the right people at the right time [19]. Both of these activities have risk where risk is a measure of the likelihood and consequence of something bad happening [33]; or in these cases the likelihood and probability of not capturing the right knowledge or getting it to the right people at the right time. Authors integrating risk management into KM are summarized below:

Jennex [13], [15] explored the risk of forgetting and losing knowledge through loss of experts and lack of persistence of knowledge storage media. The most notable example is the inability of the National Aeronautical and Space Administration, NASA, to return to the moon quickly due to the loss of knowledge on how to build moon mission spacecraft. The proposal is to use risk management in developing a KM strategy to identify what knowledge is to be captured and how it is to be stored.

Jennex and Durcikova [14] [16] used risk management to create a framework for prioritizing knowledge assets so that organizations can allocate resources as appropriate to capture critical knowledge before it is lost. This allows organizations and KM managers to manage the risk of losing knowledge to departing knowledge workers by identifying where critical knowledge resides and the likelihood of that knowledge source leaving.

Riecicky and Spichiger [31] used risk management to create a framework for valuing and managing knowledge assets. This allows organizations and KM managers to make better decisions on how to allocate resources to manage all KM assets including, hardware, software, people, and data.

Jennex and Zyngier [20] proposed using McCumber's cube [27] as a framework for analyzing a KM initiative/KMS. The goal is to use this analysis to provide a risk based approach to identifying the security policies and controls for securing KM/KMS.

To summarize, there is a small but growing body of literature that is applying risk based approaches to managing KM to be successful by addressing the risks of not capturing the right knowledge, not getting it to the right people, and not getting it to them at the right time. The current body of literature is not sufficient to address these three risks but is a start in integrating IS Security risk management techniques into KM.

3.3. Security Used to Address Issues in KM

This is a small body of literature that is focused on addressing specific security issues in KM. Particularly are the issues of access control, secure communication, and secure storage. Upadhyaya, Rao, and Padmanabhan [35] discuss the components of a KMS. These include secure languages such as security-assertion markup languages and secure knowledge query and manipulation language for secure communication; circles of trust where two or more organizations share supplier/customer authentication information (also for secure communication); and

digital rights management and secure content management for access control.

Thuraisingham [34] focused on database design to create secure database management systems and addressing the secure storage issue. Boella and van der Torre [4] identified the access control policies for managing knowledge sharing in virtual KM communities. Randeree [30] investigated access control versus the need to share medical data and information. Cannataro And Talia [5] discuss the security requirements for creating secure parallel and distributed knowledge discovery systems, PDKD, called a knowledge grid..

Finally, Neville, Powell, and Panteli [28] propose a research model and agenda for investigating the relationships between IS Security components and knowledge. The model maps factors for and barriers to security to factors for and barriers to knowledge. This allows researchers to identify issues that can be mapped into KM processes.

To summarize, KM researchers have begun a small body of literature that is starting to address the areas of concern as outlined in the McCumber cube [27].

4. Security in KM Job Postings

The second step of this research was to see what KM practitioners were looking for in new hires. We were particularly looking to see if security skills and/or knowledge were considered important. To determine this we analyzed 50 KM job postings by coding the job requirements in order to determine the most asked for skills and knowledge. The 50 job postings were grouped into two categories, KM manager jobs (21 postings) and KM technician jobs (29 postings). Table 1 lists the main job criteria (more than one job posting listing the criteria) for the KM Manager group. Seventeen criteria were identified from the job postings with possessing a Bachelor's degree and having good written and oral skills being the top criteria. What is most interesting for this paper is that two security related criteria are listed. Possessing an active security clearance (secret or top secret were requested) appeared on 7 out of 21 postings (the seventh most requested criteria). Understanding organizational security standards/policies or possess a security certification was tied for the eleventh most requested criteria (4 listings).

Table 2 lists the main job criteria (more than one job posting listing the criteria) for the KM technician group. Nineteen criteria were identified from the job postings with possessing a Bachelor's degree and having technical experience being the top criteria. What is most interesting for this paper is that two security related criteria are listed. Possessing an active security clearance (secret or top secret were requested) appeared on 9 out of 29 postings (the fourth most requested criteria). Understanding organizational security standards/policies or possess a security certification was tied for the thirteenth most requested criteria (2 listings each).

Table 1, KM Manager Job Requirements

Job Skill/Knowledge Criteria	Number Listing
BA or BS degree	18
proven oral and written skills	18
experience with project management/PMP	12
experience with knowledge management	12
advanced degree	9
experience promoting & providing technical support for collaborative tools including SharePoint 2010, web conferring tools and other Web 2.0 technologies (Communities of Interest, wikis, blogs, forums, etc.)	8
Must possess active security clearance	7
Knowledge of the SDLC	6
Able/willing to travel in the U.S./internationally	6
Ability to work independently and as part of a team	5
experience with information management	4
ITIL cert	4
understand organizational information security standards/security certs	4
experience with business process improvement	3
CKM/other Certification	3
experience with using/implementing social media	2
experience in Enterprise IT	2

Table 2, KM Technician Job Requirements

Job Skill/Knowledge Criteria	Number Listing
B.A/B.S. degree.	18
technical experience	18
Communication Skills (written and oral)	12
security clearance	9
proficient: HTML, XHTML, CSS, Microsoft SharePoint 2007/2010, Microsoft Office 2007/2010, Adobe Acrobat Professional.	8
KM project experience/PMP	6
Experience in KM Systems	4
U.S. Citizen.	3
web portal design techniques: SharePoint portal 2007/2010; maintenance, permissions management, and web environment design.	3
experience in Enterprise IT	3
Advanced degree	3
ITIL Cert	3
Change Management/Business Readiness	2

Training Delivery Expert	2
Training Development Expert	2
JavaScript, SQL, and ASP.NET (VB and/or C#), Microsoft SQL Server, Microsoft SharePoint Designer, Adobe Acrobat Professional (8.0+), Adobe Photoshop (CS3+).	2
certifications in A+/Net+, Security+ GAIC GSEC	2
understand organizational information security standards	2
experience with multiple countries/cultures	2

Prior to analyzing the KM job postings it was postulated that there would be little to no security requirements listed. This is only partly true. Security clearances are an access control mechanism that appeared on 16 postings. This was surprising at first until a review of the postings found that eleven postings were specifically for defense related KM positions (defense related positions required access to classified materials in order to manage the knowledge). This implies that really only five out of 39 postings requested a clearance of some type and so is not as impressive.

5. Survey of KM Practitioner Security Attitudes

An online exploratory survey was designed to gather data on KM practitioners' attitudes with respect to the role of IT Security in KM. The participants were KM professions who subscribed to a KM listserv. A call to fill out a survey on IT Security and KM was posted on this listerv and a reminder was sent out one week after the initial call for participation. The survey was open for 14 days and we received 13 usable responses.

Scales for this survey were adapted from DeSouza [9] and all items were measure on a five and seven-point Liker scale anchored on 1 (strongly disagree) and 5 (strongly agree). The survey focused on three distinct areas of KM security: (1) organizational believes about security, (2) preventative measures to secure knowledge assets, and (3) KM professionals' opinions about KM security.

The response rate to the survey was 48% (13 out of 27 people that viewed the survey filled it out). The average age of respondents was 48 years, and 9 were males. Our subjects worked for various industries, including IT, telecommunications, nonprofit, utility; the number of employees in these organizations were from 100 to 100,000. These KM professionals were employed at their respective organizations on an average for 13 years, and as KM professionals on an average of 5 years. These organizations used a variety of KM tools including SharePoint. The results to our survey are in Table 3.

Table 3, Survey Results

My organization… (7 point Likert scale)	
1. has a way of identifying intellectual assets	5.93
2. considers knowledge one of the most important assets in my organization.	5.40
3. is concerned with knowledge being lost.	5.33
4. is concerned with knowledge being stolen.	5.73
5. is concerned with knowledge being destroyed.	4.33
6. believes that security skills are necessary for a knowledge management professional.	4.47
7. is concerned with knowledge access rather than securing knowledge.	4.33
8. has a knowledge security framework in place.	4.00
9. has a contingency plan in place in case a knowledge breach would occur.	3.80
10. monitors access to knowledge.	4.33
11. experienced a knowledge breach in the past.	4.47
My organization employs the following preventative measure to secure the knowledge assets (7 point Likert scale)	
12. Background checks on employees	5.38
13. Counter-intelligence	3.00
14. Incentive schemes for employees	3.77
15. Educating employees	5.54
16. Securing electronic channels	5.23
17. Securing duplication and storage of knowledge	4.58
18. Securing the application of knowledge	4.23
Tell us about your opinions on secure knowledge management (5 point Likert scale)	
19. I consider security issues in my KM initiative(s)	3.46
20. I am asked by organizational leaders about security in my KM initiative(s)	2.77
21. I have had to deal with a security issue in my KM initiative(s)	2.23

The results of this survey suggest that majority of the companies consider knowledge to be an asset

(items 1-4) but also suggests that the organizations they work for are not that concerned with loosing or potential damage to the knowledge they created (items 5-7). This might be reason that they are not that concerned with creating a knowledge security framework nor they have a contingency plan in place (item 8-10). While companies do background checks on employees, they are not too worried about other ways of securing the knowledge in their organizations (items 12-18). While KM professions do consider about security issues (item 19) it seems that organizational leaders are not too concerned about security issues around KM (item 20).

We also asked respondents to insert comments about KM and security. Interestingly, five respondents indicated that they their organization dealt with a security issue in their KM initiative and several mentioned that the main issue that KM security professionals face is the "… ability to balance security issues with accessibility issues" (a KM security specialist).

6. Discussion

Ultimately, security is about controlling access to data, information, and knowledge while KM is about getting needed data, information, and knowledge to the right people at the right time. Given the competitive value this data, information, and knowledge has to the organizations possessing it, it is only natural that organizations would want to take steps to protect these assets. The review of the academic research literature found that there is a small body of literature that is addressing the key issues of showing the linkage between IS Security and KM success; applying risk management approaches managing KM activities, and applying Information Security technologies to addressing issues such as access control, secure communications, and secure storage. This is a good finding but the research needs to continue. 2012 was the year of Big Data, 2013 may well be the year of the Persistent Threat. Cybercrime, cyber espionage, cyber war, and cyber terrorism are in the 2013 headlines. Additionally, the development and adoption of cloud and mobile technologies all lead to the volatility of security approaches, making this an area needing further research. Interestingly enough Information Security practitioners are investigating the use of KM as a way improving overall Information Security through the sharing of attack methods and defense approaches.

While the findings in the KM research literature were better than expected, the findings in KM practitioner job postings were as expected, disappointing. The findings reflect that KM practitioners still totally focus on knowledge capture, storage and sharing and that Information Security is an afterthought. Only just over 10% of the job postings had requirements for understanding organizational security standards or policies and only two KM technician postings requested Information Security certifications. The survey results mimic this suggesting that the focus is on capturing and sharing knowledge and much less focus is paid on security access to knowledge. Organizations that understand the value of their knowledge would want their KM personnel to be able to protect it. It is expected that all KM managers should be familiar with organizational Information Security standards and policies. It is understandable if organizations were to create new KM technician positions focused on secure KM but this study found only one posting that fit this: Knowledge Management Secured Messaging Specialist. Since there were 11 postings focused on defense organizations it is surprising to note this specialist posting was for a commercial bank.

7. Conclusions

The conclusion of this paper is that the protection of knowledge artifacts used in KM is not well enough developed. KM governance/management needs to integrate organization Information Security standards and policies. Information Security practitioners need to work with KM practitioners. Innovations such as cloud and mobile technologies are improving the ability of organizations to capture and make available knowledge to those that need it. However, these organizations need to balance the ease and speed of knowledge sharing with controls that ensure only those authorized to have access to that knowledge are the ones getting that knowledge. Additionally, many KM researchers focus on identifying and defeating barriers to knowledge transfer/sharing. These same researchers need to be aware of Information Security access controls and so ensure that overcoming barriers to knowledge transfer/sharing do not invalidate needed access control schemes or make it more difficult to design and implement a access control paradigm on what is normally considered a critical organizational asset.

Ultimately, the conclusion of this paper is that while Information Security and Knowledge Management need to be integrated, insufficient progress is being made by both researchers and practitioners to do so.

7.1. Limitations

The chief limitation is with respect to KM practitioner job requirements. 50 job postings were examined and analyzed. While 50 postings is a significant number, only two of these postings were for jobs that were outside the United States. This makes it nearly impossible to generalize these findings to KM practitioners outside the United States.

What is not a limitation is the breadth of the postings. While 48 are for United States positions, these 48 postings reflect 48 different organizations ranging from consultants to banks to health care to construction to automotive to defense and finally to information services. This is a wide range of organizations that does support generalizing the findings to all United States organizations.

7.1. Areas for Future Research

This paper identifies many areas for future research. Secure KM in cloud and mobile environments needs much attention. Access control schemes for large numbers of knowledge objects and knowledge users need to be developed. KM governance needs to be developed to include Information Security management issues. Additionally, how to add skills such as risk assessment and management and secure communications and storage into KM practitioner skill sets needs to be explored.

8. References

[1] Alavi, M. and D.E. Leidner, Knowledge Management Systems: Issues, Challenges, And Benefits, Communications of the AIS, 1(7), 1999.

[2] Alazami, M. and Zairi, M., "Knowledge management critical success factors," Total Quality Management, 14(2), pp. 199–204, 2003.

[3] I. Becerra-Fernandez and R. Sabherwal, "Organizational Knowledge Management: A contingency perspective," Journal of Management Information Systems, vol. 18, no. 1, pp. 23-55, 2001.

[4] Boella, G. and van der Torre, L., (2006) "Security Policies for Sharing Knowledge in Virtual Communities, IEEE Transactions On Systems, Man, And Cybernetics, 36(3).

[5] Cannataro, M. and Talia, D., (2003). "The Knowledge Grid," Communications of the ACM, 46(1), pp. 89-93.

[6] Davenport, T.H., DeLong, D.W., and Beers, M.C., "Successful Knowledge Management Projects," Sloan Management Review, Winter pp. 43-57, 1998.

[7] Davis, F., "Perceived usefulness, perceived ease of use, and user acceptance of information technology." MIS Quarterly, 13, pp. 319-339, 1989.

[8] DeLone, W.H. and McLean, E.R. (2003). The DeLone and McLean Model of Information Systems Success: A Ten-Year Update. Journal of Management Information Systems, 19(4), 9-30.

[9] DeSouza, K.C. (2007) "Managing Knowledge Society: Strategies for Protecting Your Company's Intellectual Assets." Kogan Page, 1st edition,

[10] Gold, A.H., Malhotra, A., and Segars, A.H., (2001). "Knowledge Management: An Organizational Capabilities Perspective," Journal of Management Information Systems, 18(1), pp. 185-214.

[11] Holsapple, C.W. and Joshi, K.D., (2000) "An investigation of factors that influence the management of knowledge in organizations," Journal of Strategic Information Systems 9 pp. 235-261.

[12] Jennex, M.E., "What is Knowledge Management?" International Journal of Knowledge Management, 1(4), pp. i-iv, 2005.

[13] Jennex, M.E., "Why We Can't Return to the Moon: The Need for Knowledge Management." International Journal of Knowledge Management, 2(1), pp. i-iv, 2006.

[14] Jennex, M.E. "Assessing Knowledge Loss Risk." 15th Americas Conference on Information Systems, AMCIS15, August 2009.

[15] Jennex, M.E., "Knowledge Management: The Risk of Forgetting." iKNOW, the magazine for Knowledge Workers, 3(1), pp. 4-7, 2013.

[16] Jennex, M.E. and Durcikova, A., "Assessing Knowledge Loss Risk." 46th Hawaii International Conference on System Sciences, HICSS46, IEEE Computer Society, January 2013.

[17] Jennex, M.E. and Olfman, L., "Assessing Knowledge Management Success" International Journal of Knowledge Management, 1(2), pp. 33-49, 2005.

[18] Jennex, M.E. and Olfman, L., "A Model of Knowledge Management Success" International Journal of Knowledge Management, 2(3), pp. 51-68, 2006

[19] Jennex, M.E., Smolnik, S., and Croasdell, D., "The Search for Knowledge Management Success." Global Perspectives on Engineering Management, 2(2), pp. 34-44, 2013.

[20] Jennex, M.E. and S. Zyngier, “Security as a Contributor to Knowledge Management Success,” Information Systems Frontiers: A Journal of Research and Innovation, 9(5), pp. 493-504.

[21] Kajiyama, T., Jennex, M.E., Addo, T, Paolini, C., “Cloud Computing Security: How Risks And Threats Are Affecting Cloud Adoption Decisions.” 12th Security Conference, April 10, 2013.

[22] Kamphol, W., (2009). "Information Security Compliances and Knowledge Management Capabilities in International Diversification" AMCIS 2009 Proceedings.

[23] Lee, Y., Davis, S., and Lee, Z., (2000). “Security Knowledge Management Systems: A Solid Shield Against Computer Abuse,” AMCIS 2000 Proceedings,.

[24] Lindsey, K. (2002). Measuring Knowledge Management Effectiveness: A Task-Contingent Organizational Capabilities Perspective. Eighth Americas Conference on Information Systems, 2085-2090.

[25] Malhotra, Y., (2002). “Why Knowledge Management Systems Fail: Enablers and Constraints of Knowledge Management in Human Enterprises,” retrieved on June 1, 2013 from http://www.brint.org/kms.pdf, .

[26] Mandiant, APT1: Exposing One of China’s Cyber Espionage Units, www.mandiant.com, 2013.

[27] McCumber, J., “Assessing and managing security risk in IT systems: A structured methodology,” .Boca Raton, FL: Auerbach Publications, 2005.

[28] K. Neville, P. Powell, and N. Panteli, Knowledge and Security, Ninth Americas Conference on Information Systems, 2003.

[29] Ponemon Institute, 2012 Cost of Cyber Crime Study: United States, Ponemon Institute, October 2012.

[30] Randeree, E., (2005). "Secure Health Knowledge: Balancing Security, Privacy and Access" AMCIS 2005 Proceedings.

[31] Riecicky, V. and Spichiger, A., (2012) “Knowledge Asset Risk Management Framework,” Human Resource Management Research 2(4) pp. 38-45.

[32] Sophos, Security Threat Report 2013, Sophos, 2013.

[33] Stoneburner, G., Goguen, A., and Feringa, A., “NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems,” United States National Institute of Standards and Technology, 2007.

[34] Thuraisingham, V. and Nonmonotonic, A., (1992). Typed Multilevel Logic for Multilevel Secure Data / Knowledge Base Management Systems - I1, The MITRE Corporation, Bedford, MA.

[35] Upadhyaya, S.,. Rao, H.R., and Padmanabhan, G., (2006). “Secure Knowledge Management,” Encyclopedia of Knowledge Management, D. Schwartz editor, Idea Group Inc., pp. 795-801.