Dakota State University

Beadle Scholar

Faculty Research & Publications

College of Business and Information Systems

2006

Guest Editorial Part 2: Emerging Issues for Secure Knowledge Management—Results of a Delphi Study

Insu Park

Guest Editorial
Part 2: Emerging Issues for Secure Knowledge Management—Results of a Delphi Study

***Abstract*—Secure Knowledge Management (SKM) is one of the emerging areas in both knowledge management and information system disciplines. SKM refers to the management of knowledge while adhering to principles of security and privacy. This study identifies key issues on SKM and draws a consensus among domain experts on the key issues. This study is an attempt to accelerate further research and development in the SKM field. In this study, the authors conducted a three-round Delphi study, identifying 21 issues in the SKM area, along with their importance and urgency ratings. Analyses show that participating experts achieved a higher level of consensus on the importance and urgency of the issue as the rounds progressed. The findings will allow both practitioners and researchers to focus and prioritize research needs in the SKM area. The paper also discusses some future-research directions.**

***Index Terms*—Delphi study, information security, knowledge-management systems, Secure Knowledge Management (SKM).**

I. Introduction

THE advancement in networking, storage, and processor technologies has increased the amount of digitalized organizational knowledge at an unprecedented rate [1], making knowledge management one of the most salient sources of sustainable competitive advantages [2]. As a consequence, the growing dependence of organizations on knowledge-management technologies, such as data warehouses, knowledge repositories, and interoperable knowledge-management systems, is creating new challenges for protecting the information and knowledge within an organization [3]. Researchers in what has previously been called the information security area are now required to cover a wider range of knowledge-management practices, such as creating, storing, communicating, and advancing organizational knowledge.

As Desouza and Vanapalli [4] point out, researchers have largely ignored a crucial question: "How can we secure our knowledge assets?" Although the current literature on knowledge management addresses such questions as how, why, when, and where to leverage the knowledge assets, it has yet to pay due attention to protecting and securing those knowledge assets [5], [6]. One problem in the lack of understanding in securing knowledge is that organizations are reluctant to share knowledge because of the unknown threats associated with industrial espionage as well as concerns about diverting or overloading the employees' work-related attention [7]. This problem prevents unleashing the power of information technology (IT)-enabled knowledge management [8].

Acquiring the knowledge that an organization needs to remain competitive while safeguarding the knowledge that it already has is a complicated task [9]. Apropos to this, the first Workshop on Secure Knowledge Management (SKM 2004), held at Buffalo, New York, USA, in September 2004, took an important initiative in raising awareness of the research needs and developing research questions that need to be addressed by the research community. This paper, as a follow-up study of the workshop, identifies and explicates some key issues in the area of SKM.

Two questions regarding SKM stand in the way of a more disciplined SKM research community. 1) What are the most important issues that SKM researchers are faced with? 2) Which of the key issues do researchers believe deserve more urgent research effort? The primary purpose of the paper is to address these questions in order to lay a foundation for further research and development in the area of SKM. To achieve this purpose, we adopted a Delphi-study method that is known to be effective for consensus making.

II. Literature Review

A. Secure Knowledge Management

Since a loss of knowledge resources can cause an organization to fail in its mission, the knowledge generation process and related applications must be protected from unauthorized disclosure or snooping, loss or destruction, and unauthorized modifications [4]. Therefore, organizations must find cost-effective and reliable security solutions that will allow them to ensure the privacy of, to communicate sensitive information with, and to offer value-added knowledge to their business partners and other stakeholders. From this perspective, SKM can be defined as a knowledge-management practice that adheres to the principles of security and privacy [9], while knowledge management refers to a process through which an organization develops knowledge assets that can promote the organization's objectives [10]. SKM extends knowledge-management concepts, tools, and strategies associated with security concerns. To have an effective SKM in place, organizations need to have security strategies, secure processes for business operations, and security metrics that support secure operations [11].

SKM systems may include generic security measures, such as authentication and authorization mechanisms, cryptography programs, and intrusion detection systems [12], while the factors influencing SKM include mechanisms to establish cyber trust, mobile workforce, importance of privacy, and other issues associated with corporate governance and employee responsibilities for IT security (e.g., establishing, refining, and enforcing appropriate security policies) [13]. The SKM framework

Digital Object Identifier 10.1109/TSMCA.2006.871644

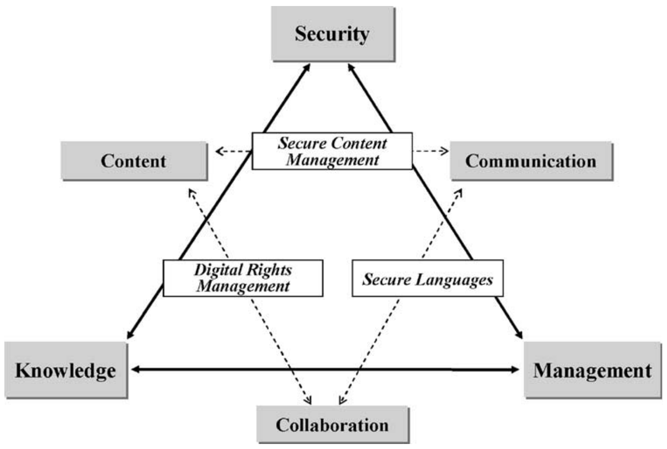


Fig. 1. Framework for SKM systems adopted from [9].

suggested by Upadhyaya *et al.* provides a conceptual backdrop for the aforementioned SKM technologies and factors [9]. According to the framework, SKM embraces three fundamental activities of organizations: communication, collaboration, and content (3 Cs) (see Fig. 1—the boxes inside the triangle are examples of SKM instances) in the context of security, knowledge, and management.

Beginning from these fundamental activities, SKM expands its duty as two or more activities co-occur in more complex knowledge-management practice. Some applications included in the scope of SKM are digital right management for digital asset sharing, secure content management for dynamic access control, and secure language for trusted collaboration networks (e.g., circle of trust).

Although some researchers have attempted to address a wide variety of issues in the SKM area, the current state of the field is, at best, chaotic. The research community has not yet developed coherent research agenda or a framework to integrate the two major themes: information security and knowledge management. Clearly, the research community needs to talk and develop a shared understanding on the relevance and implications of the various research issues in the SKM field.

III. Research Method and Design

A. Delphi Method

The Delphi research method is a systematic and iterative consensus building process often used to estimate future phenomena or answer ill-structured questions. The use of the Delphi method involves the administration of sequentially developed questionnaires to a group of experts. An important feature of the Delphi method is that the method can report a decision or view derived from divergent opinions in the absence of full consensus [14]. This is accomplished by two distinctive characteristics of this method: anonymity and iteration [15]. Anonymity allows participants to express or change their opinions without embarrassment and prevents interpersonal biases from interfering with the evaluation of the presented ideas (e.g., influence of dominant individuals). The iterative feedback process retains the positive aspects of collaborative work, such as an increased degree of consensus, while reducing the negative aspects of group dynamics such as the expression of an unrefined idea or confined group thinking [16]. The primary objective of this study is to develop a list of agreed upon key research issues in the SKM area. Achieving this objective requires gathering ideas from domain experts and crystallizing the ideas through an iterative consensus-making process. Therefore, the aforementioned characteristics of Delphi study make it an ideal method for this study.

The Delphi study has been a popular tool in information-system research [17]–[20]. It has also been applied to formulating various governmental or corporate policies, forecasting the impact of technologies on industry performance, and estimating frequencies. The iterative process of Delphi can continue until a satisfactory level of consensus is made or for a preset number of iterations, after which a voting or ranking procedure is used to finalize the decision or conclusion. In addition, Delphi studies often ask the participating experts to reason their estimates or decisions, which will also be fed back to other experts in the next round [21], [22]. The validity of the Delphi study depends as much on the nature of the study participants and the task as on the technique itself [23]. Delphi requires disparate experts who possess an expertise or knowledge on the task that they need to perform for the study. Thus, the accuracy of the Delphi-study results increases as the group expertise is increased by expert participants or by iterating feedback rounds [24].

B. Study Design

Adhering to the Delphi process described in the previous section, the study conducted three rounds of e-mail surveys. Nonetheless, one difference from the more usual Delphi process was that we did not collect personally identifiable information from the participating experts. Although this approach makes it difficult to track each expert's participation over the feedback rounds, the anonymity would prevent unintended influences from the researchers, on this Delphi study, who are also in the SKM research community. This privacy was achieved by using an ftp site, to which the participants could anonymously upload their survey responses.

1) **Participants**: The study used a group of experts in SKM-related areas (e.g., information security, knowledge management). The experts were identified from various sources such as related journals, workshops, interest groups, professional associations, etc. In the first and second rounds of the Delphi study, the questionnaires were sent to a subgroup consisting of 128 members of academia and practitioners who registered for or had a direct interest in the 2004 Workshop on Secure Knowledge Management (SKM 2004). This subgroup represented experts who were already in the SKM domain. The third-round survey was sent to the entire group.
2) **Round one**: In the first round, an open-ended questionnaire was sent via an e-mail to the 128 experts. The e-mail also included a letter of request for participation, an introduction to the study, and a description of the Delphi-study procedure. Questions about demographic information were included in the open-ended questionnaire.

TABLE I
RANKING OF ISSUES BY IMPORTANCE

#	Key Issues	Description
01	Developing access controls and policies for organizational knowledge	This issue is concerned with the ability of disclosure of information to users, or use control, or both. Also, this is influenced by how security mechanisms can be implemented in business organizations.
02	Data mining/utilization techniques under security and privacy constraints	Traditional data mining and utilization techniques do not consider the possibility that some data can be confidential.
03	Understanding economics of knowledge sharing and information security investment	Business value of security investment, risk and return on security investment issues; incentives and mechanisms for controlling the sharing of information need to be developed; rational security related actions.
04	Designing and developing techniques for SKM systems and secure content management	Technical security controls to enforce security/maximize enterprise effectiveness; mechanisms to control dissemination of information, Securing knowledge so that integrity is not violated.
05	Adopting semantic web for interoperable knowledge management system/integration of knowledge management across heterogeneous systems	Increasingly knowledge must be discovered and integrated across multiple networked knowledge bases and information repositories. Methodologies for knowledge integration are required and should be independent of specific problem instance, knowledge areas, and also of sets of participating knowledge sources.
06	Advances in information privacy	Information privacy is both a basic right and a legislated requirement through government regulations. It is also an important element of corporate risk mitigation.
07	Understanding economics of knowledge markets	Selling private information as a commodity is becoming more important and there are just a few models to study this issue; Pricing of knowledge could be utilized as an economic mechanism for this issue.
08	Aligning business policy, business processes, and SKM policy	Increased need for sharing information can conflict with policies and mechanisms for security. Privacy preserving sharing of information; Confidential data transfer while protecting protected values; digital rights management.
09	Improving knowledge representation	Knowledge management literature has looked at factors that facilitate or hinder knowledge management but has not explicitly considered the connection with knowledge representation; areas of research include secure semantic web technologies; multi-modal knowledge across different networked sources.
10	Developing trust management mechanisms for networked systems	Collaborative information sharing environments require development of robust distributed trust management systems (e.g., trusted computing/web of trust, etc.).
11	Securely managing knowledge at the data level	Knowledge management issues typically employ data as the primary resource, and hence data protection is critical; With the push towards outsourcing, innovative secure management techniques need to be developed.
12	Exploring the roles and implications of government in information security	Government policy on information security would have significant impacts on individuals, businesses, industries, and citizens as a whole (e.g., USA PATRIOT ACT, Sarbanes-Oxley, HIPAA). Balancing privacy, security, and safety of the different stakeholders (e.g., individual privacy vs. national security) is crucial.
13	Developing mechanisms to effectively handle vulnerability/threat responses	Need an effective and efficient way of handling and responding knowledge about vulnerability /threats.
14	Improving interaction between security mechanisms & their users	Assuming a human's oversight cannot be entirely dispensed with in maintaining and restoring an SKM system, there must be an interface that will allow the (prone-to-insecure) human to effectively interact with (unforgiving) secure systems.
15	Improving effectiveness of secure systems	Security should be intrinsic and systems should be transparently secure; Research is needed in overall security architectures for knowledge based systems
16	Developing self-defending/healing mechanisms in computer systems	Systems should be capable of defending themselves and self-healing; inadequately protected systems can become hosts to propagate attacks.
17	Developing metrics for SKM productivity and improving knowledge management system productivity	Need to be able to assess the productivity of secure knowledge environments; from both information flow and user perspectives.
18	Secure knowledge management for wireless services	Wi-Fi security, interoperability of wireless devices and networks used by emergency responders, etc. Wireless data content may need to be more confidential then wired data content.

In order to build a comprehensive list of SKM issues to begin with, the participants were asked to list at least five and up to ten issues that they felt most critical, and then rank them with two criteria: importance and urgency. Important issues refer to the issues that will have a great impact on shaping SKM practice and/or theories in the next five to ten years, and urgent issues are defined as the issues that should be immediately addressed in order for the SKM practices and/or theories to advance in the next couple of years, regardless of their importance (i.e., the size of direct impact). These definitions were provided in the questionnaire to calibrate the study participants' perception on the criteria. The participants were also requested to explain the rationale behind their selection and ranking of the issues. The time window for this round was two weeks. In the first round, 15 of 128 experts (12%) contributed their expertise, yielding a list of 75 research issues for SKM. Similar or closely related issues in this list were consolidated by the coauthors of this study who went through multiple discussion sessions for 100% agreement on the final set of issues. This process resulted in 18 issues listed in Table I.

3) **Round two**: In the second round, we provided the same 128 experts with the 18 issues and the rationale behind the selection prepared in the previous step, and asked them to rate each issue in terms of its importance and urgency. For the importance and urgency rating, we used a 10-point interval scale with 1 being the least important or urgent and 10 being the most important or urgent. Also, the participants were allowed to suggest additional issues if they believed that the provided list was incomplete. As a result, three new issues were added to the consolidated list. A total of 25 experts participated in this round.
4) **Round three**: Round three questionnaires sent to the entire group included the 21 issues identified in the previous two rounds and the average importance and urgency ratings from the second round, as well as the reasoning for the selections. The potential respondents were asked to provide their own importance and urgency ratings after reviewing the average ratings of the second-round participants. This round received feedback from 12 participants.

IV. Analyses

A. Participant Demographics

The real value of a Delphi study is in the increased consensus among the participating experts rather than in the statistical power from a large sample size. The literature recommends 10–18 expert participants for a Delphi study [25]–[27]. Thus, the number of participants in our study (12–19 experts) was satisfactory [15]. Although it was impossible to count all the returning participants, because we did not collect personally identifiable information, at least seven participants[1] contributed their opinion in more than two rounds of the study. The experts participating in the study came from both academia (71%) and industries (29%). Detailed categorizations of the participants are presented in Fig. 2.

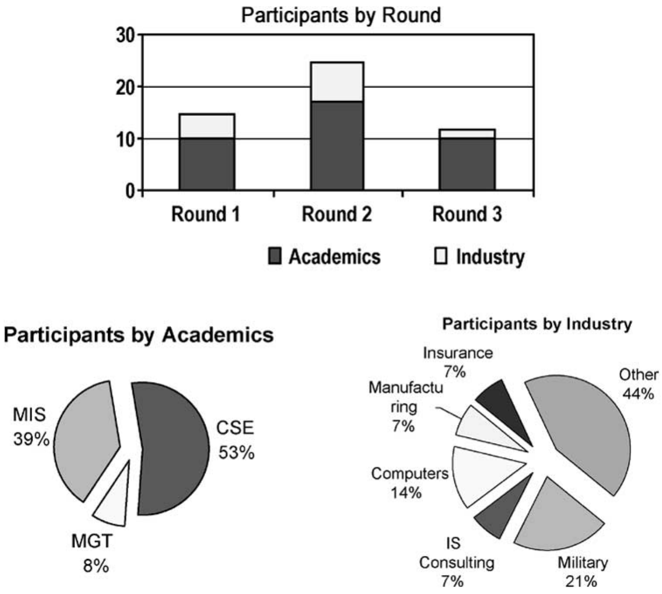


Fig. 2. Delphi participants.

TABLE II
RANKING OF ISSUES BY IMPORTANCE

Key Issues	Round 2		Round 3		Changed Value (MEAN)	Changed Value (SD)
	MEAN	SD	MEAN	SD		
Issue 01	8.25	1.82	8.58	1.24	0.33	-0.58
Issue 04	8.17	1.46	8.42	1.51	0.25	0.05
Issue 08	7.67	1.97	8.42	1.00	0.75	-0.97
Issue 06	7.63	2.26	7.67	1.37	0.04	-0.89
Issue 12	7.46	2.32	7.58	1.56	0.13	-0.76
Issue 18	6.63	2.45	7.50	1.45	0.88	-1
Issue 15	7.21	2.02	7.42	2.11	0.21	0.09
Issue 14	6.38	2.00	7.33	1.83	0.96	-0.17
Issue 10	6.71	2.40	7.25	1.96	0.54	-0.44
Issue 05	6.79	2.30	7.17	1.90	0.38	-0.4
Issue 11	6.50	2.40	7.08	1.31	0.58	-1.09
Issue 16	7.25	2.09	7.08	1.44	-0.17	-0.65
Issue 02	6.83	1.95	6.83	1.27	0.00	-0.68
Issue 13	6.17	1.95	6.50	1.78	0.33	-0.17
Issue 03	6.33	2.26	6.00	1.41	-0.33	-0.85
Issue 09	5.88	2.94	5.50	2.07	-0.38	-0.87
Issue 07	5.25	2.31	5.17	1.64	-0.08	-0.67
Issue 17	5.71	2.29	4.75	1.22	-0.96	-1.07

B. Consensus Improvement

An important consideration in a Delphi study is the degree of convergence, or consensus, to which the participating experts arrived. If the degree of consensus is high, then the results can be considered credible. Empirically, the consensus of the Delphi participants has been determined by measuring the variance in the responses. The lower the standard deviation is, the higher is the consensus achieved. Thus, perfect consensus on an issue has a standard-deviation value of zero [28]. Accordingly, the success of a consensus-making process can be measured by the reduction in the standard deviation throughout the process.

To test the consensus level, we also compared the standard deviations of each issue's importance and urgency ratings at round two with their corresponding standard deviations at round three [29]. The last column in Tables II and III shows that most standard deviations of the importance and urgency ratings in the third round are lower than their counterparts in the second round. This indicates that the participants' consensus on the importance and urgency of most issues improved over time, and the study has achieved a greater consensus.

As Niederman *et al.* [30] mentioned, it is difficult to achieve a perfect consensus in this type of study because perception of the issues heavily depends on multiple factors, such as industry, job position, and research focus of the participants. One issue (issue 15) failed to achieve a higher consensus level in the third round. In contrast, issue 4, which was ranked as the second important and third urgent issues, shows a very steep decrease in its standard deviations on both ratings. Fig. 3(a) and (b) presents the changes in the standard deviations of the 18 issues.

In addition to the standard deviation, the results show a polarization of the mean values. Fig. 4 shows that the issues with high importance/urgency ratings (e.g., issue 1, 6, 4) tend to

[1] This includes only those who explicitly declined anonymity and voluntarily disclosed their identity.

TABLE III
RANKING OF ISSUES BY URGENCY

Key Issues	Round 2		Round 3		Changed Value (MEAN)	Changed Value (SD)
	MEAN	SD	MEAN	SD		
Issue 01	7.96	2.19	8.42	1.44	0.46	-0.75
Issue 06	7.36	2.02	8.25	1.66	0.89	-0.36
Issue 04	7.84	1.97	8.08	1.08	0.24	-0.89
Issue 08	7.12	2.52	7.50	1.62	0.38	-0.9
Issue 12	6.80	2.74	7.42	1.51	0.62	-1.23
Issue 14	6.44	2.52	7.25	1.86	0.81	-0.66
Issue 18	5.83	2.85	7.17	1.53	1.33	-1.32
Issue 15	6.60	2.27	7.00	1.71	0.40	-0.56
Issue 11	6.40	2.52	6.92	1.24	0.52	-1.28
Issue 13	5.88	2.22	6.58	2.02	0.70	-0.2
Issue 10	6.08	2.48	6.42	1.62	0.34	-0.86
Issue 16	5.72	2.17	6.25	1.96	0.53	-0.21
Issue 02	5.80	2.40	6.17	2.69	0.37	0.29
Issue 05	6.72	2.35	5.83	2.04	-0.89	-0.31
Issue 03	5.48	2.87	5.42	1.24	-0.06	-1.63
Issue 07	4.84	2.64	4.75	1.82	-0.09	-0.82
Issue 09	5.48	2.73	4.75	1.54	-0.73	-1.19
Issue 17	5.00	2.47	4.42	1.44	-0.58	-1.03

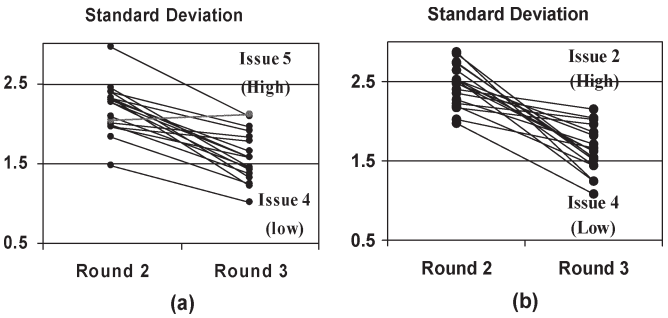


Fig. 3. Consensus for key issues by standard deviation. (a) Importance and (b) urgency.

get even higher ratings in the next round, while the issues with low ratings (e.g., issue 7, 9, 17) received even lower ratings in the next round. From these results, it is evident that the participating experts achieved a higher level of consensus on the importance and urgency of the 18 key issues in the SKM area.

V. RESULTS

The three most important issues in Round three include "developing access controls and policies," "designing and developing techniques to secure knowledge systems and to secure the contents," and "aligning business policy, business processes, and SKM policy" with a mean value of 8.42 or higher (see Table II). In terms of urgency, "developing access controls and policies," "advances in information privacy," and "designing and developing techniques to secure knowledge systems and to secure the contents" are the three most urgent issues with a mean value of 8.08 or higher (Table III). An interesting aspect of these two-dimensional (i.e., importance/urgency) rating results is that the five issues ranked at the top of the important-issue list are also ranked as the top five most urgent issues. Indeed, with few exceptions, this correlation between importance rank and urgency rank persists throughout the whole list.

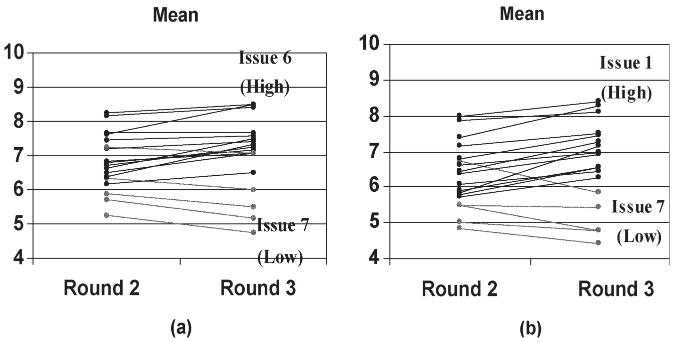


Fig. 4. Consensus for key issues by mean. (a) Importance and (b) urgency.

The three issues added in round two were analyzed separately as the consensus-improvement test is not applicable (see Table IV). Their importance and urgency ratings, which are independent from other issues' ratings, are similar to or slightly beyond the average, ranking them in the 7th, 10th, and 17th place in importance and 7th, 11th, and 5th place in the urgency list.

The results indicate that the participating experts consider "developing access controls and policies for organizational knowledge" is one of the most critical issues that needs to be urgently addressed. "Developing technical solutions for SKM systems and secure content dissemination" is also a very important and urgent issue for effective utilization of the organizational knowledge (Table IV). While these two issues focus more on the technical side of SKM, the experts also placed managerial, institutional, and cultural issues within the top five important and urgent issues. "Aligning business policy, business process, and SKM policy" emphasizes the needs for organizational changes that can integrate the SKM practice with every business activity. This issue can be reinforced by heightened awareness of the "importance of privacy" in the production and dissemination of information. "Exploring the role and implication of the government" is another critical issue that concerns the effects of government policies and regulations on the advancement of information privacy and integration of SKM in business policies and process.

VI. DISCUSSION AND CONCLUSION

The purpose of this study was to identify agreed upon key issues for future research on SKM. A three-round Delphi study yielded 21 key research issues in the SKM area. Also, the results of the standard-deviation analyses suggest that the study improved the participating experts' consensus on the identified issues in terms of importance and urgency.

This study has several contributions to the SKM field. First, the findings can benefit the researchers in the field by providing a broader view and a better understanding of what the important issues are in dealing with SKM. Second, the findings offer researchers a guideline that can ensure that important and urgent issues are taken into consideration in the early states of the SKM research. Third, the list of key issues identified by domain experts can help managers develop a comprehensive checklist for their SKM practice.

TABLE IV
RATING OF NEW ISSUES IN ROUND 3

Key issues and their Description	Importance		Urgency	
	MEAN	SD	MEAN	SD
New Issue 1: Security in the context of Extended Enterprise and/or Value Nets with the Customer in the Center	7.455	1.695	7.182	1.722
New Issue 2: Techniques for automatically transforming knowledge (guards)	7.273	1.555	6.727	2.102
New Issue 3: Modeling and using organizational and institutional trust	6.636	0.924	6.182	1.079

Although previous research suggests that an expert group of 10–18 is satisfactory for a Delphi study, the respondent rates for our study were lower than the ideal. In order to alleviate this limitation, future research may use a prearranged expert panel for a Delphi study. However, it was evident that a large portion of our expert group repeatedly participated in the three-round opinion-gathering processes, which would have a similar effect to that of a panel study. Another limitation of the study is the categorization of the issues. There were many criteria for categorizing key issues identified in the first round, such as unit/level of analysis, research context, approach, or technology/technique at a specific abstraction level. Although such an objective-categorization technique might generate a shorter list of less ambiguous issue statements, we focused on consolidating redundant or similar issues with an intention to preserve as many initial issue statements as possible. As the first study to develop research agenda in the SKM area, we believe that this approach would allow more flexible and liberal communication among domain experts. As the research community crystallizes relevant issues and develops shared concepts and terms, this limitation should be addressed by follow-up studies.

It is important to note that this study was not intended to capture the entire range of issues nor involve all experts in the SKM area. Nevertheless, this study leverages expertise from some of the pioneers in this developing field and offers a useful starting point for fellow researchers. Future research may extend our study and elaborate those key issues. In addition, the results of this study offer a baseline for future structuring of the SKM field. With researchers largely from both information security and knowledge-management communities, the field of SKM needs to build a consensus on its research criteria that can harmonize their different research orientations. By providing a chance to share opinions, this study helps the experts draw a unified and integrated map of the field.

ACKNOWLEDGMENT

This work was supported in part by the National Science Foundation (NSF) under Grants No. 0417095 and No. 0423014. The usual disclaimer applies.

REFERENCES

[1] S. Xu and W. Zhang, "PBKM: A secure knowledge management framework," in *Proc. Workshop Secure Knowledge Management (SKM)*, Buffalo, NY, Sep. 2004, pp. 207–212.

[2] B. Kogut and U. Zander, "Knowledge of the firm, combinative capabilities and the replication technology," *Organ. Sci.*, vol. 3, no. 3, pp. 383–397, 1992.

[3] J. Lee, S. J. Upadhyaya, H. R. Rao, and R. Sharman, "Secure knowledge management and the semantic web," *Commun. ACM*, vol. 48, no. 12, pp. 48–54, Dec. 2005.

[4] K. C. Desouza and G. K. Vanapalli, "Securing knowledge in organizations: Lessons from the defense and intelligence sectors," *Int. J. Inf. Manage.*, vol. 25, no. 1, pp. 85–98, 2005.

[5] J. P. Liebeskind, "Knowledge, strategy, and the theory of the firm," *Strateg. Manage. J.*, vol. 17, p. 93, Winter, 1996.

[6] M. B. James and S. Wm David, "Understanding the influence of organizational change strategies on information technology and knowledge management strategies," *Decis. Support Syst.*, vol. 31, no. 1, p. 55, May 2001.

[7] D. Constant, S. Kiesler, and L. Sproull, "What's mine is ours, or is it? A study of attitudes about information sharing," *Inf. Syst. Res.*, vol. 5, no. 4, p. 400, 1994.

[8] H. E. Tanriverdi, "Information technology relatedness, knowledge management capability, and performance of multibusiness firms," *MIS Q.*, vol. 29, no. 2, p. 311, 2005.

[9] S. Upadhyaya, H. R. Rao, and G. Padmanabhan, "Secure knowledge management," in *Encyclopedia of Knowledge Management*, E. D. Swartz, Ed. Hershey, PA: Idea Group Publishing, 2005, pp. 795–801.

[10] T. H. Davenport and L. Prusak, *Working Knowledge: How Organizations Manage What They Know*. Boston, MA: Harvard Business School Press, 1998.

[11] B. Thuraisingham, "Secure knowledge management: Workshop keynote," presented at the Workshop Secure Knowledge Management (SKM), Buffalo, NY, 2004.

[12] B. Thuraisingham, D. Chadwick, S. M. Olivier, P. Samarati, and E. Sharpston, "Privacy and civil liberties," presented at the 16th Int. Conf. Data and Applications Security, Cambridge, U.K., 2002.

[13] M. P. Grayson, "The challenges of secure knowledge management," presented at the Workshop Secure Knowledge Management (SKM), Buffalo, NY, 2004.

[14] B. L. MacCarthy and W. Atthirawong, "Factors affecting location decisions in international operations—A Delphi study," *Int. J. Oper. Prod. Manage.*, vol. 23, no. 7, pp. 794–818, Jul. 2003.

[15] J. P. Martino, *Technological Forecasting for Decision Making*, 2nd ed. New York: North-Holland, 1983.

[16] P. Ray and S. Sahu, "Productivity management in India: A Delphi study," *Int. J. Oper. Prod. Manage.*, vol. 10, no. 5, pp. 25–51, 1990.

[17] J. C. Brancheau, B. D. Janz, and J. C. Wetherbe, "Key issues in information systems management: 1994–95 SIM Delphi results," *MIS Q.*, vol. 20, no. 2, pp. 225–242, Jun. 1996.

[18] J. C. Brancheau and J. C. Wetherbe, "Key issues in information systems management," *MIS Q.*, vol. 11, no. 1, pp. 23–45, Mar. 1987.

[19] C. W. Holsapple and K. D. Joshi, "Knowledge manipulation activities: Results of a Delphi study," *Inf. Manage.*, vol. 39, no. 6, pp. 477–490, May 2002.

[20] S. Nambisan, R. Agarwal, and M. Tanniru, "Organizational mechanisms for enhancing user innovation in information technology," *MIS Q.*, vol. 23, no. 3, p. 365, Sep. 1999.

[21] P. L. Roth, "Group approaches to the Schmidt–Hunter global estimation procedure," *Org. Behav. Human Decis. Process.*, vol. 59, no. 3, p. 428, 1994.

[22] R. Corotis, R. Fox, and J. Harris, "Delphi methods: Theory and design load application," *J. Struct. Div.*, vol. 107, no. 6, pp. 1095–1105, Jun. 1981.

[23] G. Rowe and G. Wright, "The Delphi technique as a forecasting tool: Issues and analysis," *Int. J. Forecast.*, vol. 15, no. 4, p. 353, 1999.

[24] M. A. Jolson and G. Rossow, "The Delphi process in marketing decision making," *J. Mark. Res.*, vol. 8, no. 4, pp. 443–448, Nov. 1971.

[25] C. Okoli and S. D. Pawlowski, "The Delphi method as a research tool: An example, design considerations and applications," *Inf. Manage.*, vol. 42, no. 1, pp. 15–29, Dec. 2004.

[26] M. Turoff, "The policy Delphi," in *The Delphi Method: Techniques and Applications*, H. A. Linstone, M. Turoff, and O. Helmer, Eds. Reading, MA: Addison-Wesley, 1975.
[27] K. Brochhoff, "The performance of forecasting groups in computer dialogue and face-to-face discussion," in *The Delphi Method: Techniques and Applications*, H. A. Linstone, M. Turoff, and O. Helmer, Eds. Reading, MA: Addison-Wesley, 1975.
[28] G. W. Dickson, R. L. Leitheiser, J. C. Wetherbe, and M. Nechis, "Key information systems issues for the 1980's," *MIS Q.*, vol. 8, no. 3, pp. 135–159, Sep. 1984.
[29] J. F. Preble, "The selection of Delphi panels for strategic planning purposes," *Strategic Manage. J.*, vol. 5, no. 2, p. 157, Apr./Jun. 1984.
[30] F. Niederman, J. C. Brancheau, and J. C. Wetherbe, "Information systems management issues for the 1990s," *MIS Q.*, vol. 15, no. 4, p. 474, Dec. 1991.

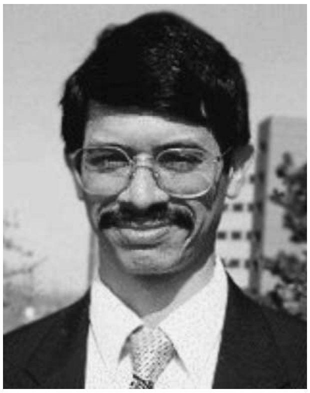
INSU PARK, *Guest Editor*
JINKYU LEE, *Guest Editor*
H. RAGHAV RAO, *Guest Editor*
Department of Management Science and Systems
State University of New York at Buffalo
Amherst, NY 14260
SHAMBHU J. UPADHYAYA, *Guest Editor*
Department of Computer Science and Engineering
State University of New York at Buffalo
Amherst, NY 14260

Insu Park received the M.S. degree in marketing from Hanyang University, Seoul, Korea, in 1996. He is currently working toward the Ph.D. degree in management science and systems at the School of Management, the State University of New York at Buffalo, Amherst.

His research interests are information security and privacy, security in knowledge sharing in the public/private sector, behavioral and economic decision making with risk, and uncertainty in the online context.

Jinkyu Lee received the Master of information systems degree from Griffith University, Australia, in 1999. He is currently working toward the MIS Ph.D. degree at the School of Management, the State University of New York at Buffalo, Amherst.

He will join the William S. Spears School of Business, Oklahoma State University, as an Assistant Professor of Management Science and Information Systems in August, 2006. His research interests are risk and trust in public/private sector e-service relationships, diffusion of information-security awareness/practice, and security in interorganizational knowledge sharing.



H. Raghav Rao received the Ph.D. degree from the Krannert Graduate School of Management, Purdue University, IN, in 1987.

He is a Professor of management science and systems at the State University of New York at Buffalo. His interests are in the areas of management information systems, decision support systems, and expert systems and information assurance. He has chaired sessions at international conferences and presented numerous papers. He has authored or coauthored more than 100 technical papers, of which more than 70 are published in archival journals. He has received funding for his research from the National Science Foundation (NSF), the Department of Defense and the Canadian Embassy, and has received the University's prestigious Teaching Fellowship. He has also received the Fulbright fellowship in 2004. He is a co-editor of a special issue of *The Annals of Operations Research*, the *Communications of ACM*, and Associate Editor of *Decision Support Systems, Information Systems Research* and IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS, and co-editor-in-Chief of *Information Systems Frontiers.* He is co-editor of a forthcoming book on *Managing Information Assurance in Financial Services* to be published by Idea Group. He would like to dedicate this issue to the memory of his mother and likes to thank his family for their support in this endeavor.

Dr. Rao received Best Paper and Best Paper Runner Up Awards at AMCIS and ICIS.

Shambhu J. Upadhyaya (S'84–M'86–SM'01) received the Ph.D. degree from the University of Newcastle, Newcastle, Australia, in 1987.

He is an Associate Professor of Computer Science and Engineering and Director of the Center of Excellence in Information Systems Assurance Research and Education at the State University of New York at Buffalo, Amherst, NY. Prior to July 1998, he was a Faculty Member at the Electrical and Computer Engineering department. His research interests are information assurance, computer security, fault diagnosis, fault tolerant computing, and very large scale integration (VLSI) testing. He has authored or coauthored more than 150 articles in refereed journals and conferences in these areas. His current projects involve intrusion detection, insider threat modeling, security in wireless networks, SoC test scheduling, analog circuit diagnosis, and RF testing. His research has been supported by the NSF, Rome Laboratory, the U.S. Air Force Office of Scientific Research, Defense Advanced Research Projects Agency (DARPA), and National Security Agency. In May 1999, International Business Machines (IBM) Corporation sponsored a new Electronic Test and Design Automation Lab to support his teaching and research on VLSI testing. He has been awarded an IBM Faculty Partner Fellowship for year 2000–2001 in recognition of his research accomplishments in the area of testing and fault tolerance. He was also a National Research Council (NRC) faculty fellow, in 2001 and 2002. In 2005, he received Cisco equipment donation to build a computer security lab. He has held Visiting Research Faculty positions at the Center for Reliable and High-Performance Computing, University of Illinois, Urbana–Champaign, Intel Corporation, Folsom, CA, AFRL, Rome, NY, and the Naval Research Laboratory, Washington, DC. He was the Program Co-Chair of the Fifth IEEE/Association for Computing Machinery (ACM) Great Lakes Symposium on VLSI, 1995. He has served on various Conference Committees including the IEEE Simulation Conference, Fault Tolerant Computing Symposium, IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems, and IEEE Symposium on Reliable Distributed Systems. He was the Publicity Chair of 1998 IEEE International Computer Performance and Dependability Symposium, and served as the USA Program Chair of IEEE Symposium on Reliable Distributed Systems at Nuernberg, Germany, in 2000. He was a guest co-editor of a book entitled: *Mobile Computing: Implementing Pervasive Information and Communication Technologies* (Kluwer Academic, 2002). He was a guest co-editor of a special issue on *Reliable Distributed Systems* in IEEE TRANSACTIONS ON COMPUTERS, February 2003. He was on the Program Committee of the *Third IEEE International Information Assurance Workshop*, Washington, DC, March 2005, the Sixth Annual IEEE Information Assurance Workshop, West Point, NY, June 2005, and the Dependable Computing and Communications Symposium of IEEE International Conference on Dependable Systems and Networks (DSN)-2005, among others. He is an Associate Editor of IEEE TRANSACTIONS ON COMPUTERS.

Dr. Upadhyaya is a member of the editorial board of the *International Journal on Reliability, Quality, and Safety Engineering* published by the World Scientific Publishers and is a member of IEEE Computer Society since 1984.