Knowledge Management and Security:
A Call for Research

Murray E. Jennex, Editor-in-Chief, IJKM

Welcome to the first issue of the third volume! This issue brings seven diverse articles. The first article from Land, Amjad, and Nolas comes from the Hawaii International Conference on System Sciences, HICSS, 2006 KM workshop and explores the issue of ethics in KM and is also a call for research. The second article from Passerini, Jennex, and Khaldoun reviews the KM forum that was held in Tunis, Tunisia in April 2006. This review looks at KM in North Africa, a region we have not looked at before (except for Egypt). The first research article from Ibrahim and Nissen looks at KM in organizations with discontinuous membership. The second research article from Wah, Menkhoff, Loh, and Evers explores social capital impacts on knowledge sharing in a Singapore educational institution. The third research article from Jackson and Webster describes a contingent methodology developed for the elicitation of working knowledge from policy makers within an Australian government agency. The fourth research article, from Zhang, attempts to assess the economic impacts of IS support for knowledge transfer on labor productivity and profitability. The fifth research article, from Priestly and Samaddar, explores the impacts on knowledge transfer from using the various multi-organizational networks.

This editorial explores security and KM and ultimately issues a call for research in this area. The inspiration for this editorial was the 2nd Workshop on KM and Security held in the fall of 2006. The focus of the workshop was on security technologies for securing knowledge in knowledge management systems. Security is an important topic, but is it important for KM? As Editor in Chief of the International Journal of Knowledge Management and co-Track Chair for the KMS Track at HICSS, I get to see a lot of KM research and I am fairly well integrated into the KM research community. To date, little KM research is coming through with a security focus; in fact, the IJKM has not published any articles on this topic. This editorial explores why this is so and where security can be integrated into KM.

KM can be defined as the capturing of knowledge from past decision making for application to current decision making with the express purpose of improving organizational performance (Jennex, 2005). KM success has been defined as supplying the right knowledge to those that need it when they need it (Jennex & Olfman, 2006). Both of these definitions focus on the core of KM: the capture and transfer of knowledge. Security is not emphasized although it can be inferred from “to those that need it” to mean not everyone has...
the need for knowledge, therefore we have to discern who are appropriate recipients and that access control is a form of security. Actually, security and KM may be considered an oxymoron as many researchers consider security a barrier to knowledge sharing and transfer. Jennex and Olfman (2005) summarized the literature on KM/KMS critical success factors into a set of 12 KM critical success factors (CSFs). These CSFs were then rated based on the number of studies identifying the CSF. Security and protection of knowledge resources was identified as the twelfth and last CSF. To put into perspective how researchers ranked security only one study, Jennex and Olfman (2000), identified security as a CSF while thirteen studies identified the top a CSF. A knowledge strategy that identifies users, sources, processes, storage strategy, knowledge and links to knowledge for the KMS. Having an organizational culture that supports learning and the sharing of knowledge was the fourth CSF most often mentioned by nine studies. Jennex and Olfman (2005) then compared the KM success/effectiveness models found in the literature with the list of CSFs. Of the five models evaluated, only one (Lindsey, 2002) directly addressed security. What this tells me is that we are focused on the barriers to knowledge sharing and transfer. To be honest, that probably is what we should be focusing on. Ultimately, the question that needs to be asked is: Why is security not considered a stronger CSF and important to KM success? The second question to ask is what aspect of KM success should emphasize security?

To explore these questions the Jennex and Olfman (2006) KM success model (based on the DeLone & McLean, 2003, IS success model) will be used (see Figure 1). This model was chosen due to its strong theoretical grounding; DeLone and McLean IS success model was first proposed in 1992 and has been validated by several studies with the 2003 version reflecting additions also suggested by these studies. The Jennex and Olfman (2006) KM success model has three basic dimensions: system quality dealing with the technical infrastructure, knowledge/information quality dealing with KM strategy for identifying critical knowledge and then how that knowledge is stored, and service quality dealing with management support and allocation of resources. The model also has the dimensions of perceived benefit, user satisfaction, and net benefits. These dimensions ensure that the KM initiative meets the needs of the users and the organization. Looking at these dimensions it is noted that there are points where applying security would make sense. Security could be an integral part of a KM strategy and of the technical resources such as networks, Web sites, and databases used for knowledge repositories and knowledge transfer.

Jennex and Olfman (2000) found that knowledge has value and so recommended protecting it. Value is shown in the KM success model in the net benefits and perceived benefit dimensions. Additionally, there is a growing body of research on intellectual capital that also stresses the value of knowledge and knowledge holders to the organization. It is expected that anything of value should be protected so it is logical that KM incorporate security. This was the thinking behind the Jennex and Olfman KM success model. It was expected that the technical components of KM such as networks, Websites, and databases would have security integral to them. I expect that this is the case with most KM success models and something that is assumed by KM researchers, that security is built into KMS components and that the topic does not need to be addressed separately in KM research. However, this is very important to maintain the integrity and confidentiality of stored knowledge and information, but it is not the most important area for applying security and this may necessitate more attention be applied to security in KM.

Security awareness is a key component of all security programs. Good security and good security awareness depend upon management support in generating, communicating, and implementing the security plan. In addition to my KM research activities I am also a certified IS security professional, CISSP, and have been trained to incorporate this management support into my security programs. Security is an area of research I have only begun working in the last five years, while KM is something I have been doing for over ten years. If I had been working in the security field for as long as I have been doing KM, I would have been more aware of the importance of security to KM, therefore I have had to catch up on this idea. It was brought home to me about a year ago when I was addressing the United States Air Force’s first KM conference.
After my presentation, a young captain and I were talking and while she was interested in my approach to KM, her area of responsibilities was to protect the knowledge. She was hoping I could give her answers to her many questions on securing KM. I could not, and after thinking about her questions I realized this was something we need to take care of. Security should be an integral component of KM strategy and processes. Jennex and Addo (2005) discuss the functions of KM strategy as including identifying sources and users of knowledge, knowledge storage strategies, and processes for using and capturing knowledge. These functions are ideal and necessary for also identifying security policies to go with the capture and use of knowledge.

What should these policies address? We need to identify access control policies and technologies, privacy policies that take into account aggregation of knowledge, risk assessment policies so we can access value and threats to our knowledge, knowledge retention policies, and knowledge dissemination policies, secure storage policies, unapproved knowledge disclosure and other response procedures, and so forth. All these need to be determined as a part of our KM strategy process and need management support for resource allocation and enforcement.

To conclude, while the study of security techniques and technologies for technical aspects of KM is important, it is more important that security be factored into the KM strategy and processes.
used by the organization. Also, we need to bring more security focus into our KM research. This leads to the exploration of the above issues as well as bringing in a host of new issues such as how to encourage knowledge sharing in a secure environment.

It is my hope that this editorial will lead to security being a more integral part of KM research and that the IJKM will start seeing submissions focusing on security in KM issues.

REFERENCES