Inf Syst Front (2007) 9:493–504
DOI 10.1007/s10796-007-9053-4

Security as a contributor to knowledge management success

Murray E. Jennex · Suzanne Zyngier

Published online: 9 October 2007

Abstract Security is an important topic, but is it important for Knowledge Management (KM)? To date, little mainstream KM research is coming through with a security focus. This paper asks why, and proposes that security be integrated into KM success models. The Jennex and Olfman (International Journal of Knowledge Management 2(3):51–68, 2006) KM success model is used to illustrate how security, specifically risk management, and the National Security Telecommunications and Information System Security Committee (NSTISSC) security model can be applied to KM management support and governance and KM Strategy. Finally, two case studies are provided that illustrate the application of risk management through governance to KM.

Keywords Knowledge management · Knowledge management success · Knowledge management strategy · Security · Knowledge management governance · Knowledge transfer

1 Introduction

Security is about protecting something. Information System, IS, security is about protecting IS assets such as networks, databases, computers, and applications. Knowledge management (KM) is about sharing and transferring knowledge from knowledge producers to knowledge users.

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 2005b, p. iv). KM helps organizations better leverage their knowledge, or what they know, by applying the processes of knowledge identification, capture, storage, search, and retrieval, and by creating processes that facilitate the transfer of knowledge from those that generate it to those who use it to make decisions. KM results in business organizations generating value and competitive advantage (Zyngier et al. 2006). Military and government organizations also use KM to support decision making and to create intelligence value and tactical and strategic advantage (Maule 2006).

It is not intuitive to KM researchers and practitioners that security and KM are related. This is borne out in the literature. A review of the first 12 issues of the International Journal of Knowledge Management (IJKM) found no articles discussing security within KM out of the 41 published (although two editorials have been written: Jennex (2006) focuses on the persistence, i.e. integrity, of knowledge and Jennex (2007) is a call for research on KM security). Additionally, searches of Communications of the Association for Information Systems (CAIS) and Journal of the AIS also found no articles specific to KM security. An exception is the "Encyclopedia of Knowledge Management" edited by David Schwartz and published in 2006. This is a comprehensive work that attempts to provide a discipline specific body of knowledge for KM. Of the 117 entries, two deal with security. Both discuss applying security technologies to KM systems (Upadhyaya et al. 2006 and Wilson et al. 2006). This lack of research

M. E. Jennex (✉)
San Diego State University,
San Diego, CA, USA
e-mail: mjennex@mail.sdsu.edu

S. Zyngier
School of Business, La Trobe University,
Bundoora, VIC 3086, Australia
e-mail: S.Zyngier@latrobe.edu.au

suggests that KM security does not appear to be a topic of interest to KM researchers.

The objective of this paper is to explore why security research is not more important to KM research and to attempt to establish a research foundation and theoretical basis for why KM security should be a field of research in the KM discipline rather than just a context for applying security research. This paper focuses on those aspects of security that are unique to KM. To accomplish this we will look at what KM is, how KM success is defined, models of KM success/effectiveness, and support for KM success through KM governance as a mechanism to support the operationalization of KM success. The models will be used to provide a theoretical foundation for fitting security research into KM research and illustrate that security, and in particular risk management, needs to be a part of KM strategy and KM management support. The paper concludes with two case studies illustrating the application of risk management to KM strategy.

Why is this important? KM is about generating value and advantage for an organization. Value comes from having something that others want and may not have. Advantage comes from utilizing resources better than your competition or opposition. There are time and access elements to this value and advantage that affect its protection. KM researchers tend to focus on overcoming barriers to the transfer of knowledge rather than on how to ensure that only the right individuals get the knowledge. This is why incorporating security into KM becomes important. Threats against organizations exist and can target critical knowledge requiring organizations to implement security. Examples include opportunistic and organized criminals, espionage agents, and terrorists seeking to steal critical knowledge in the form of trade secrets, intellectual property, key processes, client/customer knowledge, research reports, etc. (Colarik 2006 and Gordon et al. 2006). Additionally, the glut of knowledge and information that is being generated and the increasing transience of workers can overwhelm organizational attempts to manage knowledge leading to concerns that organizations may not capture critical knowledge or that critical knowledge sources may leave (Jennex 2006). Finally, there is a concern that knowledge will be inappropriately applied leading to incorrect decision making and the possible erosion of value and competitive advantage (Walsh and Ungson 1991). Researchers need to incorporate security into KM models and theories so KM practitioners are aware that this issue is as important as knowledge representation, transfer, and other key KM issues that tend to be their focus. Also, this topic is important for managers so that they can better care for critical organizational resources and avoid possible Sarbanes–Oxley issues by making bad decisions through misuse of knowledge. Finally, this is important for KM researchers as they need to ensure their theories and models do not just create high value targets for outsiders and opportunities for organizations to lose or misuse valuable knowledge assets.

2 Knowledge management

KM was defined in the introduction however it is important to emphasize that KM is an action discipline that supports decision making. It is a fusion of technical, organizational, and social issues. This concept is furthered by Jennex (2005a) where a KM system (KMS) is defined using Churchman's (1979) view of systems and includes the processes and users as part of the KMS in addition to the IT components. The KMS consists of processes and technologies for identifying and capturing knowledge, knowledge repositories, processes for storing, searching, retrieving, and displaying knowledge, and users. It is not required that the KMS be computer-based and in many cases repositories consist of "in-the-head" knowledge. Within this Churchman (1979) view of a KMS, KM security needs to address the complete system view and as will be shown later in the paper, this system view better fits existing security models than that of a purely technical system view. To further set the stage for discussion, the concepts of knowledge and knowledge transfer are briefly defined below.

2.1 Knowledge

Davenport and Prusak (1998) view knowledge as an evolving mix of framed experience, values, contextual information and expert insight that provides a framework for evaluating and incorporating new experiences and information. They found that in organizations, knowledge often becomes embedded in artifacts such as documents, video, audio or repositories and in organizational routines, processes, practices, and norms. They also suggest that for knowledge to have value it must include the human additions of context, culture, experience, and interpretation. Polanyi (1967) and Nonaka and Takeuchi (1995) describe two types of knowledge, tacit and explicit. Tacit knowledge is understood within a knower's mind, cannot be directly expressed by data or knowledge representations, and is commonly understood as unstructured knowledge. Explicit knowledge, on the other hand, can be directly expressed by knowledge representations and is commonly known as structured knowledge. Current thought has knowledge existing as neither purely tacit nor purely explicit. Rather, knowledge is a mix of tacit and explicit with the degree of explicitness varying with each user. This is the knowledge continuum where purely tacit and purely explicit form the end points and specific knowledge artifacts existing somewhere on the continuum. Smolnik et al. (2005) take a position on the knowledge continuum through context explication where context explication reflects the experience and background of the individual. Nissen and Jennex (2005) expand knowledge into a multidimensional view by adding the dimensions of reach (social aggregation), life cycle (stage of the knowledge life cycle), and flow time (timeliness) to explicitness. Research continues to refine the concept of knowledge and its dimensions.

2.2 Knowledge transfer

Knowledge transfer in an organization occurs when members of an organization pass knowledge to each other. Nonaka and Takeuchi (1995) propose four modes of knowledge creation and transfer.

- Socialization is the process of sharing experiences and thereby creating tacit knowledge such as mental models and technical skills. Tacit knowledge can be obtained without using language through observation, imitation, and practice.
- Externalization is the process of articulating tacit knowledge in the form of explicit concepts, taking the shapes of metaphors, analogies, concepts, hypotheses, or models.
- Combination is the process of systemizing concepts into a knowledge system by combining different bodies of explicit knowledge. Explicit knowledge is transferred through media such as documents, meetings, email, and/or phone conversations. Categorization of this knowledge can lead to the generation of new knowledge.
- Internalization is the process of converting explicit knowledge to tacit knowledge and is closely related to learning by doing.

3 Knowledge management success

3.1 Definition

KM success is a multidimensional concept. It is defined by capturing the right knowledge, getting the right knowledge to the right user, and using this knowledge to improve organizational and/or individual performance. KM success is measured using the dimensions of impact on business processes, strategy, leadership, efficiency and effectiveness of KM processes, efficiency and effectiveness of the KM system, organizational culture, and knowledge content (Jennex et al. 2007). This definition, as well as the definitions of KM and KMS, focuses on the core of KM, the capture, transfer, and application of knowledge from knowledge creators to knowledge users. Security is not emphasized nor mentioned in these definitions. Indeed, security and KM may be considered conflicting concepts as many researchers consider security a barrier to knowledge sharing. To support this statement and to better understand KM success we need to look at what KM researchers have identified as KM/KMS critical success factors (CSFs). CSFs are those factors that are found to have to be present for KM/KMS success to occur. They are not grounded in theory, they are observed phenomena. The following section presents KM/KMS success factors.

3.2 KM critical success factors

Jennex and Olfman (2005) summarized and synthesized the literature on KM/KMS critical success factors into an ordered set of 12 KM CSFs. CSFs were ordered based on the number of studies identifying the CSF. The following CSFs were identified from 17 studies looking at over 200 KM projects. They are listed in order of frequency:

1. A KM Strategy that identifies users, sources, processes, storage strategy, knowledge and links to knowledge for the KMS.
2. Motivation and Commitment of users including incentives and training
3. Integrated Technical Infrastructure including networks, databases/repositories, computers, software, KMS experts
4. An organizational culture and structure that supports learning and the sharing and use of knowledge
5. A common enterprise wide knowledge structure that is clearly articulated and easily understood
6. Senior Management support including allocation of resources, leadership, and providing training
7. Learning organization
8. There is a clear goal and purpose for the KMS
9. 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
10. The search, retrieval, and visualization functions of the KMS support easy knowledge use
11. Work processes are designed that incorporate knowledge capture and use
12. Security/protection of knowledge

As can be seen, security and protection of knowledge resources was identified as the 12th, and least identified, CSF. To put into perspective how researchers ranked security only the study by Jennex and Olfman (2001) identified security as a CSF, while 13 studies identified the top CSF and nine studies identified the fourth most mentioned CSF.

To ground KM CSFs with a theoretical framework, researchers construct KM success and/or effectiveness models that incorporate CSFs into established theory. Jennex and Olfman (2005) compared several KM success/effectiveness models found in the literature to the above list of CSFs. Of the five models found and evaluated, only the Lindsey (2002) KM Effectiveness Model directly addressed security, while the Jennex and Olfman (2006) KM Success Model considered security as an implicitly understood need. The next sections look at those two models to examine how security fits into KM/KMS success/effectiveness.

3.3 Lindsey KM effectiveness model

Lindsey (2002) proposed a conceptual KM effectiveness model based on combining Organizational Capability Perspective theory (Gold et al. 2001) and Contingency Perspective Theory (Becerra-Fernandez and Sabherwal 2001). The model defines KM effectiveness in terms of two main constructs: Knowledge Infrastructure Capability and Knowledge Process Capability, with the Knowledge Process Capability construct being influenced by a Knowledge Task. Knowledge infrastructure capability represents social capital, the relationships between knowledge sources and users, and is operationalized by technology (the network itself), structure (the relationship), and culture (the context in which the knowledge is created and used). Knowledge process capability represents the integration of KM processes into the organization, and is operationalized by acquisition (the capturing of knowledge), conversion (making captured knowledge available), application (degree to which knowledge is useful), and protection (security of the knowledge). Tasks are activities performed by organizational units and indicate the type and domain of the knowledge being used. Tasks ensure the right knowledge is being captured and used. KM success is measured as satisfaction with the KMS. Jennex et al. (2007) found satisfaction with a KMS to be a weak definition of success. Figure 1 below illustrates the Lindsey (2002) KM Effectiveness Model.

Lindsey (2002) included protection as an activity needed by an organization to support knowledge processes where protection can be interpreted to include technical security controls such as firewalls and virus protection, access controls to limit access to those that need the knowledge, and secure storage media with backup and recovery. Lindsey (2002) considered protection important due to the critical impact knowledge can have on a firm's competitive advantage. This is a key issue for mainstreaming KM security research, recognizing that knowledge is a critical asset needing to be protected. However, the protection activity in this model is tied to regular protection activities and controls and does not really include anything unique to KM. Also, this is a theoretical model that has not been tested by research. The Jennex and Olfman (2006) KM Success Model is based on research and will be discussed next.

3.4 Jennex Olfman KM success model

The Jennex and Olfman (2006) KM success model was generated based on several case studies and quantitative research studies and is theoretically grounded on the DeLone and McLean (2003) IS success model. This model is considered a better description of KM success due to its strong theoretical grounding [the DeLone and McLean (1992) IS success model has been accepted for several years and has been validated by several studies with DeLone and McLean (2003) reflecting additions also

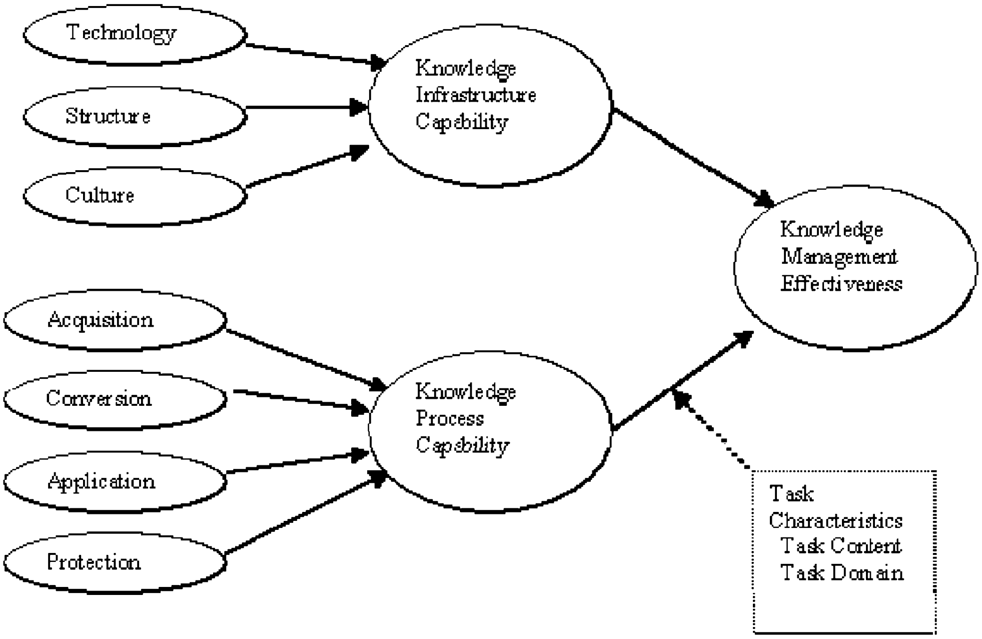


Fig. 1 Lindsey (2002) KM effectiveness model

suggested by these studies], its reflection of observed phenomena, and its close fit to the set of 12 CSFs. Reflecting security in this model generates a theoretical grounding for KM security research.

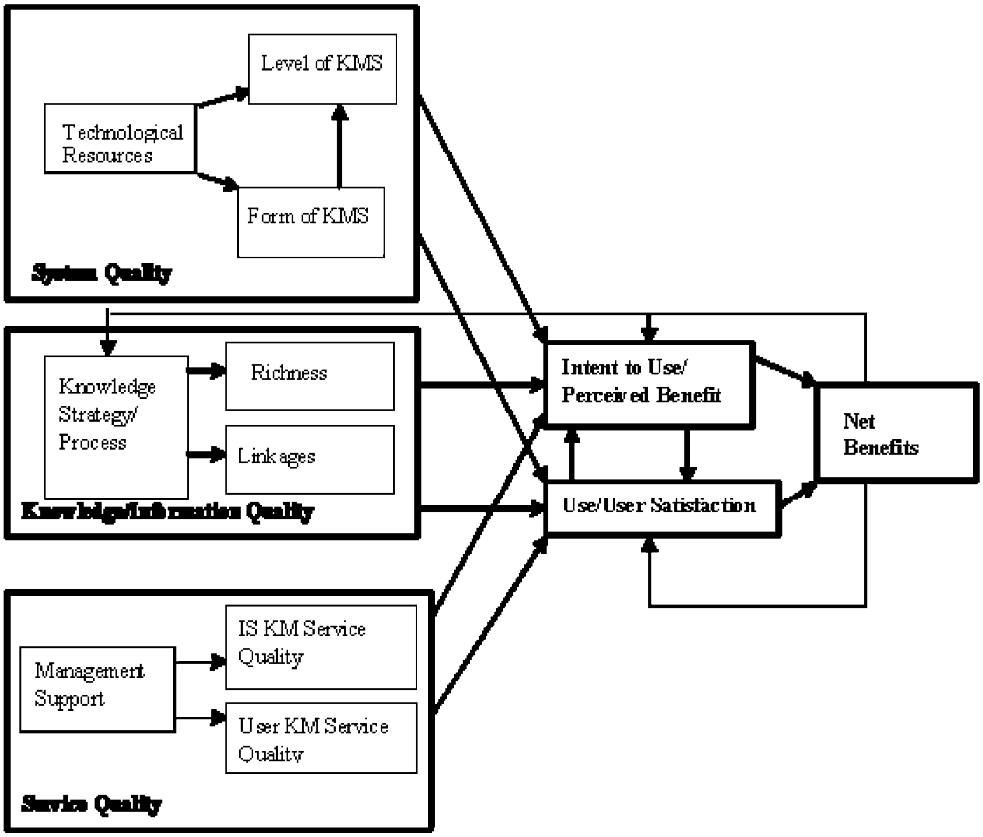
The Jennex and Olfman (2006) KM success model is a causal model. It has three basic dimensions as antecedents to KM success: system quality which deals with the technical infrastructure; knowledge/information quality which deals with KM strategy for identifying critical knowledge and then how that knowledge is stored; and service quality which deals with management support and allocation of resources. The model also has the dimensions of perceived benefit, user satisfaction, and net benefits. These dimensions deal with ensuring that the KM initiative meets the needs of the users and the organization. Figure 2 illustrates this model.

This model doesn't directly include security. However, Jennex and Olfman (2001) in their study of Year 2000 (Y2K) KMS found that security was a needed design recommendation. This recommendation was based on analyzing the systems using an earlier version of the Jennex Olfman KM Success Model. Jennex and Olfman (2001) found that for knowledge to have value it must be correct and able to be trusted. Security was seen as needed to ensure the integrity of knowledge stored in the KMS knowledge base. This was considered critical as KM is seen as creating organizational value through improved decision-making. To improve decision-making KMS users must trust the knowledge that is retrieved so its integrity must be protected (this is shown through the perceived benefit model's near term job impact construct). This is consistent with the Lindsey KM Effectiveness model (2001) as both models recognize the need to protect integrity. The final version of the Jennex and Olfman (2006) KM Success Model included this integrity protection implicitly in its description of the Knowledge Quality constructs so does not omit security as being an antecedent to KM success.

The important nature and qualities of leadership in KM and the need for alignment of KM strategy with the aims and objectives are generally proclaimed (Amidon and Macnamara 2003; Holsapple and Joshi 2002a, b; Jennex and Olfman 2006; Probst et al. 2000; Zyngier and Burstein 2004). These are embedded in the Jennex and Olfman (2006) KM Success Model through the quality approach to systems, knowledge/information, and service. This is expanded by incorporating the governance of KM processes to the above model by adding *explicit* alignment with organizational strategy, through: authorization of activity; risk management; fiscal fiduciary duty; and measurement as factors supporting the knowledge security of the organization.

KM governance centers the decision-making authority to an executive framework to deliver the expected benefits of

Fig. 2 Jennex and Olfman (2006) KM success model



the strategy (Zyngier 2006). KM programs are then delivered in a controlled manner, through the establishment of checks and balances in the mode of service delivery. Governance processes manage the risks of KM to acknowledge and contend with cultural issues, structural obstacles and other relevant issues as they arise. The management of these risks assist in the resolution of these issues and in turn strengthen the strategies to manage knowledge that are employed within the organization. Acknowledging specific knowledge as the organization's strategic asset and differentiator is the ultimate responsibility of the governance process and a component of KM strategy and management.

The next section discusses how security further fits into KM success and is more important than just maintaining integrity.

4 KM success and security

Both the Lindsey (2002) and the Jennex and Olfman (2006) models consider KM success to be reflected through some organizational impact, usually as improved organization effectiveness that results from improved decision-making that improves the organization's competitive advantage. Knowledge is therefore seen as a valuable asset. There is a growing body of research on intellectual/social capital that also stresses the value of knowledge and knowledge holders to the organization. This research is being embraced by the KM research community (Davenport and Holsapple 2006; Sherif and Sherif 2006; Wah et al. 2007). The concepts of due diligence and fiduciary responsibility generate the expectation that anything of value should and will be protected so it is logical that KM incorporate security. This was the thinking behind the Jennex and Olfman (2006) KM success model. It was expected that the technical components of KM such as networks, web sites, and databases would have security integral to them as suggested by Jennex and Olfman (2001). It is expected that this is the case with most, if not all, KM success models and something that is assumed by KM researchers, that security is built into KMS components and that the topic doesn't need to be addressed separately in KM research. However, while this is very important to maintaining the availability, integrity, and confidentiality of stored knowledge and information, it is not the most important area for applying security and this may necessitate more attention be applied to security in KM. As stated previously, Jennex and Olfman (2005) assessed the various KM success models and determined that the Jennex and Olfman (2006) KM success model is a better fit to the 12 identified CSFs than the Lindsey (2002) KM effectiveness model. For this reason the following discussion on security and KM utilizes the Jennex and Olfman (2006) KM success model.

Looking at the Jennex and Olfman (2006) KM Success model dimensions it is noted that there are points where applying security would make sense. In addition to the previously noted technical resources such as networks, web sites, and databases used for knowledge repositories and knowledge transfer, security should also be an integral part of a KM strategy. Also, due to legal requirements stemming from the Health Information Portability and Accountability Act (HIPAA) and the Sarbanes Oxley Act, there is more of an expectation from management that knowledge will be protected, its integrity maintained, and when appropriate, its confidentiality maintained. These are considered critical KM security areas and will be discussed in the next section.

5 KM security

Current thoughts on information security management view security as a function that incorporates technical, managerial, and organizational issues into a plan that manages organizational risk. Security includes technical, administrative, and managerial controls. It includes a formal plan that contains policies stating how the organization intends to implement security. It involves education and awareness. The National Security Telecommunications and Information System Security Committee model (NSTISSC 1994) is a standard model used in information security management. The NSTISSC model is shown in Fig. 3 below and illustrates that all of the above concepts are part of an overall security strategy and plan. This is a comprehensive model for designing the security plan for protecting information systems. The model stands independent of technology as it does not specify any specific technologies, just the functions technologies perform, and can be applied to any organization without being affected by organizational

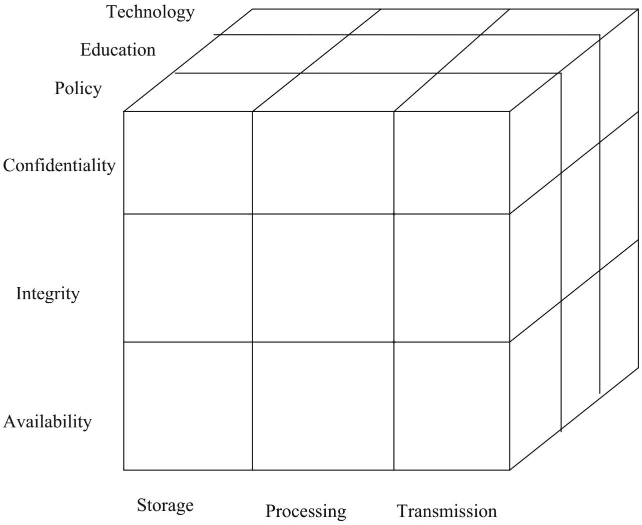


Fig. 3 NSTISSC security model (NSTISSC 1994, p. 18)

differences as it does not incorporate any specific organizational needs or characteristics.

Figure 3 shows the focus on protecting storage, processing, and transmission assets. When this is applied to KM the focus is on protecting knowledge repositories, knowledge mnemonic functions (search, retrieve, compare, etc.) used to process and manipulate knowledge, and knowledge transfer communication processes. It also demonstrates that we need to protect integrity, confidentiality, and availability that when applied to KM means protecting the integrity of knowledge artifacts, controlling who gets access, or has the need to know, to knowledge, and when the KMS and knowledge repositories need to be operational. Finally, it also shows the need for education and policy that applied to KM are reflected in KM training and governance. Combined, these constitute the components of an overall KM security program.

A security program includes policies that determine what should be protected, who should have access (based on need to know analysis), and allowable use of information; along with security awareness education and management support and direction. Security should be an integral component of a KM initiative and traditional security is reflected with the Technical Resources construct of the System Quality dimension and includes the technical controls needed to protect the basic technical system components of the KMS. The components of this construct include databases, web sites, networks, and other IS components. System Quality refers to how well these components work and for them to work as expected, technical security controls such as firewalls, intrusion detection, cryptography, and access controls are utilized. Again it is stressed that this is regular security and not what is proposed as KM Security.

KM Security starts with the Management Support construct of the Service Quality dimension of the Jennex and Olfman (2006) KM Success Model. Management support refers to the direction and support an organization provides to ensure that adequate resources are allocated to the creation and maintenance of KM, a knowledge sharing and using organizational culture is developed, encouragement, incentives, and direction is provided to the work force to encourage KM use, knowledge reuse, and knowledge sharing; and that sufficient control structures are created in the organization to monitor knowledge and KM use (Jennex and Olfman 2006). Zyngier (2006) describes these functions along with risk management and leadership as KM governance. It is the addition of risk management to this construct that clarifies part of the role of security in KM and is essential part of the NSTISSC (1994) security model as it ensures that management is aware of risks in the KM initiative, that these risks are managed through appropriate policies and controls, and that KM users are aware of and trained in these policies and controls. Risks to be managed include the risk of not capturing or losing critical knowledge, misusing critical knowledge, and disclosing critical knowledge to those that should not get it.

While Management Support or governance provides the leadership and risk management direction for creating a security plan, it is the KM Strategy/Processes construct of the Knowledge Quality dimension that provides the information needed to identify what security policies and controls are to be generated. Jennex and Addo (2005) discuss the functions of KM strategy as including identifying knowledge to be captured, sources and users of knowledge, knowledge storage strategies, and processes for using and capturing knowledge. Zyngier et al. (2006) establishes the relationship between KM governance, KM strategy implementation, and KM success or as in the case of the Jennex and Olfman (2006) KM Success Model, the relationship between the Management Support and the KM Strategy/Process constructs to KM success. Both are necessary for KM success and both are necessary for incorporating security into KM initiatives.

What should KM security policies address? Security policies need to identify access control policies and technologies, privacy policies that take into account aggregation of knowledge, risk assessment policies for guidance in assessing the value and threats to knowledge, knowledge retention policies, knowledge dissemination policies, secure storage policies, unapproved knowledge disclosure and other response procedures, etc. All these need to be determined as a part of the KM strategy process and need management support for resource allocation and enforcement. As these constructs are part of the theoretically grounded Jennex and Olfman (2006) KM Success Model we consider incorporating security into these constructs as providing the theoretical basis for incorporating security research into KM research.

To summarize, KM security is about analyzing risk and protecting knowledge assets appropriately. This requires the generation of a KM security plan. This plan is generated based on KM governance/management support and KM strategy/process. Policies and controls are determined through the generation of KM strategy. The key enabler of this process is the incorporation of risk management into KM governance/management support. This is where KM security research needs to focus. Previous KM research has focused on applying security technology to a KMS context through the application of technological controls to knowledge repositories and transfer processes. This is necessary but is not research into KM security. KM security research should be focused on the integration of security principles as illustrated by the NSTISSC (1994) security model, into KM. The following sections provide two case studies that explore the application of KM governance/management support and KM strategy that incorporates risk management to KM initiatives.

6 Research design

The purpose of this paper is to provide a theoretical grounding to KM security research. This has been provided by incorporating KM security into the Jennex and Olfman (2006) KM Success Model. KM Security is postulated as incorporating risk management into KM strategy and governance. To provide qualitative support for this postulation exploratory research was conducted using case study research methodology to examine risk management, KM, and governance within an organizational context. Eisenhardt (1989) and Yin (1994) were used to construct a research approach that includes multiple, converging sources of data and data collection methods that included observation, semi-structured interviews and document analysis. Two cases are presented where risk management was used with KM. The cases contrast organizational KM efforts before and after the application of risk management and governance to the KM initiative. Case study analysis took place over a period of several months collecting, examining and analyzing data in its original context.

The research focused on understanding how senior officers in organizations understand KM and how they govern KM as a tool for the transfer of organizational knowledge. KM and governance theories provided the basis for focused observation and for the recording of the observations. Organizations were selected through searching lists of Most Admired Knowledge Enterprises Study winners (Chase 2004), referral by other KM professionals, databases of companies, and examination of candidate organizational websites. By purposefully locating organizations that were considered successful with KM it was speculated that they may have had governance structures in place. The observation sample sought to include both users of KM and those who were implementing KM strategy as stakeholders. The case study subject selection criteria were:

- Large organizations with over 2,000 employees;
- Single organizations without independent subsidiaries;
- Multi-sited organizations;
- A reputation as knowledge intensive; and
- A reputation for the pursuit of knowledge management strategies.

Research comprised semi-structured interviews using open-ended questions, observation, and collection of secondary data in the form of available documentary evidence from within the organizations plus additional publicly available materials. Interviews were tape recorded, supplementary notes were taken, and additional documentary material was collected for analysis. For each case, the interviews were transcribed and submitted to the interviewees for their comment thus establishing the defensibility of that data (Eisenhardt 1989; Schoenberger 1991).

Interviewee selection criterion was that the informant be a senior executive in their organization who is actively involved in the leadership and implementation or the governance of the KM strategy. The interviews were transcribed and analyzed using QSR5 software as a tool for thematic analysis. In each case, the informants gave semi-structured; in-depth interviews each lasting approximately one hour.

7 Research findings XYZ Consulting

XYZ Consulting is a dispersed multinational enterprise selected due (Lincoln and Guba 1985) to its large size and its distributed nature and for having a positive reputation as reflected in their Knowledge Group Global Director being invited as a participant in the Knowledge Group Global Director Summit (Oxbrow 2003, 2004) and as reflected in the business press as a knowledge intensive organization. It is a top six, internationally ranked, multinational management consulting firm with its global headquarters located in the USA. It works with leading organizations to improve their course and performance by stimulating innovative ideas. The company was started in the 1960s with a single consultant and now employs over 2,600 consultants worldwide through a network of 60 offices in 37 countries. The company was established as, and continues to operate as, a partnership. In 2003, the company recorded revenues of US$1.12 billion.

The current KM strategy was initiated when the Partnership decided that they and their consultants needed to know “how to know what we know and how to find the people who know” (informant 1). When the informant was employed to develop the KM initiative as a global initiative it was seen as being “primarily to bring together what had been a completely uncoordinated set of researchers working in different places and in different ways.” This was due to the informant’s view that the company researchers and the KM initiative were inseparable. The thrust of this KM initiative was to create a global structure and set of processes to capture and manage explicit knowledge resources. This KM strategy reflects managing risk of failing to capture or losing critical knowledge.

7.1 Prior systems—obstacles

The company had a practice of retaining PowerPoint presentations together with the supporting documentation.

These were kept in individual office locations on shared drives. One of the partners who sponsored the early KM initiative was a practice area leader who tried to encourage all the other practice area leaders to be systematic about the management of intellectual property. "Specifically they had assistants who 'kept the keys to the safe', you know and would dish out these decks that people would ask for by email or however" (informant 1). This underlines the problems faced by the organization. There was little or no coordination or control over what was understood to be a highly valuable resource. Additionally, the transfer of tacit knowledge was traditionally facilitated by pro-active staff education and training. The work structure in teams and by practice areas and practice interest groups created a clustering of expertise within individual locations and regions. Working in specialist teams that were led by senior management who played an active part resulted in mentoring of less experienced staff by those senior staff. However, there was little or no coordination or control over the transfer of tacit knowledge. Company growth from 2 consultants in one location in 1963, to 12 consultants in two countries in 1965 to its current size of 2,600 consultants in 60 locations globally. The obvious consequence of this was the difficulties in personalization of knowledge to transfer knowledge between individuals locally and its transfer between locations globally (Hansen et al. 1999; Nonaka 1991).

Three major risks in the management of knowledge resources were identified:

- The risk of unauthorized access to material about client affairs and the preservation of client confidentiality. Responsibility for the management of these resources was handled by assistants—specifically the Partner's secretary "some of whom were very careful about it and others who weren't" (informant 1).
- The risk of not capturing or losing critical knowledge resources as "there was not a really good system of indexing or anything so the recovery or retrieval was a bit random and depended really on how much the secretary knew about the work" (informant 1). Specifically the lack of a systematic, organization wide approach to search and retrieval of documents and related resources was a serious limitation on the availability of explicit knowledge resources.
- The risk of the right people not getting the knowledge needed to make decisions. This is due to problems in the transfer of knowledge.

7.2 XYZ Consulting: Risk management through governance

Risks to the KM strategy are managed in a reactive rather than a proactive manner. Attitudes expressed by the informant have been couched in terms of ameliorating risks to both the structural and cultural aspects of the KM strategy. In particular, at the global level the KM Team is responsible for and report to the governance authority to:

- Protect inadvertent disclosure of knowledge to competing client teams through the use of 'Chinese walls' access controls;
- 'Ensure our materials are sanitized [to prevent security breaches], and make sure the most recent stuff is there' (informant 1);
- Mine databases to identify and leverage existing best practice;
- Act on security issues for levels of access to electronic resources; and
- Proactively report to and listen to partners and staff in order to ensure that the KM strategy continues to meet organizational needs.

Risk is jointly identified by the KM Team together with the Practice Area Leaders—who are partners and therefore the governing body, by reporting to them and "listening to their ideas and their needs and meeting them" (informant 1).

8 Research findings ABC Exploration and Drilling

ABC Exploration and Drilling is a publicly listed multinational oil and gas exploration and production company. Its global headquarters is in Western Australia. It has an international presence beyond its Australia ownership base. This enterprise was selected due to its large size and its distributed nature and for having been a finalist in the 2004 Asian MAKE awards (Chase 2004). Additionally it has been showcased and discussed at a number of Australian and European conferences as a knowledge intensive organization.

ABC Exploration and Drilling is Australia's leading company in its field. Established in 1954 the company has developed from being regarded as a junior player in the industry to being among Australia's largest independent listed oil and gas companies with a market capitalization of approximately $10 billion. The company is the operator of multiple joint ventures with other companies and has substantial oil and gas production assets. During 2003 the company recorded revenues of AUD$2059.3 million.

8.1 Prior systems—obstacles

The initial KM strategy for ABC Exploration and Drilling focused on explicit knowledge capture. This was achieved through purchase of a collaboration tool and portal to manage explicit knowledge across the company. This was intended to structure, retain and support the range of work required by the firm and to facilitate the sharing of this work. There had been no policies set in place to determine the alignment of the KM strategy with the aims and objectives of the company. There was no company wide KM strategy in place to establish priorities for explicit knowledge capture, nor for how it should be done. It was realized that while collaboration through a portal was possible, it also was a limited approach that didn't take into account the understanding of how knowledge was transferred between organizational members. Additionally, there were no specific strategies used to leverage tacit knowledge. Tacit knowledge transfer was ad hoc and took place incidentally to the structured activities of the firm. One key risk was identified: the risk of not capturing or losing critical knowledge and its subsequent security physical and commercial in confidence status within the company.

8.2 ABC Exploration and Drilling: Risk management through governance

KM governance was implemented through formation of a steering group. The steering group ensures that management's KM goals are incorporated into the KM strategy by requiring reviews of KM activities and by developing policies that take into account the regulatory, market and human resources issues that are identifiable by the stakeholders on the Steering Group. As a member of the group, the Team Leader of Knowledge & Management Systems also discusses these same issues with the Steering Group and with his implementation team.

Identified KM security policies include:

- Misuse of intellectual capital or breach of copyright issues; and
- Security breaches of the IT systems

Legal liability risks are monitored for breaches and are managed through training. Security breaches of IT systems are monitored and controlled for through the use of firewalls although “technology is always going to be a problem” (informant 2).

Risk management as a tool of governance has resulted in strategies being developed to the specific identified obstacles to the implementation of this strategy. These can be seen as an outcome of the governance process in that while strategies are developed in accordance with policy, they have been modified in order to overcome the obstacles.

9 Conclusion

This paper asks why security is not considered a stronger CSF and important to KM success. We conclude that KM security is an important KM CSF but just wasn't articulated as such by researchers who considered it an integral part of KMS technology. If the only application of security to KM was technology this would be fine. However, this paper broadens KM security to include risk management in KM strategy, KM management/governance support, and ultimately, to increasing the value of knowledge, KM and its impact on the organization by managing risks such as reluctance to share knowledge, disclosure of knowledge to those that don't need it, and losing, not capturing, or misapplying critical knowledge. KM Success models can incorporate this aspect of security. The Jennex and Olfman (2006) KM Success Model explicitly included security in its knowledge strategy and implicitly in other success constructs such as management support and technical resources. It would be useful for this and other models to clearly and more fully articulate the need for security in all applicable KM success dimensions but we suspect this will be left to the KM security researchers to do.

The incorporation of security into KM strategy utilizes risk analysis and management. The cases presented in this paper link KM management/governance, KM strategy, and management of KM risks. Risk management activities were not only identified but solutions to those risks were found through:

- Analysis of the KM risks
- Articulation of the KM requirements of the organizations;
- Strategic alignment of solutions; and
- Authorized activity to address the risks.

The cases present risk management activity as a tangible benefit of KM governance identifying and including risk management as a component of their KM strategy. It should also be noted that the case studies are not comprehensive in reflecting security in KM. Rather, they are meant to illustrate that security and KM are related and that security can be applied to KM through application of a KM success model incorporating KM governance.

As shown earlier, the extant KM literature documents many CSFs necessary to the effective implementation of a KM strategy (lack of these CSFs can be considered risks to successful KM). Risk management supports action to resolve obstacles to existing problems. Proactive approaches anticipate and manage risks by setting benchmarks and goals (Standards Australia 2000, 2001, 2004). The main elements are communication and consultation, internal and external organizational context, identification, analysis and evaluation. In the cases presented here, risk management is an iterative and ongoing process. From the evidence, it can be suggested that successful risk management outcomes reported by informants can be attributed to support of such activity by the governing body.

This research has made a contribution to KM literature. It has identified bodies that are responsible for governance activities within this framework, their roles, and their tasks. It has made a new contribution to research literature through identification and analysis of processes that govern KM. This research facilitates effective implementation of KM strategies by providing a framework for organizations to use to ensure that authority, risk-management, financial control, and measurement are operationalized in order to realize benefits from KM strategy implementation. We strongly suggest that KM governance maximizes strategic benefits and manages the risks in successful implementation of KM strategies in specifically large, distributed organizations.

Additionally we have made a contribution to practice. Grimes (2007) states the need for a better understanding of data, information, and knowledge and incorporating security into a research design will increase the ability to share data, information, and knowledge. This paper has incorporated security into KM success which forms the basis for KMS design. Understanding how to create secure KMS will increase the ability of all organizations, business, government, or military, to improve the transfer of knowledge to key decision makers. This will lead to increased organizational performance, the primary goal of KM.

References

Amidon, D. M., & Macnamara, D. (2003). The 7 C's of knowledge leadership: Innovating our future. In C. W. Holsapple (Ed.) *Handbook on knowledge management, 1: Knowledge matters* (pp. 539–551). Berlin: Springer-Verlag.

Becerra-Fernandez, I., & Sabherwal, R. (2001). Organizational knowledge management: A contingency perspective. *Journal of Management Information Systems*, *18*(1), 23–55.

Chase, R. L. (2004). *Asian most admired knowledge enterprises—Executive summary*. Bedford, UK: Teleos—The KNOW Network.

Churchman, C. W. (1979). *The systems approach (revised and updated)*. New York: Dell Publishing.

Colarik, A. M. (2006). *Cyber terrorism: Political and economic implications*. Hershey, PA, USA: Idea Group Publishing.

Davenport, D. I., & Holsapple, C. W. (2006). Social capital knowledge. In D. G. Schwartz (Ed.) *Encyclopedia of knowledge management* (pp. 809–817). Hershey, PA: Idea Group Reference.

Davenport, T. H., & Prusak, L. (1998). *Working knowledge*. Boston, MA: Harvard Business School Press.

DeLone, W. H., & McLean, E. R. (1992). Information systems success: The quest for the dependent variable. *Information Systems Research*, *3*, 60–95.

DeLone, W. H., & 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.

Eisenhardt, K. M. (1989). Building theories from case study research. *The Academy of Management Review*, *14*(4), 532–550.

Gold, A. H., Malhotra, A., & Segars, A. H. (2001). Knowledge management: An organizational capabilities perspective. *Journal of Management Information Systems*, *18*(1), 185–214.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2006). *CSI/FBI computer crime and security survey*. Computer Security Institute, retrieved on June 1, 2007 from http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf.

Grimes, J. G. (2007). Harnessing information for military operations, intelligence and business. *Military Information Technology, 11*(1), 21–26.

Hansen, M. T., Nohria, N., & Tierney, T. (1999). What's your strategy for managing knowledge. *Harvard Business Review*, *77*(2), 106–116.

Holsapple, C. W., & Joshi, K. D. (2002a). Knowledge management: A threefold framework. *The Information Society*, *18*, 47–64.

Holsapple, C. W., & Joshi, K. D. (2002b). Knowledge manipulation activities: Results of a Delphi Study. *Information & Management*, *39*, 477–490.

Jennex, M. E. (2005a). Knowledge management systems. *International Journal of Knowledge Management*, *1*(2), i–iv.

Jennex, M. E. (2005b). What is knowledge management. *International Journal of Knowledge Management*, *1*(4), i–iv.

Jennex, M. E. (2006). Why we can't return to the moon: The need for knowledge management. *International Journal of Knowledge Management*, *2*(1), i–iv.

Jennex, M. E. (2007). Knowledge management and security: A call for research. *International Journal of Knowledge Management*, *3*(1), i–iv.

Jennex, M. E., & Addo, T. B. A. (2005). *Knowledge management strategy issues*. Proceedings of the 2005 Information Resource Management Resource Conference.

Jennex, M. E., & Olfman, L. (2001). Development recommendations for knowledge management/organizational memory systems. In M. K. Sein, B. E. Munkvold, T. U. Orvik, W. Wojtkowski, W. G. Wojtkowski, S. Wrycza, & J. Zupancic (Eds.) *Contemporary trends in IS development* (pp. 209–222). Norwell, MA: Kluwer.

Jennex, M. E., & Olfman, L. (2005). Assessing knowledge management success. *International Journal of Knowledge Management*, *1*(2), 33–49.

Jennex, M. E., & Olfman, L. (2006). A model of knowledge management success. *International Journal of Knowledge Management*, *2*(3), 51–68.

Jennex, M. E., Smolnik, S., & Croasdell, D. (2007). Knowledge management success. *International Journal of Knowledge Management*, *3*, (2), i–vi.

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. Beverly Hills, Calif.: Sage Publications.

Lindsey, K. (2002). *Measuring knowledge management effectiveness: A task-contingent organizational capabilities perspective* (pp. 2085–2090). Eighth Americas Conference on Information Systems.

Maule, R. W. (2006). Military knowledge management. In D. G. Schwartz (Ed.) *Encyclopedia of Knowledge Management* (pp. 627–634). Hershey, PA: Idea Group Reference.

Nissen, M., & Jennex, M. E. (2005). Knowledge as a multidimensional concept: A call for action. *International Journal of Knowledge Management*, *1*(3), i–v.

Nonaka, I. (1991). The knowledge-creating company. *Harvard Business Review*, November–December, 96–104.

Nonaka, I., & Takeuchi, H. (1995). *The knowledge-creating company—How Japanese companies create the dynamics of innovation*. Oxford: Oxford University Press.

NSTISSC (1994). *National Training Standard For Information Systems Security (INFOSEC) Professionals, NSTISSI No. 4011*. National Security Telecommunications and Information Systems Security Committee. Retrieved from http://niatec.info/pdf/4011.pdf on March 1, 2006.

Oxbrow, N. (2003). *Second CKO summit for the public sector*. London: TFPL.

Oxbrow, N. (2004). *'Sticky' knowledge strategies CKO summit 2004*. London: TFPL.

Polanyi, M. (1967). *The tacit dimension*. London: Routledge.

Probst, G., Raub, S., & Romhardt, K. (2000). *Managing knowledge: Building blocks for success*. Chichester: Wiley.

Schoenberger, E. (1991). The corporate interview as a research method in economic geography. *Professional Geographer*, *43*(2), 180–189.

Sherif, K., & Sherif, S. A. (2006). Think social capital before you think knowledge transfer. *International Journal of Knowledge Management*, *2*(3), 21–32.

Smolnik, S., Kremer, S., & Kolbe, L. (2005). Continuum of context explication: Knowledge discovery through process-oriented portals. *International Journal of Knowledge Management*, *1*(1), 27–46.

Standards Australia (2000). *AS/NZS ISO 9000:2000 Quality management systems—Fundamentals and vocabulary* (3rd ed.). Sydney: Standards Australia, Standards New Zealand & International Organization for Standardization.

Standards Australia (2001). *HB 275–2001 Knowledge management: A framework for succeeding in the knowledge era*. Sydney: Standards Australia International Limited.

Standards Australia (2004). *AS/NZS 4360:2004 Risk management* (3rd ed.). Sydney: Standards Australia & Standards New Zealand.

Upadhyaya, S., Rao, H. R., & Padmanabhan, G. (2006). Secure knowledge management. In D. G. Schwartz (Ed.) *Encyclopedia of knowledge management* (pp. 795–801). Hershey, PA: Idea Group Reference.

Wah, C. Y., Menkhoff, T., Loh, B., & Evers, H. D. (2007). Social capital and knowledge sharing in knowledge-based organizations: An empirical study. *International Journal of Knowledge Management*, *3*(1), 29–48.

Walsh, J. P., & Ungson, G. R. (1991). Organizational memory. *Academy of Management Review*, *16*(1), 57–91.

Wilson, R. L., Rosen, P. A., & Al-Ahmadi, M. S. (2006). Secure knowledge discovery in databases. In D. G. Schwartz (Ed.) *Encyclopedia of knowledge management* (pp. 787–794). Hershey, PA: Idea Group Reference.

Yin, R. K. (1994). *Case study research: Design and methods* (2nd ed.). Newbury Park, CA: Sage Publications.

Zyngier, S. (2006). Knowledge management governance. In D. G. Schwartz (Ed.) *Encyclopedia of knowledge management* (pp. 373–380). Hershey, PA: Idea Group Reference.

Zyngier, S., & Burstein, F. (2004). Knowledge management strategies: Leaders and leadership. In H. Linger, et al. (Ed.)*'Constructing the infrastructure for the knowledge economy; methods and tools, theory and structure' Proceedings of the 12th. International Conference on Information Systems and Development (ISD'03)* (pp. 405–416). Melbourne: Kluwer Academic.

Zyngier, S., Burstein, F., & McKay, J. (2006). *The Role of knowledge management governance in the implementation of strategy.* 39th Hawaii International Conference on System Sciences, HICSS, IEEE Computer Society.

Murray E. Jennex is an associate professor at San Diego State University, editor in chief of the International Journal of Knowledge Management, editor in chief of Idea Group Publishing's Knowledge Management book series, and president of the Foundation for Knowledge Management (LLC). Dr. Jennex specializes in knowledge management, system analysis and design, IS security, e-commerce, and organizational effectiveness. Dr. Jennex serves as the Knowledge Management Systems Track co-chair at the Hawaii International Conference on System Sciences. He is the author of over 100 journal articles, book chapters, and conference proceedings on knowledge management, end user computing, international information systems, organizational memory systems, ecommerce, security, and software outsourcing. He holds a B.A. in chemistry and physics from William Jewell College, an M.B.A. and an M.S. in software engineering from National University, an M.S. in telecommunications management and a Ph.D. in information systems from the Claremont Graduate University. Dr. Jennex is also a registered professional mechanical engineer in the state of California and a Certified Information Systems Security Professional (CISSP).

Suzanne Zyngier is a Research Fellow in the School of Business at La Trobe University, Melbourne. Her research centres on the governance of knowledge management (KM) strategies and the development of a framework for the effective, sustainable implementation of KM. The framework describes the roles and tasks involved at each point of governance: authorization, planning and development, and the implementation of KM programs. Suzanne completed her PhD at Monash University and has written journal articles, technical reports, book chapters and has presented papers at international conferences and at presentations to industry.