December 2005

Impact of Security Measures on the Usefulness of Knowledge Management Systems

Chen Ting
National University of Singapore

Chen Ting
National University of Singapore

Atreyi Kankanhalli
National University of Singapore

Impact of Security Measures on the Usefulness of Knowledge Management Systems

Chen Ting
School of Computing
National University of Singapore
chentin1@comp.nus.edu.sg

I.M.Y Woon
School of Computing
National University of Singapore
iwoon@comp.nus.edu.sg

Atreyi Kankanhalli
School of Computing
National University of Singapore
atreyi@comp.nus.edu.sg

Abstract

Knowledge Management (KM) has been recognized as a critical management strategy in generating competitive advantage for the organization. In order to protect organizational knowledge stored in or transferred through company's Knowledge Management Systems (KMS), information security controls have to be incorporated into these systems. However, overly strict controls may adversely impact the perceived usefulness of the system and consequently its usability. This research examines the impact of security measures on perceived usefulness of KMS. More specifically, we investigated the impact of security training, security policy and technology on the perceived usefulness of KMS. Security self-efficacy, perceived personal responsibility, content quality, and perceived ease of use were included as mediating factors. The proposed research model was tested empirically through a survey of 51 IT professionals working at a large public university who are currently using a secure knowledge repository. Results show that security training impacts perceived personal responsibility directly and through security self-efficacy of the user. KMS security level affects perceived ease of use both directly and through content quality of the system. As expected, perceived personal responsibility and perceived ease of use impact perceived usefulness of the KMS. The theoretical and practical implications of the findings are discussed.

Keywords: Knowledge management system, security measures, perceived usefulness

1. Introduction

Knowledge management (KM) has been recognized as a critical management strategy in generating competitive advantage for the organization (Grant, 1996). Information technology is recognized as an important enabler for the implementation of KM initiatives (Alavi & Leidner, 2001). The class of information technologies that support and enhance the various KM processes is known as Knowledge Management Systems (KMS) (Alavi & Leidner, 2001).

KMS Technology	Technical Security Solution
KMS Supporting Technology: • Database, Repository • BBS, Forum, Groupware	Access Control (Authentication, Authorization) Encryption, Issue Specific Policies
KMS Platform Technology: • Intranet	Firewall, SSH, VPN, IDS, Issue Specific Policies

Table 1. Technical Security Solutions for KMS

The advent of modern web technology has enhanced the capability of KMS by allowing larger amounts of knowledge resources to be made available to organizational employees. However, the greater availability of online knowledge has also increased the likelihood of its

unauthorized access and abuse by both employees and outsiders. Previous research (Gold et. al, 2001; Liebeskind, 1996) highlights that only upon securing its valuable knowledge assets can the organization sustain the competitive advantage created by them. Thus, in order to guard KMS from security threats, various security technologies have been incorporated into these systems. Table 1 shows various security technologies that could be used to guard KMS. The term secured knowledge management systems (secured KMS) refers to those KMS that are under the protection of such security mechanisms (Thuraisingham, 2004). However, security technologies such as firewalls and anti-virus software alone are insufficient to manage the security challenges of the Internet age (Dhillon and Backhouse, 2001). As humans are often an inherent source of security threats and vulnerabilities, security policies that specify acceptable and unacceptable actions in using these systems are necessary (Whitman & Mattord, 2003).

Though added security mechanisms (policies and technology) could provide better protection for knowledge assets in the organization, if applied inappropriately, they may be restrictive in nature and conflict with the open sharing culture required to promote KM initiatives (Liebeskind, 1996). Motivated by these concerns which has not been addressed by previous literature, the purpose of this study is to identify and understand the security related factors that influence users' perception of the usefulness of secured KMS. Such an understanding may lead to organizational interventions or technology design considerations which can promote usage of secured KMS and thereby enhance the effectiveness of the organization's KM strategy (Gray 2000).

2. Literature Review

Past KMS studies have identified various factors that might affect users' perception of KMS usefulness. These include the output quality of the KMS, effort of using KMS, an individual's KMS experience, and social norms (Liaw & Huang, 2003; Kankanhalli, 2002). However, the impact of security mechanisms on KMS usefulness has not been considered. The information security and organizational behavior literature are reviewed to investigate the possible impacts.

Information security is defined as the protection of information and systems that use, store and transmit that information (NSTISS, 1994). The purpose of information security is to protect the three characteristics of information, namely confidentiality, integrity and availability, through both technical solutions and managerial actions (NSTISS, 1994). Some previous literature (e.g., Whitman and Mattord 2003) has suggested that the increase in system security strength would protect the content quality and overall quality of the system perceived by users. On the other hand, other studies (e.g., Johansson 2001) pointed out that high security strength could reduce the usability of the information system. For example, Nelson (2003) showed that high security strength might hinder users in their work if it denies them access to resources or services they need. Such an impact of security measures on the convenience of using a system might affect users' perception of usefulness of the overall system.

Past information security and organizational behavior literature has also shed light on the individual characteristics that might affect the user acceptance of and resistance to security measures and secured information systems. Frank et al. (1991) showed that perceived personal responsibility, informal norms, personal computer (PC) knowledge, and PC experience might have an impact on the security related behaviors of PC users in an organization. Other studies (Adams and Sasse 1999) found that users' understanding of

security issues and awareness of security threats greatly affect their perception of the usefulness of security mechanisms and the overall secured system. Based on the above literature and concepts, we have developed a research model that relates system security measures (level and training), system characteristics (content quality) and individual factors (security self-efficacy and perceived personal responsibility) to the acceptance of secured KMS.

3. Research Model and Hypotheses

Figure 1 presents the research model and hypotheses of this study. We propose that *KMS security level* impacts *perceived ease of use of secured KMS* both directly and mediated through *content quality*. *Security Training/Awareness Effort* is expected to impact *perceived personal responsibility* both directly and through *security self-efficacy*. In turn, *perceived ease of use* and *perceived personal responsibility* are proposed to influence *perceived usefulness of the secured KMS*.

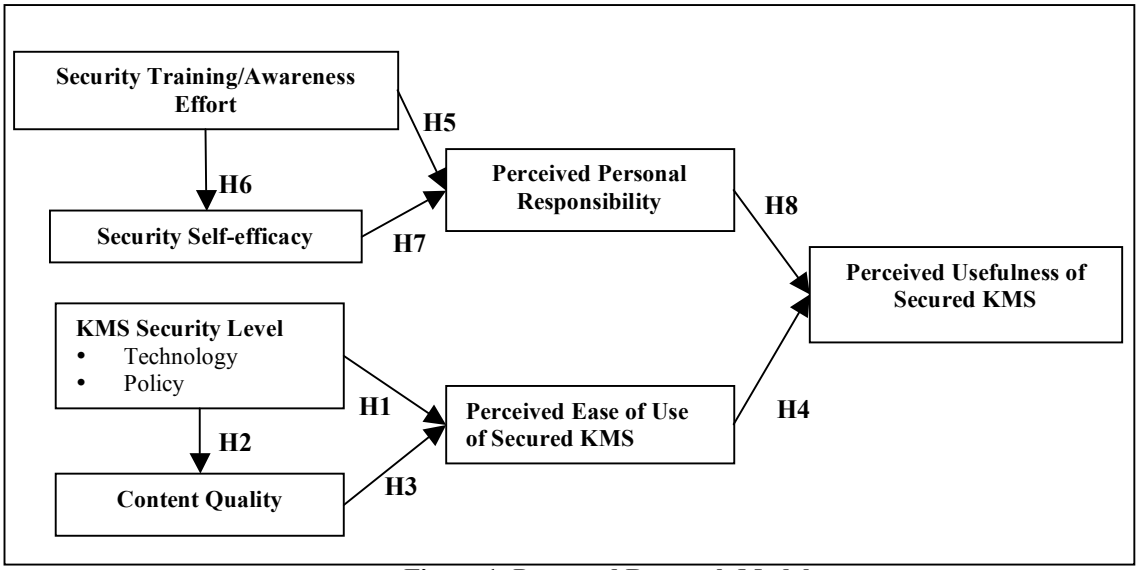

Figure 1. Proposed Research Model

KMS Security Level refers to the clarity, comprehensiveness, and intensity of the security controls implemented in the secured KMS. Both technical security solutions implemented and security policies imposed on the system are part of the security controls (Whitman & Mattord, 2003). *Perceived ease of use* refers to "the degree to which a person believes that using a particular system would be free of effort" (Davis 1989). A broader view of ease of use includes elements such as ease of learning, ease of control, and understandability (Davis 1989). Strict policies imposed on the system restrict users from accessing the content when needed (Nelson, 2003). Security technologies such as complex authentication models and encryption methods using concepts unknown to users also make the system difficult to understand and to use (Johansson, 2001). Therefore, we posit that,

H1. KMS security level is negatively related to the perceived ease of use of the secured KMS.

On the other hand, by protecting the integrity, availability and confidentiality of the content in the system, security controls could help to preserve the overall *content quality* of the system (Whitman & Mattord, 2003). Content quality is a major determinant of overall IS quality (Liaw & Huang, 2003), which has a positive effect on individual's perceived ease of use of information systems. Hence, we hypothesize,

H2. KMS security level is positively related to the content quality of the secured KMS.
H3. Content quality is positively related to the perceived ease of use of the secured KMS.

Perceived usefulness is defined as "the degree to which a person believes that using a particular system would enhance his or her job performance" (Davis, 1989). The less effort needed to use a system, the more it may be used to increase job performance. Effort saved due to improved ease of use may be redeployed, enabling a person to accomplish more work for the same effort (Davis, 1989). Thus, we expect that,

H4. Perceived ease of use is positively related to the perceived usefulness of the secured KMS.

Security Training/Awareness Effort refers to the organization's effort in building in-depth security knowledge and improving understanding of the security needs of its employees (Whitman & Mattord, 2003; Adam & Sasse, 1999). Users' *perceived personal responsibility* for the results of their actions is a form of psychological contract which is defined as "expectations about the reciprocal obligations that compose an employee-organization exchange relationship" (Morrison & Robinson, 1997). Previous research showed that organizational effort in providing security training and awareness programs could help users of the system better understand the purpose for security and recognize their respective responsibilities in safeguarding the security of the system (Adam & Sasse, 1999). Therefore, we hypothesize,

H5. Security Training/Awareness Effort is positively related to user's perceived personal responsibility.

Moreover, studies (Compeau and Higgins 1995) have shown that support from the organization could increase individuals' judgment of self-efficacy. We refer to self-efficacy with respect to the secured use of the secure system as *security self-efficacy*. The organizational effort of providing training and awareness programs to employees is expected to improve their judgment and their ability (Bandura, 1982) in using the system in a secured manner. Also, people with strong self-efficacy beliefs in performing certain tasks will be more committed to the tasks and more likely to take responsibility for their actions (Staples et. al., 1998). Therefore, we posit,

H6. Security Training/Awareness Effort is positively related to security self-efficacy.
H7. Security self-efficacy is positively related to perceived personal responsibility.

Previous studies (Morrison and Robinson 1997) indicate that individuals would seek to assign responsibility when they are faced with unknown situations in performing a task. This process results in the assignment and recognition of responsibility. Once users recognize their responsibilities in using a secured KMS, their perceptions regarding the usefulness of the technology will be favorably enhanced (Ozag & Duguma, 2004). This leads us to the following hypothesis,

H8. Perceived personal responsibility is positively related to the perceived usefulness of the secured KMS.

4. Research Methodology

The survey research method was adopted to collect data for testing our theoretical model. A step-by-step process recommended by Churchill (1979) was used to develop the survey instrument.

4.1 Construct Operationalization

Where available, constructs have been measured using tested items from prior studies to enhance validity. Where this was not possible, we generated new items based on a review of

past literature. KMS security level (KMSL) was measured using items (self-developed and from Straub 1990) for technology aspects (KMST) and policy aspects (KMSP). KMST assessed access control, authentication, firewall, and encryption levels. KMSP measured clarity, comprehensiveness, and accessibility of policies and enforcement of penalties. Security training and awareness effort (STAE) measured the effectiveness of security training programs in the organization and their frequency (based on Martins & Eloff 2001). Content quality (CTQL) assessed the accuracy, reliability, and timeliness, of content (from Kankanhalli 2002) as well as belief in the integrity of the content (from Whitman and Mattord 2003). Perceived personal responsibility (PPRP) was measured as the understanding of roles and responsibilities related to use of secured KMS. Security self-efficacy (SSEF) items were modified from computer self-efficacy items (Compeau & Higgins 1995) to suit the security context. Perceived ease of use (PEOU) and perceived usefulness (PUFN) of the secured KMS were assessed using standard measures from Venkatesh (2000), Venkatesh & Davis (2000), and Rai et al. (2002). Two items for STAE were frequency measures based on a six-point scale ranging from 0 ("Never Before") to 5 ("less than once in 6 months"). The rest of the items were measured using the 7-point Likert scale. Table 2 gives the items for the constructs after validation.

KMS Security Level (Policy)	
KMSP1	There are clearly written rules and procedures guiding the use of secured knowledge management system.
KMSP2	There are comprehensive written rules and procedures guiding the use of secured knowledge management system.
KMSP3	There are too many rules and procedures guiding the use of secured knowledge management system.
KMSP4	There is strict enforcement of written rules and procedures.
KMSP5	The penalties for misuse of the secured knowledge management system are severe enough.
KMSP6	The information security policies are readily available for reference.
KMS Security Level (Technology)	
KMST1	The level of access control for the secured knowledge management system is fine-grained.
KMST2	The authentication level for the secured knowledge management system is high.
KMST3	The security setting level of the firewall securing the secured knowledge management system is high.
KMST4	The encryption strength of the encryption algorithm used by the secured knowledge management system is high.
Security Training and Awareness	
STAE1	My organization holds information security awareness program. [] Weekly [] Monthly [] Quarterly[] Half yearly [] Less than once in 6 months [] Never Before
STAE2	My organization sends me for information security training. [] Weekly [] Monthly [] Quarterly[] Half yearly [] Less than once in 6 months [] Never Before
STAE3	My organization ensures that I am aware of information security relating to the use of the secured knowledge management system.
STAE4	My organization educates me about the concept of information security of the secured knowledge management system.
STAE5	My organization gives me specific training about the information security procedures which I need to follow when using the secured knowledge management system.
Content Quality	
CTQL1	The secured knowledge management system provides me with reliable knowledge that I need.
CTQL2	The secured knowledge management system provides me with timely knowledge that I need.
CTQL3	The secured knowledge management system provides me with accurate knowledge that I need
CTQL4	I am confident that the knowledge in the secured knowledge management system is kept secure.
CTQL5	I am confident that the knowledge in the secured knowledge management system cannot be illegally modified.
CTQL6	I am confident that the knowledge in the secured knowledge management system will be

	available when I require it.
CTQL7	I believe that knowledge in the secured knowledge management system is always in its original state, and hence can be trusted.
Perceived Personal Responsibility	
PPRP1	I understand the consequences of circumventing security practices of the secured knowledge management system.
PPRP2	I understand that user's level of responsibility for the security of the secured knowledge management system.
PPRP3	If I discover suspicious/unusual occurrences happening on the secured knowledge management system, I will report it to the security personnel.
PPRP4	I feel that I need to comply with all the security practices guarding the secured knowledge management system when I am using the system.
Security Self Efficacy	
SSEF1	I know what knowledge should be kept confidential.
SSEF2	I know what knowledge should be kept confidential. if there was someone giving me step by step instructions.
SSEF3	I know what knowledge should be kept confidential if there was no one to tell me what to do.
SSEF4	I know what knowledge should be kept confidential if I have seen someone using it before
	I know what knowledge should be kept confidential if I have a copy of written procedures and rules to refer to
Perceived Ease of Use	
PEOU1	Interacting with the secured knowledge management system does not require a lot of my mental effort.
PEOU2	It is not laborious to comply with the security mechanisms when I am using the system.
PEOU3	The security mechanisms do not impede my access to the knowledge I want from the system.
PEOU4	It is easy to understand the interaction requirements of the system and any messages generated by the system.
PEOU5	I find it is easy to get the secured knowledge management system to do what I want it to do.
Perceived Usefulness	
PUFN1	Using secured knowledge management system improves my job performance
PUFN2	Using secured knowledge management system enhances my effectiveness on the job
PUFN3	I find that the secured knowledge management system is useful to my job.
PUFN4	The secured knowledge management system makes my job easier to accomplish.

Table 2. Constructs and Items

4.2 Survey Administration

The 50 item survey was administered to 68 IT professionals working in the IT departments of a large public university. Out of these distributed questionnaires, 51 were returned, resulting in a total response rate of 75%. All chosen respondents are users of a KMS called "Developer's Corner", which is used to store and exchange software system development related knowledge within the IT departments of the university. Role-based access control is implemented in guarding the system, and the system is strictly open only to the developers within the departments. A cover letter explaining the significance of the study and assuring the confidentiality of responses was included with the survey instrument. All the respondents were volunteers. Nevertheless, they were given a token payment for their participation.

	Frequency	Percentage
Gender		
Male	35	68.6%
Female	16	31.4%
Age		
21-29	13	25.5%
30-34	26	51.0%
35-39	6	11.8%
40-50	6	11.8%

Education		
Diploma	1	2.0%
Bachelor	28	54.9%
Master	21	41.2%
Doctorate	1	2.0%
Working Experience		
0-3	3	5.9%
3-6	12	23.5%
6-9	15	29.4%
9-12	13	25.5%
12-15	4	7.8%
>=15	4	7.8%

Table 3. Profile of Respondents

4.3 Descriptive Statistics

Table 3 delineates the profile of the respondents. The majority of the respondents are male (68.6%), aged between 30 and 34 (51%) and have either a Bachelor or Master degree (96.1%). Over 94% of the respondents have at least 3 years of working experience.

5. Data Analysis

Partial Least Squares (PLS) analysis, a Structure Equation Modeling (SEM) technique, was employed to assess our model. PLS evaluates the measurement model (relationships between items and constructs) within the context of the structural model (relationships among constructs) (Fornell and Larcker, 1981). This technique does not require multivariate normal distribution or large sample sizes for its data. In addition, it is able to handle both formative and reflective manifest variables jointly occurring in one structural model (Falk & Miller, 1992). In the current study, KMS security level is a formative construct as it consists of several dimensions and the indicators of each dimension are measures that form or cause the creation or change in the construct (Bollen, 1984). Besides, given that the sample size for this study is relatively small, PLS is appropriate for this study. PLS-Graph version 3.0 was used in data analysis to assess the measurement and structural models.

Constructs and Items	**Item Weights**	**Constructs and Items**	**Item Weights**
KMS Security Level		**KMS Security Level**	
KMSP1	0.43***	KMST1	0.31**
KMSP2	-0.18*	KMST2	0.08
KMSP3	-0.60***	KMST3	0.47***
KMSP4	0.35***	KMST4	0.07
KMSP5	0.10	* Indicates item is significant at $p < 0.05$ level;	
KMSP6	-0.22*	** $p < 0.01$ level; *** $p < 0.001$ level	

Table 4. Item Weights for KMS Security Level

5.1 Evaluation of Measurement Model

The measurement model consists of relationships between the constructs and the items used to measure them. Its strength is demonstrated through convergent and discriminant validity (Hair et. al, 1998). It should be noted that reflective and formative constructs need to be treated differently during the evaluation. Examination of correlations or internal consistency among the measuring items of formative constructs is irrelevant (Mathieson et al., 1996). However, the absolute value of the items weights for formative constructs will be examined instead. The evaluation of formative constructs and reflective constructs will be separately discussed in the following sections.

Formative Construct

There is one formative construct in this study, the KMS Security Level. The item weights are examined to identify the relevance and level of contribution of the items to this construct. From Table 4, we can see that KMSP3 and KMST3 contribute most to the KMS Security Level. This suggests that users of the system consider that the KMS security level is mainly determined by the number of rules and procedures guiding the use of the system and the strength of firewalls imposed on the system.

Constructs and Items	Item Reliability	Cronbach's Alpha	Alpha if Item Deleted	Average Variance Extracted (AVE)
Security Training and Awareness Effort		0.85		0.64
STAE1	0.64		0.87	
STAE2	0.67		0.85	
STAE3	0.91		0.79	
STAE4	0.91		0.78	
STAE5	0.82		0.81	
Content Quality		0.94		0.73
CTQL1	0.89		0.93	
CTQL2	0.90		0.92	
CTQL3	0.85		0.93	
CTQL4	0.81		0.93	
CTQL5	0.79		0.94	
CTQL6	0.84		0.93	
CTQL7	0.90		0.92	
Perceived Personal Responsibility		0.91		0.78
PPRP1	0.93		0.86	
PPRP2	0.91		0.86	
PPRP3	0.90		0.87	
PPRP4	0.79		0.92	
Security Self Efficacy		0.82		0.56
SSEF1	0.83		0.86	
SSEF2	0.62		0.72	
SSEF3	0.89		0.72	
SSEF4	0.59		0.75	
Perceived Ease of Use		0.87		0.67
PEOU1	0.65		0.88	
PEOU2	0.89		0.82	
PEOU3	0.86		0.84	
PEOU4	0.80		0.85	
PEOU5	0.87		0.83	
Perceived Usefulness		0.96		0.90
PUFN1	0.95		0.95	
PUFN2	0.96		0.95	
PUFN3	0.95		0.95	
PUFN4	0.94		0.96	

Table 5.Convergent Validity for Reflective Constructs

Reflective Constructs

The rest of the constructs, other than the KMS Security Level, are reflective constructs. Convergent validity is assessed for these constructs by testing a) item reliability, b) Cronbach's Alpha and c) average variance extracted (AVE) by each construct (Fornell and Larcker, 1981). As shown in Table 5, all 29 items have loadings on their respective constructs

greater than 0.50, and 24 out of 29 items have a loading above 0.78. This indicates that these items have sufficient item reliability (Barclay et al., 1995). All constructs have Cronbach's Alpha values of 0.70 and above, indicating adequate internal consistency (Nunnally, 1978). All AVE are well above 0.5 (Fornell & Larcker, 1981). Hence all reflective constructs of our model showed adequate convergent validity.

Constructs	Items	Component					
		1	2	3	4	5	6
Security Training/ Awareness Effort (STAE)	STAE1	-0.18	0.01	0.24	0.61	0.12	0.29
	STAE2	-0.23	0.17	0.12	0.69	0.14	0.18
	STAE3	0.32	0.13	0.25	0.80	0.03	-0.06
	STAE4	0.34	-0.02	0.19	0.85	0.03	-0.01
	STAE5	0.29	0.21	-0.01	0.81	-0.01	0.01
Content Quality (CTQL)	CTQL1	0.80	0.27	0.04	0.22	0.22	0.20
	CTQL2	0.79	0.25	0.15	0.16	0.05	0.22
	CTQL3	0.82	0.08	0.10	0.11	-0.09	0.21
	CTQL4	0.74	0.15	0.14	0.00	0.20	0.20
	CTQL5	0.74	0.13	0.21	0.04	0.15	0.01
	CTQL6	0.85	0.13	0.03	-0.03	-0.05	0.17
	CTQL7	0.86	0.04	0.16	0.14	0.08	0.10
Perceived Personal Responsibility (PPR)	PPRP1	0.08	0.24	0.88	0.20	0.04	0.10
	PPRP2	0.06	0.21	0.86	0.21	0.08	0.13
	PPRP3	0.22	0.23	0.81	0.14	-0.02	0.17
	PPRP4	0.40	0.14	0.66	0.11	0.06	0.16
Security Self Efficacy (SSEF)	SSEF1	0.26	0.15	0.31	0.12	0.51	0.14
	SSEF2	-0.04	0.06	-0.06	-0.07	0.91	0.02
	SSEF3	0.17	0.04	0.18	0.25	0.79	0.10
	SSEF4	0.06	0.14	-0.07	0.02	0.88	-0.07
Perceived Ease of Use (PEOU)	PEOU1	0.23	0.05	0.29	0.05	0.06	0.69
	PEOU2	0.30	0.43	0.08	0.20	-0.02	0.68
	PEOU3	0.44	0.40	0.12	0.08	0.09	0.56
	PEOU4	0.43	0.21	0.31	0.24	0.04	0.55
	PEOU5	0.44	0.47	0.02	-0.06	0.05	0.60
Perceived Usefulness (PUFN)	PUFN1	0.12	0.89	0.21	0.14	0.13	0.12
	PUFN2	0.15	0.89	0.19	0.13	0.04	0.15
	PUFN3	0.27	0.82	0.26	0.16	0.17	0.17
	PUFN4	0.20	0.88	0.21	0.06	0.11	0.18
Eigenvalue		6.07	4.14	3.41	3.35	2.72	2.45
Variance (%)		20.93	14.29	11.75	11.54	9.37	8.45
Cumulative Variance (%)		20.93	35.21	46.97	58.51	67.88	76.34

Table 6. Factor Loadings for Reflective Constructs

Discriminant validity of the reflective constructs can be assessed by two ways: a) examine factor loadings, and b) examine item correlations (Fornell and Larcker, 1981). In our study, six factors were extracted from factor analysis using principal components (Table 6). All item loadings on stipulated constructs are greater than the required 0.5 (Hair et. al., 1998) and all eigenvalues are well above one, indicating that the construct is stable and items anchor well

All the non-diagonal entries in Table 7 are smaller than the six diagonal entries of the specific constructs, indicating that measures of the constructs correlate more highly with their own items than with items measuring other constructs in the model. Thus, we conclude that discriminant validity of the scales is adequate in this study.

	STAE	CTQL	PPRP	SSEF	PEOU	PUFN

STAE	**0.64**					
CTQL	0.12	**0.73**				
PPRP	0.20	0.16	**0.78**			
SSEF	0.13	0.15	0.14	**0.56**		
PEOU	0.12	0.45	0.26	0.13	**0.67**	
PUFN	0.11	0.20	0.26	0.13	0.40	**0.90**

Table 7. AVE vs. Squares of Correlations among Constructs

5.2 Evaluation of Structural Model

Given an adequate measurement model, the hypotheses could be tested by examining the structural model. The result of structural model analysis for the proposed model is presented in Figure 2. The predictive and explanatory power of the model is assessed first based on the amount of variance in the endogenous constructs for which the model could account. Our model explained 25% of the variance in perceived personal responsibility, 55% of the variance in perceived ease of use, and 44% of the variance in perceived usefulness of the secured KMS. As the threshold for adequate explanatory power is 10% (Falk and Miller, 1992), we consider our model possesses sound predictive validity.

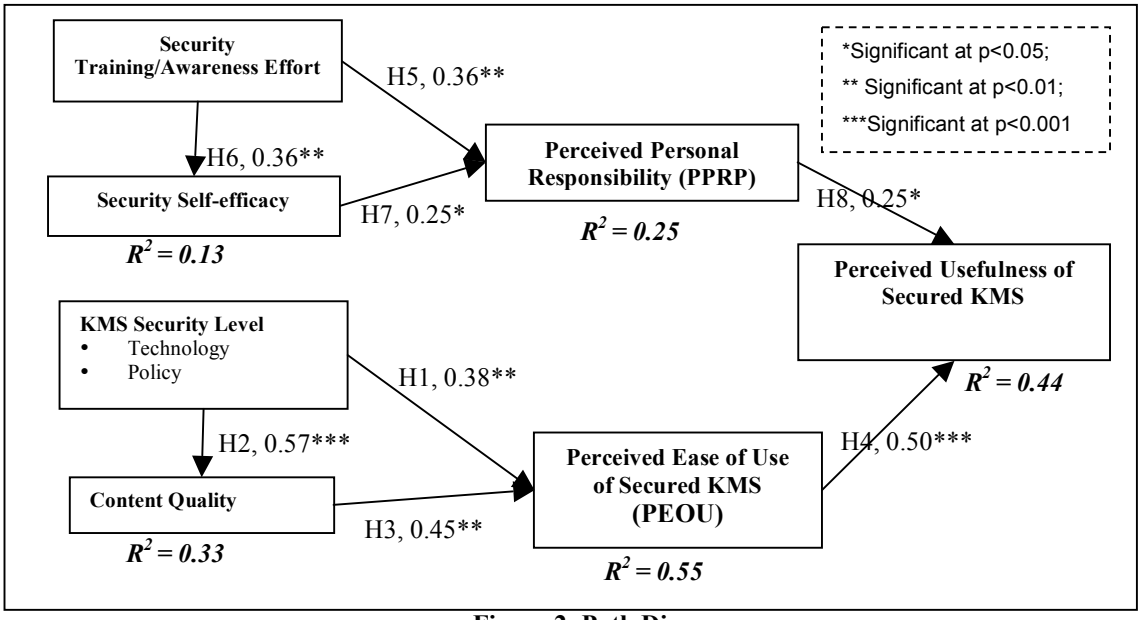

Figure 2. Path Diagram

Hypothesis	Path Coefficient	T-value	P-value	Outcome
H1: KMSL to PEOU	0.38	2.80	0.01	Not Supported
H2: KMSL to CTQL	0.57	7.04	0.001	Supported
H3: CTQL to PEOU	0.45	3.24	0.01	Supported
H4: PEOU to PUFN	0.50	3.57	0.001	Supported
H5: STAE to PPRP	0.36	2.54	0.01	Supported
H6: STAE to SSEF	0.36	2.48	0.01	Supported
H7: SSEF to PPRP	0.25	1.92	0.05	Supported
H8: PPRP to PUFN	0.25	2.09	0.05	Supported

Table 7. Hypotheses Testing Results

After computing parameter estimates for all paths in the structural model, bootstrap resampling method was employed to compute T-values for all paths (Table 7). Given that each hypothesis corresponded to a path in the structural model, support for each hypothesis could be determined based on the sign (positive or negative) and statistical significance for its corresponding path. As shown in Table 7, H2, H3, H4, H5, H6, H7, and H8 are supported at

the significance level of 0.05 while H1 is not supported (significant but in the opposite direction hypothesized).

6. Discussion and Implications

This research addresses the impact of security related factors on individual cognitive reactions to the secured KMS. Consistent with many other system acceptance studies, *perceived ease of use* has been shown to be an important determinant of the *perceived usefulness* of the secured KMS. As expected, *KMS security level* impacts *perceived ease of use* both directly and through the *content quality* produced by the KMS. This result suggests that the usefulness of the KMS can be enhanced by increasing content quality and perceived ease of use. Users of the KMS are concerned with the quality of knowledge they obtain from the system. Hence, security mechanisms (e.g. file hashing, access control and encryption) that are used to protect knowledge integrity, availability, and confidentiality will be welcomed by users.

Besides, our results also indicate that individuals with high *security self-efficacy* beliefs and good understanding of their security responsibilities (*perceived personal responsibility*) tend to have a more positive perception of the *usefulness of the secured KMS*. We also found that organizational effort in building *security training and awareness* programs is effective in developing such individual characteristics. This finding suggests that for the effective protection of KMS, merely introducing strong security measures is not enough. People feel the secure systems are useful when they fully understand the purpose of security and their own roles in securing the KMS. Organizations could provide training and awareness programs to promote an individual's understanding and awareness.

Surprisingly, the hypothesized negative impact of *KMS security level* on *perceived ease of use* of the system was not supported. Though trade-offs between security measures and system usability have been examined and evaluated in previous studies (Johansson, 2001; Nelson, 2003; Phelps & Mok, 1999), our result showed that end users of the system might perceive such trade-offs differently. Similar to several other studies (Chadwick et. al. 2002; Whitman & Mattord 2003) we found that security strength enhances perceived ease of use. In sight into this phenomenon is revealed from Chadwick et al's study (2002). Their interviews with users of the system reveal that once users had gained access to the system, no-one thought the security software was an imposition, as they did not feel its existence after they had successfully logged on. This shows that added security does not impose a further burden on users of the system, if it appears to be transparent to users. Moreover, all respondents in our study are IT professionals who have an understanding of the security mechanisms behind the system. Hence, the strength of security mechanisms did not affect their perceptions towards KMS. This finding suggests that in order to minimize the trade-offs between usability and security of the system, security mechanisms should be designed so that they are as transparent to users as possible.

7. Conclusion

In this study, we proposed a research model that attempts to explain the impact of security related factors on the user's perception of usefulness of secured KMS. The research model is tested empirically through survey questionnaires administered with current users of a secured KMS. Results indicated that security related individual characteristics, such as security self-efficacy and perceived personal responsibility, have a significant effect on the perceived usefulness of the system. Organizational effort in holding security training and awareness program could help the users of the system to build up such individual characteristics. The

study also found that high security strength imposed on the system has a positive impact on users' perceived ease of use of the system, both directly and indirectly through the improvement in the content quality of the system. The perceived ease of use of the system affected the individual perception of system usefulness.

It is important to note that these results should be interpreted in light of the study's limitations. A larger sample size can be used in future studies to improve the statistical power of the results. Moreover, respondents in this study are all IT professionals with technical expertise, so attempts to generalize the results to other contexts must be done cautiously. In moving forward, the research model could be evaluated with subjects of different IT expertise in the future.

This study has made an initial attempt to investigate how security measures imposed on the KMS affect users' perception towards the usefulness of the system. Future research could further extend our study to investigate the impact of security measures on the overall usage pattern of the secured KMS. Besides, this research focuses only on the effect of security related factors. These factors were able to account for 44% of the variance in perceived usefulness. Future research could include other possible antecedents of KMS usage such as trust and pro-sharing norms. It will be interesting to study how these factors interrelate to the factors of this study in determining users' perceptions on the secured KMS.

As more organizational knowledge resources are made available online through KMS, this increases both benefits and threats to organizations. Security measures are required to protect the knowledge assets within. However, just the presence of such mechanisms does not guarantee KMS effectiveness. By understanding the impact of these mechanisms on individual's perceptions towards KMS, organizations can learn how to make the mechanisms more effective.

References

Adams, A. and Sasse, M.A. "Users Are Not The Enemy. Why users compromise computer security mechanisms and how to take remedial measures", *Communications of the ACM*, Vol. 42, No.12, pp. 42-46, 1999.

Alavi, M. and Leidner, D.E. "Review: Knowledge management and knowledge management systems: Conceptual foundations and research issues", *MIS Quarterly,* Vol. 25, No.1, pp. 107-136, 2001.

Bandura, A. "Self-efficacy mechanism in human agency", *American Psychologist*, Vol. 37, No. 2, pp. 122-147, 1982.

Barclay, D., Higgins, C., and Thompson, R. "The Partial Least Square Approach to Causal Modeling: Personal Computer Adoption and Use as an Illustration", *Technology Studies*, Vol. 2, No. 2, pp. 398 – 422, 1995.

Bollen, K.A. "Multiple Indicators: Internal Consistency or No Necessary Relationship?" *Quality & Quantity*, Vol.18, pp. 377-385, 1984.

Chadwick, D.W., Carroll, C., Harvey, S., New, J., Young A. J. "Experiences of Using a Public Key Infrastructure to Access Patient Confidential Data over the Internet", *Proceedings of the 35th Hawaii International Conference on System Sciences*, pp. 156-166, 2002.

Churchill, G.A. "A Paradigm for Developing Better Measures of Marketing Construct", *Journal of Marketing Research*, Vol. 16, No. 1, pp. 64-73, 1979.

Compeau, D.R. and Higgins, C.A. "Computer Self-Efficacy: Development of a Measure and Initial Test", *MIS Quarterly*, Vol.19, No.2, pp. 189-211, 1995.

Davis, F.D. "Perceived Usefulness, Perceived Ease Of Use, And User Acceptance of Information Technology", *MIS Quarterly*, Vol.13, No.3, pp. 319-341, 1989.

Dhillon, G.. and Backhouse, J. "Current directions in IS security research: Towards socio-organizational perspectives", *Information Systems Journal*, 11(2), 127-153, 2001.

Falk, R.F. and Miller, N.B. *A Primer for Soft Modeling*, Akron, Ohio, Univ. of Akron Press, 1992.

Frank, J., Shamir, B. and Briggs, W. "Security-related behavior of PC users in organizations", *Information & Management*, Vol. 21, pp. 127-135, 1991.

Fornell, C. and Larcker, D.F. "Evaluating structural equation models with unobservable variables and measurement error", *Journal of Marketing Research*, Vol.18, No.1, pp. 39-50, 1981.

Gold, A.H., Malhotra, A. and Segars, A.H. "Knowledge Management: An Organizational Capabilities Perspective", *Journal of Management Information Systems*, Vol.18, No.1, pp. 185-214, 2001.

Gray, P.H. "The effects of knowledge management systems on emergent teams: towards a research model", *Journal of Strategic Information Systems,* Vol. 9, pp. 175-191, 2000.

Grant, R.M. "Towards a Knowledge-based Theory of the Firm", S*trategic Management Journal*, Vol. 17, pp. 109-122, 1996.

Hair, J.F., Anderson, R.E., Tatham, R.L., and Black W.C. *Multivariate Data Analysis*, Fifth Edition, Prentice-Hall Int. Inc, 1998.

Johansson, L. *Trade-offs between Usability and Security,* M.E. Thesis, Linköping Institute of Technology, Sweden, 2001.

Johnson, R.A. and Wichern, D.W. *Applied Multivariate Statistical Analysis*, Fourth Edition, Prentice-Hall Int. Inc., Englewood Cliffs, New Jersey, USA, 1992.

Kankanhalli, A. *Understanding Contribution and Seeking Behavior in Electronic Knowledge Repositories*. PhD. Thesis, National University of Singapore, Singapore, 2002.

Liaw, S.S. and Huang, H.M. "An investigation of user attitudes toward search engines as an information retrieval tool", *Computers in Human Behavior,* Vol. 19, pp. 751–765, 2003.

Liebeskind, J.P. "Knowledge, Strategy and the Theory of the Firm", *Strategic Management Journal*, 17, pp. 93-107, 1996.

Martins, A. and Eloff, J. "Measuring Information Security", *Proceedings of 1st Workshop on Information-Security-System Rating and Ranking*, Williamsburg, Virginia, ACSA, 2001

Mathieson, K., Peacock, E., and Chin, W.W. "Extending the Technology Acceptance Model: The Influence of Perceived User Resources", Working Paper WP 96 – 18, Faculty of Management, University of Calgary, 1996.

Morrison, E.W. & Robinson, S.L. "When employees feel betrayed: A model of how psychological contract violation develops", *Academy of Management Review*, Vol.22, No.1, pp. 226-256, 1997.

National Security Telecommunications and Information System Security. *National Training Standard for Information Systems Security Professionals,* 20 June 1994, file, Available from World Wide Web <http://www.nstiss.gov/Assets/pdf/4011.pdf>.

Nelson, R. Institutional Information on the Web: Balancing Security and Access. Presented at the Higher Education Data Sharing Consortium Conference (HEDS), 2003, retrieved Feb 2005 at: http://ir.ups.edu/IROffice/HEDS%20Paper%202003.htm

Nunnally, J.C. *Psychometric Theory*. Second Edition, McGraw-Hill Book Company, New York, 1978.

Ozag, D. and Duguma, B. "The Relationship between Cognitive Processes and Perceived Usefulness: An Extension of TAM2", Proceedings of 23rd Annual Organizational Systems Research Association Conference, Pittsburgh, Pennsylvania, 2004, retrieved Feb 2005 at: http://www.osra.org/2004/ozag.pdf

Phelps, R. and Mok, M. "Managing the Risks of Intranet Implementation: An Empirical Study of User Satisfaction", *Journal of Information Technology*, Vol.14, pp. 39-52, 1999.

Rai, A., Lang, S.S. and Welker, R.B. "Assessing the Validity of IS Success Models: An Empirical Test and Theoretical Analysis", *Information Systems Research*, Vol.13, No.1, pp. 50–69, 2002.

Staples, D.S., Hulland, J.S. and Higgins, C.A. "A Self-Efficacy Theory Explanation for the Management of Remote Workers in Virtual Organizations", *Journal of Computer-Mediated Communication*, Vol.3, No.4, 1998.

Straub, D.W. "Effective IS security: An Empirical Study", *Information Systems Research*, Vol.1, No.3, pp. 255-276, 1990.

Thuraisingham, B. "Secure Knowledge Management", Secure Knowledge Management Workshop, Buffalo, New York, Sept 2004, retrieved Feb 2005 at: http://www.cse.buffalo.edu/caeiae/skm2004/presentation_slides/invited/Keynote-D1-Bhavani-final/Keynote-D1-Bhavani.ppt

Venkatesh, V. "Determinants of Perceived Ease of Use: Integrating Control, Intrinsic motivation, and Emotion into the Technology Acceptance Model", *Information Systems Research,* Vol.11, No.4, December 2000, pp. 342-365.

Venkatesh, V. and Davis, F.D. "A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies", *Management Science*, Vol. 46, No.2, pp. 186-204, 2000.

Whitman, M.E. and Mattord H.J. *Principles of Information Security*. First Edition, Course Technology, Canada, 2003.