The Dark Side of Sharing Knowledge in the Social Media Era: Faculty Members' Perspectives

Kamla Ali Al-Busaidi[1] and Ibtisam Al-Wahaibi[2]
[1]*Infomration Systems Department, Sultan Qaboos University, Muscat, Sultanate of Oman*
[2]*Business Communications Unit, Sultan Qaboos University, Muscat, Sultanate of Oman*

Keywords: Social Media Platform, Knowledge Sharing, Knowledge Management, Information Systems Security.

Abstract: This pilot study examines the dark side of social media platforms (SMPs) for knowledge sharing (KS) from knowledge management (KM) and information systems security(ISS) perspectives. SMPs have become a mainstream technology with several potential opportunities for KS especially during the COVID 19 pandemic. However, the literature indicates a dark side to SMPs, and knowledge workers may encounter several challenges that might negatively affect their use. Hence, this study specifically assesses the negative effects of knowledge power loss, codification efforts, privacy breaches and cyberattacks on KS through SMPs. Based on 42 faculty members and structure equation modelling-based analysis, the results indicate that only knowledge power loss is the main negative influencer of knowledge workers' use of SMPs for KS. Further analysis indicated that knowledge power loss negatively affects sharing implicit not explicit knowledge. This study provides initial insights for researchers and practitioners.

1 INTRODUCTION

Human resources play a crucial role in today's digital and knowledge-based economy. Social media platforms (SMPs) are recognized as one of the information and communications technologies (ICT) that facilitate knowledge sharing and collaboration among knowledge workers particularly during the COVID-19 pandemic (Sakusic et al., 2021). In a time when digital transformation and virtual connections were essential for survival in organizations worldwide (Swart et al., 2022). Drucker (2013) emphasized that the productivity of knowledge workers is the most asset in the 21st century. Knowledge sharing systems, which fall under the category of knowledge management systems (KMS), are defined as systems that enable the seamless dissemination of individual and organizational knowledge (Davenport and Prusak, 1998). Among knowledge workers, social media platforms are widely used technologies due to their various functionalities including email, chat and discussion forums tools, content and document management, search capabilities, and virtual meetings. These platforms make it effortless for knowledge workers to share and reshare knowledge and information. SMPs as knowledge sharing systems have several potential advantages such as improved reach and richness (Al-Busaidi and Al-Wahaibi, 2022), improved connectivity and knowledge collaboration (Ghalavand et al., 2022), improved learning and creativity (Al-Busaidi et al, 2017), and improved relationships with coworkers (Yoganathan et al., 2021). However, they also have potential threats including productivity loss , power loss, privacy breaches, cybercrimes, and many others(Freni et al., 2010, Chen et al., 2021; Ghalavand et al., 2022). The success of knowledge management including knowledge sharing depends mainly on the willingness of knowledge workers to share their valuable knowledge and expertise. With these potential threats, their willingness may be uncertain.

Consequently, this pilot study aims to assess the threats of social media platforms that may influence knowledge workers' knowledge sharing practices, based on knowledge management practices and information systems security. Based on knowledge management practices, knowledge workers may be hesitant to share knowledge due to the fear of losing knowledge power and the effort required for codification (Kankanhalli et al. 2005). From the perspective of information systems security, Chen et al. (2021) indicated that users can encounter several

Al-Busaidi, K. and Al-Wahaibi, I.
The Dark Side of Sharing Knowledge in the Social Media Era: Faculty Members' Perspectives.
DOI: 10.5220/0012204700003598
In *Proceedings of the 15th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management (IC3K 2023) - Volume 3: KMIS*, pages 219-223
ISBN: 978-989-758-671-2; ISSN: 2184-3228

threats with social media platforms including privacy breaches and cyberattacks. Understanding the negative factors on sharing knowledge through SMPs is critical for analysing and understanding an organization's status in any SMPs deployment (Al-Busaidi, 2014; Phadermrod et al., 2019).

2 THE DARK SIDE OF SOCIAL MEDIA PLATFORMS

The literature on KM, ISS and SMPs has highlighted several potential threats of using social media platforms to share knowledge among knowledge workers in organizations. According to the KM literature, knowledge workers may experience a loss of knowledge power and face time loss due to codification efforts (Kankanhalli et al. 2005). Additionally, Chen et al. (2021) have pointed out that social media platforms raise several security concerns including privacy breaches and cyber-attacks.

2.1 Knowledge Power Loss

Knowledge is a powerful asset not only for organizations but also individuals. The concept of knowledge power loss refers to the perception of the knowledge workers that their unique value and power will be diminish due to the sharing of knowledge (Davenport & Prusak (1998), Kankanhalli et al. 2005). Employees, who view their knowledge as private and powerful, are likely to be unwilling to share it, as they believe doing so would result in losing their competitive advantage (Bock et al., 2005). Consequently, knowledge power loss hinders knowledge sharing (Kankanhalli et al. 2005) because individuals' fear that losing their knowledge power will make them replaceable.

Hypothesis 1 (H1): *knowledge power loss concern is negatively associated with sharing knowledge through social media platforms.*

2.2 Codification Efforts

Codification efforts refer to the amount of effort and time required for knowledge workers to organize and codify knowledge into the system (Kankanhalli et al. 2005). Common risks associated with knowledge sharing include wasting time on private conversations and un-related issues (Hysa & Spalek, 2019).
Time waste and decreased productivity are identified as major threats to the use of SMPs, as irrelevant posts and information overload negatively impact employees' time and productivity (Al-Busaidi, 2014; Nusrat et al., 2021).

Hypothesis 2 (H2): *Codification efforts/time concern is negatively associated with sharing knowledge through social media platforms.*

2.3 Privacy Breach

Privacy threats such as location privacy and absence privacy (i.e. users' presence or absence at a specific location during a given period) are common risks (Freni et al., 2010). Using SMPs for work activities poses privacy risks as it may lead to the in disclosure of confidential project data by employees (Hysa & Spalek, 2019). Ghalavand et al.(2021) indicated that physicians' use of SMPs in healthcare settings may violate patients' privacy. Additionally, Chen et al. (2021) suggested that privacy breaches can occur through various activities, such as SMPs providers sharing or selling users' data, or coworkers accidentally revealing private users' data without their knowledge. Thus,

Hypothesis 3: *Privacy breach concern is negatively associated with sharing knowledge through social media platforms.*

2.4 Cyberattack

With the emergence of the Internet and SMPs, cyber-attacks are ever-increasing (Arora et al., 2022). The widespread use of SMPs and the amount of information shared put users at risk of identity theft and hacking (Hoy and Milne, 2010, Al-Busaidi, 2014). Insufficient security controls may also result in several cyberattacks that exploit human vulnerabilities. Some common cyber-attacks using SMPs to exploit human vulnerabilities include in scams, malicious content, social weakness jacking and spam as identified by the FBI, Symantec, and TrendMicro (Chen et al., 2021). Employees consider fear of internet piracy as one of the main inhibitors of using SMPs (Al-Busaidi et al, 2017).

Hypothesis 4: *Cyberattack concern is negatively associated with sharing knowledge through social media platforms.*

3 METHODOLOGY AND RESULTS

3.1 Research Methodology

3.1.1 Data Collection and Questionnaire

The data was collected through online questionnaire using the SurveyMonkey website. An online invitation was sent to academic institutions (universities and colleges) in the Sultanate of Oman. Forty-two faculty members participated in the study. The questionnaire was developed based on the literature. The measurements for the knowledge sharing construct were adopted from Bock et al. (2005). The measurements for knowledge loss and codification effort constructs were adopted from Kankanhalli et al (2005), and the measurements for privacy breaches and cyberattacks constructs were adopted from Chen et al. (2021). A 5-point Likert scale was used to rate the measurements: 1= Strongly Disagree, 2=Disagree, 3=Neutral, 4-Agree and 5-Strongly agree.

3.1.2 Participants

This pilot study included responses from 42 academicians. Approximately 54.76% of participants were from the private sector, while 45.24% were from the public sector. Around 35.71% were Omani. Approximately 59.52% were female, while 40.48% were male. Approximately 42.86% of participants had a master's degree, while 47.62% had doctoral degree; the remaining participants did not identify their degree. Approximately 4.76% of participants were below 30 years old, 35.71% were in their 30s, 45.24% were in their 40s, and 14.29% were 50 years old and above. Participants classified their level of expertise as: 0% as novice, 14.29% as advanced beginner, 9.52% as competent, 47.62% as proficient, and 38.10% as an expert. Participants indicated their frequency of using social media platforms for sharing knowledge with co-workers as always(45.24% of participants), very often (38.10%), sometimes (16.67%), and rarely (0%).

3.2 Analysis and Results

3.2.1 Analysis Method

Smart PLS 4.0 software was used for data analysis. Construct measures were evaluated for internal consistency reliability and validity, which was measured by the average variance extracted (AVE) is representing the amount of variance a latent construct captures from its indicators. The recommended level for internal consistency reliability at least 0.70 and is at least 0.50 for AVE (Chin, 1998). Table 1 indicates that the constructs' reliability and AVE are above the recommended levels for all the constructs. Table 2 illustrates that the constructs' discriminant validity is satisfied, which is assessed by the square root of the AVE of each construct, which should exceed the correlations shared between this construct and the other (Fornell and Larcker, 1981).

Table 1: Constructs' Reliability and Validity.

Construct	Total Measures	Composite reliability	Average variance extracted (AVE)
Knowledge Power Loss (KPL)	4	0.958	0.852
Codification Efforts/Time (CET)	4	0.944	0.809
Privacy Breach(PRB)	3	0.935	0.826
Cyberattack (CYA)	4	0.981	0.927
Knowledge Sharing (KSH)	5	0.902	0.649

Table 2: Constructs' Discriminant Validity.

	KPL	CET	PRB	CYA	KSH
KPL	0.923				
CET	0.658	0.899			
PRB	0.611	0.835	0.909		
CYA	0.413	0.726	0.769	0.963	
KSH	-0.468	-0.192	-0.263	-0.090	0.806

3.2.2 Constructs' Significance Results

With PLS, R2 values are used to evaluate the predictive relevance of a structural model for the dependent latent variables, and the path coefficients are used to assess the effects of the independent variables (Chin, 1998). A 95% confidence level was used to assess the significance of all statistical tests. Table 3 shows the significance of the constructs and the results of hypotheses testing. The R2 value of the dependent construct "Knowledge Sharing" through Social Media Platforms was 0.247, indicating that the model explains 24.7% of the variance in knowledge

workers' knowledge sharing through Social Media Platforms during the COVID-19 pandemic lockdown.

The pilot study found the only significant construct on sharing knowledge through social media platforms by knowledge workers during the COVID 19 pandemic lockdown is the knowledge power loss construct (β = -0.553; p-value = 0.003); Therefore, hypothesis 1 is supported. The effects of codification efforts/time loss (β =0.344, p-value =0.245), privacy breach (β =-0.283, p-value =0.423), and cyber-attack (β = 0.114, p-value =0.662) were not significant on sharing knowledge through social media platforms by knowledge workers during the COVID 19 pandemic lockdown; hence hypotheses 2, 3 and 4 were not supported. Further analysis, which separated implicit knowledge sharing measurements from explicit knowledge measurements indicated that the negative effect of knowledge power loss is only on sharing implicit knowledge (β =-0.588, p-value =0.009), but not tacit knowledge (β =-0.305, p-value =0.330).

Table 3: Constructs Paths Significance.

Hypoth.	OS	SM	SD	TS	P-V
KPL -> KSH (H1)	-0.553	-0.472	0.255	2.165	**0.030***
CET -> KSH (H2)	0.344	0.194	0.296	1.162	0.245
PRB -> KSH(H3)	-0.283	-0.228	0.353	0.801	0.423
CYA -> KSH(H4)	0.114	0.151	0.262	0.437	0.662
*significant Hypoth.= Hypothesis; OS= Original sample; SM= Sample mean; SD= Standard Deviation; TS= T statistics; P-V= P values					

4 CONCLUSIONS

This pilot study examined the effect of various factors including knowledge power loss, codification efforts, privacy breach and cyberattack on sharing knowledge through SMPs during the COVID-19 pandemic by faculty members. The findings revealed that only knowledge power loss has a significant negative effect on sharing knowledge through SMPs. The COVID-19 pandemic may have heightened job insecurity among knowledge workers, leading to an intensified perception of knowledge power loss. As a result, employees may be inclined to conceal their knowledge to maintain a competitive advantage (Nguyen et al., 2022). These findings have implications for both practitioners and researchers. Decision makers should address this issue to foster a knowledge-sharing culture within their organizations, particularly regarding the implicit tacit knowledge, which is highly valuable (Chugh, 2012).

However, it is important to note that this study has certain limitations. The sample size was relatively small, and a larger sample size would enhance the significance of the other factors. Additionally, this study solely focused on the negative aspects that affect using SMPs for knowledge sharing. Therefore, it is essential to also consider the positive aspects. Furthermore, this study was conducted in a Middle Eastern country, and future research could compare findings across different countries and culture.

REFERENCES

Al-Busaidi, K. (2014). SWOT of social networking sites for group work in government organizations: An exploratory Delphi study from IT managers' perspective. *VINE: The journal of information and knowledge management systems*, 44(1), 121-139.

Al-Busaidi, K. A., & Al-Wahaibi, I. (2022). Sharing Knowledge in the Social Media Era: Strengths and Weaknesses for Knowledge Workers. *In 14th International Conference on Knowledge Management and Information Systems, KMIS 2022 as part of IC3K 2022-Proceedings of the 14th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management* (pp. 192-199). Science and Technology Publications, Lda.

Al-Busaidi, K. A., Ragsdell, G., & Dawson, R. (2017). Barriers and benefits of using social networking sites versus face-to-face meetings for sharing knowledge in professional societies. *Int. J. Bus. Inf. Syst*., 25(2), 145-164

Arora, H., Manglani, T., Bakshi, G., & Choudhary, S. (2022). Cyber security challenges and trends on recent technologies. In *2022 6th International Conference on Computing Methodologies and Communication* (ICCMC) (pp. 115-118). IEEE.

Bock, G. W., Zmud, R. W., Kim, Y. G., & Lee, J. N. (2005). Behavioral intention formation in knowledge sharing: Examining the roles of extrinsic motivators, social-psychological forces, and organizational climate. *MIS Quarterly*, 87-111.

Chen, R., Kim, D. J., & Rao, H. R. (2021). A study of social networking site use from a three-pronged security and privacy threat assessment perspective. *Information & Management*, 58(5), 103486.

Chin, W. (1998). The partial least square approach to structural equation modelling. In Marcoulides, G.A. (Ed.), *Modern Methods for Business Research*, Lawrence Erlbaum Associates, London, pp. 295-336.

Chugh, R. (2012). Knowledge Sharing with Enhanced Learning and Development Opportunities. In *IEEE International Conference on Information Retrieval and*

Knowledge Management 2012, Kuala Lumpur, Malaysia, March 13-15, 2012, pp. 100-104.

Davenport, T. H., & Prusak, L. (1998). *Working knowledge: How organizations manage what they know.* Harvard Business Press, Boston, Mass.

Drucker, P. F. (2013). Implementing the effective management of knowledge: Knowledge-worker productivity: The biggest challenge. *In The knowledge management yearbook 2000-2001* (pp. 267-283). Routledge.

Fornell, C. and Larcker, D. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 18(1), pp. 39-50.

Freni, D., Vicente, C., Mascetti, S., Bettini, C. and Jensen, C. (2010). Preserving location and absence privacy in geo-social networks. *In Proceedings of the 19th ACM International Conference on Information and Knowledge Management*. Toronto, Ontario, Canada, October

Ghalavand, H., Panahi, S., & Sedghi, S. (2022). How social media facilitate health knowledge sharing among physicians. *Behaviour & Information Technology,* 41(7), 1544-1553.

Hoy, M. G., & Milne, G. (2010). Gender differences in privacy-related measures for young adult Facebook users. *Journal of interactive advertising,* 10(2), 28-45.

Hysa, B., & Spalek, S. (2019). Opportunities and threats presented by social media in project management. *Heliyon,* 5(4), e01488.

Kankanhalli, A., Tan, B. C., & Wei, K. K. (2005). Contributing knowledge to electronic knowledge repositories: An empirical investigation. *MIS quarterly*, 113-143.

Nguyen, T. M., Malik, A., & Budhwar, P. (2022). Knowledge hiding in organizational crisis: The moderating role of leadership. *Journal of Business Research,* 139, 161-172.

Nusrat, A., He, Y., Luqman, A., Waheed, A., & Dhir, A. (2021). Enterprise social media and cyber-slacking: A Kahn's model perspective. *Information & Management,* 58(1), 103405.

Phadermrod, B., Crowder, R. M., & Wills, G. B. (2019). Importance-performance analysis based SWOT analysis. *International Journal of Information Management,* 44, 194-203.

Sakusic, A., Markotic, D., Dong, Y., Festic, E., Krajinovic, V., Todorovic, Z., Sustic, A., Milivojevic, N., Jandric, M., Gavrilovic, S. and Niven, A.S., 2021. Rapid, multimodal, critical care knowledge-sharing platform for COVID-19 pandemic. *Bosnian Journal of Basic Medical Sciences*, 21(1), p.93-97.

Swart, K., Bond-Barnard, T., & Chugh, R. (2022). Challenges and critical success factors of digital communication, collaboration and knowledge sharing in project management virtual teams: a review. *International Journal of Information Systems and Project Management,* 10(4), 84-103.

Yoganathan, V., Osburg, V. S., & Bartikowski, B. (2021). Building better employer brands through employee social media competence and online social capital. *Psychology & Marketing,* 38(3), 524-536.