A model for describing and maximising Security Knowledge Sharing to enhance security awareness

Saad Alahmari
Karen Renaud
Inah Omoronyia

Alahmari, S., Renaud, K. & Omoronyia, I. (2020) 'A model for describing and maximising Security Knowledge Sharing to enhance security awareness'. In M. Themistocleous & M. Papadaki (eds), I*nformation systems: 16th European, Mediterranean, and Middle Eastern Conference, EMCIS 2019, Proceedings*. Springer, Cham, pp. 376-390, 16th European, Mediterranean, and Middle Eastern Conference on Information Systems, Dubai, United Arab Emirates, 9-10 December 2019.

A Model for Describing and Maximising Security Knowledge Sharing to Enhance Security Awareness

Saad Alahmari[1], Karen Renaud[2], and Inah Omoronyia[1]

[1] School of Computing Science, University of Glasgow, Glasgow, United Kingdom
S.alahmari.1@research.gla.ac.uk,Inah.Omoronyia@glasgow.ac.uk
[2] School of Design and Informatics,Abertay University, Dundee, United Kingdom
k.renaud@abertay.ac.uk,

Abstract. Employees play a crucial role in enhancing information security in the workplace, and this requires everyone having the requisite security knowledge and know-how. To maximise knowledge levels, organisations should encourage and facilitate Security Knowledge Sharing (SKS) between employees. To maximise sharing, we need first to understand the mechanisms whereby such sharing takes place and then to encourage and engender such sharing. A study was carried out to test the applicability of *Transactive Memory Systems Theory* in describing knowledge sharing in this context, which confirmed its applicability in this domain. To encourage security knowledge sharing, the harnessing of *Self-Determination Theory* was proposed— satisfying employee autonomy, relatedness and competence needs to maximise sharing. Such sharing is required to improve and enhance employee security awareness across organisations. We propose a model to describe the *mechanisms* for such sharing as well as the means by which it can be *encouraged*.

Keywords: Security Knowledge Sharing · Security Awareness · Transactive Memory System · Self-determination Theory

1 Introduction

Employees play a crucial role in enhancing information security [1]. An essential pre-requisite is for employees to know what it is they have to do, and how to do it; in other words, that they possess the required knowledge and skills (know-how). Knowledge sharing, of all types, improves the organisation as a whole and engenders trust between employees [11]. Of particular interest in this paper is information security knowledge sharing (SKS). Knowledge sharing, which improves information security awareness, is important when it comes to preventing security breaches [14]. The knowledge held by an organisation's employees is its most important asset [51]. Moreover, information security can help employees see the importance of information SKS in enhancing security awareness [41]. While awareness drives and training are undeniably valuable and essential, a neglected way of ensuring that all employees gain the requisite knowledge and know-how is to encourage and facilitate SKS across the organisation [37].

The biggest challenge of SKS is gathering and sharing information and exploring the key factors which affect it [38]. However, many other factors need more investigation [29]. Previous studies used only a handful of different theories designed to mitigate those challenges [2]. Moreover, there have been other approaches to improving security awareness. They have generally been based on individualistic models (considering an individual in isolation) [44,45,7]

A lack of provision of an environment that facilitates and motivates the process of information exchange within organisations was also found, which is a powerful barrier to knowledge sharing. Most of the existing studies did not propose effective solutions to mitigate such barriers [2].

In order to facilitate access to this knowledge, many companies are introducing knowledge repositories. This makes it easier to store and distribute knowledge, and has also facilitated the movement of knowledge to those outside of the organisation. While companies routinely protect their information using firewalls and filtering systems, it is crucial that they do not overlook the importance of security knowledge held within the minds of their employees as well [15]. Organisations should therefore facilitate and engender organisational SKS. The aim should be to make the knowledge accessible to those who need it and ultimately to improve information security across the organisation.

To investigate this, we ask what the challenges are of Security Knowledge Sharing in terms of improving security awareness? After identifying these challenges, we will consider how information security knowledge can be facilitated. Thirdly, we explore how people can be motivated to share security knowledge. The aim is to maximise such sharing to improve and enhance organisational security awareness?

Section 2 reviews related information security and SKS research. Section 3 presents the research methodology, data collection, and data analysis we carried out to model security knowledge sharing. Section 4 proposes a model to *describe* SKS within organizations using *Transactive Memory System* (TMS) Theory. We also incorporate the satisfaction of *Self Determination Theory* (SDT) constructs in order to *encourage* SKS within organizations. Finally, Section 5.1 discusses the potential for future work. Section 6 concludes.

2 Literature Review

Knowledge and Information Security: Knowledge, which can be either tacit or explicit [12], is gained when meaning is added to information. People can gain knowledge from their environment [16] or from personal experience [16]. The former refers to skills that cannot easily be recorded or expressed, which makes it difficult to share and retain [17]. It is important for employees to transfer tacit security-related knowledge to other employees – to externalise it [18]. Explicit knowledge can be expressed in numbers and words [20] and can be recorded. In the information security context, people can indeed gain knowledge from training drives, or from recorded explicit sources, but are more likely to gain the knowledge they need from other employees in the workplace [23].

Information Security Knowledge Sharing: Many challenges deter SKS between organisations, such as the reputation of the organisation in the eyes of customers [49]. Vakilinia *et al.* [49] confirmed a strong relationship between anonymity and sharing of cyberattack information [49]. The researchers proved that the more anonymity there is, the more cyberattack information is shared. Employees are concerned about sharing personal details in the security incident record in case there are consequences that may ensue. Also, He and Johnson's study confirms the importance of sharing security incidents between employees to mitigate the risk in the workplace [23].

Kim and Kim [28] show that social pressure influences compliance intention, and that compliant behaviour is influenced by knowledge. SKS is crucial in the information security arena [28]. Safa and Von Solms [45] explored the process of information SKS in organisations and discovered that "*earning a reputation and gaining promotion" and "external motivations*" had a positive influence on SKS [45]. Mermoud *et al.* [37] report that people would share knowledge if they expected to get something valuable in return; reciprocity was deemed to be important. They suggest that organisations incentivise rather than mandate sharing [37]. Safa *et al.* [45] aimed to deliver an insight into the phenomenon of information SKS. They combined Motivation Theory and the Theory of Planned Behaviour to deliver a SKS module [45]. Dang-Pham *et al.* [12] aimed to find out why people provided information security advice to others. They discovered that the primary barriers to sharing security of knowledge were behaviour and trust [12]. Rocha Flores *et al.* [43] examined the impact of cultural factors on SKS. The results show that national and cultural factors are worth considering when it comes to the nature of sharing. They concluded that the most critical barrier to sharing security knowledge was cultural [18]. Feledi *et al.* [16] examined the efficiency of cooperation between participants during the process of SKS and found a lack of motivation to be the primary barrier to sharing [16].

Summary of the Related Work: Previous research in social network and technical systems has indicated that various reward system indicators can have a significant positive effect on SKS [19,52]. Conversely, other studies have revealed the negative impacts of reward systems [9]. Such tactics focus on short-term motivation, yet SKS ought to be seen as a long-term solution to low levels of security awareness.

Our literature review revealed that information security investigations generally use a specific limited number of theories, such as the Theory of Planned Behaviour and Theory of Reasoned Action [32]. Also, there have been other approaches to improving security awareness. They have generally been based on individualistic models (considering an individual in isolation) but our proposal is to use a collaborative model to improve security awareness [44,45,7].

Yet individual-focused models have more to do with predicting factors leading to security-related behaviours than with factors that lead to security-related knowledge sharing within organisations. We thus consider using the lens offered by TMS in order to understand and encourage SKS. TMS has been used in other contexts to model knowledge sharing between employees [50]. Moreover, researchers in information retrieval have adopted the individual experience di-

rectory of TMS to gain access to the data usage of IT-based expertise information [53]. Thus, this study considered using TMS to model the dissemination of security knowledge in organizations. Choi *et al.* argue that knowledge sharing activities have features that support specific communication and collaboration practices to facilitate team-related TMS [10]. Yet TMS only *describes* existing knowledge sharing within organizations; our interest is also in *encouraging* such sharing. We thus propose incorporating the core tenets of Self Determination Theory (SDT) into our model as well, in order to *enhance* SKS. Furthermore, Tsohou*et al.* (2015) have confirmed limited studies examining Security awareness in both levels (organisational and individual level) to have effective information security awareness programmes [48].

3 Research Methodology

3.1 Study 1 (Semi-Structured Interview):

We conducted semi-structured interviews with participants from a Saudi and a British university to elicit information regarding employees' knowledge and beliefs related to SKS [8]. By so doing we were investigating SKS-related challenges [6]. We engaged in two stages in order to extend previous research which relied purely on either surveys and/or literature reviews. Surveys, on their own, do not deliver in-depth analyses of human behaviours. Only one study was found to have used interviews or focus groups to explore SKS challenges and barriers[2]. This is surprising since observation and interviews are the most powerful techniques for delivering comprehensive insights that lead to enhanced understanding of SKS in natural environments [21,25].

Data Collection: Our study used interviews [31] in order to facilitate an in-depth look into, and exploration of, perceptions and perspectives [8]. In 2018, interviews were conducted with participants from a Saudi university and a British university. The interviews took from 15 to 20 minutes and explored how participants would respond to a security incident in the workplace. Participants were also asked some general questions about trust, privacy, experience, and the effect of the relationship in terms of sharing security advice in the security knowledge system. Participants were employees between the ages of 20 and 60 years of age. 28 people participated (7 female, 21 male). 8 had a high school certificate, 13 had a Bachelor's degree and 7 had a Masters degree.

Data Analysis: All of the audio recordings (n=28) were professionally transcribed. All transcripts were read through by the researchers while listening to the audio recordings to confirm the accuracy of the transcripts. Transcripts were de-identified and imported into NVivo 12.0 (QSR, Doncaster, Victoria). A thematic analysis approach was used to analyse the transcripts [47].

Codes were derived and categorised, with researchers using detailed and rich descriptions to represent the findings [5]. The consistency of the coding was verified by matching of the transcripts with their recording, as well as by the researchers' repeated reading and reflecting on the transcripts after coding to ensure that the definition or meaning of the codes remained the same throughout

the process. Lastly, a senior colleague unrelated to the research was asked to assess the study, looking at areas such as the relationship between the data and the research questions, the interpretation, and the level of analysis [5].

3.2 Study 2 (Quantitative Approach Survey):

The aim of this study was to examine scale reliability, correlations, and relationships between the TMS scale and other constructs in the security context in order to understand SKS in organizations.

Measurement of Constructs: A questionnaire was used to collect empirical data to support the research model and hypotheses developed from the prior literature review, as presented in Fig. 1. For each of the hypotheses, metrics were derived from the prior research and the probes were rephrased as necessary as the majority of the existing studies did not focus specifically on Security context. In order to measure the constructs of the research model, five-point Likert scales were created with options ranging from 1 (strongly disagree) to 5 (strongly agree).

Pre-test and Refinement of Measurement Items: A pilot test was carried out among a small group of computing science PhD students. The feedback received from the students was used to make improvements to the design of the instrument. Four independent researchers were then asked to carry out a final validation before the questions were distributed.

Data Collection Procedure: A link to the questionnaire was sent to a Saudi and a British university to collect information from a sample of employees. The university's information technology department was asked to send an email containing the questionnaire link and the study objectives to employees across all departments in order to obtain a diverse sample population. Participants were asked to provide basic demographic information, but not their name or email address. 204 people responded to the email request, eight of which were disregarded due to incompleteness. 196 were retained for analysis.

3.3 Findings

Results of Study 1: We now answer the research question: "***Which factors impact SKS in organizations?***" (Table 1).

Infrastructure: This refers to the software and hardware that enable to facilitate and disseminate the knowledge in the organizations. The participants agreed on the importance of the infrastructure which facilitates communication between people during the working day and after they leave the workplace such as offer an electronic knowledge repository to record information security incidents which offer a high-quality knowledge: "*there is a need for a knowledge management process and database due to the ongoing risk of losing information and knowledge as people transition from one role to another and/or leave the University*" (A21). It is important to note that we found little evidence that the Universities fostered an environment that facilitates SKS.

Table 1. Concepts and categories that emerged from the analysis

1st Order Concepts	Themes
Offer effective system to facilitate communication among those in the workplace. Offer an electronic knowledge repository to record information security incidents which offer high-quality knowledge.	Infrastructure
Experience, Qualifications and Relationships with colleagues Experience is more important than qualifications in an information security incident.	Knowledge
Sensitive documents refused to anyone working outside the IT dept. Trust based on the situation such as critical problems and need for a quick solution. Lack of experience and knowledge in the security field prevents helping others.	Trust
Security knowledge sharing, not violation of privacy. Those reporting would rather be anonymous. Recording a bad experience with an employee's skills by the incident reporting which show the employee's name in the knowledge repository. Lack of knowledge of policies, to provide a set of strategies and explain user responsibilities.	Personal Factors
Annual evaluation. Financial incentives and moral incentives. Reward system based on their contribution to recording the incident such as attending training and conferences.	Motivation
Improving decision making, Reducing information security incidents Mitigates the risk through learning from previous incidents.	IT Advantage
Gain knowledge by practice and learn lessons from previous incidents. Lessons learnt when knowledge sharing. Reduce the loss of know-how.	Employees' Advantages

Trust building: Factors involved building enough trust to request help, which focuses on the motivations, include encouraging employees to trust their colleagues enough to accept their solutions or advice which are already available in the knowledge repository. When the participants were asked about it, the majority commented that experience is one of the most important factors involved in building trust in others, and the majority of respondents revealed that experience is more important than qualifications in an information security incident : "*It is based on the relationship, and I can judge if I can trust him or not. On the other hand, the experience together with an appropriate qualification is essential in building the trust before asking anyone*" (A1).

Factors involved in building enough trust to request help include encouraging employees to trust their colleagues enough to accept their solutions or advice which are already available in the knowledge repository. When the participants were asked about it, the majority considered experience one of the most important factors involved in building trust in others, and the majority of respondents revealed this to be more important than qualifications.

Trust: The third theme is trust, which prevents employees from trusting others in the workplace, such as sensitive documents leading to the refusal of

any advice from anyone who works outside the IT department: "*I have sensitive documents which prevent me from asking anyone who works outside the IT department*" (A1). Moreover, trust based on the situation such as critical problems and need for a quick solution.

Personal Factors: What is surprising is that a lack of anonymity prevents employees from sharing their incidents. Many feel that SKS can violate privacy if they add an incident, which includes personal details, such as their names. Many employees would prefer be anonymous when reporting incidents: "*They don't have to know the personal information about me*" (A13), "*it will appear as a bad experience about me*" (A3).

Motivation: The current study found that a reward system affected the employees' likelihood of sharing knowledge. The most effective reward system is annual evaluation, encouraging employees by financial incentives and moral incentives a reward system based on their contribution to recording incidents.

The Advantage of SKS for Employees and IT Dept.: *Enhancing the IT Dept.'s response to cyber-attacks:* An important finding was that SKS – improving decision making based on recording in the knowledge repository and reducing information security incidents

Enhancing employees' information security to prevent cyber-attacks: The most interesting finding was that employees can gain knowledge by practising and learning lessons from previous incidents and security advice. This reduces the loss of knowhow and leads to increased security awareness.

4 Security Knowledge Sharing Model

To depict the factors impacting SKS, we propose the model shown in Figure 1, building on Transactive Memory System (TMS) Theory.

Transactive Memory System (TMS):

TMS has been described as "*a set of individual memory systems in combination with the communication that takes place between individuals*" (p.186), [51]. A TMS determines the specific division of cognitive labour within a group of people, as a means to facilitate encoding, storage, and retrieval of knowledge pertaining to various domains. When a TMS is being utilised, each group member is aware of "*who knows what, and who knows who knows what*" (p.260), [10]. Simply put, the characteristics of a TMS mean that three crucial qualities, common to other types of socially shared cognition, are absent; i.e. differentiated knowledge, processes of transactive encoding, storage and retrieval, and the dynamic nature of TMS functions [34]. Thus, an alternative and more suitable approach might involve a shift of focus away from repositories towards processes [27].

Liang, Moreland, and Argote (1995) described three aspects of TMS: ***Specialisation:*** this is the term used to describe the degree of differentiation of the knowledge held by team members [35]. Hence the first hypothesis is: **H1:** Specialisation (Employees knowledge) is positively related to SKS transfer within the organization.

Coordination: this describes the efficiency of the team in terms of knowledge processing while working together. The second hypothesis is: **H2:** Coordination (Infrastructure) is positively related to SKS transfer within the organization.

Credibility: this is the way in which individual team members perceive the reliability of the knowledge held by the other members of the team. The third hypothesis is: **H3:** Credibility (Trust) of shared knowledge is positively related to SKS transfer within the organization. These three dimensions are considered variables that can be used to measure the degree to which a TMS has developed among the members of a group, and they have frequently been used for this purpose in empirical studies [30,35].

As Lewis [33,50] (Lewis, 2003, p. 590) asserts, these three variables "*reflect transactive memory itself [33], as well as the cooperative processes illustrative of transactive memory use*" as shown in Figure 1.

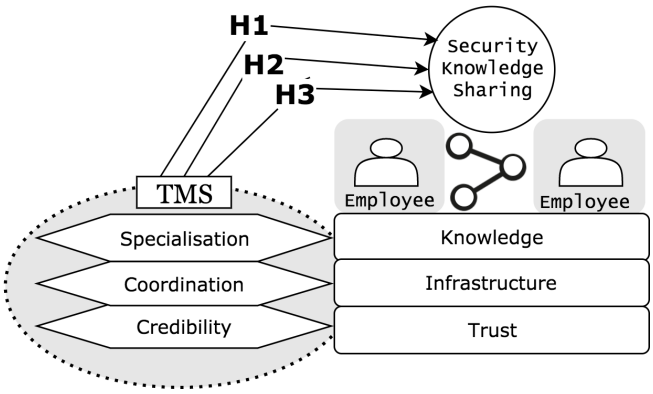

Fig. 1. Using Transactive Memory System (TMS) to Model Organizational Security Knowledge Sharing (SKS)

Davison *et al.* [13] argue that TMS facilitates knowledge sharing, leading to improved team creative performance via team creative efficacy [13]. Our premise is that organisations should facilitate and engender SKS by removing the challenges which prevent SKS i.e. "Specialization, Credibility and Coordination" [30]. The aim is to make security knowledge accessible to all of those who need it and ultimately to improve security awareness across the organisation. Our first qualitative study delivered insights about which factors impact SKS, and we are able to align these factors to the core tenets of TMS theory.

Results of Study 2: The research model and hypotheses were tested using a component-based partial least squares (PLS) regression approach to structural equation modelling (SEM). This kind of approach is the most appropriate for the current study as it has a focus on theory development and the prediction of data [29]. SmartPLS (v.3.0) was used to test the model as it is a powerful,

user-friendly instrument for graphical path modelling with latent variables. Our results of a real TMS Model strong support to two hypotheses which are Coordination (t=3.840, $p < 0.001$), and Specialisation (t=2.241, $p < 0.001$).

Table 2. Path Coefficient of the Research Hypotheses

Hypo	Relationship	Std. Beta	Std. Error	T-value	P-value	Decision
H1	SPE → SKS	0.189	0.075	2.521	0.012	Supported
H2	COO → SKS	0.359	0.090	4.001	0.000	Supported
H3	CRE → SKS	0.132	0.091	1.448	0.148	Unsupported

Path Coefficient of the Research Hypotheses was used to determine whether SPE, COO and CRE variables predict the participants' intentions to SKS transfer within the organization. Dependent variable: Facilities SKS; Independent variables: SPE, COO and CRE as shown in (Table 2.) Other results are omitted due to space limitations. H1 and H2 are supported, but H3 is unsupported. We will, however, retain all three tenets of TMS in our model, due to the smallness of our sample, and the fact that we are not at liberty to pick apart TMS. Having modeled SKS within organizations, we now turn to considering how to facilitate and encourage SKS.

4.1 Encouraging & Facilitating SKS:

We now proceed to the second question: ***"How can security knowledge sharing be facilitated and encouraged?"***

SDT requires the satisfaction of three core human needs. (1) The need for **autonomy**, which refers to an individual's desire for self-organisation of their actions. (2) The need for a sense of **competence**, i.e. an individual's sense of self-efficacy. (3) The need for **relatedness**, which refers to the desire to feel a connection with, and be supported by, people who are important to them [42]. Research has suggested that people are more likely to persist and have better qualitative performance on activities that satisfy these needs [42].

According to recently published policy compliance research, satisfying SDT has been successful in encouraging such compliance in organisations [4]. Moreover, Alkaldi *et al.* confirmed the critical effect of applying SDT to security tool adoption decisions in the security context [3]. That being so, we can *encourage* SKS by satisfying the self-determination needs of employees to enhance the TMS of the organization.

In terms of facilitation, Wang *et al.* [50] suggest that IT systems be used to enhance TMS.

4.2 Modeling SKS Description, Facilitation and Encouragement Model

We propose a model that *describes* SKS based on TMS constructs, *encouraging* SKS by using SDT constructs (Figure 2). TMS relies considerably on information technology for support. The model complements prior SKS models including Gagne's [19] model of organisational knowledge use. The differences between the models, however, are in the conceptualisation of facilitation by TMS, which is multidimensional in the SKS model and also in the inclusion of psychological factors that can impact on the quality of motivation by SDT. Our model gives a detailed explanation of how and why certain HRM practices impact on engagement with SKS behaviour, thus providing solid advice for employees [19].

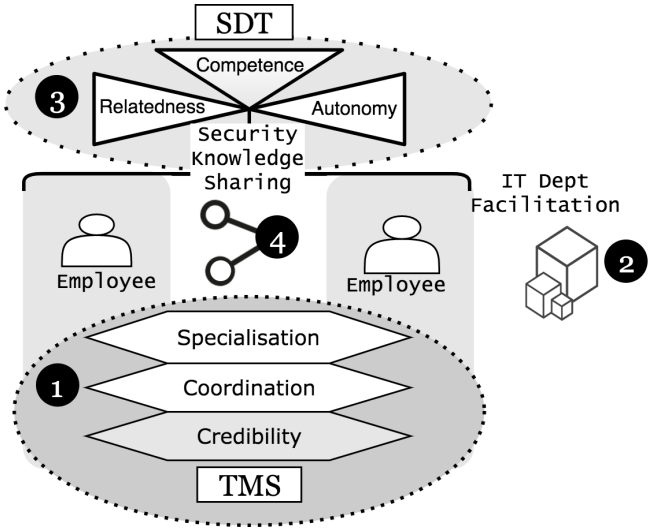

Fig. 2. A Model for Describing (1), Facilitating (2) and Encouraging (3) Security Knowledge Sharing, thereby Enhancing Sharing (4)

There is a crucial need to investigate whether information technology has an influence on the development of TMS within a team, and if so, how this happens [10].

A number of existing studies identify communication as a key determinant of TMS development. Communication is crucial for understanding the knowledge held by others, for the encoding of new knowledge into the TMS of the group, and for the retrieval of information from the TMS [24]. With this in mind, it becomes clear that the processes of communication are crucial in developing and utilising a group TMS [24,33]. It has also been posited that the frequency of interaction between team members – that is, the quantity of communication – that is important in the development of a TMS; indeed, the usefulness of the

shared information in terms of its quality is also an influencing factor [36,30]. Moreover, the TMS's function is most effectual when there is a reliance between team members on each other to work towards achieving a shared goal [54,50].

5 General Discussion

Discussion of Study 1 Study 1 showed that the biggest challenges to SKS are (1) facilitating infrastructures, (2) trust, (3) knowledge, and increasing motivation. Our results confirmed that SKS could enhance security awareness, leading to many benefits for both employees and IT department (confirming [18,39]).

Previous research has indicated the positive effects of trust, which increases interaction among employees in terms of SKS [19,52]. Prior studies that have noted the importance of trust as an influential factor in the security field as barriers can prevent the sharing of security knowledge advice [2,46].

The current study is one of the first to investigate SKS in nonprofit organisations. We showed that SKS mitigates risk [40] through learning from previous incidents and security advice [23]. It reduces the loss of knowhow [18], The outcome of the study reveal that SKS can have a positive impact on employees' willingness to comply with information security guidelines [45].

Our literature review revealed that SKS investigations use only a handful of different theories, such as the Theory of Planned Behaviour [2]. We model SKS using TMS [50,30] (the first time this will have been used in the cyber security context). We augment this descriptive model by incorporating the tenets of SDT in order to address individual sharing motivations, and IT facilitation to address organizational factors.

We wanted to confirm the importance of SKS and show how its influence on employees in the workplace leads to enhanced Security awareness [2]. Our study highlighted the advantages of SKS in an organisational setting, especially in terms of individual security awareness [2]. Hawryszkiewycz and Binsawad [22] describe the impact of barriers deterring SKS. Our study indicated that trust [14,2,22], affording anonymity [49], facilitating infrastructure [26] and engendering motivation [19,52] are factors affecting SKS. In particular, we found a lack of provision of an environment that specifically facilitates SKS. Such an environment could improve incident reporting and inspire employees to participate more fully in recording incidents and sharing their advice.

Discussion of Study 2 the path coefficient of the research hypotheses was utilised to establish whether SPE, COO, and CRE positively affect the transfer of SKS within an organisation. In terms of employees' intention to share knowledge with others, SPE and COO were the strongest predictors here. On the other hand, CRE was not supported as employees need to know who they can trust to take information from and pass knowledge on to. Trust was found to be one of the biggest challenges in the context of security knowledge sharing, mainly due to information security and sensitive issues among employees in the organisation. These challenges can be mitigated through coordination of the TMS, as this can play a key role in increasing credibility among employees

and achieving classification of the specialisation. Moreover, Wang *et al.* . suggest that technical system feed into the creation of TMSs. For instance, with the help of IT-empowered collaboration platforms, colleagues may assemble a knowledge index and mutual trust in expertise to maximise effectiveness. Moreover, the researchers referred to the benefits of collective knowledge based on TMS as a useful knowledge network for employees in organisations [50]. We will investigate the impact of SKS model adoption as an effective system for implementation as future work.

5.1 Future Work

Having confirmed the relationship between challenges in TMS and SKS, we plan to implement a SKS facilitating App, which satisfies SDT needs and mitigates SKS challenges. **Firstly,** an electronic knowledge repository of security knowledge and solutions.

Secondly, the app encourages SKS, by motivating employees to share knowledge using the App, with SDT enhancing features.

We will deploy the App in an organization and then determine whether SKS is enhanced, and security awareness accordingly improved, over a period of time.

6 Conclusion

We conducted two studies to confirm factors impacting SKS in organisations; thereby, making key contributions to the study regarding the use of SKS to improve security awareness among employees. We proposed a model that describes, facilitates and encourages security knowledge sharing in organisations; we also relied on TMS Theory (which is a new finding in the security context) and Self Determination Theory. The study investigated significant challenges associated with SKS, required to improve security awareness in organisations. Our aim was to uncover ways to maximise knowledge sharing, both by facilitating and encouraging it. As future work, we plan to build a facilitating App, and to test it in an organisation, to ascertain whether it accentuates knowledge sharing and, as as consequence, improves organisational security awareness.

References

1. Ahmed, G., Ragsdell, G., Olphert, W.: Knowledge sharing and information security: a paradox? In: 15th European Conference on Knowledge Management (ECKM 2014). pp. 1083 – 1090. Polytechnic Institute of Santarém Portugal (4-5 September 2014)
2. Al Ahmari, S., Renaud, K., Omoronyia, I.: A systematic review of information security knowledge-sharing research. In: Proceedings of the Twelfth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2018). p. 101 (2018)
3. Alkaldi, N., Renaud, K.: Encouraging password manager adoption by meeting adopter self-determination needs. In: Proceedings of the 52nd Hawai'i International Conference on System Sciences. January. Maui (2019)

4. Alzahrani, A., Johnson, C., Altamimi, S.: Information security policy compliance: Investigating the role of intrinsic motivation towards policy compliance in the organisation. In: 2018 4th International Conference on Information Management (ICIM). pp. 125–132. IEEE (2018)
5. Braun, V., Clarke, V.: Using thematic analysis in psychology. Qualitative Research in Psychology **3**(2), 77–101 (2006)
6. Bryman, A.: Quantitative and qualitative research: further reflections on their integration. In: Mixing methods: Qualitative and quantitative research, pp. 57–78. Routledge (2017)
7. Bulgurcu, B., Cavusoglu, H., Benbasat, I.: Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quarterly **34**(3), 523–548 (2010)
8. Burnard, P.: A method of analysing interview transcripts in qualitative research. Nurse Education Today **11**(6), 461–466 (1991)
9. Cabrera, E.F., Cabrera, A.: Fostering knowledge sharing through people management practices. The International Journal of Human Resource Management **16**(5), 720–735 (2005)
10. Choi, S.Y., Lee, H., Yoo, Y.: The impact of information technology and transactive memory systems on knowledge sharing, application, and team performance: a field study. MIS Quarterly pp. 855–870 (2010)
11. Dang, D., Nkhoma, M.: Effects of team collaboration on sharing information security advice: insights from network analysis. Information Resources Management Journal (IRMJ) **30**(3), 1–15 (2017)
12. Dang-Pham, D., Pittayachawan, S., Bruno, V.: Why employees share information security advice? exploring the contributing factors and structural patterns of security advice sharing in the workplace. Computers in Human Behavior **67**, 196–206 (2017)
13. Davison, R.M., Ou, C.X., Martinsons, M.G.: Information technology to support informal knowledge sharing. Information Systems Journal **23**(1), 89–109 (2013)
14. Dixon, N.M.: Common knowledge: How companies thrive by sharing what they know. Harvard Business School Press (2000)
15. Durcikova, A., Jennex, M.E.: Introduction to Confidentiality, Integrity, and Availability of Knowledge, Innovation, and Entrepreneurial Systems Minitrack. In: 49th Hawai'i International Conference on System Sciences (HICSS). pp. 39:1–39:18. IEEE (2016)
16. Feledi, D., Fenz, S., Lechner, L.: Toward web-based information security knowledge sharing. Information Security Technical Report **17**(4), 199–209 (2013)
17. Fenz, S., Ekelhart, A.: Formalizing information security knowledge. In: Proceedings of the 4th international Symposium on information, Computer, and Communications Security. pp. 183–194. ACM (2009)
18. Flores, W.R., Antonsen, E., Ekstedt, M.: Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. Computers & Security **43**, 90–110 (2014)
19. Gagné, M.: A model of knowledge-sharing motivation. Human Resource Management: Published in Cooperation with the School of Business Administration, The University of Michigan and in alliance with the Society of Human Resources Management **48**(4), 571–589 (2009)
20. Gal-Or, E., Ghose, A.: The economic incentives for sharing security information. Information Systems Research **16**(2), 186–208 (2005)

21. Gill, P., Stewart, K., Treasure, E., Chadwick, B.: Methods of data collection in qualitative research: interviews and focus groups. British Dental Journal **204**(6), 291–295 (2008)
22. Hawryszkiewycz, I., Binsawad, M.H.: Classifying knowledge-sharing barriers by organisational structure in order to find ways to remove these barriers. In: 2016 Eighth International Conference on Knowledge and Systems Engineering (KSE). pp. 73–78. IEEE (2016)
23. He, Y., Johnson, C.: Challenges of information security incident learning: An industrial case study in a chinese healthcare organization. Informatics for Health and Social Care **42**(4), 393–408 (2017)
24. Hollingshead, A.B., Brandon, D.P.: Potential benefits of communication in transactive memory systems. Human Communication Research **29**(4), 607–615 (2003)
25. InterViews, K.S.: An introduction to qualitative research interviewing (1996)
26. Islam, M.Z., Jasimuddin, S.M., Hasan, I.: Organizational culture, structure, technology infrastructure and knowledge sharing: Empirical evidence from MNCs based in Malaysia. Vine **45**(1), 67–88 (2015)
27. Jackson, P., Klobas, J.: The organization as a transactive memory system. In: Becoming Virtual, pp. 111–133. Springer (2008)
28. Kim, S.S., Kim, Y.J.: The effect of compliance knowledge and compliance support systems on information security compliance behavior. Journal of Knowledge Management **21**(4), 986–1010 (2017)
29. Kim, S., Lee, H.: The impact of organizational context and information technology on employee knowledge-sharing capabilities. Public Administration Review **66**(3), 370–385 (2006)
30. Kotlarsky, J., van den Hooff, B., Houtman, L.: Are we on the same page? knowledge boundaries and transactive memory system development in cross-functional teams. Communication Research **42**(3), 319–344 (2015)
31. Kvale, S.: Interviews: An introduction to qualitative research interviewing. Sage Publications, Inc (1994)
32. Lebek, B., Uffen, J., Neumann, M., Hohler, B., H. Breitner, M.: Information security awareness and behavior: a theory-based literature review. Management Research Review **37**(12), 1049–1092 (2014)
33. Lewis, K.: Measuring transactive memory systems in the field: scale development and validation. Journal of Applied Psychology **88**(4), 587–604 (2003)
34. Lewis, K., Herndon, B.: Transactive memory systems: Current issues and future research directions. Organization Science **22**(5), 1254–1265 (2011)
35. Liang, D.W., Moreland, R., Argote, L.: Group versus individual training and group performance: The mediating role of transactive memory. Personality and Social Psychology Bulletin **21**(4), 384–393 (1995)
36. Liao, J., Jimmieson, N.L., O'Brien, A.T., Restubog, S.L.: Developing transactive memory systems: Theoretical contributions from a social identity perspective. Group & Organization Management **37**(2), 204–240 (2012)
37. Mermoud, A., Keupp, M., Huguenin, K., Palmié, M., David, D.P.: Incentives for human agents to share security information: a model and an empirical test. In: 17th Workshop on the Economics of Information Security (WEIS). pp. 1–22 (2018)
38. Ortiz, J., Chang, S.H., Chih, W.H., Wang, C.H.: The contradiction between self-protection and self-presentation on knowledge sharing behavior. Computers in Human Behavior **76**, 406–416 (2017)
39. Parsons, K., McCormac, A., Butavicius, M., Ferguson, L.: Human factors and information security: individual, culture and security environment. Tech. rep., Defence

Science and Technology Organization Edinburgh (Australia) Command (2010), https://apps.dtic.mil/docs/citations/ADA535944 Accessed 12 November 2019
40. Persadha, P.D., Waskita, A., Fadhila, M., Kamal, A., Yazid, S.: How inter-organizational knowledge sharing drives national cyber security awareness?: A case study in indonesia. In: 2016 18th International Conference on Advanced Communication Technology (ICACT). pp. 550–555. IEEE (2016)
41. Rahim, N.H.A., Hamid, S., Mat Kiah, M.L., Shamshirband, S., Furnell, S.: A systematic review of approaches to assessing cybersecurity awareness. Kybernetes **44**(4), 606–622 (2015)
42. Roca, J.C., Gagné, M.: Understanding e-learning continuance intention in the workplace: A self-determination theory perspective. Computers in Human Behavior **24**(4), 1585–1604 (2008)
43. Rocha Flores, W., Holm, H., Svensson, G., Ericsson, G.: Using phishing experiments and scenario-based surveys to understand security behaviours in practice. Information Management & Computer Security **22**(4), 393–406 (2014)
44. Safa, N.S., Maple, C., Watson, T., Von Solms, R.: Motivation and opportunity based model to reduce information security insider threats in organisations. Journal of Information Security and Applications **40**, 247–257 (2018)
45. Safa, N.S., Von Solms, R.: An information security knowledge sharing model in organizations. Computers in Human Behavior **57**, 442–451 (2016)
46. Tamjidyamcholo, A., Baba, M.S.B., Tamjid, H., Gholipour, R.: Information security–professional perceptions of knowledge-sharing intention under self-efficacy, trust, reciprocity, and shared-language. Computers & Education **68**, 223–232 (2013)
47. Thomas, J., Harden, A.: Methods for the thematic synthesis of qualitative research in systematic reviews. BMC Medical Research Methodology **8**(1), 45 (2008)
48. Tsohou, A., Karyda, M., Kokolakis, S., Kiountouzis, E.: Managing the introduction of information security awareness programmes in organisations. European Journal of Information Systems **24**(1), 38–58 (2015)
49. Vakilinia, I., Tosh, D.K., Sengupta, S.: Privacy-preserving cybersecurity information exchange mechanism. In: 2017 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS). pp. 1–7. IEEE (2017)
50. Wang, Y., Huang, Q., Davison, R.M., Yang, F.: Effect of transactive memory systems on team performance mediated by knowledge transfer. International Journal of Information Management **41**, 65–79 (2018)
51. Wegner, D.M.: Transactive memory: A contemporary analysis of the group mind. In: Theories of group behavior, pp. 185–208. Springer (1987)
52. Wickramasinghe, V., Widyaratne, R.: Effects of interpersonal trust, team leader support, rewards, and knowledge sharing mechanisms on knowledge sharing in project teams. Vine **42**(2), 214–236 (2012)
53. Yuan, Y.C., Fulk, J., Monge, P.R.: Access to information in connective and communal transactive memory systems. Communication Research **34**(2), 131–155 (2007)
54. Zhang, Z.X., Hempel, P.S., Han, Y.L., Tjosvold, D.: Transactive memory system links work team characteristics and performance. Journal of Applied Psychology **92**(6), 1722 (2007)