Implement a Model for Describing and Maximising Security Knowledge Sharing

Saad Alahmari
School of Computing Science
University of Glasgow
Glasgow, United Kingdom
s.alahmari.1@research.gla.ac.uk

Karen Renaud
Computer and Information Sciences
University of Strathclyde
Glasgow, United Kingdom
karen.renaud@strath.ac.uk

Inah Omoronyia
School of Computing Science
University of Glasgow
Glasgow, United Kingdom
inah.omoronyia@glasgow.ac.uk

***Abstract*—Employees play a crucial role in improving information security in their enterprise, and this requires everyone having the requisite security knowledge. To maximise knowledge, organisations should facilitate and encourage *Security Knowledge Sharing* (SKS) between employees. This paper reports on the design and implementation of a mobile game to enhance the delivery of information security training to help employees to protect themselves against security attacks. The collaborative *Transactive Memory System* (TMS) theory was used to model organisational knowledge sharing. We then satisfy the self-determination needs of employees to maximise intrinsic motivation to share knowledge at the individual level, via an Educational Security Game. An empirical study evaluated the intervention, an application that facilitates and encourages Information Security Knowledge Sharing. The results are still in progress.**

***Index Terms*—Self-Determination Theory, Transactive Memory System, Information Security Awareness, Knowledge Sharing, Security Awareness Training**

I. Introduction

Collaborative interventions in information security should encourage employees to interact with each other to share their security knowledge — thus ensuring that all employees have access to security advice [1], [2].

The study will test the validity of the *Transactive Memory Systems* (TMS) theory to model *Security Knowledge Sharing* (SKS) within organizations. A *Security Knowledge Sharing System* (STOW) application models TMS to reflect organisational factors and incorporates the satisfaction of SDT needs [3] on the individual level to maximise SKS within organisations.

The research question is: "*Can security knowledge sharing be modeled using TMS and sharing encouraged by satisfying the self-determination needs of employees*? After implementing the application, we will empirically evaluate it to answer this question, as shown in Figure 1.

II. Related Work

Information Security Awareness (ISA) can be described as "*a state where users in an organization are aware of ideally committed to their security mission*" (p. 31) [4]. Several studies have contended that employees' ISA is among the most significant element for achieving the objectives of information security in organizations [4]–[6]. It is therefore crucial to enhance employees' awareness of security practices in order to mitigate risk in organizations [4], [7], [8].

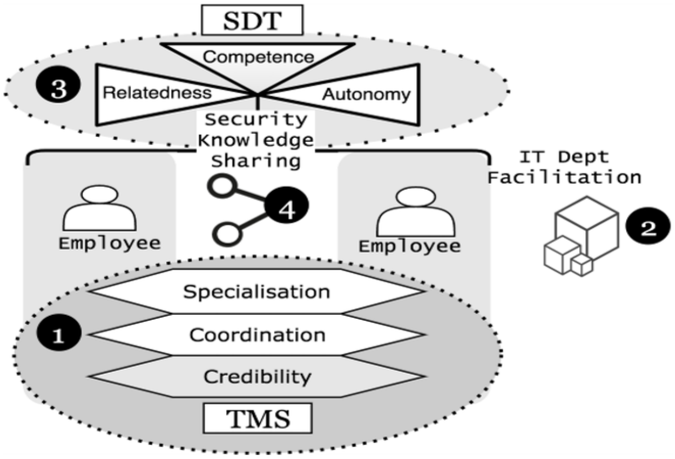


Fig. 1. A Model for Describing (1), Facilitating (2) and Encouraging (3) Security Knowledge Sharing, thereby Enhancing Sharing (4). SDT=Self-Determination Theory; TMS: Transactive Memory System

People can gain security knowledge from training programmes [5], [9], [10], from personal experience [11] or from other employees in the workplace [12]. However, approaches of this type carry with them a variety of well-known limitations, such as the difficulty in determining the effectiveness of such training [13].

One mechanism for improving ISA is for employees to transfer security-related knowledge to other employees [14].

Employees collaborate in many ways to facilitate knowledge sharing [15], [16]. Safa *et al.* [15] identified information security collaboration as a powerful and efficient approach to reducing the risks associated with managing information security. Moreover, the researchers confirmed that limited studies have been conducted collaboratively in the information security field as it pertains to organisations. Tsohou *et al.* [17] observed that several studies have explored the organisational and individual aspects to enhance Information Security Awareness.

This is a peer-reviewed, accepted author manuscript of the following article: Alahmari, S., Renaud, K., & Omoronyia, I. (2021). Implement a model for describing and maximising security knowledge sharing. In 2020 15th International Conference for Internet Technology and Secured Transactions (ICITST) (pp. 177-180). IEEE. https://doi.org/10.23919/ICITST51030.2020.9351318

A. Educational Games

Educational games have become recognized as a powerful teaching tool with the potential to result in an “instructional revolution” [18]. The principal reason for this is that game-based education permits employees to learn through experience and the utilization of a virtual environment while motivating them to think critically and problem-solve [18], [19]. Moreover, Security Games (SG) are leading employees to enjoy and collaborate, as the games comprise a form of intrinsic motivation. According to Dixon *et al.*, SG have led employees to engage with and enjoy learning, as they anticipate a smooth, agreeable and straightforward experience [20].

B. Transactive Memory System and Self-Determination

1) Transactive Memory System (TMS) Theory: TMS has been described as “*a set of individual memory systems in combination with the communication that takes place between individuals*” (p.186), [21]. Liang, Moreland, and Argote (1995) described three aspects of TMS:

(1) Specialisation: this is the term used to describe the degree of differentiation of the knowledge held by team members [22].

(2) Coordination: this describes the efficiency of the team in terms of knowledge processing while working together.

(3) Credibility: this is the way in which individual team members perceive the reliability of the knowledge held by the other members of the team.

2) Self-Determination Theory (SDT): According to De Charms [23] and Deci and Ryan [3], intrinsic motivation works by motivating an individual through their own natural interest in activities that are new or challenging. With intrinsic motivation, there is no need for the individual to be rewarded for their behaviour [3], [23]. In SDT, three key human needs must be met:

- The need for **autonomy** , which is a person’s wish to self-organise their own actions;
- The need for a sense of **competence**, which is when a person desires self-efficacy; and
- The need for **relatedness**, i.e. a person’s wish for the support and feelings of connection with others around them [24].

Studies have shown that when these three core needs are satisfied, individuals are more likely to take part in and exhibit better performance [1], [24] .

We propose a model that *describes* SKS based on TMS constructs, *encouraging* SKS by using SDT constructs (Figure 1). TMS relies considerably on information technology for support. The model complements prior SKS models, including Gagne’s [25] 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 regarding interaction systems among employees.

III. Methodology and research design

The aim of this study is to implement and empirically evaluate an application that facilitates Information Security Knowledge Sharing based on the SKS model, which was published in our previous work and is shown in Figure 1 [1]. The empirical evaluation is depicted in Figure 2.

A. Data Collection Procedure

Group A — *Intervention Group*: Employees will be given a pre-questionnaire (Information Security Assessment). They will then be given Game in App which will include some knowledge about how the users can improve their awareness (two weeks). We will give them a post-questionnaire (Information Security Assessment).

Group B — *Control Group*: This group will be given a pre- and post-questionnaire (Information Security Assessment) with no intervention to maximise SKS.

B. Awareness Level Measurement

The following awareness scale has been adapted from Kruger and Kearney which was used to explain the level of awareness [26] as shown in Table I.

TABLE I
Awareness Level Measurement

Awareness	Measurement	Actions
Good	80–100	Satisfactory: badges as an expert user and can be group leader
Average	60–79	Minor– action potentially required
Poor	59 and less	UnSatisfactory: need improve

C. The STOW game overview and rules

The Security Knowledge Sharing System (STOW) is a security game presented as a mobile app (e-learning scenarios to encourage reflection and discovery among employees) which includes multiple choice questions via a virtual connection. The scenarios will be based on the Global Information Security Policy and common human errors. STOW is supposed to be played by employees as a group under the guidance of the IT department who will control the game, as shown in Figure 3

D. Design Elements for Game

Appropriate competition dynamics will help persuade employees to become more engaged in their assignments as shown in (Table II.):

IV. Conclusion

A great deal of effort has gone into designing and rolling out security awareness training. These efforts are essential, but perhaps not sufficient. If we focus primarily on the individual, we neglect one powerful mechanism for improving security knowledge and competence. Here we describe the STOW application, which uses TMS to model sharing within the

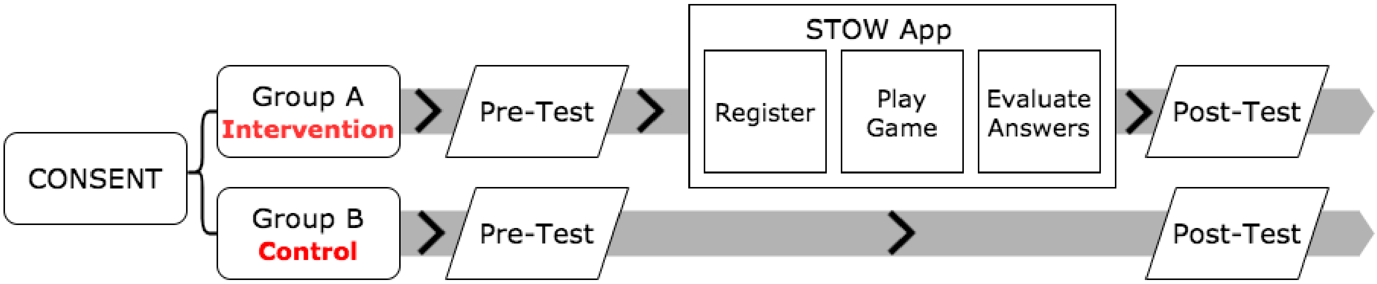
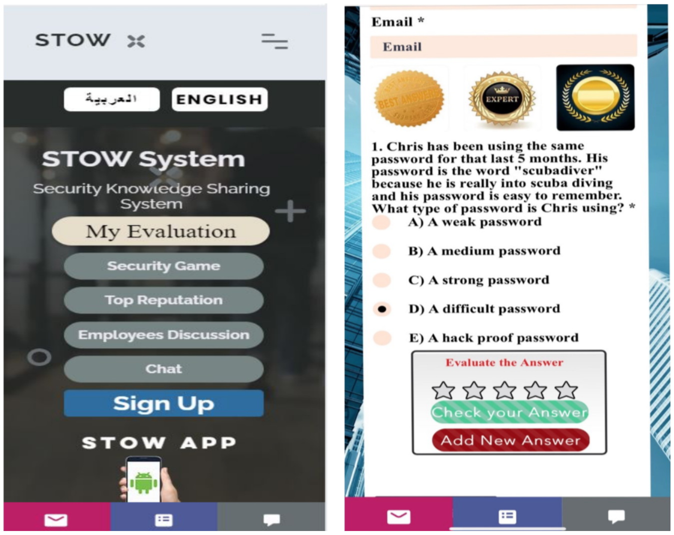


Fig. 2. Assessment and Game Flow.



Email *

Email

1. Chris has been using the same password for that last 5 months. His password is the word "scubadiver" because he is really into scuba diving and his password is easy to remember. What type of password is Chris using? *

○ A) A weak password

○ B) A medium password

○ C) A strong password

● D) A difficult password

○ E) A hack proof password

Fig. 3. STOW Application.

TABLE II
STOW DESIGN ELEMENTS

Game Dynamics	Game Elements	Description
Challenge scenarios	Points and badges	*Competence* is an important component among the intrinsic motivation and plays a key role in Credibility via Evaluation
Leader board	Badges	*Relatedness:* Employees can trust co-workers based on Leader board
Best answer	Reuse and Retrieve	*Competence:* Choosing the best answer based on the employees' personal opinion

organisation, and uses SDT to encourage individual security knowledge sharing. Analysis of results is still ongoing.

REFERENCES

[1] S. Alahmari, K. Renaud, and I. Omoronyia, "A model for describing and maximising security knowledge sharing to enhance security awareness," in *European, Mediterranean, and Middle Eastern Conference on Information Systems*. Springer, 2019, pp. 376–390.

[2] S. Al Ahmari, K. Renaud, and I. Omoronyia, "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)*, 2018, p. 101.

[3] E. L. Deci and R. M. Ryan, "Intrinsic motivation." Wiley Online Library, 2010, pp. 1–2.

[4] M. T. Siponen, "A conceptual foundation for organizational information security awareness," *Information Management & Computer Security*, 2000.

[5] S. Bauer and E. W. Bernroider, "From information security awareness to reasoned compliant action: analyzing information security policy compliance in a large banking organization," *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, vol. 48, no. 3, pp. 44–68, 2017.

[6] J. D'Arcy, A. Hovav, and D. Galletta, "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach," *Information Systems Research*, vol. 20, no. 1, pp. 79–98, 2009.

[7] A. Vance and M. T. Siponen, "Is security policy violations: A rational choice perspective," *Journal of Organizational and End User Computing (JOEUC)*, vol. 24, no. 1, pp. 21–41, 2012.

[8] M. Bada, A. M. Sasse, and J. R. Nurse, "Cyber security awareness campaigns: Why do they fail to change behaviour?" *arXiv preprint arXiv:1901.02672*, 2019.

[9] J. Killmeyer, *Information security architecture: an integrated approach to security in the organization*. CRC Press, 2006.

[10] M. E. Thomson and R. von Solms, "Information security awareness: educating your users effectively," *Information management & computer security*, 1998.

[11] D. Feledi, S. Fenz, and L. Lechner, "Toward web-based information security knowledge sharing," *Information Security Technical Report*, vol. 17, no. 4, pp. 199–209, 2013.

[12] Y. He and C. Johnson, "Challenges of information security incident learning: An industrial case study in a chinese healthcare organization," *Informatics for Health and Social Care*, vol. 42, no. 4, pp. 393–408, 2017.

[13] P. Puhakainen and M. Siponen, "Improving employees' compliance through information systems security training: an action research study," *MIS Quarterly*, pp. 757–778, 2010.

[14] W. R. Flores, E. Antonsen, and M. Ekstedt, "Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture," *Computers & Security*, vol. 43, pp. 90–110, 2014.

[15] N. S. Safa, C. Maple, T. Watson, and S. Furnell, "Information security collaboration formation in organisations," *IET Information Security*, vol. 12, no. 3, pp. 238–245, 2017.

[16] Y.-H. Chen, T.-P. Lin, and D. C. Yen, "How to facilitate inter-organizational knowledge sharing: The impact of trust," *Information & Management*, vol. 51, no. 5, pp. 568–578, 2014.

[17] A. Tsohou, M. Karyda, S. Kokolakis, and E. Kiountouzis, "Managing the introduction of information security awareness programmes in organisations," *European Journal of Information Systems*, vol. 24, no. 1, pp. 38–58, 2015.

[18] B. D. Cone, C. E. Irvine, M. F. Thompson, and T. D. Nguyen, "A video game for cyber security training and awareness," *Computers & Security*, vol. 26, no. 1, pp. 63–72, 2007.

[19] N. A. G. Arachchilage, "Serious games for cyber security education," *arXiv preprint arXiv:1610.09511*, 2016.

[20] M. Dixon, N. A. Gamagedara Arachchilage, and J. Nicholson, "Engaging users with educational games: The case of phishing," in *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, 2019, pp. 1–6.

[21] D. M. Wegner, “Transactive memory: A contemporary analysis of the group mind,” in *Theories of Group Behavior*. Springer, 1987, pp. 185–208.

[22] D. W. Liang, R. Moreland, and L. Argote, “Group versus individual training and group performance: The mediating role of transactive memory,” *Personality and Social Psychology Bulletin*, vol. 21, no. 4, pp. 384–393, 1995.

[23] R. DeCharms, “Personal causation training in the schools 1,” *Journal of Applied Social Psychology*, vol. 2, no. 2, pp. 95–113, 1972.

[24] J. C. Roca and M. Gagné, “Understanding e-learning continuance intention in the workplace: A self-determination theory perspective,” *Computers in Human Behavior*, vol. 24, no. 4, pp. 1585–1604, 2008.

[25] M. Gagné, “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*, vol. 48, no. 4, pp. 571–589, 2009.

[26] H. A. Kruger and W. D. Kearney, “A prototype for assessing information security awareness,” *Computers & Security*, vol. 25, no. 4, pp. 289–296, 2006.