A Systematic Review of Information Security Knowledge-Sharing Research

S. Al-Ahmari[1], K. Renaud[2] and I. Omoronyia[1]

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

Abstract

It is crucial for knowledge to be shared in the information security domain. In effect, sharing ensures that knowledge and skills are propagated through the organisation. Here, we report on a systematic literature review we carried out to gain insight into the literature related to information security knowledge sharing within organisations. The literature highlights the importance of security knowledge sharing in terms of enhancing organisational security awareness, and identifies gaps that can be addressed by researchers in the area.

Keywords

Sharing, Knowledge, Information, Security, Employees

1 Introduction

Employees play a crucial role in enhancing information security (Ahmed *et al.*, 2014). Their understanding of risk can have a positive influence on the improvement of information security behaviours (Becerra-Fernandez, 2014). Yet an essential pre-requisite for secure behaviour is that people know what it is they have to do and how to do it; in other words, they possess the required *knowledge* and *skills* (know-how). While awareness drives and training are undeniably valuable and essential, the most powerful way to ensure that all employees gain the requisite knowledge and know-how is to encourage and facilitate knowledge sharing across the organisation (Mermoud *et al*., 2018).

Knowledge sharing, of all types, improves the organisation as a whole. It facilitates trust between employees (Dang-Pham *et al*., 2017; Dang-Pham & Nkhoma, 2017; Politis, 2003). Of particular interest in this paper is *information security* knowledge sharing. Knowledge sharing improves information security awareness, which is important when it comes to preventing security breaches (Dixon, 2000). Organisations should therefore facilitate and engender knowledge sharing. The aim is to make the knowledge accessible to all of those who need it and ultimately to improve information security across the organisation.

We now review the core concept of 'knowledge', and discuss the kinds of knowledge that could be shared in the information security context. We then report on the systematic literature review we carried out in order to gain insight into the research

carried out into knowledge sharing in the information security context (Section 3). Section 4 presents our findings, Section 5 reflects, and Section 6 concludes.

2 Knowledge & Information Security

Knowledge is gained when meaning is added to information. People can gain knowledge from their environment (Feledi *et al.*, 2013) or from personal experience (Feledi & Fenz, 2012). In the information security context, people can gain knowledge from training drives, but are more likely to gain the knowledge they need from other employees in the workplace.

Knowledge can be either tacit or explicit (Dang-Pham *et al.*, 2017). The former refers to *skills* that cannot easily be recorded or expressed, which makes it difficult to share and retain (Fenz & Ekelhart, 2009). It is important for employees to transfer tacit security-related knowledge to other employees – to externalise it (Flores *et al*., 2014). Explicit knowledge can be expressed in numbers and words (Gal-Or & Ghose, 2005) and can be recorded. Knowledge delivers the most value when it is linked to other relevant and pertinent knowledge, thereby conveying new knowledge, a process called 'combination' (Flores *et al*., 2014).

2.1 Information Security Knowledge

Bartnes *et al.* (2016) define information security as a set of strategic management processes, policies and tools necessary for preventing, detecting, documenting and countering threats that subject non-digital and digital information systems to risks that cause damage such as loss of information and information theft. Flores et al. (2014) define knowledge sharing as the explicit or tacit transfer of values, experience, expert insight and contextual information from one person to another which helps that person to incorporate and evaluate new information and experience. Stanton et al. (2005) suggest a two-dimensional model of end-user security behaviours. The first is expertise and the second intention. We focus on benevolent intentions. In this category, people without knowledge make naïve mistakes, but knowledge leads to awareness and security assurance. Parsons et al. (2014) conclude that human errors attributable to lack of security awareness and knowledge are the principal sources of information security breaches. Using HAIS-Questionnaires and incorporating a sample of 500 employees, the authors gauged employees' awareness levels and came to the conclusion that employees with poorer security awareness subjected their organisation to security breach risks (Parsons et al., 2014). As a recommendation, the authors identified a holistic approach to employee training that emphasises knowledge and attitude as the way forward towards counteracting this problem. However, Zhang (2018) argues that knowledge expires in this field, and needs to be renewed. Moreover, Junger *et al*. (2017) show that warnings, by themselves, do not necessarily make that much of a difference to susceptibility to social-engineering attacks. Gcaza and von Solms (2017) argue that cultivating a cyber security culture, which implies that knowledge sharing has become *de rigueur*, is the best approach for addressing human factors in information security.

2.2 Information Security Knowledge Sharing

Kim and Kim (2017) show that social pressure influences compliance intention, and that compliant behaviour is influenced by knowledge. Knowledge sharing is crucial in the information security arena.

Safa and von Solms (2016) explored the process of information security knowledge sharing in organisations. They discovered that "earning a reputation and gaining promotion" and "external motivations" had a positive influence on knowledge sharing. Mermoud *et al.* (2018) 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.

Safa *et al*. (2016) aimed to deliver an insight into the phenomenon of information security knowledge sharing. They combined Motivation Theory and the Theory of Planned Behaviour to deliver a knowledge sharing module (Dixon, 2000). They discovered that trust was a barrier to knowledge sharing (Dixon, 2000). Dang-Pham *et al*. (2017) aimed to find out why people provided information security advice to others. They discovered that the primary barriers to sharing security knowledge were behaviour and trust. Rocha Flores *et al*. (2014) examined the impact of cultural factors on security knowledge sharing. 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. Feledi *et al*. (2013) examined the efficiency of cooperation between participants during the process of knowledge sharing. They identified the primary barrier to sharing security knowledge to be a lack of motivation on the part of employees.

2.3 Summary

The previous discussion identifies the importance of the organisation's incentive processes in encouraging knowledge sharing in the information security context. Moreover, the role of trust was highlighted, which suggests that an organisation that suffers from a lack of trust might well experience more security incidents because employees do not share knowledge. When we consider the fact that hackers extensively and actively share knowledge (Zhang *et al.,* 2015), we have to pay attention to fostering and encouraging sharing within organisations.

We will now report on the outcome of the literature review to see whether these same factors emerge.

3 Methodology

We followed Pickering and Byrne's (Gao *et al.*, 2015) systematic quantitative literature review methodology as follows:

- **Choose Databases**: Science Direct, Scopus, Web of Science and Google Scholar.

- **Choose Keywords:** for the searches were 'information security', 'Sharing knowledge',' Behaviour of the end-users.
- **Choose Time Range**: published between 2000 and 2017.
- **Inclusion Criteria**: Studies related to information security knowledge sharing for employees in the workplace. Studies on knowledge sharing security between firms, knowledge sharing security networks for end-users outside of the organisations, and knowledge sharing in technology security were excluded.

Database	Papers Found	Papers Rejected	Papers Analyzed
Web of Science	191	185	6
Scopus	25	16	9
Science Direct	54	42	12
Google Scholar	46	27	19

Table 1: Systematic Literature Review

4 Results

The literature review delivers insight into extant research, which will be reviewed in this section.

4.1 Factors affecting Security Knowledge Sharing

Several studies addressed the advantages of knowledge sharing in the organisation, especially in the security awareness domain. Hawryszkiewycz and Binsawad (2016) described barriers impeding knowledge sharing. They identified more than 160 barriers and identified the most significant barriers as: Lack of a motivation, Lack of trust, Lack of incentive and reward systems, Lack of organizational culture, Lack of leadership, Lack of technical support, Insufficient technology infrastructure. Table 2 and Figure 1. Display the factors confirmed by the studies. The starred items are the most significant.

Factors	Tested and Evaluated
Trust*	Hassan *et al*. (2013), Hassan *et al.* (2014), Dixon (2000), Hawryszkiewycz and Binsawad (2016), Herzog *et al*. (2007), Ibragimova *et al*. (2012), Im and Baskerville (2005), Johnson *et al*. (2001), Junger *et al*. (2017).
Attitude	Dixon (2000), Gcaza and von Solms (2017), Hassan *et al*. (2014), Herzog *et al*. (2007), Ibragimova *et al*. (2012), Kim and Lee (2006).
Culture*	Hassan et al. (2013), Herzog *et al*. (2007), Johnson *et al*. (2001), Kim and Kim (2017).
Motivation*	Dixon (2000), Hassan et al. (2013), Ibragimova *et al*. (2012), Johnson *et al*. (2001), Liu *et al*. (2011), Mermoud *et al*. (2018).
IT application	Hassan et al. (2013), Johnson *et al*. (2001), Liu *et al*. (2011), Nonaka (1994).
Organisational Leaders	Hassan et al. (2013), Johnson *et al*. (2001), Liu *et al*. (2011).

Table 2: Factors Influencing Knowledge Sharing

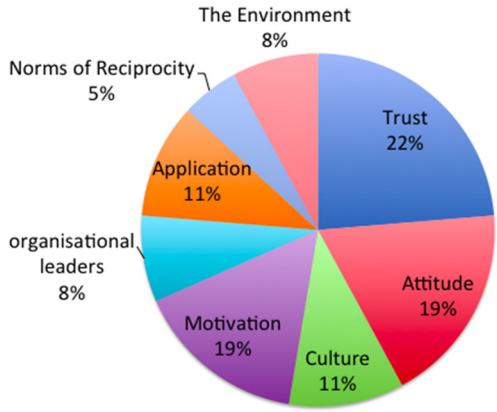

Figure 1: Factors Impacting Knowledge Sharing in the Reviewed Papers

4.2 Theory

Different theories have been proposed to explain knowledge sharing in information security. However, the *theory of planned behaviour* has proved to be the most influential. The theory revolves around the idea that an individual's attitude is a predictor of their intentions and behaviour.

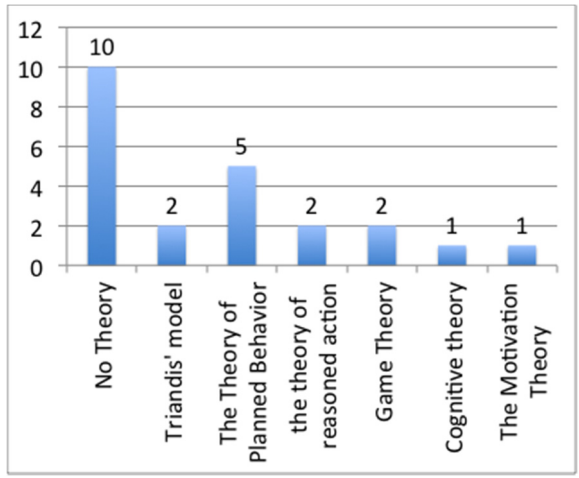

Figure 2: Theories used in the Reviewed Papers

4.3 Geographic Scope

Different investigations into knowledge sharing in information security have been conducted in various parts of the world. The Asian continent, with 41%, coverage, has experienced the highest number of studies. Europe comes in second with 27%, of studies. The North American region comes in third with 18% coverage; both Australia

and Africa benefited the least from studies related to knowledge sharing in information security. Australia gained a 9% coverage while the African continent only had 5% coverage.

4.4 Methodologies

In the methodology section, it was noted that survey and literature review conceptual models were the most common techniques for examining knowledge sharing in information security. The survey technique involved questioning participants and getting to hear about their views on the topic. Some surveys were structured with others being unstructured. Participants would choose either self- or group-administered questionnaires. The literature review conceptual model entailed investigating existing theoretical studies into knowledge sharing in information security.

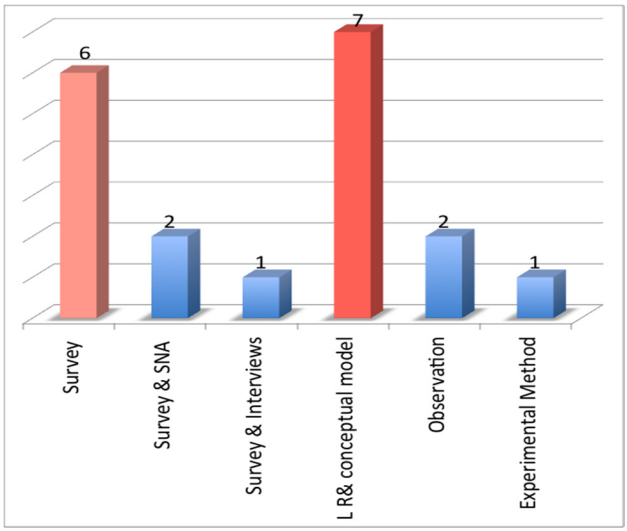

Figure 3: Deployed Methodologies used in the Reviewed Papers

5 Discussion

Knowledge sharing has a proven positive influence on security awareness among employees. We wanted to confirm the importance of security knowledge sharing and show how its influence on employees in the workplace led to enhancing resilience to cyber attacks.

The current study identified advantages of knowledge sharing in an organisational setting, especially in terms of individual security awareness. Hawryszkiewycz and Binsawad (2016) described the impact of barriers deterring knowledge sharing. The results of our study indicate that trust, motivation and culture are powerful barriers to

knowledge sharing. Most of the studies did not propose effective solutions to mitigate these barriers.

Another important finding was that the studies we reviewed used only a handful of different theories. In discussing its significance to knowledge sharing, the theory proved to be more comprehensive in providing logical reasoning. Ideally, it could be argued that an employee's cognitive state would influence them in deciding on whether to participate in knowledge sharing, or not. This result may be explained by the fact that the researchers focused on the theories related to the individual, such as the Theory of Planned Behaviour. The researchers neglected theories that address barriers, such as Trust Theory.

Additionally, what is surprising is that the Asian continent, with 41% coverage, has experienced the highest number of studies investigating how knowledge sharing is achieved in the corporate sector. A possible explanation for this might be that the Asian continent has high levels of security risk which causes more consideration of security and attempts to enhance employee awareness.

The most interesting finding was that, in the methodology section, survey and literature reviews dominated the literature. The survey method does not deliver in-depth analyses of human behaviours. Surprisingly, only one study was found that used interviews or focus groups to understand the barriers affecting security knowledge sharing. This is surprising since observation, surveys and interviews are the most powerful techniques for delivering comprehensive insights that would allow for the best understanding of knowledge sharing in natural environments. Such methods have the advantage of allowing more transparency in noting down real-time data based on direct or indirect interaction between the researcher and the participants.

Safa *et al.* (2016) set out to investigate an effective model that can reduce the negative impact of the human factor in information security. In the end, the outcomes of the analysis reveal that information security knowledge sharing, experience, and collaboration have a positive impact on employees' will to comply with information security guidelines.

6 Conclusion

In conclusion, the present study was designed to gauge the impact of security knowledge sharing, the relationship between knowledge sharing and information security, and barriers to security knowledge sharing. We confirmed that security knowledge sharing increases employee awareness, mitigates risks, improves decision-making, and improves efficiency in the workplace (Parsons *et al*., 2010; Persadha *et al*., 2016). However, many factors affect security knowledge sharing such as trust, motivation, and attitude. Researchers should investigate how a more effective sharing mechanism can be formulated, specifically to address those factors and thereby achieve improved knowledge sharing across organisations. Based on the recent study reported by Mermoud *et al.* (2018), the role of incentivisation should also be explored.

7 References

Ahmed, G., Ragsdell, G. and Olphert, W. (2014) "Knowledge sharing and information security: a paradox?" *European Conference on Knowledge Management*, Vol. 3, pp. 1083.

Becerra-Fernandez, I. (2014), *Knowledge Management: Challenges, Solutions and Technologies*. New Jersey: Pearson, Prentice Hall.

Dang-Pham, D., Pittayachawan, S. and Bruno, V. (2017) "Why do employees share information security advice? Exploring the contributing factors and structural patterns of security advice sharing in the workplace." *Computers in Human Behavior,* Vol. 67, pp. 196-206.

Dang-Pham, D. and Nkhoma, M. (2017) "Effects of team collaboration on sharing information security advice: Insights from network analysis." *Information Resources Management Journal (IRMJ),* Vol. 30, No. 3, pp. 58-72.

Dixon, N. M. (2000) *Common knowledge: How companies thrive by sharing what they know*. Harvard Business School Press.

Feledi, D., Fenz, S. and Lechner, L. (2013) "Toward web-based information security knowledge sharing." *Information Security Technical Report,* Vol. 17, No. 4, pp. 199-209.

Feledi, D. and Fenz, S. (2012) "Challenges of web-based information security knowledge sharing." In *Seventh International Conference on Availability, Reliability and Security (ARES)*, pp. 514-521.

Fenz, S. and Ekelhart, A. (2009) "Formalizing information security knowledge." In *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security*, pp. 183-194. ACM.

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

Gal-Or, E. and Ghose, A. (2005) "The economic incentives for sharing security information." *Information Systems Research,* Vol. 16, No. 2, pp. 186-208.

Gao, X., Zhong, W. and Mei, S. (2015) "Security investment and information sharing under an alternative security breach probability function," *Information Systems Frontiers,* Vol. 17, No. 2, pp. 423-438.

Gcaza, N., and von Solms, R. (2017) "Cybersecurity culture: An ill-defined problem." In *IFIP World Conference on Information Security Education* pp. 98-109.

Hassan, N. H., Ismail, Z. and Maarop, N. (2013) "A conceptual model for knowledge sharing towards information security culture in healthcare organization." In *International Conference on Research and Innovation in Information Systems (ICRIIS),* pp. 516-520.

Hassan, N. H., Ismail, Z. and Maarop, N. (2014) "Understanding Relationship Between Security Culture and Knowledge Management." In *Knowledge Management in Organizations* (Lecture Notes in Business Information Processing), pp. 397-402.

Hawryszkiewycz, I. and Binsawad, M. H. (2016) "Classifying knowledge-sharing barriers by organisational structure in order to find ways to remove these barriers." In *Eighth International Conference on Knowledge and Systems Engineering (KSE)*, pp. 73-78.

Herzog, A., Shahmehri, N. and Duma. C. (2007) "An ontology of information security." *International Journal of Information Security and Privacy (IJISP)*, Vol. 1, No. 4, pp. 1-23.

Ibragimova, B., Ryan, S. D., Windsor, J. C. and Prybutok, V. R. (2012) "Understanding the antecedents of knowledge sharing: An organizational justice perspective." *Informing Science: The International Journal of an Emerging Transdiscipline*, Vol. 15.

Im, G. P. and Baskerville, R. L. (2005) "A longitudinal study of information system threat categories: The enduring problem of human error." *SIGMIS Database*, Vol. 36, No. 4, pp. 68-79.

Johnson, G., Scholes, K. and Whittington, R. (2001) "*Exploring Corporate Strategy: Text & Cases*," Pearson Education, 200B.

Junger, M., Montoya, L. and Overink, F-J. (2017) "Priming and warnings are not effective to prevent social engineering attacks." *Computers in Human Behavior,* Vol. 66, pp. 75-87.

Kim, S. and Lee, H. (2006) "The impact of organizational context and information technology on employee knowledge-sharing capabilities." *Public Administration Review,* Vol. 66, No. 3, pp. 370-385.

Kim, S. S. and Kim, Y. J. (2017) "The effect of compliance knowledge and compliance support systems on information security compliance behavior." *Journal of Knowledge Management*, Vol. 21*,* No. 4, pp. 986-1010.

Liu, D., Ji, Y. and Mookerjee, V. (2011) "Knowledge sharing and investment decisions in information security," *Decision Support Systems,* Vol. 52, No. 1, pp. 95-107.

Mermoud, A., Keupp, M., Huguenin, K., Palmié, M. and David, D. P. (2018) "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.

Nonaka, I. (1994) "A dynamic theory of organizational knowledge creation," *Organization Science,* Vol. 5, No. 1, pp. 14-37.

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

Parsons, K., McCormac, A., Butavicius, M. and Ferguson, L. (2010) Human factors and information security: individual, culture and security environment. (No. DSTO-TR-2484). *Defence Science And Technology Organisation Edinburgh (Australia) Command Control Communications And Intelligence Div.*

Persadha, P. D., Waskita, A., Fadhila, M., Kamal, A. and Yazid, S. (2016) "How inter-organizational knowledge sharing drives national cyber security awareness: A case study in Indonesia." In *18th International Conference on Advanced Communication Technology (ICACT)*, pp. 550-555: IEEE.

Pickering, C. Grignon, J., Steven, R., Guitart, D. and Byrne, J. (2015) "Publishing not perishing: How research students transition from novice to knowledgeable using systematic quantitative literature reviews." *Studies in Higher Education,* Vol. 40, No. 10, pp. 1756-1769.

Polanyi, M. (2009) *The Tacit Dimension*. University of Chicago Press.

Politis, J.D. (2003) "The connection between trust and knowledge management: What are its implications for team performance?" *Journal of Knowledge Management*, Vol. 7, No. 5, pp. 55-66.

Rocha Flores, W., Antonsen, E. and Ekstedt, M. (2014) "Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture." *Computers & Security,* Vol. 43, pp. 90-110.

Safa, N. S. and von Solms, R. (2016) "An information security knowledge sharing model in organizations." *Computers in Human Behavior,* Vol. 57, pp. 442-451.

Safa, N. S.,von Solms, R. and Furnell, S. (2016) "Information Security policy Compliance Model in Organizations." *Computers & Security,* Vol. 56, pp. 70-82.

Said, A. R., Abdullah, H., Uli, J. and Mohamed, Z. A. (2014) "Relationship between organizational characteristics and information security knowledge management implementation," *Procedia-Social and Behavioral Sciences,* Vol. 123, pp. 433-443.

Sarkheyli, A. (2016). "Relationship between Knowledge Sharing Security and Organizational Context in the Public and Private Organizations," *AMCIS2016. Information Systems Security and Privacy (SIGSEC)*, pp. 8.

Schrage, M. (1990) *Shared minds: The new technologies of collaboration* (Ed.) New York, NY: Random House.

Stanton, J. M.. Stam, K. R., Mastrangelo, P. and Jolton, J. (2005) "Analysis of end user security behaviors." *Computers & Security*, Vol. 24, No. 2, pp.124-133.

Tamjidyamcholo, A., Baba, M. S. B., Tamjid, H. and Gholipour, R. (2013) "Information security: Professional perceptions of knowledge-sharing intention under self-efficacy, trust, reciprocity, and shared-language." *Computers & Education*, Vol, 68, pp. 223-232.

Tamjidyamcholo, A., Baba, M. S. B., Shuib, N. L. M. and Rohani, V. A. (2014) "Evaluation model for knowledge sharing in information security professional virtual community." *Computers & Security*, Vol. 43, pp. 19-34.

Wright, L. (2017) "Rethinking people, risk, and security." In *People, Risk, and Security* (pp. 7-24), Springer.

Zhang, T. (2018) "Knowledge expiration in security awareness training." *Annual ADFSL Conference on Digital Forensics, Security and Law*. Vol. 2.

Zhang, X., Tsang, A., Yue, W. T. and Chau, M. (2015) "The classification of hackers by knowledge exchange behaviors." *Information Systems Frontiers*, Vol. 17, No. 6, pp. 1239–1251.