Information Security Culture as an Enabler: Addressing the Gap between Organisational Knowledge Sharing and Information Security

Authors: Enamul Haq Pathan, Gang Huang, Jiamin Xu, MD Hassan,

Rusol Zoma, Sujatha Rajagopalan, Wenlong Dong

Abstract

Knowledge sharing is a vital business strategy that creates value for an organisation. It also leads to accidental or deliberate loss of information and knowledge. With an ideal culture, the knowledge sharing barrier can be broken without leaking information. We gathered data from the literature on the benefits of knowledge sharing in organisations and the related risks, addressing the role of a positive organisational culture. We interviewed information security specialists in small and large organisations in Melbourne and overseas. The study confirms the findings from literature that organisations value knowledge sharing to gain a competitive advantage. They also revealed that the preventive measures of knowledge leakage usually involved fostering a sharing culture with strategy, policies and controls in place with regular training and awareness. Based on these observations, we propose the need for future research on organisations that have fostered a culture of sharing knowledge without compromising its security.

Introduction

With the need to capitalize on the capabilities of an organisation and to stay ahead of the curve, Knowledge Management Initiatives have been identified as a key business strategy for developing a competitive advantage (Zack, 1999). Knowledge can be defined as the kind of understanding of information that is acquired through experience after careful comparison, deriving consequence and developing connection from information (Davenport and Prusak, 1998). Organisational knowledge is the collective knowledge within an organisation that can be realistically tapped by that organisation to achieve a sustainable and competitive advantage (Gold et al., 2001). Knowledge sharing among individuals has been identified as a key component in organisational knowledge management (Davenport and Prusak, 1998; Gold et al., 2001). Therefore, knowledge exchange among individuals, groups or organisations is a critical activity for organisations (Randeree, 2006; Bukowitz and Williams, 1999).

Knowledge sharing is one form of a socio-technical system, and recent research shows that knowledge sharing is greatly influenced by cultural values of employees (Ardichvili et al., 2006; Bukowitz and Williams, 1999). With the emerging trends of organisational knowledge management initiatives and the increase in knowledge sharing activities, knowledge leakage has become a potential threat for organisations (Ahmad et al., 2014). Organisational knowledge can be leaked via many different ways. From technical perspective, insufficient information protecting systems such as firewalls will decrease the safety of organisational knowledge and make it easier for external sources to steal the knowledge. More importantly, from cultural perspective, the loss of knowledgeable employees may cause a large amount of leakage deliberately or accidentally.

While there are several literatures that address the benefits of organisational knowledge sharing as a power and a resource of competitive advantage (Zack, 2001; Gold et al., 2001). Likewise, sufficient research exists into the importance of information security. However, more research is required to address the risks involved in knowledge sharing and the various ways knowledge can be leaked particularly via humans and more importantly how information security practices can reduce those risks by building a proper security culture. This paper is attempting to bridge the gap between these two ideas and propose to answer the question:

Can an organisation's culture enable knowledge sharing without compromising on its security?

From the existing literature available, this paper attempts to introduce the concept of knowledge, role of ICT in knowledge sharing, knowledge leakage and the gaps between knowledge sharing and information security. Using interviews with information security officers at sample organisations and the supporting literature available, we have found that in order to facilitate intra-organisational knowledge sharing while preventing knowledge leakage, organisations need to foster a conducive information security culture.

Literature Review

Knowledge

The term 'knowledge' is categorized into two different types: explicit and tacit (Hislop, 2013). Explicit knowledge can be shared through various ways, including knowledge management systems, training programs, documents sharing and traditional communication styles such as face to face communication, phones, or emails. On the other hand, tacit knowledge is more dynamic and difficult to codify. It often refers to the ability, experience and skill possessed by a person that is embedded in his/her mind and utilized in practice.

Zack (1999) defined three levels of organisational knowledge: core knowledge, which is the minimum need for an organisation to run its business; advanced knowledge, which enables an organisation to survive in the competition; innovative knowledge, which differentiates an organisation from its competitors and become a market leader. The position of an organisation in the market in terms of its competitive advantage against competitors is determined by the knowledge level of the organisation and the competitors. For example, if you possess only the core knowledge while your competitors have innovative knowledge, you are at risk in the market.

Organisational Knowledge Sharing

Knowledge sharing is important primarily due to the nature of knowledge creation. The SECI model of knowledge creation identifies four stages of knowledge conversion from explicit knowledge to tacit knowledge (Monika et al., 2000). Nonaka et al. (2000) argue that knowledge sharing not only distributes the existing knowledge, but also creates new knowledge. People may come up with new ideas by reading explicit knowledge from documents or direct socializing with other individuals to acquire tacit knowledge. Hislop (2013) also pointed out that collaboration methods, such as social events, experience workshops and communities of practice are widely used in R&D to generate innovative knowledge.

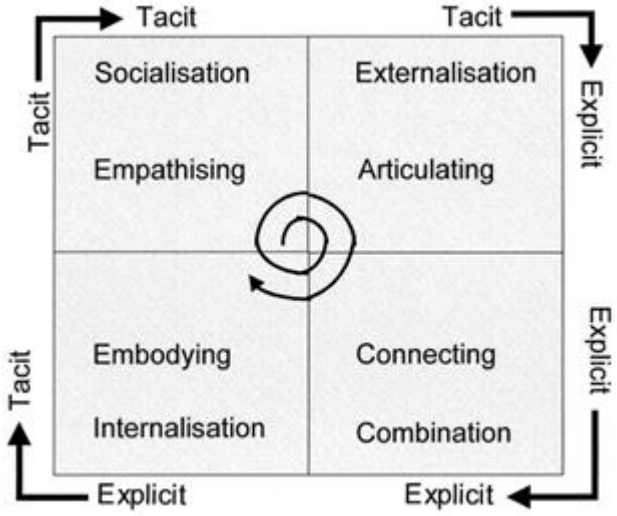

Figure 1. The SECI Model of Knowledge Creation (Monika et al., 2000)

ICT has become a powerful tool in supporting knowledge sharing process because it helps organisations to remove physical barriers (Hendriks 1999). Communication is no longer limited to the same geographic location; once a document is digitized, it can be accessed anywhere at the same time by different people.

Much attention has also been paid to non-physical barriers of knowledge sharing, typically the motivation and culture (Cabrera & Cabrera 2002; Lin 2007; McDermott & O'Dell 2001; Riege 2005). Riege (2005) listed several examples that individuals do not share their knowledge with others, including the fear of losing one's own job, the lack of trust in people, the low awareness of the value of knowledge sharing, differences in national culture and ethical background (such as language) etc.

Organisational Knowledge Leakage

The literature defines knowledge leakage as the disclosure of sensitive organisational knowledge to unauthorised people or a competitor, where knowledge leaks away from the organisational knowledge boundary either accidentally or deliberately (Ahmad et al., 2014; Annan Singh, 2012).

A Former or current employees, contractors, or even business partners could be a potential malicious threat to the organisation. An insider threat that is authorised to access the organisation's information, systems, or network and is capable of misusing this access, can result in a negative impact on the integrity, availability, or confidentiality of the organisational information (Hutch et al., 2013).

According to Ahmad et al. (2014), the risk of leakage increases with the growing exchange of knowledge. Inadequate information management practices and the availability of organisational knowledge over various sources can lead to knowledge leakage attributable to human error which may occur in a deliberate or discreet manner. Moreover, accidentally disclosing sensitive organisational knowledge to unlawful parties can result from practices such as outsourcing and offshoring.

The Role of Information Security

In order for organisations to benefit from the practice of knowledge sharing and stay competitive, it is essential to protect their organisational knowledge from leakage. Knowledge is an asset and good information security practices should be in place to secure that knowledge and help the knowledge management practices to be effective (Ahmad et al., 2014; Dsouza and Vanapalli, 2005; Gold et al., 2001; Randeree, 2006).

Researchers highlighted the security dimension of organisational knowledge and that an organisation's strategic objectives, goals, and knowledge management processes should be designed to protect knowledge from theft, leakage, or misuse (Gold et al., 2001; Dsouza and Vanapalli, 2005; Randeree, 2006).

Competitive advantage assets in the form of knowledge are unique and scarce, and security measures should be in place to protect those valuable assets. Mechanisms such as copyright, patents, employee conducts, technical controls, intensive alignment, policies and procedures, audits, sanctions, etc. are built to protect knowledge. However, informal protection controls in the form of employees' behavioural management, education, training and awareness are as necessary as the formal and technical controls. This form of control is required to encourage security culture. Organisations should develop a culture that adopts knowledge protection facets and raise employee awareness in this context (Ahmad et al., 2014; Gold et al., 2001).

A significant dilemma with regards to organisational knowledge management and information security is the need to bring together the increase and support of knowledge sharing and the protective role of information security (Ahmad et al., 2014; Randeree, 2006).

The Gap between Knowledge Sharing and Information Security

Becerra et al. (2008) discussed that tacit knowledge is more susceptible to loss (availability issue) than leakage (confidentiality issue) because those experience and skills cannot be easily replicated and reused by someone else. On the other hand, explicit knowledge is more relevant to leakage (confidentiality issue) since competitors are more likely to replicate another's product with the acquired information.

Scholars from information security domain have noticed that such knowledge sharing can always accompanied with the risk of knowledge leakage. Smith et al. (2012) described a scenario in "the dark side of online knowledge sharing" that programmers are likely to seek for solutions of programming problems from online forums with a considerable possibility to leak confidential information. Such behaviour may happen outside the organisation's boundary, both physical and virtual, which is not controlled by most of the information security mechanisms. The presence of online forums makes it possible for individuals to seek for knowledge and collaborate with people outside the organisation to solve problems, which creates competitive advantage for the organisation. However, this may also put the organisation's critical knowledge in danger.

Easterby-Smith et al. (2008) examined such risk on organisational level. It is argued that knowledge sharing between organisations can also happen if such sharing can bring both of them more competitive advantage. And "the donor and the recipient are often in a situation of power asymmetry, with the former being in a more superior position". In terms of the risk, it is possible that the competitive advantage shifts from one organisation to its partner after the collaboration.

Both authors have noticed the social enablers behind the knowledge sharing. Smith et al. (2012) found that the reason programmers refer to forums for help is based on the mutual trust and commitment. Members of the online community have a strong sense of responsibility to help each other rather than intending to get sensitive information. Though posting questions online results in high likelihood of confidential information disclosure, it is also suggested that the awareness of security policy may influence the programmers' decision to post confidential information. Though the willingness of knowledge sharing is also established on mutual trust between two organisations, Easterby-Smith et al. (2008) argued that such alliance can be easily terminated if the bargain power is shifted between the organisations after the knowledge sharing.

Methodology

The research question in this paper has been developed by first conducting a literature review on mainly high quality journal articles. The literatures were sourced using Google Scholar, the university of Melbourne library catalogue and online databases and discovery technologies. The following keywords were primarily used: Knowledge Sharing, Knowledge Leakage, Knowledge Disclosure, Organisational Knowledge, Information Security, Security Culture, Employees Behaviour, and Competitive Advantage.

Our team also conducted a set of interviews with professionals including information security officer, information compliance manager, HR officer (IT and compliance department, regional office), assistant manager of internal audit and IS security, regional manager-information security, and assistant manager-information security and audit. Organisations included small IT service company in Melbourne as well as large multinational telecommunication operators and vendors - local offices in Bangladesh.

Interview questions were centred around the following aspects: the availability of a knowledge sharing process, risk considerations behind knowledge sharing, mechanisms used to handle knowledge leakage issues (if any), the gap between the importance of knowledge sharing the its related information security risks, the role of IS cultural. Organisations' names will remain anonymous for privacy reasons.

Discussion

Knowledge sharing is critical for an organisation to nurture innovation. The findings from our interviews with security specialists indicate that organisations see innovation as the growth engine. They promote a culture of collaboration and sharing to foster innovation. Although organisations realize that the risk of sharing information may lead to knowledge leakage, they value efficiency, flexibility, and sharing over complexity, bureaucracy and security concerns.

The security personnel of organisation 'G' stressed the fact that knowledge sharing may increase the potential risk of leakage but without knowledge sharing the organisations are at great risk of knowledge loss for reasons such as unavailability of particular resource, employees leaving the organisation etc. Company 'G' even introduced an employee rotation policy where employees need to carry out the same responsibilities of another role along with their own core responsibility to ensure there is sharing of business knowledge. It is evident from our interviews that organisations not necessarily see knowledge

sharing and cooperation as the sole driver for knowledge leakage but also recognizes the role of employee's perception, behaviour and ethics regarding information security.

However, Company 'H' strictly monitors the access to the repository and defines policies to control access permissions. Their policies ensure that knowledge is restricted among relevant employees. For example, they have a knowledge repository which is accessed by its employees when they face any technical issues while troubleshooting. The repository works as "lessons learned and best practices" guidelines. Furthermore, knowledge is classified based on the sensitivity and associated risks of knowledge leakage. In addition to that, knowledge environment safety is evaluated regularly by choosing random samples, and employees are subject to consequences when found noncompliant with company information security policies. Moreover, respective managers are also held responsible as he/she is responsible to monitor the team's adherence to information security policies.

Based on these interviews, it is apparent that organisations take necessary measures to prevent knowledge leakage while sharing takes place. They have policies in place that clearly define to what extent employees can share particular information and knowledge. They also have policies outlining the handling of information at the event of employees leaving the organisation. Employees need to sign a non-disclosure agreement including clauses that prevent the employee from joining a competitor or a client for a specified time period after leaving the company. Moreover, employees need to go through the clearance process for all work related devices, documents and access upon joining or leaving the organisation.

Are strategies, policies and controls enough to assure the security when knowledge is being shared around? It is also mentioned by the information security officer of company 'B' that strategies, policies and controls would not be able to cover all aspects of information security, and even if it is completely covered, there is a possibility of gaps in terms of misunderstanding when strategies, policies and controls are communicated, which in turn brings risks to information security. What could we do to close the gap? The key to the question is culture.

"Culture is a pattern of basic assumptions – invented, discovered, or developed by a given group as it learns to cope with the problems of external adaptation and internal integration – that has worked well enough to be considered valid, and therefore, to be taught to new members as the correct way to perceive, think and feel in relation to these problems" (Schein, 1985). Amos and Weathington (2008) proposed that person-organisation (P-O) fit decides how well an employee can adapt in the organisational context, and perfect fit cultivates positive attitude and behaviour. Information security culture is also influenced by other key elements, such as security strategy, policies and controls. Our interview findings indicated that information security culture is built when security strategies, risks, policies and controls are well established and the expected information security values, assumptions, and behaviours are well understood through effective security training and awareness programs. Such culture should be the prerequisite of promoting knowledge sharing.

Knowledge can be shared in so many different ways, formal or informal, oral or written, implicit or explicit, paper-based or electronically, one-on-one or one-to-many, within or cross boundary, which are impossible to be fully covered by any security strategies, policies and controls. Vroom and Solms (2004) discussed three levels of organisational behaviour: individual, group and the formal organisation. Our literature review indicates that individual behaviour is guided by security culture, and individuals have the concern that they may lose competitive advantages if they share their knowledge with others. Although culture seems intangible, it provides guidance to individuals to take appropriate actions when they are about to share knowledge, which takes competitive advantage on organisational level into consideration. Positive attitude and behaviour make individuals think twice before sharing knowledge to parties that may come from outside the organisational knowledge boundary. For example, organisational values and beliefs remind individuals about compliance when posting on social media that are addressed in policies of social networking use, and culture drives certainty of detection and consequences of misbehaviour in a knowledge sharing domain.

Conclusion

We conclude that an organisation can gain competitive advantage by sharing knowledge. Knowledge Management needs a culture where people are encouraged to share knowledge while tighter Information Security fosters a culture where people protect their information asset first. As we have highlighted from

the literature and our findings, the two themes do not conflict with each other. If organizations want to gain competitive advantages from knowledge sharing, a conformable information security culture is essential to have a perfect balance between information security compliance and knowledge sharing activities. Culture influences all activities in the workplace at all levels since it's the basic assumption of employee behaviour. The individual's value congruence with an organisation promotes a positive attitude and behaviour. Therefore, a proper security culture helps to balance the benefit of knowledge sharing and the risk of knowledge leakage. To further conclude that the benefits outweigh the risks, we propose the need for future research on organisations that have fostered a culture of sharing knowledge without compromising its security.

References

Ahmad, A, Bosua, R, & Scheepers, R 2014, 'Protecting organisational competitive advantage: A knowledge leakage perspective', Computers & Security, 42, pp. 27-39.

Amos, E, & Weathington, B 2008, 'An Analysis of the Relation Between Employee—Organisation Value Congruence and Employee Attitudes', *Journal Of Psychology*, 142, 6, pp. 615-632.

Annan Singh, F 2012, 'Exploring the Risks of Knowledge Leakage: An Information Systems Case Study Approach' 2012.

Ardichvili, A, Maurer, M, Li, W, Wentling, T, & Stuedemann, R 2006, 'Cultural influences on knowledge sharing through online communities of practice', Journal Of Knowledge Management, 10, 1, pp. 94-107.

Becerra, M., Lunnan, R. & Huemer, L., 2008. Trustworthiness, Risk, and the Transfer of Tacit and Explicit Knowledge Between Alliance Partners. Journal of Management Studies, 45(4), pp.691–713. Available at: 10.1111/j.1467-6486.2008.00766.x.

Bukowitz, W, & Williams, R 1999, The Knowledge Management Fieldbook / Wendi R. Bukowitz And Ruth L. Williams, n.p.: London : Financial Times Management, 1999.

Cabrera, A. & Cabrera, E.F., 2002. Knowledge-sharing dilemmas. Organisation studies, 23(5), pp.687–710.

D'Arcy, J, & Hovav, A 2007, 'DETERRING INTERNAL INFORMATION SYSTEMS MISUSE', Communications Of The ACM, 50, 10, pp. 113-117.

Da Veiga, A, & Eloff, J 2010, 'A framework and assessment instrument for information security culture', Computers & Security, 29, 2, pp. 196-207.

Davenport T, Prusak L. Working knowledge: how organizations manage what they know. Boston: Harvard Business School Press; 1998.

Dsouza, K, & Vanapalli, G 2005, 'Securing knowledge in organisations: lessons from the defense and intelligence sectors', International Journal Of Information Management, 25, 1, pp. 85-98.

Easterby-Smith, M., Lyles, M.A. & Tsang, E.W.K., 2008. Inter- organisational knowledge transfer: Current themes and future prospects. Journal of management studies, 45(4), pp.677–690.

Gold, A, Malhotra, A, & Segars, A 2001, 'Knowledge Management: An Organisational Capabilities Perspective', Journal Of Management Information Systems, 18, 1, pp. 185-214.

Hendriks, P., 1999. Why share knowledge? The influence of ICT on the motivation for knowledge sharing. Knowledge and process management, 6(2), pp.91–100.

Hislop, D., 2013. Knowledge management in organisations: A critical introduction, Oxford University Press.

Hutch, C, Chadwick, D, Claycomb, W, & You, I 2013, 'Guest editorial: A brief overview of data leakage and insider threats', Information Systems Frontiers, March.

LIM, J, Chang, S, Ahmad, A, & Maynard, S 2012, Towards An Organisational Culture Framework For Information Security Practices, n.p.: Information Science Publishing, University of Melbourne Digital Repository.

Lin, H.-F., 2007. Effects of extrinsic and intrinsic motivation on employee knowledge sharing intentions. Journal of information science.

McDermott, R. & O'Dell, C., 2001. Overcoming cultural barriers to sharing knowledge. Journal of knowledge management, 5(1), pp.76–85.

Nonaka, I., Toyama, R. & Konno, N., 2000. SECI, Ba and Leadership: a Unified Model of Dynamic Knowledge Creation. Long range planning, 33(1), pp.5–34.

Randeree, E 2006, 'Knowledge management: Securing the future', Journal Of Knowledge Management, 10, 4, pp. 145-156.

Riege, A., 2005. Three-dozen knowledge-sharing barriers managers must consider. Journal of knowledge management, 9(3), pp.18–35.

Schein, Edgar H 1985, 'Organisational Culture and Leadership', John Wiley & Sons.

Smith, A.L. et al., 2012. The dark side of online knowledge sharing. Journal of Information Systems, 26(2), pp.71–91.

Stewart, G, & Lacey, D 2012, 'Death by a thousand facts: Criticising the technocratic approach to information security awareness', Information Management And Computer Security, 20, 1, pp. 29-38, British Library Document Supply Centre Inside Serials & Conference Proceedings.

Vroom, C, & von Solms, R 2004, 'Towards information security behavioural compliance', Computers & Security, 23, 3, pp. 191-198.

Zack, M.H., 1999. Developing a knowledge strategy. California management review, 41(3).

University Library

MINERVA ACCESS

A gateway to Melbourne's research publications

Minerva Access is the Institutional Repository of The University of Melbourne

Author/s:
Pathan, Enamul Haq;Huang, Gang;Xu, Jiamin;Hassan, M D;Zoma, Rusol;Rajagopalan, Sujatha;Dong, Wenlong

Title:
Information security culture as an enabler: addressing the gap between organisational knowledge sharing and information security

Date:
2014-08-01

Publication Status:
Unpublished

Persistent Link:
http://hdl.handle.net/11343/42191