Strategies to Reduce Knowledge Leakage: A Knowledge Absorptive Capacity-based Framework

Saliha Ziam[1], Pierre-Emmanuel Arduin[2], Dragos Vieru[1]
[1]TELUQ University of Quebec, Canada
[2]Université Paris-Dauphine, PSL, CNRS, UMR 7088, DRM, Paris, France
saliha.ziam@teluq.ca
pierre-emmanuel.arduin@dauphine.fr
dragos.vieru@teluq.ca

Abstract
As a strategic resource, knowledge must be shared across organizational structures in order to increase users' ability to retain it and re-create it. In an organizational context, hackers may convince individuals to share sensitive data with them through social engineering methodologies. This situation may generate dramatic information security issues given that individuals are unprepared to anticipate the security breaches that may emerge from their actions and the potential impact of these infringements on organizations. Based on a systematic literature review, this theoretical study proposes a framework that enables us to better identify the necessary skills users need in order to acquire and securely share sensitive knowledge in their work environment.

Keywords: Knowledge sharing, Information and Knowledge System, Knowledge absorptive capacity, Security violation, User skills.

1. Introduction

In order to efficiently share knowledge across their structures, organizations may introduce Information and Knowledge Systems (IKS) (Arduin et al., 2015; Taylor and Joudrey, 2017), where individuals can easily share their knowledge, be it tacit or made explicit. The extant literature on knowledge management shows that most of the studies focus on how to improve the knowledge exchange process and the benefits that this process brings to the society in general (Estabrooks et al. 2008). These studies suggest that individuals' prior knowledge and expertise represent the antecedents of the absorptive capacity, a concept defined by Cohen and Levinthal (1990) as a firm's ability "to recognize the value of new information, assimilate it, and apply it to commercial ends" (p.128). However, with massive digital use, these exchange processes raise important issues in terms of data security. Authors such as Watson et al. (2014) highlight how employees, as knowledge holders, may have their access to sensitive information hacked. Through manipulation techniques such as social engineering (Wilson, 2010), hackers may lead employees to share knowledge without them knowing it. In this way, employees become an insider threat to the security of the IKS (Arduin, 2018). This context generates crucial information security questions given that users are unprepared to anticipate the security issues that may arise from their actions and their potential impact on organizations (Willison and Warkentin, 2013).

Based on the absorptive capacity perspective (Cohen and Levinthal, 1990), this research aims to shed light on two aspects of the knowledge exchange process that have been less researched so far: (1) users' ability to share research-based knowledge to improve the quality of their practices (Zahra and George, 2002; Deschenes et al., 2013); and (2) methods of securing knowledge access against hacker attacks during the knowledge sharing process in organizations (Keeney et al., 2005; Stanton et al., 2005). To do this, our study proposes a conceptual framework that enable us to better understand the necessary skills users need to develop to securely share knowledge resulting from research data in their work environment. Conclusions and next steps of this work are presented at the end of the article.

2. Theoretical background

2.1 Knowledge absorption

In their seminal article, Cohen and Levinthal (1990) argue that innovative organizations must possess absorptive capacity. The ability to exploit new knowledge is thus a critical component of organizational innovative capabilities. In this context, the authors focus on the impact of individuals' prior cognitive structures on the knowledge absorption process. By prior cognitive structures, Cohen and Levinthal (1990) are referring to the individuals' prior knowledge, whether it is linked to their educational baggage or to their experiential abilities. In the same vein, Szulanski (1996) finds that the knowledge receiver's lack of absorptive capacity constitutes a

major obstacle to the transfer of best practices. Other authors also confirmed a clear relationship between individuals' absorptive capacity and the use of information systems (Park et al., 2007) or the creation of new knowledge.

2.2 Relationship between knowledge sharing and security in the organizational context

Within organizations, IKS may be hacked as well as employees themselves (for tacit knowledge). Hackers may target employees by convincing them to make their knowledge explicit and eventually share it without their acknowledgement. According to Willison and Warkentin (2013), employee violations of the information security policies can be categorized as: (1) non-intentional, i.e. mistakes committed by careless or inexperienced employees; (2) intentional but not malicious, i.e. deliberate actions performed by employees obtaining a personal benefit with no intention to harm; and (3) intentional and malicious. Several authors have already addressed how non-malicious violations of information security policies may be avoided (Dhillon et al., 2017; Pfleeger and Pfleeger, 2002). In the same vein, but from a different perspective, we suggest that skill development through absorptive capacity (Ortiz et al., 2017; Todorova and Durisin, 2007) may be a way of mitigating non-malicious information security policy violations.

Based on the above argumentation, we conjecture that cognitive processes and specific organizational contexts influence the possibility of violations of the information security policies by employees. Our goal is twofold: we aim to identify (1) actions that may be useful to support employees against cyberattacks and (2) knowledge that may be used by malicious employees to violate the information security policy in place. We suggest that, the higher the absorptive capacity is, the more likelihood the information security policy will be respected.

3. A knowledge absorptive capacity-based framework

In this study we adapted Todorova and Durisin's (2007) model of absorptive capacity to the context of IKS users and propose a knowledge absorptive capacity-based framework (Figure 1).

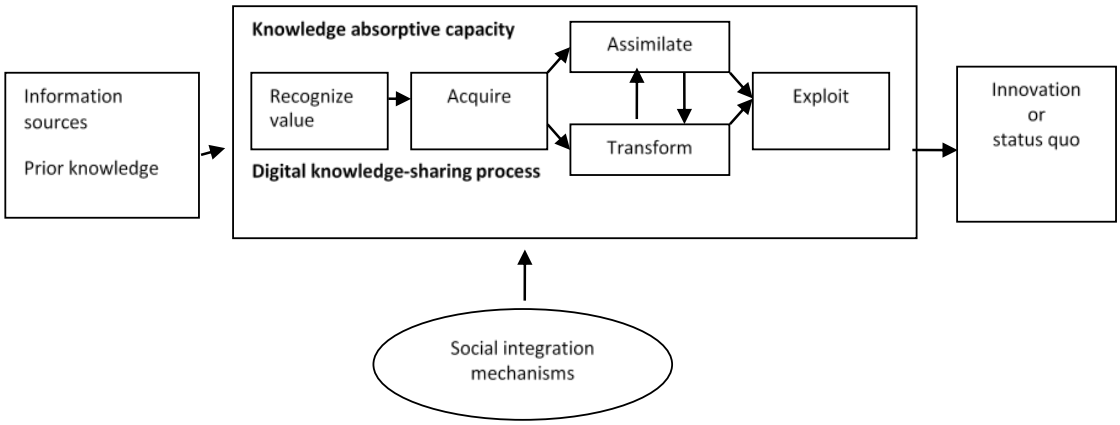

Figure 1: A knowledge absorptive capacity conceptual framework through the use of IKS

- **Recognition of knowledge value**

Identification of valuable knowledge by users is a strategic step as it enables the selection of pertinent information (Todorova and Durisin, 2007). Several authors suggest that the time allocated to activities such as reading, understanding and interacting with other stakeholders enhances people's ability to recognize the value of knowledge (Cohen et Levinthal, 1990). During the process of digital acquisition and sharing, recognizing the value of new knowledge also means being aware of and alert to any situation that might infringe the implemented information security policies that can put at risk the organization (Ocasio, 1997).

- **Knowledge acquisition**

Knowledge acquisition refers to users' ability to acquire external relevant knowledge for their activities or those of other members of their organization (Zahra and George, 2002). According to Hagardon and Sutton (1997), users acquisition of external knowledge provides organizations with solutions or ideas for future applications. This skill is influenced by the cognitive capacity and prior knowledge of individual.

- **Knowledge assimilation**

The assimilation of knowledge helps to translate, interpret and clarify information acquired from external sources (Pawlowski and Robey, 2004). This step in the absorption process further mobilizes people's basic skills, such as basic education, experience or motivation to learn new knowledge.

- **Knowledge transformation**

According to Hargadon and Sutton (1997) "valuable solutions seldom arrive at the same time as the problems they solve, they seldom arrive to the people working on those problems, and they seldom arrive in forms that are readily recognizable or easily adaptable"(p. 717). Hence, users primarily innovate by combining, adapting and synthesizing in new ways existing knowledge.

- **Knowledge exploitation**

The exploitation of knowledge helps to extend or create new knowledge by combining transformed knowledge (Zahra and George 2002). It is effective when knowledge users initiate activities that may facilitate the formalization of knowledge and its incorporation in routines and day-to-day activities (Pawlowski and Robey, 2004).

From the perspective of the knowledge absorptive capacity theory, the factors that affect users' capacity to securely mobilize knowledge are:

- **Prior knowledge and experience**

It has been suggested that the more educated users are, the more they can understand, interpret and exploit relevant knowledge for their organization and its security-related issues (Lane et al., 2006).

- **External information sources**

External information sources facilitate access to the strategic pool of ideas, which knowledge users can use to initiate innovations or solve current problems (Ziam et al., 2009). According to Hargadon (2003), it is the constant stream of problems and solutions, combined with exchanges between individuals, that can create new opportunities that lead to learning from others and developing one's own skills.

- **Organizational investment in social integration mechanisms**

The resources that are provided by the organization to its employees have an influence on the success of their activities. Users cannot perform their tasks if they do not have sufficient resources to facilitate the acquisition, sharing, and exploitation of knowledge (Todorova and Durisin, 2007). Social integration mechanisms include all knowledge-sharing activities and those that are related to information security policies (training, security policies documents, social media with the goal of providing awareness of knowledge sharing security issues). According to Todorova and Durisin (2007), social integration mechanisms affect all dimensions of the knowledge absorptive capacity of users.

4. Conclusions and future research

Our study focuses on the importance of educating knowledge holders and developing their skills needed to engage in a secure knowledge sharing process. Our proposed framework relies on a systematic literature review and suggests that individuals must be trained to acquire and master the skills needed to share knowledge and take advantage of information and knowledge systems while ensuring the protection of sensitive information. The skills-based approach used in this study opens a new avenue for research that will encourage researchers and practitioners alike to identify and assess the necessary skills to securely share new knowledge. The next step in our study is to empirically validate our conceptual framework by using a multi-case study method. We will adopt an explanatory theory-building-from-cases approach (Eisenhardt, 1989). Following Eisenhardt's (1989) methodological recommendations, we will anchor our preliminary construct specification in the extant literature and we will craft our data collection instruments and protocols on the basis of this literature, following a deductive pattern. This will be followed, after our entry in the field, by a "flexible and opportunistic" (Eisenhardt, 1989, p. 533) data collection approach, and a within-case and cross-case data analysis, which are inductive in

nature. We will use a multiple-case design and will select the cases applying a logic of replication, maximizing variation, thus predicting "contrasting results but for predictable reasons" (Yin, 2003, p.47), yet allowing comparison. Interviews will be the main method of data collection. In line with our theory building approach, we will remain open to the exploration of new topics and themes during data collection (Eisenhardt, 1989).

References

Arduin, P-E. (2018). *Insider threats,* Wiley-ISTE.

Arduin, P-E., Grundstein, M., and Rosenthal-Sabroux, C. (2015). *Information and Knowledge System*, Wiley-ISTE.

Cohen, W. M. et D. A. Levinthal (1990). "Absorptive Capacity: A New Perspective on Learning and Innovation," *Administrative Science Quarterly*, 35(1), p. 128-152.

Dhillon, G., Syed, R., & de Sá-Soares, F. (2017). Information security concerns in IT outsourcing: Identifying (in) congruence between clients and vendors. Information & Management, 54(4), 452-464.

Eisenhardt, K. M. (1989). "Building Theories from Case Study Research," *Academy of Management Review* 14(4), pp. 532-550.

Hargadon, A., and R., I. Sutton (1997). "Technology brokering and innovation in a product development firm," *Administrative Science Quarterly*, 42(4), p. 716-749.

Kim, D. and Solomon, M.G. (2010). *Fundamentals of Information Systems Security*, Jones & Bartlett Publishers.

Liebowitz, J. (2008). *Knowledge Retention: Strategies and Solutions*, CRC Press, New York.

Lane, P., J., R. K. Balaji, R. K. and P. Seemantini (2006). "The Reification of Absorptive Capacity: A critical review and rejuvenation of the construct," *The Academy of Management Review,* 31(4), p. 833-863.

Nonaka, I. and Takeuchi, H. (1995) *The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation*, Oxford University Press.

Ocasio, W. (1997). Towards an attention-based view of the firm. *Strategic Management Journal*, p. 187-206.

Ortiz, B., Donate, M. J., & Guadamillas, F. (2017). Relationships between structural social capital, knowledge identification capability and external knowledge acquisition. European Journal of Management and Business Economics, 26(1), 48-66.

Park, J.-H., H.-J. Suh and H.-D. Yang (2007). « Perceived absorptive capacity of individual users in performance of Enterprise Resource Planning (ERP) usage: The case for Korean firms », *Information & Management,* 44(3), p. 300-312.

Pfleeger, C. P., and Pfleeger, S. L. (2002). *Security in computing*, Prentice Hall Professional Technical Reference.

Polanyi, M. (1958) *Personal Knowledge: Towards a Post Critical Philosophy*, Routledge, London.

Szulanski, G. (1996). "Exploring internal stickiness: Impediments to the transfer of best practice within the firm," *Strategic Management Journal,* 17(S2), p. 27-43.

Taylor, A. G., & Joudrey, D. N. (2017). The organization of information. ABC-CLIO.

Todorova, G., and Durisin, B. (2007). "Absorptive Capacity: Valuing a Reconceptualization. Academy of Management," *The Academy of Management Review*, 32(3), p. 774-786.

Watson, G., Mason, A., and Ackroyd, R. (2014). *Social Engineering Penetration Testing*, Syngress.

Willison R. and Warkentin M. 2013. "Beyond deterrence: An expanded view of employee computer abuse", *MIS Quarterly*, 37(1), pp 1-20.

Wilson, P. (2010). *Social Engineering: The Art of Human Hacking*, John Wiley & Sons.

Zahra, S., A., and George, G. (2002). "Absorptive capacity: A review, reconceptualization, and extension," *Academy of Management. The Academy of Management Review,* 27(2), p. 185-203.

Yin, R. (2003). *Case study research: Design and methods*. Sage Publications, Inc.