Journal of Strategic Information Systems 21 (2012) 1–17

Contents lists available at SciVerse ScienceDirect

Journal of Strategic Information Systems

journal homepage: www.elsevier.com/locate/jsis

Knowledge risks in organizational networks: An exploratory framework

Peter Trkman [a,*], Kevin C. Desouza [b,1]

[a] University of Ljubljana, Faculty of Economics, Kardeljeva ploscad 17, 1000 Ljubljana, Slovenia
[b] Metropolitan Institute, Center for Public Administration and Policy, Virginia Tech., 1021 Prince Street, Suite 100, Alexandria, VA 22314, United States

ARTICLE INFO

Article history:
Received 24 October 2010
Received in revised form 2 November 2011
Accepted 2 November 2011
Available online 26 November 2011

Keywords:
Organizational networks
Knowledge
Knowledge sharing
Risk management
Management frameworks
Transaction cost economics

ABSTRACT

In a networked environment, it is essential for organizations to share knowledge among themselves if they want to achieve the global objectives such as collaborative innovation and increased effectiveness and efficiency of operations. However, sharing knowledge is not risk-free. An organization might lose its competitive edge if it shares too much or certain key knowledge. In addition, an organization might suffer if its intellectual property is improperly handled by its business partners. While the literature has touted the value of knowledge sharing within networks, there is a conspicuous absence of studies examining the risks of sharing knowledge. To address this gap, we develop an exploratory framework that categorizes knowledge-sharing risks across multiple dimensions. Such a framework is a structured approach to knowledge risk management and complements the practice-based approach to knowledge risk management that is presented in (Marabelli and Newell, 2012). Our framework outlines the various kinds of knowledge risks that organizations are facing. We use a combination of knowledge-based and transaction cost theories to show how knowledge risk impacts knowledge transfer among entities in the network, the whole network, and the risk mitigation options.

1. Knowledge sharing is not risk-free

Today's competitive environment calls for organizations to focus on their core capabilities (Gupta et al., 2009). To this end, most organizations participate in networks to satisfy their ancillary needs. Some organizations (e.g., Amazon, Dell) also rely on their networks for their core needs. For example, Amazon relies on the logistical capabilities of its business partners (e.g., UPS, FedEx) to attain its core business objectives.

As organizations become more dependent on these networks, it is clear that these networks are more than just a vehicle to acquire physical resources (e.g., raw materials) or operational capabilities (e.g., logistics) (Davis and Spekman, 2003). Networks are also critical vehicles for acquiring knowledge-based resources and capabilities. Consider the case of the Boeing Dreamliner (787). Boeing is utilizing a network of 15 business partners from Japan to Italy. For example, Mitsubishi Heavy Industries from Japan designed the wing box, while Vougut and Alexia collaborated in the building of the horizontal stabilizer and the fuselage (Baloh et al., 2008).

As noted by Grant (1996b), a firm's role is to integrate the disparate pieces of knowledge in its midst and leverage them to help attain its organizational objectives. Today, we can extend this thinking to networks. Unless networked organizations leverage the disparate and diverse collection of the knowledge found across the organizations in networks they belong

* Corresponding author. Tel.: +386 1 5892 400; fax: +386 1 5892 698.
E-mail addresses: peter.trkman@ef.uni-lj.si (P. Trkman), kev.desouza@gmail.com (K.C. Desouza).
URL: http://www.kevindesouza.net (K.C. Desouza).
[1] Tel.: +1 206 859 0091.

0963-8687/$ - see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.jsis.2011.11.001

and participate in, they will fail to meet their objectives (Agterberg et al., 2010). Consider the case of one of the most information- and knowledge-intensive networks, the US Intelligence Community (USIC). USIC's inability to share effectively information and knowledge has led to several disastrous consequences, as for example, its inability to prevent the attacks of September 11, 2001 and its incorrect assessment of Iraq's so-called weapons of mass destruction capability amply demonstrate (Desouza, 2009).

While knowledge sharing is valuable it cannot be done in a haphazard fashion. The improper sharing of knowledge and a loss of knowledge during transfer can have disastrous results (Hackney et al., 2008). In addition, knowledge sharing requires an organization to be dependent on another vital entity: for example, while major multinational pharmaceutical organizations are improving their performance through knowledge sharing via outsourcing arrangements, in the long run they may be eroding core competencies like drug discovery and clinical research (Gupta et al., 2009).

A critical challenge organizations face within networks is, therefore, how to manage the risks associated with knowledge sharing. This involves balancing between too much and too little knowledge sharing and knowing how to protect and secure the knowledge that is being shared in the network. The optimal management of these risks requires a careful consideration of the nature of the risks, the types of collaborative relationships, and the context of the network. Unfortunately, the literature on inter-organizational networks provides little theoretical or practical guidance on how to do this. Most emphasizes the importance of the exchange of information (e.g., designs, client lists, prices, customer profiles, sales forecasts, and order history) among firms in a network (Altay and Ramirez, 2010; Gunasekaran and Ngai, 2004; Zhou and Benton, 2007). Competency in information exchanges does not necessarily imply competency in knowledge transfer, however (Tarafdar and Gordon, 2007).

Moreover, while the literature on supply chain management has witnessed swift growth, a vast portion of this research focuses on a single (focal) firm managing the risks in its environment. Most often, only risk due to adverse events, either from a single firm within the network (e.g., partner non-performance) or from outside (e.g., low-probability high-impact events such as terrorism, natural disasters) are addressed (Chopra and Sodhi, 2004; Faisal et al., 2006; Finch, 2004; Hallikas et al., 2004; Ritchie and Brindley, 2007; Trkman and McCormack, 2009). Most of this research focuses on risks in purchasing and supply behavior. Little has focused on the importance of managing the risks that can arise from sharing knowledge in a network setting.

Given these gaps in the literature, the goal of this paper is to construct an exploratory framework that may facilitate the study of the various kinds of knowledge risks that emerge within networks. The framework is derived from the premise that different types of risk are perceived differently by decision makers and carry considerably different perceived costs for their mitigation. Thus, the impact of different types of risks on knowledge transfer, the network's operation and risk mitigation activities can vary considerably. While this premise may be reasonable, the practice-based approach presented in (Marabelli and Newell, 2012) provides a complementary account. The blind use of our framework could lead managers to believe that knowledge transfer is a fully manageable process that could cause them to neglect important issues such as the role of mediators in translating knowledge given its "stickiness" (Szulanski, 1996). Our framework is meant to be used as a sensitizing device in combination with the practice-based view articulated in Marabelli and Newell (2012).

The structure of the paper is as follows: in the next section we first define the term 'network'. Next, we outline the knowledge-based view of organizations and the role of transaction cost economics in managing risks. Then, knowledge risk management is discussed. Following this, we develop our theoretical framework to classify knowledge risks and demonstrate its implications.

2. Theoretical background

2.1. Networks

The term 'network' is often used casually (Cova et al., 2010). Various kinds of networks are postulated (Cova et al., 2010), such as alliance network (Baum et al., 2000); alliance partners (Becerra et al., 2008); business net (Möller and Svahn, 2006); cluster (Liao, 2010); collaborative or cooperative arrangement (Provan et al., 2007); co-opetition (Li et al., 2011); external knowledge sourcing (Carayannopoulos and Auster, 2010); innovation outsourcing (Baloh et al., 2008); inter-organizational knowledge network (Dawes et al., 2009; Hackney et al., 2008); knowledge-sharing network (Dyer and Nobeoka, 2000); network of practice (Agterberg et al., 2010); strategic alliance (Connell and Voola, 2007); supply network (Kärkkäinen et al., 2003; Straub et al., 2004), and vertical partnership (Kotabe et al., 2003) – to mention just a few.

In this paper, we conceptualize a network as a group of three or more organizations connected in ways that facilitate the achievement of a common goal (Provan et al., 2007). It includes a set of actors connected by a set of ties (Borgatti and Foster, 2003) and consists of the tangible and intangible investments that comprise the connected relationships (Hakansson et al., 2009). A network is characterized by sets of purposeful and connected exchange relationships which evolve over time (Andersen and Christensen, 2005). It is a coalition of autonomous but interdependent organizations that are willing to exchange information and coordinate some of their actions, and sometimes even to submit part of their activities and decision domains to centralized control, in order to achieve benefits that are greater than any single member of the network can create independently (Möller and Svahn, 2006; Straub et al., 2004). A network serves as a locus of innovation because it provides timely access to knowledge and resources that are otherwise unavailable (Powell et al., 1996).