

Knowledge risks – the (still) underdeveloped field of research

Susanne Durst – University of Skövde

**Information and Knowledge for All:
*Towards an Inclusive Innovation***

The World Conference on Intellectual Capital for Communities

UNESCO, July 3 & 4 2017

Background I

- Recently, researchers have started to examine various types of knowledge risks, such as risk of knowledge loss (e.g. Treleaven & Sykes 2005; Durst & Wilhelm 2011; Martins & Martins 2011; Joe et al. 2013), knowledge leakage (Mohamed et al. 2007; Parker 2012; Ahmad et al. 2014), or knowledge hiding (Connelly et al. 2012; Connelly & Zweig 2014; Cerne et al. 2014).
- This is a promising development, but these studies have addressed very specific issues and thus produced a fragmented understanding of the topic.

Background II

- There is a need to classify knowledge risks
- Developing the study of the risky side of knowledge would give us a more balanced understanding of the concept of knowledge and its management

Definition of Knowledge risks

- Likelihood of any loss resulting from the identification, storage or protection of knowledge that may decrease the operational or strategic benefit of a company (Perrott 2007).

Overview of Knowledge Risks I

Knowledge loss. Its consequence could be “the decreased capacity for effective action or decision making in a specific organizational context” (DeLong 2004, p. 21).

- It can be the result of personnel turnover, e.g. a company loses a key organization member;
- the dissolution of well-established teams;
- the outsourcing of business functions;
- a system crash, hacker attack and the theft of data are further examples that can lead to a loss of documented (explicit) knowledge.

Overview of Knowledge Risks II

Knowledge attrition. Knowledge attrition is considered to be a process where knowledge is becoming obsolete or spoiled.

- The difference between knowledge loss and knowledge attrition is that knowledge loss is a fact, a sort of result of certain phenomena, while knowledge attrition is a gradual process that can be stopped at each point and might either lead to knowledge loss or not.

Overview of Knowledge Risks III

Knowledge leakage. Knowledge leakage may be treated as a sub-form of knowledge loss (Durst et al. 2015) and can be defined as “the deliberate or accidental loss of knowledge to unauthorized personnel within or outside of an organisational boundary” (Annansingh 2012, p. 269).

- Knowledge leakage is connected with knowledge sharing and knowledge exchange between various parties both inside and outside the organization.

Overview of Knowledge Risks IV

Knowledge risks due to unlearning. Unlearning means an intentional loss of knowledge stored in the individual's long-term memory, in other words, to make room for accepting new knowledge (Cegarra-Navarro et al. 2013).

Knowledge risks due to forgetting. Forgetting can be divided into accidental and deliberate forgetting (De Holan & Phillips 2004). An example of accidental forgetting is memory loss. On the other hand, failure to capture new knowledge can be considered as an example of deliberate forgetting.

Overview of Knowledge Risks V

Knowledge outsourcing risks refer to risks that are the outcome of transferring a business activity or function from an organization to an external contractor who takes control of the activity's inputs and then performs that function, selling it back to the organization (Tadelis 2007).

Risks related to knowledge gaps. Describe a mismatch between what an organization must know, and what it actually does know, and which may hamper the organization in meeting its objectives (Perrot 2007).

Overview of Knowledge Risks VI

Relational risks are connected with the probability and consequence of having dissatisfactory cooperation and/or opportunistic behavior by partners (Delerue 2005). It also comprises the risk of knowledge sharing, which may end in the strengthening of the partner at the expense of the company's own competitive standing (Coras & Tantau 2013).

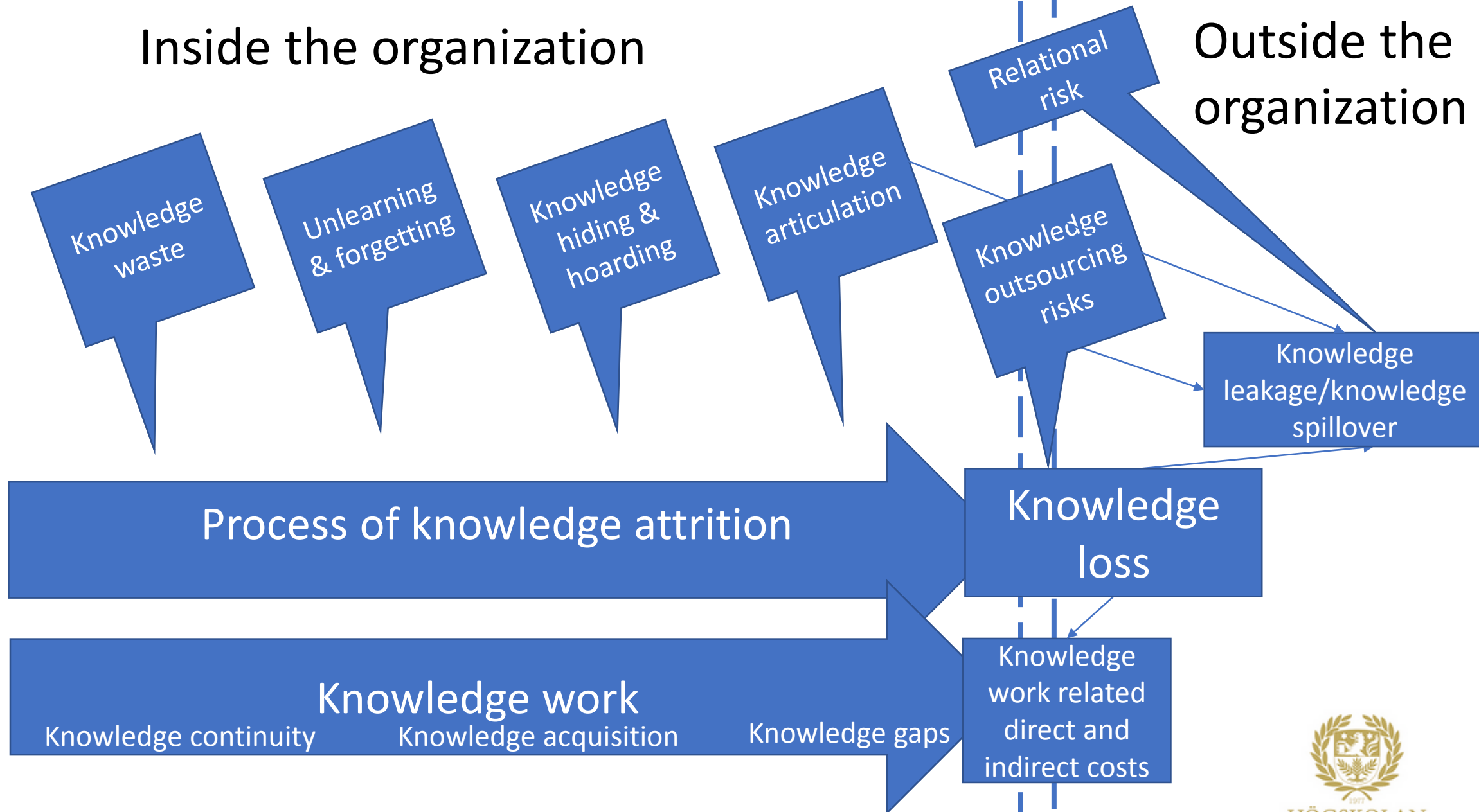
Knowledge continuity risks are closely linked to an organization's ability to keep its core capabilities over time and to its ability to maintain performance and competitive position at consistent levels.

Overview of Knowledge Risks VII

- **Risk of applying wrong (i.e. obsolete/false) knowledge.** As knowledge is in a constant state of change and it should be continuously updated. If not, there is a risk that the organization will apply wrong knowledge in its operations.
- **Risk of improper application of knowledge.** With the abundant amount of available information and knowledge, there is a risk of applying knowledge improperly or misinterpreting it.

Inside the organization

Outside the organization



Conclusion

Given the importance of knowledge to organizations, a discussion about knowledge risks is beneficial, not only for researchers but for practitioners as well.

iC

13

Intellectual Capital
for Communities
In the Knowledge
Economy

Thank you very much!

Contact: susanne.durst@his.se