JITTA

JOURNAL OF INFORMATION TECHNOLOGY THEORY AND APPLICATION

ISSN: 1532-3416

Between a Rock and a Hard Place: Facing Dilemmas in IT Risk Management

Lars Öbrand
Umeå Universtiy
lars.obrand@umu.se

Jonny Holmström
Umeå University
jonny.holmstrom@umu.se

Lars Mathiassen
Georgia State University
lmathiassen@ceprin.org

Abstract:

In this paper, we extend IT risk management theory using evidence gleaned from IT-enabled process management in a Swedish pulp and paper factory. Our analyses of risk management practices in the factory's core process revealed surprising insights. As organizational actors managed process related IT risks to ensure that the core production process was running 24/7, they generated strategic IT risks that threatened the sustainability of the process infrastructure. However, they could not manage these strategic risks without jeopardizing the 24/7 operation. Hence, they inadvertently found themselves between a rock and a hard place where they could not mitigate one high priority risk without generating another. Drawing on practice theory, we explain the observed risk management practices, introduce the notion of risk dilemmas, and discuss the practice-based view of risk as a useful approach to advancing IT risk management theory.

Keywords: Risk, Risk Management, Practice Theory, Information Technology.

Carol Hsu was the Senior Editor for this paper.

1 Introduction

Information technology (IT) risk management has traditionally focused on identifying pre-defined sources of risk and fashioning dedicated resolution techniques fitted to control them (Boehm, 1991; Lyytinen, Mathiassen, & Ropponen, 1998) in order to address risks in specific development projects or in relation to particular types of information systems (IS) challenges, such as requirement management (Davis, 1982; Fazlollahi & Tanniru, 1991; Holmström & Sawyer, 2011; Markus & Mao, 2004; Mathiassen, Tuunanen, Saarinen, & Rossi, 2007) or systems implementation (Aubert, Patry, & Rivard, 2005; Chatzoglou & Diamantis, 2009; Vitale, 1986).

Although the current literature contains studies that analyze strategies to deal with IT risks, it fails to explain why organizations find it increasingly difficult to manage such risks. Projects continue to fail, managers continue to struggle with managing IT as an organizational resource, and side effects, unintended consequences, and paradoxes continue to appear (Ciborra, 2004; Fairley & Willshire, 2003; Standish Group, 2011; Tesch, Kloppenborg, & Frolick, 2007). Work on information infrastructure in IS research (Blechar & Hanseth, 2007; Hanseth & Braa, 2000; Rönnbäck, Holmström, & Hanseth, 2007) further underscores the importance of advancing the notion of risk in our field. The expansion and increased integration of systems (e.g., in the paper and pulp industry) creates complex socio-technical infrastructures (Blechar & Hanseth, 2007) in which new risks may emerge. As a result, organizations may need new ways to manage risk.

The practice of risk management in an organization's day-to-day operations has received limited attention in the IS field to date (Scott & Perry, 2009) even though IT managers' and other organizational actors' day-to-day activities significantly impact organizations' ability to adapt and use IT as an organizational resource (Orlikowski, 2000; Orlikowski & Stephen, 2001). Building on this observation of the discrepancy between methods and their use, we propose to move beyond the canonical view of risk management in IS research.

In this paper, we suggest shifting the IT risk management discourse to zoom in on the detailed processes that constitute the day-to-day IT risk management activities in organizations. With such a practice-based approach to risk management, we can emphasize the particularities and idiosyncrasies of everyday organizational life and move the neat and uncluttered analytical abstractions of traditional risk management methods and techniques to the background. A focus on practice also reflects the pragmatic dimension of risk (Renn, 1998) since it is identified in relation to a socially constructed goal, group interests, and values (Bradbury, 1989). While one cannot always easily uncover them, one can trace them by investigating and analyzing how practitioners act on them in concrete situations. Adopting concepts from Argyris and Schön (1974), we focus on risk management actions and strategies as they play out as organizations manage their organizational processes from day to day.

Against this backdrop, we investigate the following research question (RQ):

RQ: How do practitioners manage risks in the context of IT-enabled process management?

We do so through an interpretative case study (Walsham, 1995) that we conducted at a large paper and pulp factory. The use of IT in processing industries has increased and changed dramatically over the last few decades. The integration of IT with industrial machine technology allows processing industry organizations to increase productivity by reducing production downtime, implementing new business models, and adopting planning approaches with a shorter time to market. Today, IT permeates multiple levels and all aspects of organizational activity in processing industries from production to maintenance, logistics, administration, and sales. To capture this complexity, we designed a study in which we combined interviews, observations, and a focus group to develop a nuanced account of how the factory practiced risk management.

Contribution:

Current literature on IT risk and risk management fail to explain why organizations find it increasingly difficult to deal with risks related to IT. In this study we adopt a practice-based approach to investigate how practitioners manage risk in the context of IT-enabled process management at a large paper and pulp factory. Our analyses illustrates how and why successful management of operational risk in fact diffused and increased strategic risk, creating a risk dilemma for the practitioners. Identifying and discussing a practice-based approach to risk extends the discourse on IT risk and risk management by tracing how and why risks emerge in complex settings and offering a complementary view of risk which impacts both theory and practice.

Drawing on Argyris and Schön's (1974) work in organizational learning theory, we investigated the governing variables, action strategies, and consequences of risk management practices as they played out in the day-to-day process management at the factory. As a result, we show how the way that the organization managed risks related to its day-to-day IT-enabled process management operations inadvertently generated strategic risks, which, in turn, threatened the risk management practices' purpose: continuous production. In the discussion, we argue that a practice-based approach to risk can explain this phenomenon.

2 Literature Review

Various researchers have considered IS-related risks for more than 30 years now since early work from authors such as Boehm (1973) and Alter and Ginzberg (1978). In reviewing the field, we found a rich and diverse discourse, particularly regarding risks related to software and software development projects (Alter & Ginzberg, 1978; Barki, Rivard, & Talbot, 1993; Boehm, 1991; Charette, 1989; Currie, 1998; Iversen, Mathiassen, & Nielsen, 2004; Keil & Robey, 1999; Lyytinen, Mathiassen, & Ropponen, 1998; McFarlan, 1981; Persson, Mathiassen, Boeg, Stenskrog Madsen, & Steinson, 2009; Ropponen and Lyytinen, 2000; Schmidt, Lyytinen, Keil, & Cule, 2001). As the use and importance of IT has evolved, so too has research on risk developed to encompass a rich variety of areas, phenomena, theories, tactics, and risk constructs. Applied approaches have ranged from technical (Boehm, 1991) to managerial (e.g. March & Shapira, 1987; McFarlan, 1981), and levels of analysis have ranged from project (Lyytinen et al., 1996) to organizational (Dhillon & Backhouse, 1996) and inter-organizational (Aron, Clemons, & Reddi, 2005). Other areas of concern in IS risk research relate to outsourcing (Aubert et al., 2005; Bahli & Rivard, 2003; Nakatsu & Iacovou, 2009), enterprise resource planning (ERP) (Aloini, Dulmin, & Mininno, 2007; Hakim & Hakim, 2010; Huang, Chang, Li, & Lin, 2004; Sumner, 2000; Wright & Wright, 2002), security (Cremonini & Nizovtsev, 2009; Kumar, 2002; Straub, 1990; Straub & Welke, 1998), knowledge management (Alhawari, Karadsheh, Nehari Talet, & Mansour, 2012; Massingham, 2010; Marabelli & Newell, 2012), and IT investment (Otim, Dow, Grover, & Wong, 2012). The diverse approaches of these researchers share a common fundamental definition of risk as an "effect of uncertainty on objectives" (International Standards Office, 2009), but, beyond this commonality, the IS literature contains little agreement about risk constructs in terms of levels or dimensionality.

In this paper, we focus on risk and risk management in organizations' day-to-day organizational processes (i.e., on risks that organizations identify and manage in their ongoing, daily operations rather than risks about specific events in the boundaries of particular projects). To review the literature, we apply Taylor, Artman, and Woelfer's (2012) categorization of IT project risk research streams (which focus on risk factor approaches, risk management approaches, or contingency approaches) to the wider area of IT risk in IS research: previous work on the types of risk we focus on distributed throughout IS research on risk beyond the project level. These three research streams encompass the vast majority of risk-related IS studies, but some exceptions exist, such as studies that draw on Beck's (1992) notion of risk and modernity (e.g., Ciborra, 2004; Hanseth & Ciborra, 2007; Mumford, 1996), which apply sociological concepts of risk to explore macro-level dynamics of organizational change.

Risk factor approaches focus on the first, and essential, process in the risk management cycle: risk identification. This approach assumes that risk managers can identify relevant risks ex ante and then manage them heuristically. Research in this stream has contributed comprehensive checklists of risks concerning specific risk levels, such as software projects (Aloini et al., 2007; Keil, Tiwana, & Bush, 2002; Smith, McKeen, & Staples, 2001) or organizational strategy (Aron et al., 2005; Clemons & Weber, 1990). The checklists differ in scope and detail. Taylor (2006) identifies four main categories that the 113 constructs that Moynihan (1996) identify fit into, while Lyytinen et al. (1998) synthesize risk checklists from four risk management approaches. Although this strand of risk research arguably contains the most research and appeal to practitioners, subsequent research has highlighted several drawbacks with such an approach.

First, it is difficult (at best) to decide which (if any) of the available checklists one should use to address the risks a given situation (Bannerman, 2008). Second, risk checklists tend to focus risk managers' attention on the included risks (Lyytinen et al., 1998), which increases the likelihood that they will overlook potential problems that the lists do not include. Third, the approach may cause managers to focus on the process of following the list rather than on the actual situation and the goals they want to attain (Pohlmann, 2003). Fourth, the approach implicitly assumes that risk managers have to or can obtain complete (or at least sufficient) knowledge of the risk factors that threaten their aims. However, several

studies have found that they seldom can partly because risk management often involves high levels of uncertainty and complexity (Barki, Rivard, & Talbot, 2001; Mathiassen & Stage, 1992), and partly because risk managers do not always take rational decisions (Lauer, 1996; March & Shapira, 1987).

Risk management approaches focus on providing models and methods of prescriptive risk management (e.g., Charette, 1989; Heemstra & Kusters, 1996; Lyytinen et al., 1998). Risk management research covers different levels from the project level (e.g., Heemstra & Kusters, 1996; Kumar, 2002; Lyytinen et al., 1996) to the organizational (e.g., Birch & McEvoy, 1992) and strategic levels (e.g., Ahn & Scudlark, 2002), and it typically covers variations of all or parts of the risk management processes (risk identification, analysis, evaluation, treatment, monitoring, and review). These approaches assume that, by establishing control over the risk management process, risk managers can control risk. Although risk management approaches differ from risk factor approaches, the former shares many of the latter's limitations, such as uncertainties about the optimal risk management method to use in a given situation and whether one can adapt possible approaches to specific contexts), which depend (as for all methods) on how one uses the methods (Mathiassen & Purao, 2002). Bannerman (2008, p. 2121) notes that "the quality of risk identification and analysis is dependent on the representation, participation, perception, and insight of the stakeholders in the brainstorming workshops who think through the various pointers offered by the analytical tool". Although risk management approaches provide useful tools, they provide little or no guidance regarding steps to ensure that risk managers include appropriate risks to cover a specific context. To a large extent, therefore, their success depends on risk managers' skill and judgment (Bannerman, 2008).

Contingency approaches stem from McFarlan's (1981) recommendations that risk managers should choose project-level risk-resolution strategies based on rigorously assessing the project's size, its structure, and the organization's experience with the technology involved. Mathiassen et al. (2007) present a model (dubbed reflective systems development) for establishing requirements (particularly required skills) in which risk managers map risk resolution patterns to archetypical risk profiles to find better fits between perceived risks and available approaches. In a similar vein, Barki et al. (2001) highlight the importance of balancing the emphasis on planning, internal integration, and user participation to the level of risk exposure, especially in high-risk projects. The contingency approach to risk management helps managers decide when to apply certain methods in order to maximize their chances of success. When faced with a high level of uncertainty or complexity, the contingency approach advocates increased planning and oversight in order to reduce the likelihood of failure. However, the literature provides few examples of practical implementation guidance (Taylor et al., 2012), and, as in risk management approaches, whether contingency approaches succeed depends to a large extent on risk managers' skill and judgment.

Gregor (2006) classifies theories applied in IS research according to their primary concern: analysis and description, explanation, prediction, and prescription. Closely examining the theoretical underpinnings of each stream of risk research from this perspective suggests that theory in the risk factor approach focuses on prediction whereas risk management and contingency approaches focus on prescription. Although predictive and prescriptive theories have proven to be powerful instruments for controlling risk, they have little use when risks fall outside preconceived risk lists, when risk managers' practices diverge from the assumptions underpinning risk management models, or when risks emerge that contingency approaches do not encompass. These limitations concur with the important discrepancy between methods and their use that research on systems development has highlighted (for an overview, see Mathiassen & Purao, 2002). Similarly, several studies have found that de facto risk management practices often vary from prescriptions in the literature (Marabelli & Newell, 2012; Ropponen & Lyytinen, 2000; Taylor, 2006), which—assuming that Taylor et al.'s (2012) categorization does indeed capture the vast majority of research on IS-related risks—suggests that we do not adequately understand how risks emerge and practitioners handle risk management challenges. Thus, we need more empirical research that examines risk management practices in real-world organizations' daily operations.

Moreover, although research on IS-related risk has a strong tradition and continues to diversify, Lyytinen et al. (1998) argue that it often relies on weak theoretical foundations and add that most studies focus only on specific sets of risks. Similarly, Scott and Perry (2009) express concern about the heavy concentration on software and project risk management, and Ciborra (2004) also argues that the IS literature on risk has a limited scope and adopts an inadequate theoretical base. Consequently, Smith et al. (2001) call for a holistic view of risk, and Carlo, Lyytinen, and Boland (2004, p. 59) state that IS researchers need to "look beyond the functional project level risks and carefully explain how risks emerge and are contained in

larger socio-technical networks". A few notable exceptions to this general picture of somewhat limited research exist. Mumford (1996), for example, challenges the predominant notion of risk in IS research by introducing Beck's (1992) concept of the "risk society" and contending that managers and organizations face new kinds of risk as society changes. Further, as technology becomes increasingly infrastructural (Carr, 2003; Tilson, Lyytinen, & Sorensen, 2010), the relationship between IT and risk becomes more complex (Hanseth & Ciborra, 2007). Indeed, researchers have begun to increasingly recognize complexity itself as a primary driver of risk (Drake & Byrd, 2006; Hanseth & Ciborra, 2007), and the notion of systemic risk has gained significant traction among some researchers in the field (Carlo et al., 2004; Hu, Zhoa, & Wong, 2012). Hence, Schmidt et al. (2001) invite researchers to reflect on the complex dynamics involved in risk management in intricately heterogeneous environments. Although research on information infrastructure (e.g., Hanseth & Braa, 2000) provides a useful approach to risk emergence, this research stream primarily uses the risk concept as a theoretical lens to explain and understand side effects and unintended consequences of actions. Several other authors have also challenged the orthodox notion of risk in IS research by advocating broader, more holistic approaches (Drummond, 1996; Scott & Perry, 2009; Smith et al., 2001). Thus, detailed empirical studies on risk management practices could also help advance new understandings of IT-related risks.

3 Conceptual Framework

Risk management, a specific form of problem solving, focuses on identifying and mitigating perceived threats to a desired goal. Schön (1983) argues that any problem-solving approach must consider the problem setting—an important consideration since practitioners involved in a problem-solving process always work in an uncertain, complex, and emergent situation. To capture these important aspects of risk management practice in the context of managing IT-enabled processes, we adopt a theoretical framework with key constructs (process management practices, governing variables, action strategies, and risks) and relationships between these constructs. In this section, we define these constructs, which we use as a foundation for our subsequent empirical analyses and theory development.

Argyris and Schön (1974) show how the governing variables of practitioners' theory in use guide their action strategies. Although often tacit or implicit, governing variables form the foundations for what action strategies practitioners choose. Because any given situation involves various (not necessarily compatible) governing variables, tradeoffs among governing variables can occur. The action strategies refer to the plans and measures practitioners employ to keep the dimensions of the governing variable(s) in an acceptable range. Every action has (intended or unintended) consequences. When an action strategy has the intended consequences, one confirms the theory in use. However, if unintended consequences arise, it follows that a mismatch between intention and outcome has occurred. When such a mismatch occurs, practitioners need to reconsider either their action strategies or the governing variables.

In order to explore how organizations manage risk in their day-to-day operations, we draw on the growing literature on practice theory, which Feldman and Orlikowski (2011) argue is a powerful analytical tool for addressing contemporary organizational dynamics and complexities. Practice-based approaches have made inroads in IS research during the last decade (e.g., Leonardi & Barley, 2010; Orlikowski, 2006, 2007; Schultze & Orlikowski, 2004; Wagner, Newell, & Piccoli, 2010) in which time researchers have used them to examine knowledge-related issues in organizational life. Applying a practice perspective, Marabelli and Newell (2012) revealed and criticized several assumptions regarding knowledge transfer and, thus, move beyond the conventional wisdom in the knowledge management risk literature. Practice theory has at its core the relationship between situated actions and the social world (Feldman & Orlikowski, 2011). All variants of practice theory share the idea that situated actions are consequential for social practices and relations are mutually constitutive. Relations, in this sense, refer not only to interpersonal relations but also encompass relationships among all relevant phenomena, which one cannot understand independently of their contextual relationships. Hence, for example, knowledge and practice reciprocally constitute each other, so one cannot address either in isolation in any given context. Feldman and Orlikowski (2011) note that, although practice theorists commonly assume the importance of situated actions for social interactions, individuals instantiate it in various ways. All variants, however, assume that our everyday actions have an important role in producing the contours of social life.

Here, we apply a practice perspective to risk as practitioners manage it in the context of IT-enabled process management. We examine practitioners' everyday risk management actions in order to explore how they affect the structural contours of organizational life. In applying this perspective to risk, we assume that risk management has a significant role in producing process management behaviors and

outcomes, that risk management and process management practices reciprocally constitute each other, and, thus, that one cannot meaningfully address them in isolation. Further, we assume that risk management practices reflect process management values and that risk management constitutes a rational surface layer of practice that reflects the deep layers of process management practice.

Table 1. The Analytical Framework

Construct	Definition	Assumption	Application to risk	Key references
Process management practices	The coordinated activities of individuals and groups when doing their "real work" as informed by the process management context.	Everyday actions are consequential in producing the structural contours of organizational life.	Risk management plays an important role in producing process management behaviors and outcomes.	Cook & Brown (1999), Feldman &Orlikowski (2011)
		Knowledge and practice reciprocally constitute each other, so one cannot address either in isolation.	Risk management and process management practices reciprocally constitute each other, so one cannot address either in isolation.	
Variables governing process management	A potentially conflicting set of tacit or explicit ideas, aims, and goals of process management practices.	Governing variables constitute the theory in use values and goals that shape, and are shaped by, process management behaviors and outcomes.	Risk management practices reflect process management values and goals.	Argyris & Schön (1974)
Process management action strategies	The plans and actions employed in process management to keep governing variables in an acceptable range.	Action strategies in process management constitute rational surface layers of practice that reflect deep layers of practice.	Risk management constitutes a rational surface layer of practice that reflects deep layers of process management practice.	Argyris & Schön (1974)
Process management risks	Discrete events that may occur and have a quantifiable impact on process goals and sustainability; risk arises when risk managers manage processes in the face of uncertainty along with capability and cost constraints.	Risk is a matter of perspective since how risk managers view the process, situated goals, and knowledge shape how they identify risks.		Bannerman (2008), Boehm (1989, 1991), Taylor et al. (2012)

4 Methodology

4.1 Case Study

As we establish in the previous section, everyday actions have an important role in producing process management behaviors and outcomes, and the reciprocal relationship between practices and knowledge implies that risk management practices depend on more than formalized risk methods and checklists. Thus, to understand micro-level risk management, one needs to address other factors that operate in the social context. To do so, we conducted an interpretative case study. Single cases allow researchers to investigate phenomena in great depth and often yield rich descriptions and understanding (Walsham, 1995). In addition, Schramm (1971, p. 6) notes how "the essence of a case study…is that it tries to illuminate a decision, or a set of decisions: why they were taken, how they were implemented, and with what result", which reflects our research question.

4.2 The Real-world Context

The research site (which we refer to as "P&P") is one of Europe's largest factories that produces kraftliner, a kind or paper used to manufacture high-quality corrugated packaging. The factory resides in Sweden and employs some 600 people, including approximately 200 shift workers. The factory receives the raw materials (timber and recycled paper), pulps and processes them, and then ships finished products to customers (mainly in Europe). Thus, the manufacturing and delivery chain has several steps. Besides personnel who manage the pulp and paper machines, the factory has staff with various other vital functions, including maintenance, administration, logistics, sales, and research and development (R&D).

The role of IT in the plant has evolved continuously since the 1980s such that it has a virtually ubiquitous role today. Output at the mill has doubled since the mid-80s, while the number of employees has fallen by approximately 30 percent. Operators' and technicians' responsibilities have grown as middle management has decreased. The factory has IT-enabled product processes and highly integrated IT infrastructure. Two separate departments at the plant deal with the use of IT: the IT department and the process IT department. The process IT department manages IT used in the factory's technological systems, which cover control systems, process stations, field units, and remote sensors, whereas the IT department manages IT used in the administrative processes, which cover business systems, electronic data interchange (EDI) standards, and other things. However, due to the increasing system integration at the factory, the boundary between the two departments' responsibilities sometimes blurs.

4.3 Data Collection

We collected data using three techniques: observation, qualitative interviews, and a focus group session. In order to identify relevant data sources (Mason, 2002) and better understanding the day-to-day process management context, we conducted observations throughout the factory for four hours before we conducted the interviews and focus group session. We then selected interviewees from different levels in order to cover the company's risk management practices as fully as possible. Since the study focuses on IT-enabled process management, we identified the main processes (production, maintenance, and projects) and, accordingly, selected operators, technicians, maintenance personnel, and project managers as key informants. In addition, we interviewed the IT manager, the process IT manager, and the maintenance and projects manager. Each interview focused on the following four interconnected themes: the process management practices, identified risks associated with these practices, identified IT-enabled risks, and the management of identified risks.

We accessed the firm through a regional innovation collaboration project and initially discussed our study with the IT manager at P&P. The IT manager facilitated all stages of data collection by administering practicalities related to them (e.g., obtaining access cards, booking rooms, distributing information about the project, and coordinating meeting times for the focus group). The first author carried out the observation over the course of one day and took field notes. These notes served as an input for developing themes for the qualitative interviews. The first author developed themes in collaboration with the other authors. Two weeks later, the first author conducted the 12 interviews. The first and second authors conducted the focus group after we all initially analyzed the data that the first author collected in round one and two (observation and interviews) six weeks after the observation. The first author digitally recorded and transcribed the interviews and focus group session.

In total, we conducted 11 interviews at the factory that lasted approximately one hour each. In addition, we interviewed a representative from ITV, P&P's main IT vendor, who had previously worked at the factory and now worked closely with P&P on their operations and with strategic IT issues. The final stage of data collection comprised a focus group session in which the IT manager, the process IT manager, and the manager of maintenance and projects represented P&P, while the ITV representative and a risk management consultant from a large IT firm participated to provide additional insights into risk management at P&P. The focus group focused on presenting, discussing, evaluating, and ranking the risks that we and the interviews identified.

Table 2. Data Sources

Data sources	Rationale	Description	Use of data
Observations	We used observations in order to better understand the contextual specifics.	Observation of P&P practitioners and their workplace environments (four hours total).	We used the data to develop general and specific themes for the qualitative interviews. Further, we used it to develop interview guides for the different roles in order to investigate the same themes with different actors with diverse knowledge bases and backgrounds. Further still, we used it identify patterns and processes that stretched between different parts of the plant.
Qualitative interviews	We used qualitative interviews in the second data-collection stage. These interviews occurred two weeks after the observations over the course of two working days. Practice often has a tacit nature, and qualitative interviews, based on previous observations, played a crucial role in our generating relevant data on risk management practices in the plant.	We recorded 12 interviews that each lasted approximately an hour. Of these 12 interviews, 11 occurred at the factory and one at P&P's main IT vendor (ITV).	The data served as a primary analytical focus for understanding both action strategies related to risk and, in particular, the governing variables of both risk identification and mitigation.
Roles		P&P's process IT manager, IT manager, maintenance and projects manager, paper machine operators, technicians, and maintenance personnel, plus a representative of ITV (P&P's main IT vendor).	
Focus group participants	We used a focus group as a third data-collection stage in order to validate an initial analysis of the action strategies and the governing variables. In addition, we used it to generate data on boundary-spanning (systemic) risk and risk management actions. We conducted it six weeks after the observations.	Researchers; P&P's maintenance and projects manager, IT manager, and process IT manager; an ITV representative; and a risk management consultant.	With the data, we could analyze action strategies and governing variables in relation to boundary-spanning types of risk. We also used it to uncover the relationship between different, but dependent, practices both in and beyond the organizational boundaries.

4.4 Data Analysis

We coded transcripts of the interviews and focus group session using the atlas.ti software program in order to identify action strategies, governing variables, and consequences related to risk management practices at the factory. We analyzed the data in three iterative steps. First, we developed our understanding of the action strategies and governing variables in the process management context by coding the interview transcripts. We used this understanding as the basis to develop our focus group session. Subsequently, we coded the focus group transcripts with a particular focus on practice boundaries, practice values and goals, and the relationship between different practices. At this stage, we observed how different risk managers' goals were contextually embedded and sometimes conflicting. Second, we evaluated the dataset and organized it contextually (Mason, 2002) in risk-related process management themes. We converged on three themes: technology risks, maintenance risks, and knowledge risks. We developed these themes through an iterative process and first based them on two main aspects of risk: ontology (expressed as technology), epistemology (expressed as knowledge). However, these themes did not capture two main risk categories that pertained to risk in maintenance processes. Finally, we developed the risk dilemma notion by drawing on extant theory in concert with the case analysis.

5 Results

5.1 Risk Practice Strategies at P&P

5.1.1 Technology-related Risks

System longevity and spare part shortages: the systems that the factory used had a varied lifespan, but P&P found it difficult to obtain spare parts for systems that had a long lifespan. The factory used about 60 Contronic P process stations that played an important role in regulating the production process. The process stations have been in place since the late 1980s and work well. However, since no one manufactures spare parts for Contronic P stations anymore, P&P had begun to run out of them. The factory had begun to replace process stations with more contemporary ones but at a moderate pace (currently six a year) partly due to the high cost and partly to avoid disrupting production. When the company replaced a station, it salvaged as many parts as possible in order to boost supply. However, this salvaging did not solve the problem of spare parts shortages since the company had no way to determine if the salvaged parts would work in another process station (especially after a year or two on a shelf). P&P could not regularly test these spare parts either due to the associated risks and effort. The company had no way to tell when the spare parts would run out, and the maintenance and projects manager described the situation as precarious:

> *The big risk I can see today is that, if we have a major disturbance, resulting in the malfunction of three or four process stations…, we can't handle a situation like that because we can't buy enough spare parts to get them up and running again. That means we have to replace them with newer models. An unplanned change like this would require several months of programming activities because the software in newer process station models isn't compatible with the old…. This is a major risk, and although we're aware of this, even if we got enough money to buy all new process stations, we wouldn't be able to do it because there aren't enough people with the right engineering knowledge available. To replace the hardware is much less of a problem; the major issue is configuring the software.* (Maintenance and Projects manager)

This kind of risk would likely reoccur even if the company resolved its problems with the Contronic P stations. As the same maintenance and projects manager added: "Looking at the shorter lifespan of systems, and the rate at which we can replace old ones, before we have replaced all of our Contronic P stations the new system will be obsolete, and we'll be back to square one".

Infrastructure heterogeneity: P&P had a heterogeneous but increasingly integrated IS infrastructure. Regardless of whether the company replaced a part or installed a new system, it had to integrate the new with the old—a difficult but important process. With the high degree of systems integration, the company found even simple tasks such as indexing difficult due to the sheer number of items it needed to index. Thus, it found even standardized products challenging to implement. In order to avoid side effects and unintended consequences, P&P chose to configure new parts that mimic those it replaced regardless of any novel functionality the new parts offered. As the process IT manager said: "We cannot afford to experiment. We are supposed to be conservative with regards to functionality, because production is what matters. Experiments can be carried out on machines that can be stopped for five hours without any consequences, but five hours costs too much here.".

Path dependency: when and how to switch IT systems constituted a major concern for the organization. Technology continues to develop quickly and the market's structure has changed dramatically in recent decades. When P&P invested in the Contronic P system in the mid-80s, the vendor it used represented one of many, but, like many small vendors, another company (ITV) took it over and integrated Contronic P process stations into its product portfolio. Previously, big vendors such as ITV manufactured their own products and stocked spare parts. However, the increasing standardization of IT parts has facilitated outsourcing, and, today, ITV relies on third-party vendors to supply parts for its products. The rate at which technology develops has accelerated and vendors continually add new functionalities and features to devices such as control systems. New standards frequently emerge, and companies can find it difficult to identify the optimal time to switch or the path to choose. Due to its earlier choices, P&P found itself locked into ITV's product family. However, even when locked into a particular vendor's portfolio, a company can still make bad choices. The process IT manager said:

> *We decided to invest in a certain control system sold by ITV because it was compatible with Contronic P. Three years later, when we replaced the old system in one of our operator rooms, they told us that they'd decided to focus on another of their systems instead and wouldn't support the one we bought. Now we can't find people any closer than Germany that know anything useful about this system, and we ended up sending people there to make sure we have this kind of competency in our own organization. If we'd made a different choice three years ago things would have been rather different. So what do we do now? We've invested a lot in this system, and the cost of going back and doing it all over again would be huge.*

IT vendor relationship: ITV has increased in importance for P&P as the latter's production processes have become ever more IT enabled. The two companies have had a close relationship in the sense that some of the people from ITV's regional office have been involved with P&P for over a decade and have accumulated intimate knowledge of the plant's systems. However, to a large extent, the relationship conformed to a traditional buyer/seller arrangement, and P&P had sole responsibility over the systems once implemented. The process IT manager said:

> *In the 80s, when we bought our first major IT system for the production process, we had a whole host of vendors to choose from. We wanted the very best system, the 'Rolls Royce-version', tailored to our needs. It was supposed to work from the get go, and run for about 20 or 30 years. Now, every time there's a new version we have these consultants telling us about cool new features and how great it will be, and we know that we really don't want these extra features, we just want it to work. We also know, from experience, that any new system is basically a beta version and it will take a lot of time and effort to get it to work properly, and it's us that will have to pay for the time and effort. It would be nice if ITV could take a little more responsibility for the systems they sell us, once they are implemented, and also think more long term than just selling another update or new system.*

5.1.2 Maintenance-related Risks

Narrow timeframes: P&P found it essential to minimize stoppage time, but doing so posed substantial maintenance challenges. Every month, production stopped for a short time for maintenance, and, every year, it stopped for five days for larger-scale maintenance tasks. Thus, the company had a narrow window for tasks such as testing vital parts of the production systems. Hence, it carefully planned the tasks and activities during this week long in advance in order to ensure it best used the stoppage. During the rest of the year, maintenance activities primarily focused on making sure the production process did not stop, fixing things that broke down, and solving problems as they arose. As the process IT manager said:

> *It's kind of frustrating. I mean, we see all these things that we sort of need to, or want to, fix, but unless they're vital for production they'll get bumped by what we absolutely need to do during these stops. Things we have to address, and can't do while the machines are running. We plan these breaks minutely because there's so little time to get vital things done, and we never seem to be able to fit in things from the 'things we should do something about' list. It's not that they're unimportant, just that they're not regarded as direct threats to production.*

Due to the significant costs P&P experienced in investing in new systems and conducting major maintenance projects and to the limited window of opportunity it had to do so, the IT or process IT departments planned the changes, applied for funding, and, when granted funding, prepared as rigorously as possible to ensure that the changes did not hamper production. The timeframe from initial planning to implement often lasted approximately 12 to 18 months. However, in recent years, the company has shortened the time between decisions to provide funds and the suggested implementation date and, thereby, reduced the time available for tests and preparation. As the process IT manager said:

> *We test, and test, and test, because we cannot afford any major breakdowns when we go live with the changes. It costs too much. Testing is one thing, production another, but we try to iron out as many wrinkles as possible before we implement changes. With the shorter timeframes, it's getting harder and harder to be thoroughly prepared before implementation, and we're becoming increasingly dependent on a few people with the knowledge required to do these kinds of things.*

IT support availability: when a disturbance occurred somewhere in the production line, P&P had to quickly address it or risk heavy economic losses. Since the company operated in northern Sweden (a large, sparsely populated area), the company risked long delays before help arrived if it needed external

assistance. In addition, the heterogeneity and idiosyncrasies of the infrastructure exacerbated the difficulties of engaging outside help in such situations. Therefore, P&P has invested in developing the competencies it needs inside the organization. As the process IT manager said:

> *It's hard enough as it is now. We have our own people on standby 24/7 if something goes wrong. Sometimes you wish that a guy hadn't gone away when they're on vacation, because he might be the only one who knows something. It would be much easier if everything was standardized and there were enough people with the right kind of competence about, readily available, that we could call upon when we need help. We try to have all the competence we need in-house, because then we don't have to depend on others.*

Collaboration between operators, technicians, and maintenance personnel also helped P&P significantly shorten the time it took to locate and solve problems that arose. The fact that these personnel shared knowledge about the process and process-related technology greatly facilitated this collaboration. Paper machine operators had enough knowledge about the technology in their work environment to greatly reduce troubleshooting for the maintenance personnel. Technicians worked in small, often mobile, work groups and made a point of checking in with their fellow employees while moving about in order to stay updated and maintain the social bonds that help facilitate collaboration. To some extent, the information systems (e.g., the intranet) supported this collaboration; however, staff members accomplished much with telephone calls and face-to-face meetings.

5.1.3 Knowledge-related Risks

Process integration: when solving a problem or detecting a potential problem, collaboration between different parts of the workforce at P&P proved essential. Since the production process was deeply interconnected, problems in one part had consequences for the other parts. Furthermore, restarting the process after a complete halt was much more difficult than speeding up after operating at half speed. Thus, by closely cooperating, the operators could coordinate adjustments along the process line and prevent complete stoppages when problems occurred in addition to optimizing process flows during periods of routine operation. The paper machine operator said:

> *Let's say the boiler isn't working properly, that there's some kind of problem there, then they'll give us a call and we'll slow the pace of the paper machine to make the pulp already in the system last as long as possible. This buys the boiler operators time to fix whatever's wrong. A lot of us have been here a long time, we know each other, and most of us have worked on different parts of the process before, so we know how to adjust the production when there's a problem without stopping it. That is really the last resort, because it takes a lot of time to start up again.*

Process representation*:* because P&P has continued to increase automation and implement new control systems over the years, the operators have increasingly come to operate in an information-rich environment and, in particular, rely on digitalized representations when interacting with the machines. As a result, these representations have needed to adequately and reliably translate relevant information about events at the mill. The operators used the control systems to monitor the performance of the machines and extensively used graphs to depict trends (e.g., process temperature changes). The graphs provided continuously updated overviews of the status of processes in different parts of the mill, which allowed the operators to take pro-active measures if necessary. The control systems included numerous warnings to help the operators recognize problematic situations. In addition, the control system needed to provide quick and clear feedback because unforeseen events often required rapid responses to avoid process disruption. However, the control system could not represent some relevant variables (e.g., due a lack of appropriate sensors). In such cases, the operators used other technological devices to troubleshoot (e.g., TV cameras strategically placed to monitor events in awkward places where problems sometimes arose that the operators found difficult to inspect). When something went wrong, experienced operators also used their own senses (e.g., smell, hearing, and touch) to locate and fix the problem. A control system could not easily successfully represent such subtle levels of experience and knowledge, but they represented important tools for accomplished operators. The operators at the mill also customized the paper machine control system themselves by adding and removing representations. Different operators in different crews even used slightly different process representations on the screens based on their individual preferences.

How management views IT: the way in which management views IT-related issues is also important. Developing and maintaining the IT at the mill represented an expensive and continuous activity due to its complexity and ubiquity. The views of the people who decided how to allocate resources regarding IT investments and maintenance needs had a significant impact on how they made decisions. Unless management at P&P saw a good reason for investing heavily in (for instance) a new control system, they seldom authorized the release of the required resources. As the maintenance and projects manager said:

> *It's really difficult to ask for money to replace something that works fine…. I mean, how do you explain to someone that we have to make huge investments in something that will, if we are lucky and work hard, work exactly the same as our current system. When you speak to the vendors they agree that the new product probably won't add any value to our process, but that there of course are new possibilities. In other words, we cannot really say we ever will have a return on the investment, our production will not get better, quality will not improve. Our only justifications are safety reasons, risks. But, of course, there are no models for determining the risks for the system; at best someone has looked at a component. The only thing we know about new systems is that they take quite a while to break in, so to speak, there are a lot of problems. How do you explain this to the management?*

Knowledge transfer: most of the workforce had worked at the mill for a long time and had much experience. Due to their experience and knowledge, they could successfully handle many everyday problems and risks that occurred at the mill. Thus, it risked losing valuable competence if it did not secure this deep collective experience and knowledge that it acquired over the years. A changing of the guard also loomed: the mill had seen relatively low personnel turnover, and most employees had worked there for over 20 years. In the next decade, many current employees will retire and, thereby, deprive the organization of their knowledge and experience.

Dependence on key individuals: P&P's infrastructure has continually increased in complexity due to its heterogeneity, integration, and continuous technical development. The company has found replacing (essentially irreplaceable) people increasingly difficult, and the demands on the remaining workers have constantly risen. As a result, the company had little room to maneuver, which it should consider a serious risk. As the process IT manager said:

> *For instance, just before coming here I spoke to the manager of another division here at P&P. One of my guys has put in for a transfer within the organization, with better hours and less time on call. So, this other manager, under whom my guy will work, asked me when I'm willing to let the transfer go through. Truthfully, I'd say "in about two years" because that's how long I reckon it will be before we have a fully trained replacement for this guy…. If he leaves in three months, then we have to cancel a major maintenance project, because we can't replace him*.

5.2 Governing Variables and Action Strategies at P&P

Based on the data in Section 5, we analyzed the variables governing the risk practices enacted at P&P. *Continuous production* was a deeply rooted and paramount priority throughout the organization. The company could not halt production even for a few hours without incurring considerable costs, and so 24/7 production took precedence when a conflict of governing variables arose. Indeed, this precedence manifested in both risk identification and risk assessment in that the process managers deemed risks that did not pose an immediate threat to the production process as secondary, which, for instance, the way in which the company used the planned production stops shows. Efforts to maintain equilibrium dominated the action strategies that the company employed, which one can see in the company's carefully configuring new parts to mimic those it replaced, in the slow rate the company changed the process stations, and in the workforce's inertia in adopting new technology. In order to maintain infrastructural equilibrium and, by extension, continuous production, P&P has focused on tailoring technology to fit its needs rather than moving towards standardization and exploring innovative features that developing new technology offers.

The tailoring approach to technology reveals another governing variable in the organization: the widespread view of IT as a tool. The action strategies that P&P employed would suit mechanical technology (e.g., cog wheels, levers, etc.) that remain stable over time, standardized, and exchangeable in ways that infrastructural IT cannot match. One can also see the *tool view of technology* as a governing variable in P&P management's approach to investments in infrastructure technologies. The way that the company chose to deal with infrastructural heterogeneity risks shows that this view permeated the whole

organization and not only upper management. In downplaying IT's infrastructural characteristics and features via isolating different infrastructure parts as a strategy to maintain equilibrium, P&P in effect more widely diffused risk through an increased idiosyncrasy and heterogeneity of the installed base.

In order to maintain continuous production and equilibrium in an increasingly interconnected, integrated, and heterogeneous infrastructure, P&P focused on *establishing control* of the resources it needed to do so. To minimize the number of unexpected consequences and cope with breakdowns swiftly, the company chose to develop and keep relevant knowledge in house. Due to this strategy, the company has successfully accomplished (for instance) large-scale maintenance and system replacement projects, but it has also resulted in the company's depending on key individuals with deep, situated knowledge about its idiosyncrasies. At the same time, P&P heavily relied on the experience, knowledge, and collaboration of its homogeneous workforce to successfully manage day-to-day threats to its production process. To keep the highly integrated production process running, operators, maintenance personnel, and technicians shared knowledge, information, and control to coordinate responses to disturbances throughout the process chain. This action strategy suggests that the company recognized the importance of its workers' situated knowledge and reflective skills. However, since a changing of the guard loomed for P&P as we mention in Section 5, the company has yet to resolve how it will transfer knowledge.

Table 3. Action Strategies and Governing Variables

	Risk	Action strategies	Governing variables
Technology	Systems longevity	Software/hardware configuration to mimic the old	Infrastructure equilibrium Continuous production Long-term investments
	Spare parts shortage	Harvest parts	Continuous production In-house control
	Infrastructure heterogeneity	Isolation of functionality and other potential threats	Infrastructure equilibrium Short-term production goals
	Path dependency	In-house knowledge	Tailored technology
	Vendor relationship	Buyer/seller	Tailored technology
Support/ maintenance	Support availability	In-house knowledge	Self-sufficient/control
		Prioritizes Production Testing, testing, testing	Continuous production
Knowledge	Increased dependency on process representations	Customize Depend on senses and knowledge	
	Process integration	Adaptive collaboration	Continuous production
	Knowledge transfer	Practice/informal	
	Changing of the guard	None	Industrialism (exchangeable)
	Dependence on key individuals	Case to case/none	Continuous production
	(Management) view of IT	Ad hoc argumentation	Conservatism

As Table 3 shows, we recognize that one may answer our research question (i.e., How is risk managed by practitioners in the context of IT-enabled process management?) in multiple ways since both the risks and their management influence and are influenced by numerous factors that interact in a complex, dynamic techno-social environment. Thus, we consider it impossible to unequivocally state the most important factor (or combination of factors), to rank the identified risks (which may shift as the context changes), to identify the times and points when an emergent risk may perturb the equilibrium and compel P&P, or to identify any other process in a similar situation. Nonetheless, recognizing the possible complexities can help warn organizations to fully consider their IT risk management options.

6 Discussion

Drawing on Argyris and Schön (1974), we analyze the governing variables, action strategies, and consequences of risk management processes at multiple levels of P&P as enacted in day-to-day process management. Any given situation involves various governing variables (Argyris & Schön, 1974), and the number of diverse action strategies tends to increase with the number of actors involved. At P&P, the actors shared a common overriding goal to maintain continuous production but differed in their needs and ideas regarding the optimal means to address specific problems; all of their actions involved a tradeoff between competing governing variables. From identifying the governing values, we could better understand the observed risk management practice since it explained how the involved actors identified the possibilities of unwanted outcomes related to process goals and, subsequently, planned and acted to avoid them. Against this backdrop, in this section, we discuss in detail the governing variables and action strategies we observed, explicate and elaborate on what we call a risk dilemma, and argue how these empirical and conceptual findings may help advance the risk management discourse in IS research.

6.1 The Risk Dilemma

In our analysis, we found that P&P followed risk management practices whose governing variables and action strategies suggested that, by successfully managing short-term threats to ensure it ran its operations 24/7, the company threatened the process configuration's long-term sustainability. Put differently, by successfully managing risks related to its daily operations and organizational processes, the company generated and diffused strategic risks as the IT configuration evolved. Further, although the practitioners at P&P identified these strategic threats, they could not address them without disturbing the continuous 24/7 operations. This situation represents a risk dilemma in which practitioners face two conflicting risks that threaten the same overall goal and attempt to mitigate one reinforce the other. Thus, the observed action strategies paradoxically both successfully achieved and severely threatened the foundational governing variable of continuous production. Although process managers at different levels recognized this dilemma, they could not transform or modify the governing variable because halting production, even for a short time, proved so costly that it could jeopardize the sustainability of the entire organization.

In *The Innovator's Dilemma*, Christensen (1997) demonstrates why organizations fail to invest in requisite disruptive technologies and, consequently, how they become weaker and ultimately fail by continuing to follow established, previously good business practices. As for P&P, it acted rationally and in accordance with sound business practices. When halting production incurs such high costs, continuous production as a primary governing variable constitutes a financially rational practice. In addition, P&P's customer base made no demand that the company change its modes of operation; thus, it had no incentive of this kind to make the investments it needed to reconfigure its operations in order to mitigate strategic risks. Furthermore, because management and practitioners had a tool view of technology, they struggled to appreciate the potential strategic advantages that advanced infrastructural technology offered. As a result, the company's decision to mitigate risks that directly threatened its organizational operations rather than to mitigate strategic risks constituted a highly rational choice. Looking at extant IS literature on risk, we know that, with high levels of uncertainty and complexity, risk managers seldom have sufficient knowledge of risk factors (Barki et al., 2001; Mathiassen & Stage, 1992) and that they sometimes make irrational decisions (Lauer, 1996; March & Shapira, 1987). In our case, however, despite sources of uncertainty and a high degree of complexity, the practitioners identified important risks and displayed fully rational behavior; however, they still ended up in a risk dilemma that they could not resolve with increased planning and oversight.

6.2 A Practice-based View of Risk

The core idea that one can mitigate risk, once properly identified, with appropriate risk management techniques has hitherto dominated research in the field. With few exceptions, risk research has focused on either predicting risk (risk factor research) (Aloini et al., 2007; Keil et al., 2002; Smith et al., 2001; Taylor, 2006) or prescribing methods to manage it (risk management research and contingency approaches) (Ahn & Scudlark, 2002; Birch & McEvoy, 1992; Charette, 1989; Heemstra & Kusters, 1996; Kumar, 2002; Lyytinen et al., 1998). In contrast, we focused on uncovering and understanding how practitioners produce and manage in the context of IT-enabled process management by examining organizing's micro-dynamics.

A practice-based view highlights the relative nature of risks by assuming that they emerge from the interactions between actors and their practices, situated goals, and knowledge (Feldman & Orlikowski, 2011; Orlikowski, 2002). Thus, the practice-based view recognizes a pragmatic aspect of risk where what constitutes risk for one actor or practice might represent an opportunity for another (Carlile, 2002). As such, it recognizes that multiple interacting and possibly conflicting risks may arise in any given situation. In other words, actors and practices always have a stake in naming and framing (Schön, 1983) risks. Consequently, the practice-based view helps explain how actors may continually fail to identify possibly risky situations if they emerge outside or between practices. This view of risk may be particularly relevant in contexts where logics conflict (Feldman & Orlikowski, 2011). A practice-based view also supports and helps explain Drake and Byrd's (2006) findings from synthesizing research in strategic information systems planning: they found how IT portfolio risk increases when complex dependencies between projects exist and how risk will decrease due to increased knowledge sharing. In the third and final cycle of their action research study, Ou Yang, Hsu, Sarker, and Lee (2017) adopt a practice approach to operational risk in a financial institution in order to address its problems and, thus, show the usefulness of a practice approach to risk and risk management issues beyond our particular context.

One can view risk resolution as a particular form of problem solving. Building on the idea of reflection in action (Schön, 1983), a practice-based view highlights how, by resolving risks, individuals trigger situated learning activities in and across practices in order to adapt to a given situation's particularities (Feldman & Orlikowski, 2011). Through reflective conversations with the situation, practitioners address risks in a way that is shaped by and adapted to the situation at hand. For instance, we found how practitioners across P&P's production process collaborated in order to avoid halting production when a problem occurred somewhere in the factory.

From a practice-based perspective, practitioners primarily make sense of risks not by following risk management methods but by framing risks in conjunction with ongoing negotiation and learning (Orlikowski, 2002). Accordingly, in our case study, we observed close collaboration between operators, the IT manager, the process IT manager, and the maintenance and projects manager to identify, negotiate, and assess risks. The way maintenance personnel worked also illustrates the importance of networking in and between teams in framing risks.

Furthermore, from a practice-based perspective, all practitioners (not only formally appointed risk managers) are understood to perform risk management as part of their everyday activities. Practitioners identify risks in relation to their shared (or conflicting) goals, their knowledge, and situated constraints. Risk management is invested in practice (Carlile, 2002) since it focuses on helping practitioners reach their goals and sustain their practice. Therefore, risk management needs to be adaptive in order to sense changes; it must afford practitioners the opportunity to reflect in action (Schön, 1983) and transform knowledge in their practice (Carlile, 2002). For example, we found that P&P's paper machine operators used all of their senses (except taste) when resolving problems and that the maintenance personnel adapted general technical knowledge to specific situations in order to identify and manage risk.

Philosophically, the practice-based perspective assumes a pragmatic ontological stance (Van de Ven, 2007) and views risk as situated, emergent, and socially constructed through practices (Feldman & Orlikowski, 2011). Hence, risk factors and risk management methods—however comprehensive—cannot account for all relevant risks nor necessarily help practitioners manage risk in their everyday work. Thus, research on risk rooted in a practice-based view focuses on theorizing practice (Feldman & Orlikowski, 2011) to increase our understanding of how risk is produced and managed both within and beyond the scope of experts and risk management methods.

We argue that a practice-based view of risk and risk management helps extend research and practice by revealing and explaining how risk is actually produced and managed in contemporary organizing. At P&P, actors identified relevant risks and, in one sense, mitigated them. However, by successfully mitigating process risks, they diffused strategic risk, which threatened the sustainability of the process configuration. Although the actors clearly identified and keenly appreciated these strategic risks, they could not mitigate them without compromising the organization's paramount governing variable. Furthermore, the practitioners and managers made financially rational risk management choices. This risk dilemma illustrates how rational risk management actions may actually lead to an increasingly untenable situation that threatens risk-mitigation efforts.

Concern over discrepancies between theories about what they posit that people do and what people actually do has given rise to the "practice" approach in the management literature (Feldman & Orlikowski,

2011). By viewing knowledge as embedded in practices and actions, knowledge management scholars have begun to focus on how actors share knowledge through a process of transformation, not transfer (Bechky, 2003; Carlile, 2002). Likewise, Orlikowski (2002) argues that, because knowledge inherently depends on embedded practices, the notion of transferring best practices does not make sense. We extend the notion of IT risk management towards a practice-based understanding of risk. Above all, this perspective underscores the importance of learning because new knowledge about specific situations (which often concerns problems or failures (Pisano, 1994)) may arise from dialogue and interaction (Brown & Duguid, 1991; Cook & Brown, 1999).

Thus, in summary, building on a practice-based approach to risk and risk management, we explore the gap in IS research on IT-enabled process risk. In doing so, we create a holistic view on risk (Smith et al., 2001) that we use as a vehicle to answer Carlo et al.'s (2004) call to look beyond the project level and to explain how risks emerge and are contained in larger socio-technical networks. The risk dilemma we identify illustrates the increasingly interactive nature of IT, social contexts, and risk (Hanseth & Ciborra, 2007) and supports the need for researchers and actors to reflect more fully on the dynamics and complexities involved in risk management (Schmidt et al., 2001).

7 Conclusion

In this paper, we investigate risk management in IT-enabled process management. Based on a case study and drawing on concepts adapted from organizational learning theory, we explore the specific governing variables and action strategies involved. We observed a situation in which the effective management of process risk led to the diffusion of strategic risk, which threatened the goal of the process risk management practices. Grounded in this observation, we introduce a practice-based view of risk and risk management as a complementary approach, and we believe that this view significantly advances IT risk management theory in IS research.

References

Ahn, J.-H., & Skudlark, A. (2002). Managing risk in a new telecommunications service development process through a scenario planning approach. *Journal of Information Technology*, *17*, 103-118.

Alhawari, S., Karadsheh, L., Nehari Talet, A., & Mansour, E. (2012). Knowledge-based risk management framework for information technology project. *International Journal of Information Management*, *32*(1), 50-65.

Aloini, D., Dulmin, R., & Mininno, V. (2007). Risk management in ERP project introduction: Review of the literature. *Information & Management*, *44*, 547-567.

Alter, S., & Ginzberg, M. (1978). Managing uncertainty in MIS implementation. *Sloan Management Review*, *20*(1), 23-31.

Aron, R., Clemons, E. K., & Reddi, S. (2005). Just right outsourcing: Understanding and managing risk. *Journal of Management Information Systems*, *22*(2), 37-55.

Argyris, M., & Schön, D. (1974). *Theory in practice: Increasing professional effectiveness*. San Francisco, CA: Jossey-Bass.

Aubert, B. A., Patry, M., & Rivard, S. (2005). A framework for information technology outsourcing risk management. *The DATABASE for Advances in Information Systems*, *36*(4), 9-28.

Bahli, B., & Rivard, S. (2003). The information technology outsourcing risk: A transaction cost and agency theory-based perspective. *Journal of Information Technology*, *18*(3), 211-221.

Bannerman, P. L. (2008). Risk and risk management in software projects: A reassessment. *The Journal of Systems and Software*, *81*(12), 2118-2133.

Barki, H., Rivard, S., & Talbot, J. (1993). Toward an assessment of software development risk. *Journal of Management Information Systems*, *10*(2), 203-225.

Barki, H., Rivard, S., & Talbot, J. (2001). An integrative contingency model of software project risk management. *Journal of Management Information Systems*, *17*(4), 37-69.

Bechky, B. A. (2003). Sharing meaning across occupational communities: The transformation of understanding on a production floor. *Organization Science*, *14*(3), 312-330.

Beck, U. (1992). *Risk society: Towards a new modernity* (vol. 17). Thousand Oaks, CA: Sage.

Birch, D. G. W., & McEvoy, N. A. (1992). Risk analysis for information systems. *Journal of Information Technology*, *7*, 44-53.

Blechar, J., & Hanseth, O. (2007). From risk management to “organized irresponsibility”? Risks and risk management in the mobile telecom sector. In O. Hanseth & C. Ciborra (Eds.), *Risks, complexity and ICT*. Cheltenham, UK: Edward Elgar Publishing.

Boehm, B. W. (1973). Software and its impact: A quantitative assessment. *Datamation*, *19*(5), 48-59.

Boehm, B. W. (1989). *Software risk management*. Los Alamitos, CA: IEEE Computer Society Press.

Boehm, B. W. (1991). *Software risk management*: Principles and practices. *IEEE Software, 8*(1), 32-41.

Bradbury, J. A. (1989). The policy implications of differing concepts of risk. *Science, Technology & Human Values*, *14*(4), 380-399.

Brown, J. S., & Duguid, P. (1991). Organizational learning and communities-of-practice: Toward a unified view of working, learning, and innovation. *Organization Science*, *2*(1), 40-57.

Carlile, P. R. (2002). A pragmatic view of knowledge and boundaries: Boundary objects in new product development. *Organization Science*, *13*(4), 422-455.

Carlo, J. L., Lyytinen, K., & Boland, R. J., Jr. (2004). Systemic risk, IT artifacts, and high reliability organizations: A case of constructing a radical architecture. *Sprouts: Working Paper on Information Environments, Systems and Organizations*, *4*(4).

Carr, N. G. (2003). IT? Does it matter? *Network Magazine*, *18*(7), 6.

.

Charette, R. N. (1989). Software engineering risk analysis and management. New York, NY: McGraw-Hill.

Chatzoglou, P. D., & Diamantidis, A. D. (2009). IT/IS implementation risks and their impact on firm performance. *International Journal of Information Management*, *29*(2), 119-128.

Christensen, C. M. (1997). The innovator's dilemma: When new technologies cause great firms to fail. Boston, MA: Harvard Business School Publishing.

Ciborra, C. (2004). *Digital technologies and the duality of risk.* London, UK: London School of Economics.

Clemons, E. K., & Weber, B. W. (1990). Strategic information technology investments: Guidelines for decision making. *Journal of Management Information Systems*, *7*(2), 9-28.

Cook, S. D. N., & Brown, J. S. (1999). Bridging epistemologies: The generative dance between organizational knowledge and organizational knowing. *Organization Science*, *10*(4), 381-400.

Cremonini, M., & Nizovtsev, D. (2009). Risks and benefits of signaling information system characteristics to strategic attackers. *Journal of Management Information Systems*, *26*(3), 241-274.

Currie, W. L. (1998). Using multiple suppliers to mitigate the risk of IT outsourcing at ICI and Wessex Water. *Journal of Information Technology*, *13*(3), 169-180.

Davis, G. (1982). Strategies for information requirements determination. *IBM Systems Journal*, *21*(1), 4-30.

Dhillon, G., & Backhouse, J. (1996). Risks in the use of information technology within organizations. *International Journal of Information Management*, *16*(1), 65-74.

Drake, J. R., & Byrd, T. A. (2006). Risk in information technology project portfolio management. *Journal of Information Technology Theory and Application*, *8*(3), 1-11.

Drummond, H. (1996). The politics of risk: Trials and tribulations of the Taurus project. *Journal of Information Technology*, *11*, 347-357.

Fazlollahi, B., & Tanniru, M. R. (1991). Selecting a requirement determination methodology-contingency approach revisited. *Information & Management*, *21*(5), 291-303.

Fairley, R. E., & Willshire, M. J. (2003). Why the Vasa sank: 10 problems and some antidotes for software projects. IEEE Software, *20*(2), 18-25.

Feldman, M. S., & Orlikowski, W. J. (2011). Theorizing practice and practicing theory. *Organization Science*, *22*(5), 1240-1253.

Gregor, S. (2006). *The nature of theory in information systems*. MIS Quarterly, 30(3), 611-642.

Hakim, A., & Hakim, H. (2010). A practical model on controlling the ERP implementation risks. *Information Systems*, *35*, 204-214.

Hanseth, O., & Braa, K. (2000). Globalization and "risk society". In C. U. Ciborra, K. Braa, A. Cordelia, B. Dahlbom, A. Failla, O. Hanseth, V. Hepso, J. Ljungberg, E. Monteiro, & K. A. Simon (Eds.), From control to drift: The dynamics of corporate information infrastructures (pp. 41-55). Oxford, K: Oxford University Press.

Hanseth, O., & Ciborra, C. (2007). Risk, complexity and ICT. Cheltenham, UK: Edward Elgar Publishing.

Heemstra, F. J., & Kusters, R. J. (1996). Dealing with risk: A practical approach. *Journal of Information Technology*, *11,* 333-346.

Holmström, J., & Sawyer, S. (2011). Requirements engineering blinders: Exploring information systems developers' black-boxing of the emergent character of requirements. *European Journal of Information Systems*, *20*(1), 34-47.

Hu, D., Zhao, J. L., Hua, Z., & Wong, M. C. (2012). Network-based modeling and analysis of systemic risk in banking systems. *MIS Quarterly*, 1269-1291.

Huang, S.-M., Chang, I.-C., Li, S.-H., & Lin, M.-T. (2004). Assessing risk in ERP projects: Identify and prioritize the factors. *Industrial Management & Data Systems*, *104*(8), 681-688.

International Standards Office. (2009). *ISO 31000:2009: Risk management—principles and guidelines* (1st ed.). Geneva.

Iversen, J., Mathiassen, L., & Nielsen, P. T. (2004). Managing risks in software process improvement: An action research approach. *MIS Quarterly*, *28*(3), 395-433.

Keil, M., & Robey, D. (1999). Turning around troubled software projects: An exploratory study of the de-escalation of commitment to failing courses of action. *Journal of Management Information Systems*, *15*(4), 63-87.

Keil, M., Tiwana, A., & Bush, A. (2002). Reconciling user and project manager perceptions of IT project risk: A Delphi study. *Information Systems Journal*, *12*(2), 103-119.

Kumar, R. L. (2002). Managing risks in IT projects: An options perspective. *Information & Management*, *40,* 63-74.

Lauer, T. W. (1996). Software project managers' risk preferences. *Journal of Information Technology*, *11*(4), 287-295.

Leonardi, P. M., & Barley, S. R. (2010). What's under construction here? Social action, materiality, and power in constructivist studies of technology and organizing. *The Academy of Management Annals, 4*(1), 1-51.

Lyytinen, K., Mathiassen, L., & Ropponen, J. (1996). A framework for software risk management. *Journal of Information Technology*, *11*(4), 275-285.

Lyytinen, K., Mathiassen, L., & Ropponen, J. (1998). Attention shaping and software risk—a categorical analysis of four classical risk management approaches. *Information Systems Research*, *9*(3), 233-255.

Massingham, P. (2010). Knowledge risk management: a framework. *Journal of Knowledge Management*, *14*(3), 464-485.

Mason, J. (2002). *Qualitative researching* (vol. 2). Thousand Oaks, CA: Sage.

Marabelli, M., & Newell, S. (2012). Knowledge risks in organizational networks: The practice perspective. *Journal of Strategic Information Systems*, *21*(1), 18-30.

March, J., G., & Shapira, Z. (1987). Managerial perspectives on risk and risk taking. *Management Science*, *33*(11), 1404-1418.

Markus, L. M., & Mao, J.-Y. (2004). Participation in development and implementation—updating an old, tired concept for today's IS context. *Journal of the Association for Information Systems*, *5*(11), 514-544.

Mathiassen, L., & Stage, J. (1992). The principle of limited reduction. *Information Technology & People*, *6*(2), 161-179.

Mathiassen, L., & Purao, S. (2002). Educating reflective systems developers. *Information Systems Journal*, *12*(2), 81-102.

Mathiassen, L., Tuunanen, T., Saarinen, T., & Rossi, M. (2007). A contingency model for requirements development. *Journal of the Association for Information Systems*, *8*(11), 569-597.

McFarlan, F. W. (1981). Portfolio approach to information systems. *Harvard Business Review*, *59*(5)*,* 142-150.

Moynihan, T. (1996). An inventory of personal constructs for information systems project risk researchers. *Journal of Information Technology*, *11*, 359-371.

Nakatsu, R. T., & Iacovou, C. L. (2009). A comparative study of important risk factors involved in offshore and domestic outsourcing of software development projects: A two-panel Delphi study. *Information & Management*, *46,* 57-68.

Mumford, E. (1996). Risky ideas in the risk society. *Journal of Information Technology*, *11*, 321-331.

Orlikowski, W. J. (2000). Using technology and constituting structures: A practice lens for studying technology in organizations. *Organization Science*, *11*(4), 402-428.

Orlikowski, W. J., & Stephen R. (2001). Technology and institutions: What can research on information technology and research on organizations learn from each other? *MIS Quarterly*, *25*(2), 145-165.

Orlikowski, W. J. (2002). Knowing in practice: Enacting a collective capability in distributed organizing. *Organization Science*, *13*(3), 249-273.

Orlikowski, W. (2006). Material knowing: The scaffolding of human knowledgeability. *European Journal of Information Systems*, *15*(5), 460-466.

Orlikowski, W. (2007). Sociomaterial practices: Exploring technology at work. *Organization Studies*, *28*(9), 1435-1448.

Otim, S., Dow, K. E., Grover, V., & Wong, J. A. (2012). The impact of information technology investments on downside risk of the firm: Alternative measurement of the business value of IT. *Journal of Management Information Systems*, *29*(1), 159-193.

Ou Yang, S., Hsu, C., Sarker, S., & Lee, A. S. (2017). Enabling effective operational risk management in a financial institution: An action research study. *Journal of Management Information Systems*, *34*(3), 727-753.

Persson, J. S., Mathiassen, L., Boeg, J., Stenskrog Madsen, T., & Steinson, F. (2009). Managing risks in distributed software projects: An integrative framework. *IEEE Transactions of Engineering Management*, *56*(3), 508-532.

Pisano G. (1994). Knowledge, integration, and the locus of learning: An empirical analysis of process development. *Strategic Management Journal*, *15*(3), 85-101.

Pohlmann, T. (2003). How companies govern their IT spending. Cambridge, MA: Forrester Research.

Renn, O. (1998). Three decades of risk research: Accomplishments and new challenges. *Journal of Risk Research*, *1*(1), 46-71.

Ropponen, J., & Lyytinen, K. (2000). Components of software development risk: How to address them? A project manager survey. *IEEE Transactions on Software Engineering*, *26*(2), 98-112.

Rönnbäck, L., Holmström, J., & Hanseth, O. (2007). IT-adaptation challenges in the process industry: An exploratory case study. *Industrial Management and Data Systems*, *107*(9), 1276-1289.

Schmidt, R., Lyytinen, K., Keil, M., & Cule, P. (2001). Identifying software project risks: An international Delphi study. *Journal of Management Information Systems*, *17*(4), 5-36.

Schramm, W. (1971). *Notes on case studies of instructional media projects* (working paper). Washington, DC: The Academy for Educational Development.

Schön, D. A. (1983). *The reflective practitioner: How professionals think in action*. New York, NY: Basic Books.

Schultze, U., & Orlikowski, W. J. (2004). A practice perspective on technology-mediated network relations: The use of Internet-based self-serve technologies. *Information Systems Research*, *15*(1), 87-106.

Scott, S., & Perry, N. (2009). The enactment of risk categories: The role of information systems in organizing and re-organizing risk management practices in the energy industry. *Information Systems Frontiers*, *14*(2), 125-141.

Smith, H. A., McKeen, J. D., & Staples, D. S. (2001). Risk management in information systems: Problems and potentials. *Communications of the Association for Information Systems*, 7, 5-36.

Standish Group. (2011). *CHAOS manifesto: The laws of CHAOS and the CHAOS 100 best PM practices*. Boston, MA.

Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research*, *1*(3), 255-276.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*, *22*(4), 441-469.

Sumner, M. (2000). Risk factors in enterprise-wide/ERP projects. *Journal of Information Technology*, *15,* 317-327.

Taylor, H. (2006). Critical risks in outsourced IT projects: The intractable and the unforeseen. *Communications of the ACM*, *49*(11), 75-79.

Taylor, H., Artman, E., & Woelfer, J. P. (2012). Information technology project risk management: Bridging the gap between research and practice. *Journal of Information Technology*, *27* 17-34.

Tilson, D., Lyytinen, K., & Sorensen, C. (2010). Digital infrastructure: The missing research agenda. *Information Systems Research*, *21*(4), 748-759.

Tesch, D., Kloppenborg, T. J., & Frolick, M. N. (2007). IT project factors: The project management professionals perspective. *Journal of Computer Information Systems*, *47*(4), 61-69.

Van de Ven, A. (2007). *Engaged scholarship: A case for organizational and social research*. Oxford, UK: Oxford University Press.

Vitale, M. R. (1986). The growing risks of information systems success. *MIS Quarterly*, *10*(4), 327-334.

Wagner, E., Newell, S., & Piccoli, G. (2010). Understanding project survival in an ES environment: A sociomaterial practice perspective. *Journal of the Association for Information Systems*, *11*(5), 276-297.

Walsham, G. (1995). Interpretative case studies in IS research: Nature and methods. *European Journal of Information Systems*, *4*, 74-81.

Wright, S., & Wright, A. M. (2002). Information system assurance for enterprise resource planning systems: Unique risk considerations. *Journal of Information Systems*, *16,* 99-113

About the Authors

Lars Öbrand is an Associate Professor in Infomatics at Umeå University, and part of the Swedish Center for Digital Innovation. His research focuses on issues related to risk in the broader area of IT managment and organizational change processes. He is a senior lecturer with extensive teaching experience covering a wide range of topics and levels. His research has been published in journals and conferences such as Information Systems Journal, Industrial Management and Data Systems, Technology in Society, Hawaii International Confrerence on System Sciences, European Conference of Information Systems, and European Group for Organizational Studies.

Jonny Holmström is a Professor of Informatics at Umeå University and director and co-founder of Swedish Center for Digital Innovation. He writes, consults and speaks on topics such as IT management, digital innovation, digital strategy, digital entrepreneurship, and strategies for leveraging value from digitalization. His work has appeared in journals such as Communications of the AIS, Convergence, Design Issues, European Journal of Information Systems, Information and Organization, Information Systems Journal, Information Technology and People, Journal of the AIS, Journal of Strategic Information Systems, Research Policy, and The Information Society. He currently serves as senior editor for Information and Organization.

Lars Mathiassen is Georgia Research Alliance Eminent Scholar, Professor at the Computer Information Systems Department, and cofounder of the Center for Process Innovation at Georgia State University. His research focuses on development of software and information services, on IT-enabled innovation of business processes. He has published extensively in major information systems and software engineering journals and has coauthored several books. He has served as senior editor for MIS Quarterly, and serves as senior editor for Information and Organization and for the Journal of Information Technology.