Technology in Society 53 (2018) 1–8

Contents lists available at ScienceDirect

Technology in Society

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

Navigating Rumsfeld's quadrants: A performative perspective on IT risk management

Lars Öbrand [a, *], Jonny Holmström [a], Mike Newman [b]

[a] Umeå University, 901 87 Umeå, Sweden
[b] Alliance Manchester Business School, The University of Manchester & Turku School of Economics, The University of Turku, Finland

ARTICLE INFO

Article history:
Received 4 November 2015
Received in revised form
15 September 2017
Accepted 27 September 2017
Available online 29 September 2017

Keywords:
Risk
Digital technologies
Practice
Case study

ABSTRACT

In this paper, we contribute to risk management theory by investigating the internal dynamics of IT risks in contemporary organizations. We explore how digitization of previously physical organizational contexts trigger risk by conceptualizing risk management from a performative perspective and the assumption that risks are sociomaterial by nature. Through an exploratory case study of the risk management practices at a paper and pulp factory, we analyze the different epistemic strategies employed by the practitioners as proactive, reactive and adaptive. We discuss how and why these strategies emerge as a result of the sociomaterial configurations.

> " *... as we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – the ones we don't know we don't know. And if one looks throughout the history of our country and other free countries, it is the latter category that tend to be the difficult ones*"
>
> Donald Rumsfeld, US Secretary of Defence at a press briefing 2002 [42]

1. Introduction

Digital technologies in contemporary organizations challenge established organizational practices in all aspects of organizational life. Information technology is also a source of new kinds of risk in organizations, and where traditional management measures fail to mitigate or control the risks, the opposite tends to occur [45]. Concepts such as "technological society", "infor society", "risk society", "postindustrial society" and "knowledge society" suggest a common understanding that contemporary western societies are ruled by knowledge and expertise ([20]: 27). Risk is a key concern for today's society, no matter what label we chose, and they are increasingly pervasive as all facets of society become increasingly armed with expansive digital capabilities.

Despite the growing research on IT risk management, it remains unclear under what conditions IT risks emerge and why they emerge. In particular, we know little about the effects of digitizing previously physical contexts. In such highly digitized and sociomaterial contexts risk managers need to pay attention to multiple domains such as devices, networks, contents, and services thus increasing the complexity and diversity of their task (cf [44]). Moreover, as Yoo et al. [44] note, the inherent properties of digital technology challenge traditional organizing logics that underlie manufacturing of physical products which all assume hierarchically organized modular product structures. In other words, IT risk management as we know it is challenged due to the increased digitization of production processes.

Today's risk management methods are are rife with risk checklists, and techniques and tools to manage them. Frameworks and checklists to identify risks related to IT issues are plentiful as are suggestions on how to mitigate them. A survey of extant literature on IT risk shows how it allows for a proactive approach to, for example, IT development projects. These approaches have had considerable, and positive, effect on typical risks related to IT issues. However, despite our best efforts, risks seem to emerge outside the scope of our carefully constructed and comprehensive checklists.

* Corresponding author.
E-mail address: lars.obrand@umu.se (L. Öbrand).

https://doi.org/10.1016/j.techsoc.2017.09.009
0160-791X/

Although given as a response on the lack of evidence of weapons of mass destruction in Iraq, in his statement the then U.S. Secretary of Defence Donald Rumsfeld articulated a key aspect of the relationship between knowledge and reality. If we cannot imagine a potential outcome, we cannot take actions aimed at influencing it. As such, Rumsfeld's statement highlights a core aspect of risk and risk management – our ability to imagine what might possibly happen. We can easily understand risk checklists as populating the known-known quadrant of a Rumsfeldian matrix, but as he notes, the unknown-unknown quadrant tends to yield more difficult problems.

In this paper we propose to explore why new and difficult risks continue to emerge, and how research on risk can be extended beyond its current status to better explain and manage emergent risks. Drawing on the growing literature on the role of practice in understanding organizational change, we propose that extant literature on risk within IS could be conceptualized as mainly focusing on ostensive aspects of risk management – i.e. the ideal or schematic form – and largely ignoring the performative aspects of it [14].

To investigate performative aspects of risk management, we have conducted an exploratory study at P&P, a paper and pulp factory. By combining observations with qualitative interviews and a workshop we aimed at uncovering relevant aspects of the risk management in the day-to-day operations of the paper and pulp factory. The risk management strategies, patterns of practices drawn on by practitioners to act, employed in the factory are characterized as reactive, proactive and adaptive to denote the different configurations of risk identification and risk resolution employed by the practitioners.

2. IT risk management

Looking at the extant IS research on risk it is clear that there is a rich discourse on risks related to software development projects [1,7,17,27,29,40,46,47]. The high rate of systems development project failure [48,49] has been, and still is, one of the central risks associated with IS practice [41].

Lyytinen et al. [27] conducted an extensive overview of different risk management approaches dealing with four areas of software development project risks; software risks, implementation risks, project portfolio risks, and requirement risks. Each of these categories now encompass a richness of theories, tactics and views of risk and risk management, from technical approaches focusing on risks related to the hard- and software (e.g. Ref. [7]), to managerial approaches focusing on risk management processes and behavioural aspects (e.g. Refs. [28,50]). The levels of analysis range from the project (e.g. [51]) to the organization (e.g. Ref. [12]) and includes the inter-organizational, especially in terms of research on outsourcing risks (e.g. Refs. [3,5,4,52]). Other areas of concern in IS risk research are ERP risks [16,53–56], and security risks [21,38,39,57,58].

As is evident in this rich stream of research, there are a multitude of variations on risk definitions, but at its core risk is a matter of an "effect of uncertainty on objectives" (ISO 31000). Risk is thus very much a matter of perspective, where the very thing that constitutes a risk for one actor can be an opportunity for another, and simply not matter for a third. Risk management, then, connotes "the coordinated activities to direct and control an organization with regard to risk" (ISO 31000). As the first necessary step in risk management is to identify the something that could occur as a something that could have an (adverse) effect on a desired outcome or activity. The aim and knowledge of the one enacting risk management thus becomes pivotal. The next steps are to assess and prioritize the identified risk, followed by a plan of action to deal with it and finally feeding back to the initial identification of the risk in order to revise the initial framing of the risk if necessary.

Risk, and risk management, is thus closely related to knowledge. First, knowledge form the basis for identifying something as a risk. Second, knowledge govern possible options for risk resolution. In this respect, risk management can be regarded as inherently proactive, as it builds on the idea that risks need first to be identified (as something in the future posing a threat). However, in practice, the risk management loop is not always completed, and the time between identifying a risk and taking further action can vary significantly. In all steps of the risk management loop, knowledge is key; it guides the identification of risk (in relation to the aims), and creates the conditions for (but does not govern) how these can be addressed.

To date, extant research has paid scant attention to questions such as how IT risks emerge in the wake of digitization – the merger of physical and digital components. In spite of it's richness, Lyytinen et al. [27] argue that it is weakly grounded in theory and that most research efforts focus exclusively on predefined sets of risks. There is also a clear bias towards research on risks in relation to software development projects even though IT-related risks now extends far beyond these [59]. These views are shared by Ciborra [60], who further argues that risk research tend to black box the dynamics of IT-related risk through "excessive fixation on notions of control and equilibrium".

In fairness, both research on and the practice of risk management has been both important and significantly successful in managing a large number of risks related to the use of information technology. Today, through the use of IT risk management models, we avoid or manage many of the critical and commonly found risks with which we have previously struggled. However, for every new successful risk mitigations, new risks seem to emerge and our models, techniques and tools continue to fall just a little bit short of the mark. After roughly 40 years of research, we propose to explore a different perspective to see if it could complement extant research in a useful way. Against this backdrop, we propose an analysis of the risk research in our field as focusing largely on the ostensive aspect of risk management – i.e. the idealized or schematic form of the process. In this paper we instead argue for exploring the internal dynamics of IT risks by conceptualizing IT risk management from a performative perspective [14,34] which captures the "real actions, by real people, in specific times and places" ([15]: 302). We approach the study of IT risk management in a process industry plant from a performative perspective building on the assumption that risks are socially constructed [10] and sociomaterial by nature [25,33] and build our work on the proposition that some risks are emergent over time. We propose to address these dynamics by investigating the performative aspects of risk management as it is played out in the context of organizations.

3. A performative perspective

It has been demonstrated within the practice-based perspective on information systems, that technology create the conditions for – and does not govern – people's encounters with technology [8,32,61]. Technology allows "interpretive flexibility", implying that "for different social groups, the artifact presents itself as essentially different artifacts" ([6]; p.76). Orlikowski ([62], p.412) underscores the discretion of the user as "every encounter with technology is temporally and contextually provisional, and thus there is, in every use, always the possibility of a different structure being enacted".

The concept of practice has been introduced to solve at least two related theoretical problems. First, it has been used to transcend the limitations of a representational concept of knowledge and the

realist epistemology behind it. Second, it has been introduced as a reaction against social constructivism and to re-establish the significance of material artifacts in the study of human behaviour. In this paper, we draw on the Reckwitz ([63]: 249) definition of practice as "*routinized types of behviour which consist of several elements, interconnected to one another: forms of bodily activities, forms of mental activities, 'things' and their use, a background knowledge in the form of understanding, know-how, states of emotion and motivational knowledge*". Additionally, we position ourselves in line with works that take a practice-based approach on organizing (e.g. Refs. [14,64]) which emphasize how specific and situated actions, interactions, and negotiations shape and re-shape organizations through the enactment of strategy by practitioners. As such, a performative approach to risk management is can be defined as socially constructed through the actions of multiple actors and the situated practices they draw upon.

4. Case setting and method of analysis

4.1. Research setting

This paper reports on a qualitative study conducted at one of Europe's largest producers of kraftliner, a kind of paper used to manufacture high quality corrucated packaging. The P&P factory is located in Sweden and employs some 600 people, of whom approximately 200 are shiftworkers. The factory receives the raw materials, timber and recycled paper, which in turn are processed into first pulp then kraftliner to be shipped to P&P's customers, mainly across Europe.

The role of information technology in the plant has evolved continuously since the 1980's and today its presence is substantially ubiquitous. Every process concerning the production of kraftliner is today supported by IT, and the IT infrastructure at the factory is characterized by a high degree of integration between components and systems. There are two separate departments at the plant dealing with the use of IT: the IT department and the Process IT department. Simply put, the Process IT department focus on technologies and systems in use at the actual mill, including control systems, process stations, field units and remote sensors. The IT department is in charge of information technology use in the administrative processes such as business systems and EDI standards. The increased interconnectivity of systems at the plant means that the borders between the two departments are not always clear cut.

4.2. Data collection

As this aim of this study is to performative aspects of risk management as they are played out in the day-to-day operations of P & P, we designed the study in such a way that a useful number of different practitioners would be included. In order to generate relevant data concerning practices and practitioners, we chose to make observations, conduct qualitative interviews and to organise a workshop.

In order to generate an initial sense of praxis a total of 5 h of unstructured observations were carried out in the factory setting. This helped in the task of identifying practitioners that performed risk identification and risk resolution in the course of their day-to-day work. It was also instrumental in the work with preparing the thematic interviews, as situated knowledge is an important factor in being able to navigate the dynamics of the interview situations. The observations were carried out by the first author in different settings at the factory, following the production process from one end of the factory to the other.

In order to explore the risk management practices at the factory, and drawing on the idea that the practitioners themselves are the best source of knowledge regarding this, we conducted eleven qualitative interviews. Based on the observations and an initial interview with the IT manager, we identified the following key categories of practitioners at the factory: operators, technicians, maintenance personnel and project managers. Futhermore, the IT manager, the Process IT manager and the manager for Maintenance and Projects were also identified as important data sources as they identified and resolved risk as part of their everyday work. In addition we interviewed a representative from P&P's main IT vendor, ITV, who had intimate knowledge of the operations of P&P as he now worked closely with them on their operational and strategic IT issues – especially relating to potentials for risk resolution. He had previously been employed by P&P as a member of their IT department. Each interview followed a thematic interview guide how the main risks identified by the practitioners, how risk was identified and resolved by them.

The interviews were digitally recorded and transcribed. The data was coded by the first and second authors, first individually, and then together. The transcribed interviews were coded using ATLAS.ti. The main codes used were: risk; risk identification; risk resolution. For each of these sub-codes were used to identify the practices accessed by the practitioners – e.g. risk resolution was broken down into risk assessment, prioritization, negotiation, alternative resolution option, and decision. For each instance of risk, risk identification and risk resolution, specific circumstances, actors and knowledge (including where knowledge was located and how it was accessed) were coded.

4.3. Data analysis

We organized the coded data according to how risks were identified and resolved. Categories were generated based on identifying patterns of practices drawn on by practitioners in carrying out risk identification and risk resolution. After several iterations by the author team, we convereged on three distinct types of strategies of risk management performed at the factory: proactive; reactive; and adaptive. Proactive strategies are characterized by an priori knowledge of risk, and an accessible system of knowledge throughout the risk resolution process. Reactive strategies encompass early risk identification (based on situated knowledge) in concert with a lack of specific and pre-defined risk resolution options. Adaptive epistemic strategies are employed when both risk identification and risk resolution evolve dynamically and are adapted to the particularities of the situation.

5. Results

5.1. Proactive strategies

5.1.1. Planned maintenance

Continuous production is paramount to P&P as the cost of halting production is very high. This means minimizing stoppage time is an essential aim for the organization. This poses a challenge for conducting maintenance processes. In addition to a monthly one day planned maintenance stop there is a yearly five-day period when larger maintenance and project work that require production stoppage can be conducted. These maintenance windows are minutely planned and only high priority tasks and activities are conducted.

5.1.2. Infrastructure evolution

IT-vendors and the information technology industry develop new tools and systems at an increasing rate, products they want to sell. Spare parts go out of production and stock, education and

support are hard to come by if you use old systems and technologies. P&P strive for control and infrastructural equilibrium and the tactics employed aim at upgrading only when necessary, and making a huge effort in integrating the new part as seamlessly as possible. This often means that new functionality offered by the upgraded part, or system, is not put to use.

> *"Experiments can be carried out on machines which can be at a stand still for five hours without any consequences. Five hours here cost too much"* (Process IT manager)

5.1.3. Knowledge access

The competence needed to conduct maintenance, replacing components and systems or handling unexpected situations are in part to be found at the IT-vendors. In the case of P&P it is very important that people with the right kind of knowledge are located in the vicinity, because the cost of a stand-still is quite high and many problems require that experts are present at the mill. Therefore they have opted to as much as possible keep this kind of competence in the organization.

They cannot cover all bases, so it is important for them to coordinate their efforts with people from their IT-vendors, especially when time is a critical factor. This means that besides from knowing where to turn for help in a certain situation, it is important to establish areas of responsibility between P&P and their vendors.

5.1.4. Hazards and security issues

Falling within the scope of plant risk management, P&P have addressed issues of physical hazards such as flooding or fire in e.g. server rooms, by formulating plans of action in such cases. Data recovery measures in case of, for example, hard drive failures are in place and back-up systems to the most vital components are up an running.

> *"This is something we are very good at. I mean, we have been doing this for a long time now, and we've been on top of these issues for quite a while."* (Process IT manager)

5.2. Reactive strategies

5.2.1. Systems longevity and spare parts

There are a number of IT-based systems in use at the factory, with different life spans – both expected and actual. Discrepancies between the expected and acual life span of a system is a source of risk for P&P. Their process station system is a case in point. There are about 60 Contronic P process stations in use at the factory today, regulating the production process. In terms of functionality and integration in the plant's infrastructure they work well and the practitioners know the system intimately and are satisfied with it. However, Contronic P is no longer on the market and spare parts are not manufactured anymore. The important role of the process stations and the rapidly dwindling stock of P&P's spare parts for Contronic P stations is problematic. As the life expectancy for this system was longer when P&P invested in it, the pace of process station replacement for more modern ones has been moderate - at six per year. Faced with a situation with no available spare parts P&P salvage what they can from the six stations they replace every year, however there is no way of knowing if the salvaged parts will work. In addition, system replacement is constrained by other factors. As the Projects and Mainenance manager puts it:

> "*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 cannot 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 aren't compatible with the old … this is a major risk" …. "and even though we are aware of this, even if we were to get 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[…]Looking at the shorter life span of systems, and the rate at which we are able to replace old ones, before we have replaced all of our Contronic P stations, the new system will be obsolete, and we're back in the same situation again"* (Project and Maintenance manager)

5.2.2. Operational maintenance

As described above, he window of opportunity to perform maintenance is narrow, especially when it concerns testing. Throughout the year maintenance activities primarily focus on ensuring that the production process runs, solving occurring break downs. During this work maintenace personnel identify a large number of issues that they would like to address, but are not critical for continuous production. These issues end up on the "things we should do something about"-list. Items on this list are seldom prioritized enough to warrant a spot on the planned maintenance schedule.

5.2.3. Infrastructure heterogeneity

The heterogeneity and integrated character of P&P's infrastructure is consequential for maintenance and changes as the integration of new components is challenging. Any new parts must be configured to be compatible with what's already in place, whichs e.g. makes a seemingly simple thing like indexing difficult by the sheer volume of items to be indexed. As a consequence, even standardized products are challenging to implement. P&P tends to configure new parts to mimic the one being replaced, regardless of the functionality the new part affords.

> *We cannot afford to experiment. We are supposed to be conservative with regards to functionality because production is what matters"* (Process IT manager).

5.2.4. Knowledge management

An important challenge for P&P is to be found in how they manage the knowledge base. Today, a key factor for managing everyday problems and risks in the production process is the experience and knowledge of the work force. The personnel turnover at P&P has been low and most of them have worked at the factory for over 20 years. They know each other well and work together well, which in many ways is beneficial for P&P. However, it also hampers change. Relationships, attitudes and practices are cemented, often shared and deeply rooted. New perspectives and ideas that challenge the equilibrium can be difficult to implement. When new technology is proposed and implemented there is a tendency to use it the same way as the previous technology.

Within a decade, the bulk of the work force will have been replaced and, lest they want to lose it, P&P needs to find ways to recognize relevant knowledge amongst their employees, and then devise ways of either formalizing it or make it transferable in other ways (e.g. through trainee programs). Some of the knowledge is tacit, making it difficult to spot, let alone formalize.

Looking at the work performed by operators, technicians and maintenance personnel it is clear that they perform complex, demanding tasks that basically corresponds to descriptions of work typically performed by engineers. Recruiting people with the desired skill and not too high demands on wages will also be an issue.

Another risk issue is the dependency on key individuals. The production of kraftliner at the mill has doubled since the mid-eighties but at the same time the number of employees has been reduced by approximately 30%. The demands and responsibilities on operators, technicians etc. grow as layers of middle management are being removed. The foremen were removed from the mill in the nineties, now (in the 2000s) the production planners will disappear. Coupled with the idiosynchracies of the infrastructure, it means that replacing people becomes increasingly difficult, and the demands on those who are available are raised. This certainly narrows P&P's room to maneuver, and should be considered a risk.

> *"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. If I were to answer truthfully I'd say "in about two years", because that's how long I reckon it will 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*"(Process IT manager).

5.2.5. Project timeframes

Under usual circumstances IT projects are often high-cost endeavours. For P&P the costs are even higher as most major IT projects – maintenance or new system implementations – involve extraordinary amounts of testing and planning that goes into ensuring minimal production process disturbances. For these kinds of projects, the timeframe from initial plan to implementation is often in the region of twelve to eighteen months. With any major project, the IT or Process IT department makes an initial plan and then apply for funding from upper management and once the go ahead is given the project can start. Recently, however, the decision from upper management has tended to come later in the process, thus shortening the time available for testing. As a result, testing is not as comprehensive and the risks of unforseen effects higher. In addition, P&P becomes even more dependant on a few key personnel with sufficient knowledge about both the new technology and the intricacies of the installed base.

5.2.6. Path dependency

The pace of technological development has increased since the 80's when the digitalization of the factory began, and the IT market has changed from many smaller vendors to a few dominant ones. IT systems, products and parts are standardized to a much higher degree today, and development and production of hardware, e.g. spare parts, has moved from the IT vendors to third-party operations.

This has been cosequential for P&P as they have quite a few legacy systems as part of their infrastructure, such as Contronic P, that impacts their range of options when it comes to new investments and potential changes. Systems in the 80's tended to be uniqe and tailor made for the organization in question, and as a result P&P's infrastructure is far from standardized and homogenous. As such, it hampers the range of viable options P&P has in terms of implementing new functionality or, indeed, benefiting from shared standards. All changes to the infrastructure need to be carefully adapted and configured to maintain equilibrium, making major changes increasingly difficult and costly. By strategic choice, P&P are tied to one IT vendor, ITV, in order to increase the conditions for long term sustainability of their infrastructure and to secure access to relevant and timely expertise. However, even within the portfolio of a single vendor things tend to change.

> "*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"* (Process IT manager)

Had P&P decided on the other control system within the ITV product family, things would have been rather different. Now they are faced with yet again having to seriously consider changing technological direction, at a large cost: a path dependent consequence.

5.3. Adaptive strategies

Collaborative problem solving is essential for P&P in both detecting and solving problems. The integrated nature of the production process means that the whole process is effected when a breakdown occurs somwhere. Through instant, and often informal, communication, operators at different parts of the process coordinate their actions in order to avoid a complete production stop. Usually, this entails creating buffers and adjusting the speed of e.g. paper machines until the problem is solved and the process can ease back into normal speed. It is made possible by the shared knowledge about the process and it's technologies.

> "*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."* (Paper machine operator)

While operators are stationary at different parts of the factory, technicians work in small mobile teams operating throughout the factory. Moving between their specific assignments for the day, they keep themselves and others updated by checking in with stationary personnel. As such, they also play an important role in maintaing the social bonds that help facilitate the collaborative efforts.

5.3.1. Data representation

The rationale for contemporary control systems is the clear and reliable representation of relevant process data. In addition, it affords decision support in the form of built in warnings and alarms triggered by input from a large number of sensors measuring e.g. temperature changes. As a result, operators work in an environment filled with detailed information about the current status and

trends of the process. Ironically, the level of detail makes it difficult for operators to get a quick overview of the process as a whole. Experienced operators regurlarly use their senses of smell, hearing and touch to assess the process, and as an early warning system to detect slight changes in e.g. how a paper machine is performing. This knowledge is largely tacit and comes as a result of long experience and familiarity with the environment. As such, it is difficult to measure or successfully represent in a control system.

6. Discussion

In the present study, we aimed to uncover perfomative aspects of risk management in the day-to-day operations of the paper and pulp factory. We will next discuss how our findings are corroborated by the current IT risk management literature and, in turn, how our findings enrich it.

We categorized the risk management practices enacted according to the different strategies employed by practitioners at P&P: proactive, reactive, and adaptive.

The *proactive* strategies hinged on the possibility to generate relevant knowledge in advance, both in terms of *a priori* risk identification and the subsequent risk resolution options taken to mitigate these risks. In the case of P&P this implied in-house access to relevant knowledge. The risks are also clearly identified and delimited in scope. By identifying clearly defined risks and regarding them as possible to mitigate with resources and knowledge within the scope of P&P's control this approach was successfully employed to manage certain kinds of risks.

The examination of the risk management practices at P&P revealed that a significant part of these can be characterized as *reactive* in the sense that although risk factors were identified where there were no plans for how to deal with them when and if they became a reality. The management of these risks can be characterized as emergency measures taken 'after the fact.' The resources available for conducting these actions were constrained by the situation at hand. The knowledge needed for the successful management of these risks was limited to what resources could be accessed locally. Our analysis of how the routinized types of behaviour by practitioners showed a lack of communication between functions and levels at P&P as well as a lack of collaboration with outside actors who possessed knowledge and resources relevant for the management of these risks. Common to the risks reactively managed at P&P was a lack of ability to identify and access the knowledge needed.

The third type of strategy uncovered in this case study is *adaptive.* It is characterized by continuous monitoring of the situation, boundary spanning and situated generation of relevant knowledge. As the situation evolved and unfolded, the practitioners carried out a "reflective conversation with the situation" (Schön, 1983), thus continuously generating knowledge. In these practices, the knowledge needed to manage risks was found in different systems of knowledge, both within the organization and outside it. The combination of knowledge to manage risks was typically made up collaboratively, drawing on knowledge across functions, levels and organizational borders.

Local knowledge was found to be necessary for all strategies (particularities, idiosyncrasies), but the need for flexible combinations of knowledge, and the ability to draw on external knowledge increased in relation to the adaptive type. The adaptive type required that new systems of knowledge need to be identified, assessed and accessed. The knowledge needed to manage risks associated with these evolving information infrastructure issues was increasingly found and generated across functions, levels and organizations.

The strategies employed in risk identification depended on whether the risks were known *a priori* or not, i.e. pre-conceivable or emergent risks. The IT-triggered risks became increasingly emergent as the factory went through a digitization process, and as a consequence necessitated adopting adaptivity in the strategies involved in risk identification.

Risk resolution practices were independent of the ones performed in risk identification. They were rather a consequence of the local, social and situated knowledge invested in the practices of P & P. This knowledge was either enough to take to decide on and take risk actions, or it was not. The knowledge was unknown - either in the sense that the practitioners had no readily available way of accessing a sufficient system of knowledge, or in the sense that they did not know which kind of knowledge would allow them to take efficient risk management measures.

Putting together these dimensions or risk identification and risk resolution, we arrive at a matrix depicting four distinct kinds of possible risk management approaches (see Fig 1 below). Adopting the vocabulary of (Deetz, 1996); we refer to these as discourses to highlight the blurred boundaries between them.

Understood like this they reflect the content of Rumsfeld's statement. The proactive discourse concerns the "known-knowns" of risk management. The risks are pre-conceived as are the risk resolution options with which to address them. It is in this discourse we find the literature on risk in IS concerned with establishing checklists and prescribing risk management methods. These have been, and are, instrumental in our efforts to manage the known-knowns of risk. As a result of both research and practice we can see how we today successfully manage risks that were previously difficult to deal with.

The reactive discourse encompasses the "known-unknowns" of risk management, where risks are identified but the risk resolution options are unknown. Risk literature on contingency approaches, as well as literature on emergency actions makes up this discourse. Contingency approaches to risk (e.g. Refs. [2,65]) belong to this discourse despite their focus on adaptive behaviour by risk managers, as the adaptivity in contingency approaches deal with risk identification rather than subsequent risk resolution options. Both these streams of research build on an instrumental notion of risk, where risk – once identified – can be managed by applying risk management heuristics. These approaches have been particurlarly helpful in focusing the attention of practitioners towards contextual factors in e.g. IT projects and to increase the possibility of swift responses once a certain risk can be identified.

Rumsfeld's missing quadrant - The adaptive discourse, the "unknown knowns", concerns situations where risk is emergent, and subsequently dealt with drawing on (internal or external) systems of knowledge accessible at the time. This has to an extent been addressed by the work on risk in information infrastructure

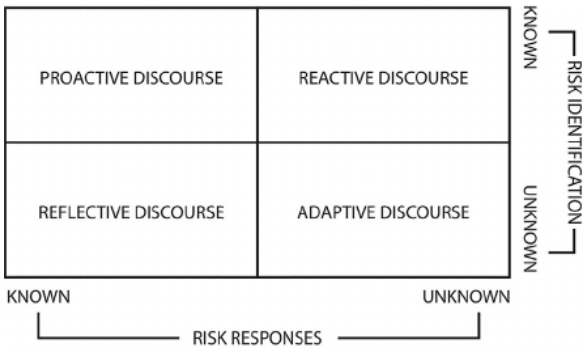

Fig. 1. Risk management discourses.

theory, building on Beck's notion of risk to explore the emergence of risk and side-effects in contemporary organizations. These are situations where sufficient knowledege to deal resolve a risk situation can be accessed within the organization or network, but has it has not been used to identify risk. Our study shows how P & P increasingly draw on these kind of strategies to cope with emergent risks.

The reflexive discourse, the "unknown unknowns" concern situations where both risk identification, and risk resolution options are unknown. To identify and solve these kinds of risks entails reflexivity in terms of the operational aims as well as potentially useful systems of knowledge. This is not covered by extant literature on risk in IS research. Looking at the risks and risk management practices at P & P, we saw a situation where successful management of operational risk generated and diffused strategic risk, as the epistemic strategies in place at P & P are built around in-house access to relevant knowledge systems – which in turn threatened the long term sustainability of their production process configuration.

The figure thus reveals that research on risk in IS research cover the top two discourses, while leaving the bottom two basically untouched. This is problematic as IT-triggered risks are increasingly emergent. Understanding risk management from a practice perspective, then, reveals severe limitations in a checklist approach. The literature on risk and risk management in IS research is heavily biased towards an instrumental view of risk. The checklist approach is an extension of such a view and furthermore builds on the idea that risk can be properly identified and then mitigated with the use of appropriate action strategies. However, as information technology and the use of IT has evolved, new risks appear. Side-effects, unintended consequences and paradoxes increase as the infrastructural character of information technology, and its use, grow stronger. Thus the conditions for risk management changes.

7. Conclusions

In this paper we approached risk management at P&P from a performative perspective, where we explored how risk management strategies – whether they were proactive, reactive, and adaptive – tended to create risks rather than attending to them by addressing IT risks in a very narrow sense. Different types of risk demand different risk management strategies, and what e.g. works for known-knowns will not work for any other type of risk. As such, the discourses identified in this paper are complementary. The sociomaterial nature of technology and increased digitalization seems to lead towards a clear trend of risks becoming increasingly unknown-unknowns and unknown-knowns. Therefore, contemporary organizations need to develop adaptive and reflexive capabilities in order to cope.

References

[1] S. Alter, M. Ginzberg, Managing uncertainty in MIS implementation, Sloan Manag. Rev. 20 (1978) 23–31.
[2] H. Barki, S. Rivard, J. Talbot, An integrative contingency model of software project risk management, J. Manag. Inf. Syst. 17 (4) (2001) 37–70.
[3] R. Aron, E.K. Clemons, S. Reddi, Just right outsourcing: understanding and managing risk, J. Manag. Inf. Syst. 22 (2) (2005) 37–55.
[4] B.A. Aubert, H. Barki, M. Patry, V. Roy, A multi-level, multi-theory perspective of information technology implementation, Inf. Syst. J. 18 (1) (2008) 45–72.
[5] B. Bahli, S. Rivard, The information technology outsourcing risk: a transaction cost and agency theory-based perspective, J. Inf. Technol. 18 (2003) 211–221.
[6] Bijker, The social construction of fluorescent lightning, or how an artifact was invented in its diffusion stage, in: W.E. Bijker, J. Law (Eds.), Shaping Technology/building Society. Studies in Sociotechnical Change, MIT Press, Cambridge, Mass, 1992.
[7] B.W. Boehm, Software Risk Management, IEEE Computer Society Press, Los Alamitos, California, 1989.
[8] M.-C. Boudreau, D. Robey, Enacting integrated information technology: a human agency perspective, Organ. Sci. 16 (1) (2005) 3–18.
[10] J.A. Bradbury, The policy implications of differing concepts of risk, Sci. Technol. Hum. Values 14 (4) (1989) 380–399.
[12] G. Dhillon, J. Backhouse, Risks in the use of information technology within organizations, Int. J. Inf. Manag. 16 (1) (1996) 65–74.
[14] M. Feldman, B.T. Pentland, Reconceptualizing organizational routines as a source of flexibility and change, Adm. Sci. Q. 48 (1) (2003) 94–118.
[15] M. Feldman, B.T. Pentland, Routine dynamics, in: D. Barry, H. Hansen (Eds.), Handbook of New and Emerging Approaches to Management and Organization, Sage, Thousand Oaks, 2008, pp. 302–315.
[16] A. Hakim, H. Hakim, A practical model on controlling the ERP implementation risks, Inf. Syst. 35 (2010) 204–214.
[17] J.H. Iversen, L. Mathiassen, P.A. Nielsen, Managing risk in software process improvement: an action research approach, MIS Q. 28 (3) (2004) 395–433.
[20] K. Knorr-Cetina, A. Preda, The epistemization of economic transactions, Curr. Sociol. 49 (4) (2001) 27–44.
[21] R.L. Kumar, Managing risk in IT projects: an options perspective, Inf. Manag. 40 (2002) 63–74.
[25] P.M. Leonardi, B.A. Nardi, J. Kallinikos (Eds.), Materiality and Organizing: Social Interaction in a Technological World, Oxford University Press, Oxford, 2012.
[27] K. Lyytinen, L. Mathiassen, J. Ropponen, Attention shaping and software risk – a categorical analysis of four classical risk management approaches, Inf. Syst. Res. 9 (3) (1998) 233–255.
[28] J.G. March, Z. Shapira, Managerial perspectives on risk and risk taking, Manag. Sci. 33 (11) (1987) 1404–1418.
[29] F.W. McFarlan, Portfolio approach to information systems, Harv. Bus. Rev. 59 (5) (1981) 142–150.
[32] W.J. Orlikowski, Using technology and constituting structures: a practice lens for studying technology in organizations, Organ. Sci. 11 (4) (2000) 404–428.
[33] W.J. Orlikowski, Sociomaterial practices: exploring technology at work, Organ. Stud. 28 (9) (2007) 1435–1448.
[34] B.T. Pentland, M.S. Feldman, Organizational routines as a unit of analysis, Industrial Corp. Change 14 (5) (2005) 793–815.
[38] D.W. Straub, Effective IS Security: an empirical study, Inf. Syst. Res. 1 (3) (1990) 255–276.
[39] D.W. Straub, R.J. Welke, Coping with systems risk: security planning models for management decision making, MIS Q. 22 (1998) 441–470.
[40] R. Schmidt, K. Lyytinen, M. Keil, P. Cule, Identifying softtware project risks: an international delphi study, J. Manag. Inf. Syst. 17 (4) (2001) 5–36.
[41] B.C. Stahl, Y. Lichtenstein, A. Mangan, The Limits of Risk Management – a social construction approach, Commun. Int. Inf. Manag. Assoc. 3 (3) (2003) 15–22.
[42] U.S. Department of Defence, News transcript DoD news briefing february 12th. http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=2636, 2002.
[44] Y. Yoo, O. Henfridsson, K. Lyytinen, Research commentary: the new organizing logic of digital innovation: an agenda for information systems research, Inf. Syst. Res. 21 (4) (2010) 724–735.
[45] O. Hanseth, C. Ciborra (Eds.), Risk, Complexity and ICT, Edward Elgar Publishing, 2007.
[46] R.N. Charette, Software Engineering Risk Analysis and Management, Intertext Publications, New York, 1989.
[47] J.S. Persson, L. Mathiassen, J. Boeg, T.S. Madsen, F. Steinson, Managing risks in distributed software projects: an integrative framework, IEEE Trans. Eng. Manag. 56 (3) (2009) 508–532.
[48] W.L. Currie, Using multiple suppliers to mitigate the risk of IT outsourcing at ICI and Wessex Water, J. Inf. Technol. 13 (3) (1998) 169–180.
[49] P.L. Bannerman, Risk and risk management in software projects: a reassessment, J. Syst. Software 81 (12) (2008) 2118–2133.
[50] F.W. McFarlan, Portfolio approach to information-systems, Harv. Bus. Rev. 59 (5) (1981) 142–150.
[51] K. Lyytinen, L. Mathiassen, J. Ropponen, A framework for software risk management, J. Inf. Technol. 11 (4) (1996) 275–285.
[52] R.T. Nakatsu, C.L. Iacovou, A comparative study of important risk factors involved in offshore and domestic outsourcing of software development projects: a two-panel Delphi study, Inf. Manag. 46 (1) (2009) 57–68.
[53] D. Aloini, R. Dulmin, V. Mininno, Risk management in ERP project introduction: Review of the literature, Inf. Manag. 44 (6) (2007) 547–567.
[54] M. Sumner, Risk factors in enterprise-wide/ERP projects, J. Inf. Technol. 15 (4) (2000) 317–327.
[55] S.M. Huang, I.C. Chang, S.H. Li, M.T. Lin, Assessing risk in ERP projects: Identify and prioritize the factors, Ind. Manag. Data Syst. 104 (8) (2004) 681–688.
[56] S. Wright, A.M. Wright, Information system assurance for enterprise resource planning systems: Unique risk considerations, J. Inf. Syst. 16 (s-1) (2002) 99–113.
[57] M. Cremonini, D. Nizovtsev, Risks and benefits of signaling information system characteristics to strategic attackers, J. Manag. Inf. Syst. 26 (3) (2009) 241–274.
[58] L. Sun, R.P. Srivastava, T.J. Mock, An information systems security risk assessment model under the Dempster-Shafer theory of belief functions, J. Manag. Inf. Syst. 22 (4) (2006) 109–142.
[59] S. Scott, N. Perry, The enactment of risk categories: the role of information systems in organizing and re-organizing risk management practices in the

energy industry, Inf. Syst. Front. 14 (2) (2012) 125–141.
[60] C. Ciborra, Digital Technologies and the Duality of Risk, Centre for Analysis of Risk and Regulation, London School of Economics and Political Science, 2004.
[61] D. Robey, M.C. Boudreau, Accounting for the contradictory organizational consequences of information technology: Theoretical directions and methodological implications, Inf. Syst. Res. 10 (2) (1999) 167–185.
[62] W.J. Orlikowski, Using technology and constituting structures: a practice lens for studying technology in organizations, in: Resources, Co-evolution and Artifacts, Springer, London, 2008, pp. 255–305.
[63] A. Reckwitz, Toward a theory of social practices: a development in culturalist theorizing, Eur. J. Soc. Theor. 5 (2) (2002) 243–263.
[64] P. Jarzabkowski, J. Balogun, D. Seidl, Strategizing: the challenges of a practice perspective, Hum. Relat. 60 (1) (2007) 5–27.
[65] L. Mathiassen, T. Saarinen, T. Tuunanen, M. Rossi, A contigency model for requirements development, J. Assoc. Inf. Syst. 8 (11) (2007) 569.