ESRC Centre for Analysis of Risk and Regulation

Digital Technologies and the Duality of Risk

Claudio Ciborra

DISCUSSION PAPER NO: **27**

DATE: **October 2004**

Digital Technologies and the Duality of Risk

Claudio Ciborra

Contents

Introduction....1

Technical Approaches....4

Managerial Approaches....6

Economic Perspectives....7

Grid Technologies and Risk....10

The Duality of Risk....12

The Need for a Phenomenological Gaze....15

Concluding Remarks....17

References....17

The support of the Economic and Social Research Council (ESRC) is gratefully acknowledged. The work was part of the programme of the ESRC Centre for Analysis of Risk and Regulation.

Published by the Centre for Analysis of Risk and Regulation at the
London School of Economics and Political Science
Houghton Street
London WC2A 2AE

ISBN 0 7530 1794 6

Printed and bound by Printflow, October 2004

Digital Technologies and the Duality of Risk[1]

Introduction

The aim of this essay is to study the multiple links between risk and digital technologies such as information and communication technology (ICT). It sets the ground for the empirical analysis of risks connected to the design and deployment of ICT infrastructures in a variety of settings: corporate, public organisations and government.

The field of information systems (IS) offers a good point of departure for the study of risks connected to digital technologies, since it is populated by at least two different practices. First, there is the analysis of risk dedicated to complex projects involving software systems and methodologies of a mainly technical/ mathematical nature. Second, there are managerial concerns that initially related to this kind of software-based project, but were later extended to a range of mainly strategic and operational business factors. Thus, in IS we find both the 'harder' quantitative techniques of risk management and 'softer' approaches to the handling of so-called operational risk aspects.

The management of large software projects was the earliest problem area out of which the ICT risk management discipline emerged; subsequently, this has become part of Software Engineering (SE). Building large software modules for big corporate applications, especially for the suppliers of US defence agencies, is exposed to a variety of risks: cost overruns, wrong specifications and usability characteristics, delays in delivery, and so on. Hence, in order to improve the planning and governance of such developments to mitigate the risks of major SE failures, there was a need to develop available risk management methods and techniques in ways that made them suitable for application to the ICT field. The cultural and professional milieu in which these methods and techniques had been originally tried out led to their emergence as strictly quantitative approaches based on a positivist, probabilistic definition of risk: probability of occurrence of a problem multiplied by the value of its impact. This naïve view of risk has dominated the SE discipline and practice since the 1980s. It is supported by a myriad of sub-techniques for identifying risks, measuring impacts and assessing probabilities. To be sure, the methods and techniques are accompanied by words of caution from senior software professionals who suggest that they should be applied with a grain of salt and situational common sense. Here, as often happens in the professional field, formal models seem to get gradually substituted by rules of thumb, prescriptions and war stories disguised as articulated experience.

With time and experience, managerial attention to ICT applications such as the study of organisational impacts, management of ICT strategy and re-design of business processes has crossed the boundaries of quantitative risk management and widened its scope. As a result, an organisational/ managerial literature about information systems risks, and their management, in a business-wide perspective has emerged. This ranges from the more micro concerns about

[1] This paper is part of the research project on 'The Duality of Risk', sponsored by PwC at CARR, LSE and carried out in 2002–2003.

how to get the user requirements right (an issue that still overlaps with SE risk management) up to the strategic choice in selecting an application portfolio or an ICT infrastructure, where questions need to be asked about the risks of large ICT investments for a business as a whole. This literature, and its relative prescriptions, converges today in spirit and methodological approach with the field of operational risk. An example is the treatment of risk issues in the credit and financial sectors, as found in the 'Basel 2' documents (Basel Committee on Banking Supervision 2001). In these, digital technologies are treated on the same ground as other factors contributing to operational risk. Although the implicit underlying theory of risk used is the probabilistic one, the coexistence of many imponderable organisational factors makes the quantitative risk calculation largely beyond reach in practice. Hence, there has been a proliferation of double-entry tables aimed at qualitative classifications of situations, portfolios, instances and prescriptions on how to handle risks connected to systems and applications.

The technical and managerial perspectives share a basic belief in the powers of managerial and organisational control: it is believed that systematic assessment (as in the scientific study of work by F. W. Taylor) involving an orderly and rigorous study of risk can make its management more effective. Better control strategies are seen to be the paramount way of mitigating, reducing or annihilating risk. Typically, a linear reasoning prevails in these approaches, linked to rigid sequence identification, knowledge gathering, measurement (where possible) and plans for solutions and implementation.

With the advent of the Internet, network computing and inter-organisational systems, the boundaries of units of analysis - such as a 'software project' or a 'business firm' - seem to become too narrow for capturing all the various ramifications of the dynamics entertained by technology and risk. For example, consider recent developments in the ideas of 'democratising finance': by transferring its sophisticated calculus techniques at the level of individual existence so that life choices, change and innovation are devolved to the level of the individual, armed with better knowledge and sophisticated financial tools. This new way of looking at, and practicing, finance as a science for managing risk 'democratically' gives digital technologies an overarching importance and a new role. They become 'grid technologies', ie. an information infrastructure that allows the calculation of indexes and units of accounts, so that risks are quantified and can be traded, pooled and shared on global markets by large numbers of individuals. Digital technologies diffuse and enmesh with the structure of markets under this encompassing grid infrastructure, creating virtual enterprise networks and affecting more than ever the personal lives of workers, managers and consumers. Any breakdowns of these networks becomes potentially devastating for business and private lives, precisely because of the higher levels of integration and standardisation achieved by the new technical platforms. On the one hand, grid technologies constitute the backbone of choice for the 'risk society', to the extent they become the key co-ordination and communication infrastructure linking consumers, citizens, businesses and governments. On the other hand, as a powerful expert and calculating system, ICT becomes the paramount tool for running more and more sophisticated algorithms to quantify and manage risk at all levels, and for a greater number of economic agents. These far-reaching developments seem to elude the current discourses of software engineers as well as IS risk management consultants - but not for long.

Consider, further, the specificities that distinguish ICT as grid technologies from other modern technologies that create new risks, such as nuclear or chemical plants. Digital technologies are *technologies of representation* that can be used to augment other techniques

of representation, such as risk calculation and management. Taken *all together*, these are powerful tools to represent, calculate, control, mitigate, reduce and transfer risk. The creation of new global markets for the reallocation of risk insurance contracts is enabled by digital capabilities such as large data warehouses; the collection, communication and recombination of huge volumes of data; and the ensuing possibility of building and updating complex indexes. ICTs appear to be able to reduce costs in two key areas. Firstly, they can cut transaction costs on existing markets for goods and services, thereby making the whole economy more efficient, enterprises more global and governments more agile and responsive. Secondly, ICTs can decrease the costs of innovation, by allowing economic agents to better insure themselves against a richer variety of risks of (failure in) change. In this new financial order, the intertwining of digital technologies and risk is advancing further as the main instrument for the representation, quantification and sharing (through markets for risk and intermediaries) of hazards linked to the main life-choices of individuals.

The scope and reach (Keen, 1991) of grid technologies make the straight-jacket of the quantitative calculus of risk even more limited than it proved to be, when moving from SE projects to the broader field of risk management for corporate ICT investments. However, it would be naïve to think that the technology-enabled way to a fully calculable life, in a fully calculable world, is going to be clear-cut. Most probably, instead, it is going to be punctuated by new and surprising risks. For example, a close analysis of how large ICT infrastructures are actually deployed within and between public and private organisations has begun to unveil a number of intriguing features. Despite the tight managerial control, careful planning, appropriate risk management, and so on, ICT infrastructures tend to have a life of their own: they basically *drift* as a result of improvised usages; unforeseen technical interdependencies between old (legacy) and new platforms; quirky design choices; surprising user resistance; and other unpredictable behaviours of both systems and humans. Here, the sociology of modernity (Beck, 1992; Giddens, 1990) turns out to be a useful reference to capture the runaway dynamics of man-made risks, unexpected consequences and proliferating side-effects. The facts are even acknowledged by Basel 2 recommendations, at least in the credit and finance industry. They see digital technologies as one of the factors causing the shift of the risk management agenda from low-impact/ high-frequency incidents to high-impact/ low-frequency events. Here, the sociology of modernity complements the technical and managerial perspectives by highlighting the non-linear nature of risk management. It also points to the fact that the risk management techniques and technologies for control can themselves be the source of new man-made risks.

ICT has the potential to extend the boundaries where the future can be ordered and calculated, hence ‘colonizing’ further the wild territory of uncertainty and transforming it into the cultivated land of calculable risk. In particular, grid technologies will dramatically decrease the costs and barriers to innovation, foster new behaviours and multiply those occasions of radical new learning and new life choices that have previously been abandoned because they were considered ‘too risky’. On the other hand, the establishment of grid technologies, with their broadband communication channels and gigantic databases, would not solve possible infrastructure breakdowns; if anything, they will make such disruptions potentially more harmful. Security issues will multiply, as well as privacy concerns for the content of the databases. Compatibility problems with protocols and legacy systems are also destined to spread and cause unwanted side-effects.

In order to deal with all these new promising and puzzling developments, we submit that the economic and sociological analyses of digital technologies and risk need to be complemented

by a phenomenological/ existential one. Life, risk and technology are getting more intimate than ever. This is due to some subtler reasons than the hazards posed by GM crops or the thinning of the ozone layer. Paradoxically, the extension of the domain of quantifiable knowledge, and representation, exposes us to the danger of the further growth of ignorance generated by the mysterious new interdependencies and side-effects created by the very infrastructure deployed for the colonization of knowledge. The essence of such a 'reflexive' process needs to be captured by a new notion of risk, combined with a different perspective on the question of technology.

It is not just about us becoming dependent on the mobile phone/ computer for our communication; it is not only about transactions passing through digital networks; it is not even about jobs being automated; or human reasoning being replaced by expert systems. Looking at the next developments in ICT platforms and risk management, the challenge emerging on the horizon is that the unfolding of our life (project) becomes simultaneously conditioned, constrained or enabled by grid technologies. The technology is already there, albeit in an indirect and hidden form, for instance when we apply for a loan or seek a life insurance scheme. In the next phase, it will be at hand in helping us compute whether we should engage in a house move or a career change; or whether we can afford one course of studies rather than another. For each choice, grid technologies will be able to offer a calculus of probabilities based on objective indexes, thus contributing to the quantification of our life projects to a greater extent. That is why only a fresh exploration into the intertwining of life, risk and technology can offer us some clues to help grasp such future developments.

In what follows, all these themes are examined further. The first two sections deal with the technical and managerial approaches and their limitations. Institutional economic perspectives are introduced in the third section to tackle the issues of inter-subjectivity and psychology of risk in two main settings: markets and hierarchies. Further economic perspectives, in particular from the finance domain, are then put forward to help enhance understanding of the implications of grid technologies and the creation of new markets for individualised risk management. Next, in order to capture the puzzling aspects of the ramifications of risks stemming from the new waves of technical applications, the sociology of risk is presented by discussing the duality of risk generated by digital technologies. Finally, the phenomenologies of existence and technology are combined to study the recent developments and opportunities offered by grid technologies.

Technical Approaches

Risk management deals with risk exposure. According to the positivist definition adopted by Boehm (1991) to launch the field of software risk management, risk exposure is treated as the potential loss multiplied by the probability of loss. Potential loss is described by the components of the unsatisfactory outcome of a project, which leads management to identify lists of the risk factors that are seen as causes of overall negative outcomes. Risk factors have to be addressed, eliminated, mitigated or avoided, depending upon their probability of occurrence and the size of their impacts. Various techniques are used to carry out the analysis. For example, decision trees can provide a framework for analysing the role of risk factors and the sensitivity of final outcomes. Regression analysis allows the development of a cost model that relies on the data of past software projects (Fairley, 1994), which aims to elicit those factors that can explain the variation of the effort put into one particular project relative to the main trend identified by the regression curve. Simulation (eg. Montecarlo methods) helps in identifying the behaviour of the intervening risk factors. Other approaches

are based on disciplines such as statistics, mathematical modelling of decision-making and graph theory.

A few aspects have been identified as limiting the scope of the technical approaches, such as these mentioned by Renn (1998):

> -The quantitative combinations of variables, such as magnitude of impact and probabilities, assume equal weights. Low-probability/ high-impact events may get the same weight as high-probability /low impact ones, and this might distort the risk emerging in a given situation. On the other hand, attributing differential weights may prove to be an uncertain or impossible task.
>
> -Probabilities tend to be extracted from the relative frequencies of past events. When this is not an adequate approach to anticipate future events, the calculation may have limited predictive power.
>
> -People perceive the magnitude of impact and its probability differently, which leads to an appreciation of risk that may differ from the outcome of the algorithms.
>
> -The desirability of effects may vary among different decision-makers.
>
> -The institutional and organisational contexts may influence the actual risk levels to which human agents are exposed, and may impact on the various risk-mitigating or risk-handling actions indicated by the purely technical calculus of risk outcomes.

Note that the last objection in the above list highlights the fact that the causes and consequences of risks, as well as risk-management actions, are embedded in institutional, organisational structures and are generally intertwined in social processes and networks of relationships. All the stages of effective risk management must take place within the constraints posed by such social and organisational contexts, and exploit and respect the opportunities offered by those constraints. A few practitioners of software risk management have stressed the importance of organisational processes to complement or support the quantitative techniques. For example, Boehm (1991) indicates that when uncertainty is high and no reliable estimates can be made of the key risk factors, engaging in prototyping the new system could be a way of reducing risks by acquiring knowledge and buying information and time; improved estimates can then be made to fit the quantitative models at a later stage.

Conversely, despite their promises, the adoption of structured design methodologies may increase risk precisely because they push forward the moment at which the actual project outcomes, and their problems, will be exposed in actual operation. Hence, some authors (eg. Charette, 1996) suggest paying attention to the ‘mechanics’ of risk management: those organisational and process interventions that can transform an algorithm to calculate risk into an effective way of handling a project. The importance of processes such as planning for risk management is discussed below in this respect.

In summary, what is troubling in this first set of approaches is that the use of sophisticated formal models is accompanied by crude simplifications characterising the risk situation. In particular, only one decision-maker is identified (the management of the firm or the project) as being responsible for assessing the risks, evaluating them and formulating remedial policies based on the relevant calculus. The technical perspectives are therefore revealed as

being too narrow, except in the simplest of situations, and adopting one as the single guide to risk identification and management may therefore constitute a risky option in itself. This indicates that a broader view that encompasses management and organisational processes is essential.

Managerial Approaches

The broader organisational perspectives on risk, identified above, address the issue of implementation within the concrete organisational or institutional setting that surrounds any risk-calculating algorithm. Not only do these approaches widen the scope of risk analysis and the range of risk factors taken into consideration, but they also point to the gap between models and their deployment. This often shows that managerial practice is at odds with the prediction of the models or methods themselves.

The literature focussing on the psychological, behavioural, institutional and organisational aspects of risk management is vast (eg. see March and Shapira (1987) on the actual behaviour of managers facing risks and Perrow (1984) on the influence of organisational settings and routines). In comparison, the specific IS literature contribution is limited in terms of the quantity of published material, empirical research and, above all, its scope.

Lyytinen, Mathiassen and Rapponen (1998) address a range of organisational aspects by looking at various IS and software risk approaches. They highlight one important cognitive aspect in risk management: the scope of managerial attention towards the factors to be taken into consideration in any calculus or qualitative assessment. Thus, they find that various IS approaches to risk management may focus on different aspects, such as business strategy rather than requirements analysis, since risks can be hidden in any of the multiple stages of the development and deployment of a system. In order to introduce structure into this potentially limitless field of interest, the authors propose a socio-technical framework for comparing various approaches, according to key domains defined by Leavitt's (1964) classic diamond diagram which connects four main variables: strategy, technology, structure and tasks. But such a commendable exercise aimed at reducing complexity proves to be of dubious use, since it is based on the presumed equivalence of the socio-technical notion of variance control to attain system equilibrium with the goals and scope of risk management in an organisation. However, such equivalence is unwarranted. Within the socio-technical theoretical framework, variances are problems that need to be handled by an appropriate control system based on the co-ordination and communication of the members of the organisation among themselves, usually involving the technical infrastructure. Control actions are based on feedback from a disturbance that *has occurred*. Risk, instead, is about *future* disturbances: immediate feedback from an occurred variance is not the only issue, nor is equilibrium necessarily a main feature. Risk management is all about uncertainty regarding future events, betting on their occurrence, buying insurance to mitigate their impact, and so on. In particular, all risk management contracts must be signed *before*, not after, a breakdown has occurred or before the information that would create a sense of urgency arises (Shiller, 2003, p. 30). Variance control in a socio-technical system is, instead, about detecting breakdowns *ex post* and taking counteractive, equilibrium-restoring measures (Herbst, 1974). Even the fact that socio-technical systems must engage in equilibrium seeking when dealing with variances is an idea that has been challenged (Ciborra, Migliarese, Romano, 1984). Variances (and indeed risks) are sometimes the source of innovation and new order (or self-organisation) stemming from *disequilibrium*. Hence, reduction to a pre-exiting order may constitute a repressive policy that kills innovation.

This is just one instance showing that, unfortunately, IS approaches do not distance themselves enough from the tenets of the engineering and technical perspectives, or at least do not challenge them. At the limit, they put forward a richer list of risk factors which are often overlooked by the practitioner who focuses on a particular project as opposed to a business perspective (McFarlan, 1981). On the other hand, the IS approaches rely on the same key fictions of the purely technical perspectives, such as that of the 'unbiased' decision-maker. Thus, Keil et al. (1998) classify risks of software projects on the basis of their importance and perceived level of control, which they believe can prevent the risks from occurring. However, these authors fail to emphasise indications from the extensive behavioural literature pointing out that these perceptions can be heavily biased, depending upon a variety of psychological and contextual factors. The shape, values and enactment of a decision tree may differ according to the psychological and organisational context of the decision, since risk identification relies on cognitive aspects, such as problem framing (Tversky and Kahneman, 1974), and estimates are based on perceptions, attitudes and ultimately even feelings (Loewenstein et al., 2001) and moods.

Other managerial and behavioural aspects seem to remain elusive. Challenges have been made to the formulation of risk management that suggest there is a phase of calculation followed by the making of a choice among the risk-return combinations that are available. There is often denial of risk, or a causal relation is assumed between action and (risky) events. Also, real decision-makers seem to be more impressed by the magnitude of any negative outcome, rather than the level of its probability: implicitly, they give more weight to the former. Even ranking risks on the basis of expected impact has not been empirically supported. March and Shapira (1987) report a vice-president stating: "You don't quantify the risk, but you have to be able to feel it,". The same authors conclude that, although there is ample evidence that the risk-taking behaviour of managers is often far from optimal, such behaviour may indeed consist of accommodations of individuals and organisations to the 'subtle practical problems of sustaining appropriate risk-taking in an imperfectly comprehended world' (March and Shapira, 1987). Modelling and planning seem to possess, then, a limited scope; what matters in handling risk is 'situated action' (Suchman, 1987).

We conclude that the state of the art in the IS field concerning the management perspectives is rather uneven, if not lacking. For instance, it fails to take stock of the more sophisticated analyses of decision-making behaviour under uncertainty and knowledge distortion; does not acknowledge the plurality of decision-makers; and does not challenge the main tenets of the engineering and technical perspectives.

Economic Perspectives

Given their narrowness of focus on technology, probability and control of the development process, we need to abandon the technical and managerial perspectives in the IS field in favour of a broader inquiry into the economic views on risk (following a similar broadening of perspective to that used by Ciborra and Hanseth (1998) when addressing the strategic alignment issues of ICT infrastructures in organisations). The agenda and the facets analysed from an economics viewpoint are multiple and can help us encounter a richer vision of the relationship between digital technologies and risk. This suggests that not only is the process of developing and applying a complex technological infrastructure punctuated by more or less computable risks, but technology itself can also be harnessed to reduce, mitigate or share risk. The economics of markets, transactions and organisations allow us to approach such a

complex relationship in a way that the long, but rather flat, managerial lists of risk factors hardly make possible.

Information Systems are about ICT embedded in organisations. The risks posed by digital technologies therefore need to be understood within an organisational framework, for which institutional economics and the economics of risk can be harnessed to understand the implications of key organisational/ institutional contexts. To begin with, institutional economics indicates that there are two main organisational arrangements to be considered: markets and hierarchies (bureaucracies). We need to trace the risk factors of digital technologies within these two different contexts. In a market, risks can be shared or exchanged by creating markets for risks, measured in utilities or disutilities. The theory of social costs developed by Coase (1960) may provide further useful insights. What goes on in hierarchies is better framed by the notion of operational risk (Power, 2003). Here, many aspects of the managerial perspectives come to the fore again. But the boundaries between hierarchies and markets are not fixed (Williamson, 1975; Hart, 1995) and the different styles of handling risks regarding ICT projects may change over time, for example when the IS services are outsourced. The picture is further complicated when one considers that ICT is a factor that contributes to the change of boundaries between markets and hierarchies (Ciborra, 1981; Ciborra, 1983; Malone, Benjamin and Yates, 1987), thus impacting the styles of managing (trading) risk. If market risk can be better subjected to representation, calculation and exchange, and if digital technologies support the expansion and refinement of markets, the diffusion of ICT will not just be punctuated by risks, as for any other innovation, but will have a self-reinforcing effect. This means ICT diffusion will promote a special style of risk management, namely one based on the formal representation and calculation of risk, and the ensuing creation of specialised markets for trading risk.

Let us first look at risk in markets. The main difference between the economic and technical conceptions of risk is the possibility envisaged in economics of including a dimension of *intersubjective validity* through the notion of *utility*, which describes the degree of satisfaction or dissatisfaction with an event or an action among a variety of stakeholders (Renn, 1998). Harms and undesired effects can be framed as (social) costs (Coase, 1960) and thus become utilities or disutilities for different parties. Costs can be allocated by various mechanisms, market-like or non-market. Specifically, utilities can be traded; after all, utility can be measured by the amount of money one is willing to pay to avoid a potential harm. Economics thus introduces a social dimension, albeit in the narrow sense of a system of exchange of utilities/ disutilities. Such a dimension is missing from the IS managerial perspectives, which are unable to deal with questions such as: Risk for whom? Who is going to pay to avoid a certain risk? Also, a social dimension includes some of the psychological aspects of risk, by distinguishing risk-taking from risk-neutral or risk-averse attitudes of economic agents. Psychological and social effects can then find a common denominator to measure the degree of harm or utility: money.

Most of the techniques developed within the technical approaches, such as models of rational decision-making, probability and discounted-value calculations, also apply to the economics approach. However, here they are supported by an economic framework that connects the individual and the social (inter-subjective) dimension through the notion of utility. The economic perspectives open up various new domains of application, such as costs and benefits analyses and the possibility of sharing risk and social costs through trade. In addition, due attention is given to incentives; risk insurance, for example, can be used to influence individual behaviour by discouraging risky actions in order to save money. Finally,

new models are added to the kit of techniques for representing risk quantitatively, such as the game-theoretic ones (Jaeger et al., 2001).

One limitation of the economic perspectives and their envisioning of markets to trade risks is that not all risks or social costs can be translated into money; for example, human life can be regarded as plainly incommensurable in some cases and for some individuals or communities. Another, as Coase (1960) has shown, is that there may be transaction costs involved in exchanging utilities and disutilities. This would bring in non-market institutions, such as courts and government agencies, to take care of the handling of risks, lest no trading occurs at all. The discussion of risk in the IS field has suffered from its implicit focus on ICT in non-market organisations, ie. bureaucracies: hence any treatment of utilities or risk sharing is largely ignored, even by those authors who claim to transcend the narrow technical view (as seen in the previous section). This is a gap that needs to be filled to create a better understanding of the relationship between risk and digital technologies. We will address below, after a short survey of the notion of operational risk and its relevance for hierarchical (non-market) organisations.

The notion of operational risk emerged in the banking environment as a residual category for those (mainly internally generated) risks not covered by the more common market and credit-risk management practices. It comes from the simple regulatory principle by which banks should hold some capital as a buffer against risks to their loans and credit operations (market-risk exposure). This buffer should be larger if it is to take account of the way banks can incur risks not only, say, in lending money to outside customers, but also if their internal ICT systems fail. Thanks to the so-called Basel 2 regulatory proposals in the last few years, especially in the banking sector, operational risk has become the encompassing concept and vision for the control and regulation of a wide range of risks that can be faced while operating a business. More precisely, Basel 2 consultative documents define operational risk as: “The risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events,” (Basel Committee, 2001, par. 6). In this respect operational risk is an organisational concept that subsumes both the technical and managerial models and approaches which emerged in the discussion of IS and risk. However, the concept of operational risk has given rise in a deeper way to analyses and discussions that address the organisational dynamics of managing risks within hierarchies. In order to overcome the limitations of their narrow focus and naïve hypotheses about human behaviour and risk, it would be advisable for the managerial and technical IS literature to take notice of these developments, especially those occurring in critical accounting (Power, 1997).

The problems that emerge during the implementation of operational risk reflect themselves within the specific IS field. It is therefore useful to mention here the results of Power’s (2003) analysis of the puzzles, dilemmas and contradictions of operational risk that point to the ramifications of lack of knowledge, the role of biased data when assessing risk in organisations and the influence of internal politics and impacts of negotiation. The issues raised by this concern include items such as:

-What data is relevant to operational risk? Historic losses? Expected or unexpected ones? What about sudden catastrophic events?

-Is this data reliable? Apart from rare events for which data is unavailable, as well as for the most frequent ones, there can be opportunistic massaging to hide errors.

-Effective learning and correction of mistakes since the negative event occurred can also make historic data irrelevant, because operations have been modified in the mean time.

-Collecting data from multiple organisations (a sort of best-practice exercise in reverse) is a possible solution, but requires the sharing of troubling and embarrassing information: hence one can expect to see pooled databases of this kind remain half empty.

-The 'key under the lamppost' effect. Data that is eventually collected systematically under existing internal auditing and information systems becomes the basis for measurement of operational risk. However, this gets to be defined by the databases available and not by the actual multiplicity of potential risks, which are not all covered by the existing systems when representing and recording historical risks.

Similar dilemmas affect the risk modelling stage, where Power (2003) notes that:

-The use of risk measurement techniques is not immune from organisational politics.

-Rational calculation of use in actual situations has to be marketed and sold internally, but this is not always accomplished successfully and so its scope is rendered, at best, fragmented and a matter of negotiation.

In general, the main approaches to the management of operational risk are of two different types, similar to the ones that emerged in our discussion of risk in IS development: a 'soft' calculative approach and a 'hard' approach. The first tends to rely on a variety of ranking and scoring techniques for qualitative variables, with the goal of directing attention to key risk drivers. The hard approach is based on the discipline of market risk management and the relevant quantitative techniques based on calculating costs and utilities. The problem with the latter approach is that it aims at enacting market techniques within a fundamentally non-market organisational setting.

Grid Technologies and Risk

The economic perspectives are a good introduction to an inquiry into the reflexivity of grid technologies in relation to risk. As indicated earlier, by grid technologies we mean ICTs that increasingly have the characteristics of ubiquitous, mediating (Thompson, 1974) information infrastructures. Their hardware is characterised by the extension of the links (networks) to the individuals and organisations they support. Software guarantees the standardisation of the linkages for the seamless transfer of data and to provide access to powerful databases that can track usage and produce profiles of users. By analogy with the electricity grid, ICT-based grid technologies can provide ubiquitous access to content and people, allow fast transfer or exchange of content and communication and enable more sophisticated processing of data in relation to various patterns of usage of the grid itself. The leading public example of grid technologies is the Internet, in its present and future forms (known as I2); but within narrower corporate boundaries there are also full-scale Enterprise Resource Planning (ERP) systems, web services and intranets that feature many elements of a grid technology. The economic perspectives highlight *contract enabling* as one of the significant potential uses of grid technologies, because this kind of technology would provide the adequate information flows and databases to 'create, set up, control and maintain the network of exchanges and relevant contracts' (Ciborra, 1981) that build up the fabric of economic institutions such as markets and firms.

The infrastructure character of such technologies can contribute, on the one hand, to the generation of new, surprising risks (see Ciborra and Associates (2000) and the next section); on the other hand it can be used to manage a growing variety of risks for which appropriate financial markets can be created. For instance: "This new technology can do cheaply what once was expensive by systematizing our approach to risk management and by generating vast new repositories of information that make it possible for us to disperse risk and contain hazard," (Shiller, 2003, p. 2).

There are multiple ways in which grid technologies can act. First, there are the overall trends in formalisation of transactions, and the pushing further away of the boundaries between markets and hierarchies in favour of markets (Ciborra, 1983; Malone, Benjamin and Yates, 1987). Thanks to ICT, 'buy' has extended its reach in relation to 'make': there will be more externalisation or outsourcing of activities, regulated by market contracts. As a consequence, markets will be more efficient because of the decrease in transaction costs and will extend spatially and become closer to the functioning of a perfect market (always with the approximation determined by the initial state of a particular market).

Moreover, powerful grid technologies can have other effects on the costs of 'transition', or change and innovation, via their enabling of new opportunities for managing risk, as pointed out by Shiller (2003). In particular, grid technologies can have an impact on the realm of finance and become a powerful tool for the management of risks. Finance can reduce the harm on individuals by dispersing the negative effects among a large number of people. This already happens on the stock market, through the limited-companies arrangement, social security and some forms of individual insurance. But this could take place on a much broader scale and be tailored to the needs of individuals, way beyond their life insurance schemes, precisely thanks to grid technologies. Whenever people can mitigate their risks through new digital financial instruments, eg. when changing a career or taking up an innovative course of studies (both high-risk personal choices), personal transition costs can be reduced and more individual and social innovation can be fostered: "Financial arrangements exist to limit the inhibitions that fear of failure places on our actions and to do this in such a way that little moral hazard is created," (Shiller, 2003, p. 2).

Grid technologies would provide a new risk management infrastructure, by fostering the extension of the market and enhancing the possibilities for measuring utilities and introducing new units of account and measurement. Huge databases containing information on individuals (stemming from individual transactions like paying taxes or buying something with a credit card), allow for the construction of new powerful indexes against which everyone would be in the position to bet on the risk relating to a particular career, a profession, the house prices in a given area or the GDP of a certain country. All this would allow a person, or a country, to share on a global scale the risks of engaging in new ventures. In the past, complex financial arrangements such as insurance contracts were expensive to devise, and especially to tailor. Now, however: "Computer programs, using information supplied electronically in databases, can make complex financial contracts and instruments. The presentation of these contracts… can be fashioned by this technology to be user friendly," (Shiller, 2003, p. 10). To be sure, well-functioning markets for risk sharing require data for the effective estimation and pricing of risk. They can also reduce the transaction costs in the continuous negotiation of contracts, claims, adjustments and payments. Grid technologies can help to create 'a new financial order' by providing: "Finely detailed, continuously-updated, widely available data on incomes and asset prices as well as aggregated data on these and other values relevant to the risk faced by individuals,

organisations, and governments. Properly used, this new universe of information would allow better management of an ever wider spectrum of risks," and help to devise new risk management contracts across the globe (ibid., p. 189– 90). Risks will be objectified and quantified on an unprecedented scale, so that they can be bet against, traded, pooled etc., and the activities to which they are attached will be carried out in a much more widespread and reliable way since the relevant risks can be shared among a broader consumer audience.

The Duality of Risk

As with any previous major revolutionary technology, ICT has impacts on work, employment, skills and organisations that can be disruptive, if not destructive. Technology is a major force in the process of creative destruction of capitalism (Schumpeter, 1976). Change and innovation create new risks at individual and societal level, and ICT is one of the culprits. But, as the last section has shown, ICT in the form of grid technologies can come to the rescue by allowing a 'democratisation' of those financial tools that are today relegated to stock, market, derivatives and a restricted number of life insurance schemes: by encompassing a wide array of personal risks stemming from the relentless pace of change of technology-based capitalism. But it is here, perhaps, that Shiller's (2003) vision encounters its limits, creating a need to invoke sociological perspectives on risk and modernity.

Implicit in Shiller's (2003) advanced conception of ICT as grid technologies is an old and ubiquitous idea held by economists, according to which technology is a 'tool' that can be applied to good rather than bad ends in a contingent fashion (Ciborra and Hanseth, 1998). Thus, digital technologies represent a powerful tool for enhancing productivity as well as decreasing transaction costs; or, through the sophisticated sharing of risks on financial markets, for fostering change and innovation even at the micro-level of the individual economic agent. Of course, their application needs to be well governed, balancing costs and benefits for the various stakeholders through appropriate trade-offs. However, nowhere in the economist's conception can one trace the doubts observed by others that technology can be autonomous (Winner, 1977); behave as an actor with its own logic (Latour, 1999); or possess a far-reaching influence that affects how humans see reality and deploy technology according to patterns that are not purely instrumental, as some philosophers have suggested (eg. Heidegger, 1978).

In this respect, consider the notion of technology 'drift'. The drift of technical infrastructures has been identified as a ubiquitous phenomenon found in a variety of corporate large-scale ICT projects (Ciborra and Associates, 2002). When global companies engage in the launch of new ICT platforms to support new standardised and integrated business processes, they are immediately faced with the problem of deciding how to handle their existing and relatively successful legacy systems. Compromises need to be made with all the main actors on the stage, ranging from the angry orphans created by the substitution of the old standards to the installed base and its autonomous dynamics. Compromises require time to be devised and implemented: some form of consensus needs to be gathered to align the new resources and processes and there will be a need to make adjustments on a continuous basis. This causes a main phenomenon: technologies and processes drift, so what one obtains at the end of the implementation process is not what the system was designed for originally. The models are not only corrupted, but are in a permanent state of redefinition. Implementation never ends. Time drifts too. The corporate timescape becomes more varied, with processes that are carried out at the speed of light running alongside others that are never really finish, or need to be painstakingly worked at to be completed. Management scholars, consultants and

application vendors urge corporations, especially top management, to take action in this domain. Their prescriptions are straightforward. In order to overcome the present state of fragmentation, to avoid the widespread number of deals through which infrastructures are built, one needs to increase standardisation and the integration of data, processes and businesses. These not-so-new top-down and control-oriented directives just accelerate technology drift.

In order to explain some of the paradoxical outcomes of ICT and the practical impossibility of maintaining a steady course during deployment, we submit that the basic assumptions of management models, old or new, may suffer from the following taken-for-granted assumptions:

-Linear reasoning prevails. Organisations and their management are seen as means end chains. Goal directed decision-making, leadership and will are expected to enact and fix plans (Weill and Broadbent, 1998).

-Control and planning are regarded as key activities performed by organisations, and hence as essential design principles (Beniger, 1986).

-Evolution and change are seen as processes of improvement based on feedback that should be carefully monitored, and where possible measured and managed (Earl, 1996).

-Learning by mistakes is supposed to take place effortlessly.

-Private hoarding of knowledge and other key assets is both essential to gaining an advantage at the individual and organisational level and a source of potential opportunistic behaviour that requires to be kept in check. Again, control over key, unique resources becomes an increasing concern.

Instead, the sociological perspectives of Beck (1992) and Giddens (1990) would urge us (including the well-advised practitioners) to consider other important (and somewhat paradoxical) sources of risk, namely integration and standardisation themselves, such as:

-The effort to create through ICT a lean, agile and standardised corporation takes too long a time in itself to be compatible with the rapidly changing requirements of the business and the market. The alignment of resources remains an elusive target precisely because of such efforts.

-Technical integration may bring with it a number of side effects and unexpected consequences, for example interference between different standards or an infrastructure that is well tuned but too rigid.

-The control scope of organisations is bound to be limited, even if an enterprise invests heavily in digital technologies. Actually, huge investments in ICT may cause runaway dynamics (Arthur, 1994). Technology itself appears to evolve and diffuse along unexpected trajectories (Latour, 1999).

-Learning is not straightforward. Drift is the outcome of vicious circles where learning from mistakes fails to take place (Argyris and Schoen, 1996).

-Unpredictable knowledge spill-overs play a key role both inside and between organisations in triggering innovation and learning (Steinmueller, 1996). Learning is part of the more general phenomenon of reflexivity, by which institutions, organisations and individuals change, usually in unpredictable ways as a consequence of previous innovations and changes.

Digital technologies are contributing to both the generation of new side effects and further reflexivity: digital organisations are simultaneously more controlled and more unpredictable. Unpredictability and increased runaway dynamics are also caused by the way the new risk management apparatus tends to show consistently the characteristics of higher levels of formalisation, standardisation and integration, which is an ideal landscape where side-effects can spread and diffuse at higher speed to provoke disrupting impacts. In particular, grid technologies, as with any infrastructural technology, may pose unforeseen hazards arising from collateral or systemic risks, which are typically not the ones the technical and engineering perspectives have in mind as risks that they should avoid when developing new computing and communication platforms. The collateral risks stem from the fact that, in order to function to mitigate individual and social risk, grid technologies involve a higher degree of interdependency between individual lives, the data they generate and the common databases, for example through the use of new identification and encryption technologies. Higher levels of transparency are required to ensure the trustworthiness of transactions, claims, etc.

As mentioned above, only the pooling of individual data allows the construction of reliable indexes and units of accounts. If better indexes can mitigate moral hazard issues in individual or organisation risk contracts, the establishment of such indexes enabled by grid technologies also requires the setting of standards and complex legal devices as an essential first step. Leaving aside the legal devices, standardisation comes with a price of higher complexity and hidden new forms of fragmentation (Hanseth and Braa, 2001). Hence, every action, device or rule that sets out to reduce or mitigate risks may create side effects of uncontrollable origin and manifestation, which can disrupt the newly-established control apparatus. Again, we encounter the phenomena that seem to elude the economic analysis but have been highlighted by the sociologists of risk society and modernity: those of reflexivity and runaway dynamics (Beck, Giddens and Lash, 1994). Reflexivity refers to the fact that every new technology or regulative measures aimed at controlling risks, such as the grid technologies, inevitably create new risks which originate from regions beyond the control of the new powerful platforms. In other words, the more we are able to extend the frontier of (formalised) knowledge thanks to technology, the more dangerous could be the events emerging out of the regions of our ignorance.

In the field of IS risk study, a sort of blindness to the phenomena of reflexivity and runaway risk dynamics has been created by an excessive fixation on notions of control and equilibrium, which characterises even those authors who have put forward frameworks aimed at transcending the narrow focus of the more technical software engineering approaches (eg. Lyytinen, Mathiassen and Rapponen, 1998). The notable exception has been Mumford (1996) in a paper that identifies these phenomena very crisply and harnesses the relevant sociological literature for an IS audience. She applies the frameworks of Beck (1992) and Giddens (1990) to analyse in an anticipatory and penetrating way the devastating side-effects of Business Process Re-engineering as a tool to streamline and control organisational processes: “Business process re-engineering was offered by its developers as a solution rather than a risk and managers only became aware of the risks when they tried to introduce it into

their companies," (Mumford, 1996, p. 328). Unfortunately, this insightful but perhaps too little quoted analysis has not been extended yet to evaluate the deployment and the impacts of ICT infrastructures *per se*.

The Need for a Phenomenological Gaze

The world of risk appears even more complex when further sociological, psychological and cultural dimensions are added to the analysis carried out so far (Jaeger et al., 2001). For example, it brings an awareness that risk is socially constructed and that the adoption of the technical or naïve perspective, or any narrowly positivistic methodology, is *per se* based on a choice of values regarding the definition of what risk is and to what extent it is acceptable. Cultural and institutional formative contexts (eg. the managerial overarching mission of control) set the agenda and the problem of risk in a particular way, thereby shaping the perception of reality, (Douglas and Wildavsky, 1982) even before there has been a situated framing of risk factors (Kahneman and Tversky, 1979).

We acknowledge the role of such ramifications, but we prefer to conclude the present survey of risk perspectives relevant for the IS field by honouring the role of technology and its dynamics as triggered by the learning of the actors and the counter-moves of the technical artefact, in the spirit if not the letter of Actor-Network Theory (Latour, 1998). More precisely, we ask how the reflexivity in the dynamics of grid technologies when used as a tool to help us master risk can be related to the very human, or even existential, notion of risk.

First, let us consider the human or existential dimension. What are the key components of the notion of risk that can be found across the perspectives we have examined so far, even if at different levels of granularity? Risk is essentially a function of actions, events, future outcomes and value. Hence, the essential dimensions are a time horizon; a notion of subjective judgement (that is likely to be influenced by being socialised with fellowmen); and the openness to uncertainty and change. If one of these ingredients is missing, we are confronted with problems that have no risk in view because they involve no uncertainty, change or innovation, for example problems with no impact (no value) or those which have already occurred in the past and so render unnecessary a consideration of their prospect in the future.

The naïve or behavioural notions of risk very much belongs to the 'cogito' because they have a *cognitive* component, in that they are related to decision-making and, more specifically, calculation. Nevertheless, dimensions of risk such as value and man-made change point to the importance of human existence, the: "Who am I and what do I wish?", or to the general intrinsic mobility, openness and unpredictability of life. In other words, in positing the relationship between risk and human agency, we do not only need to overcome the narrowness of the model of the human agent as portrayed by the technical perspectives (implicitly, a calculating machine), but also the more powerful notion of economic man, his differential risk attitudes, limited cognitive capabilities, strategic orientation and proclivity to exchange. When modelling risk within each of the perspectives examined so far, we recommend the need to stay close to, and to safeguard, some essential traits of human existence, in particular the intrinsic openness of life and its fundamental indeterminacy as the key sources of our very personal worry about risk. But it is not simply about life and the indeterminacy of danger, or even death, ahead. Ontological strength is given to the mundane notion of risk through our generic disposition in life and in our care and concern about

people, things and the world that surrounds us. Risk is there both because the world is dangerous and unpredictable, as well as because we are restlessly concerned about it (*inquietum cor nostrum*, our restless heart, as St. Augustine would put it).

In particular, risk can be looked at as a hedged form of care or concern: care taking care of itself. Care is concerned both about worries relating to the present as well as for having to care about future events; more precisely, it is worried in the present about possible outbursts of care in the future. Care would wish to have a smooth unfolding, wanting to avoid peaks and crises even in its own deployment. Hence, the notion of risk would be expressed as a concern of care about itself. The objectification of concern in the form of risk is a consequence of the tendency of concern to forget about itself and life in general, focussing on the things, resources and people it relentlessly deals with, rather than the open and anxiety-ridden project of human existence that provides its momentum. In the naïve forms of risk calculation, care and concern become objects (quantities) that can be calculated and manipulated.

Now, let us turn to technology while maintaining a phenomenological approach. Through the notion of 'Gestell', Heidegger (1978) tried to grasp the essence of modern technology as 'enframing' and converting everything encountered, natural or human, into a reserve stock of resources to be harnessed and deployed for further deployment. The river is a source of hydroelectric power. A forest is the support for enrolling through newspaper advertising the public opinion. Nature becomes a gigantic petrol station! Gestell is the reunion of the processes of gathering and recycling resources for production and use, and Gestell can indeed be translated as – 'grid'. We are becoming a 'risk society' (Beck, 1987) at the same time that we are becoming an 'information society' enabled by the diffusion of the grid/ Gestell.

The analysis so far has shown that new risk management technologies, such as the one put forward by Shiller (2003), generate a mutual-reinforcement effect together with the grid technologies enacting the information society. The increasingly sophisticated formal representation and calculation of risk (concern) allows further innovations, while the regions outside the representation and calculation of risk which are sources of side-effects and unexpected consequences, become further marginalised. Grid technologies multiply the speed and impacts of effects stemming from ignorance because of the technologies' promotion of standardisation and integration. Digital technologies are harnessed to convert concern into a resource that can be represented, formalised, calculated and made deployable for allowing further representation and calculation of concern. Thus, through grid technologies, key aspects of human existence like care and concern become themselves objects of representation – 'things' that are representational substitutes for existence itself. In other words, one key activity (concern) that makes us human gets converted into yet another of those resources that can be accumulated, stored, recombined and exchanged. New forms of risk management and grid technologies contribute to the relentless march of Gestell and confirm the looming danger of modern technology pointed out by Heidegger (1978): reality and life (in our case its expression through concern) get increasingly substituted by technologically-mediated representations. What is 'real' is what technology is able to define and represent, which now includes concern in the form of calculable risk.

Concern is always in motion: it unfolds by being attracted by the unaccomplished and by the unknown, and tends naturally to objectify its target to make it more knowable and controllable. Thus, when concern looks at itself, it almost immediately sees itself as risk. Grid technologies allow concern to pursue even further its own objectification into quantifiable

risk, which can then be managed and marketed on an unprecedented scale. But grid technologies also create new side effects and unexpected consequences that, in a way, enlarges as well as reduces the regions of the unknown outside the reach of objectified concern. These regions of ignorance soon become the new attractors for further genuine and anxious concern, further objectification and, hence, a further extension of the grid. Faced by such a runaway process, one must advocate the design and diffusion of 'forgiving technologies' (Renn, 1998) or technologies of Gelassenheit (Heidegger, 1959; Ciborra and Hanseth, 1998), that is technologies which can tolerate a large range of human error or technical breakdown, providing sufficient time and room for starting counteractions as authentic, not disowned, expressions of concern.

Concluding Remarks

Information systems offer an interesting arena within which to study the complex and rapidly evolving relationship between digital technologies and risk. Given its intrinsic inter-disciplinarity, such a field has hosted in the past decades both the technical and managerial perspectives on risk management. However, the IS literature on risk has not been particularly innovative or rich in scope. Economic perspectives can help overcome some of its major limitations. They also help to reflect on the emerging ramifications of the joining up between advances in grid technologies, on the one hand, and the democratisation of financial tools on the other. The new financial order and its individualised risk management approach is a technology-based order, in which there is a reshuffling of the boundaries between the processes and activities that can be formally represented and the realm of ignorance. But the more sophisticated, integrated and standardised the technological platforms become, the more they tend to behave autonomously and drift. Sociological perspectives are needed to take into account the implications of emerging systemic risks, side-effects and runaway dynamics. Closer scrutiny is therefore required of the penetration and ubiquity of grid technologies and the opportunities they offer to manage a whole array of new risks surrounding the individual agent. A phenomenological perspective, based on the notion of risk as concern for concern itself, has been put forward in order to begin to capture and reflect upon the intricacies among life, risk and digital technologies.

References

Argyris, C., and Schoen, D.A. (1996) *Organization Learning II*, Reading, Mass: Addison-Wesley.

Arthur, W.B. (1994) *Increasing Returns and Path Dependence in the Economy*, Ann Arbor, University of Michigan Press.

Basel Committee on Banking Supervision (2001) Consultative Document: *Operational Risk, Bank for International Settlements*, Basel, January.

Beck, U. (1992) *Risk Society: Towards a New Modernity*, London, Sage.

Beck, U., Giddens, A., and Lash, S. (1994) *Reflexive Modernization: Politics, Traditions and Aesthetics in the Modern social Order*, Cambridge, Polity Press.

Beniger, J.R. (1986) *The Control Revolution: Technological and Economic Origins of the Information Society*, Cambridge, Mass., Harvard University Press.

Boehm, B.W. (1991) Software risk management: Principles and practices, *IEEE Software, January, 32– 41*.

Charette, R.N. (1996) The mechanics of managing IT risk, *Journal of Information Technology,* 11, 373– 78.

Ciborra, C. (1981) Information systems and transaction architecture, *International Journal of Policy Analysis and Information Systems,* 5, 4, 305– 24.

Ciborra, C. (1983), Markets, bureaucracies and groups in the information society, *Information Economics and Policy,* 1, 145– 60.

Ciborra, C. and Associates, (2000*) From Control to Drift – The Dynamics of Corporate Information Infrastructures,* Oxford, Oxford University Press.

Ciborra, C. and Hanseth, O. (1998) From tool to Gestell, *Information Technology and People,* 11,4, 305– 27.

Ciborra, C., Migliarese, P. and Romano, P. (1984) Analysing organizational noise, *Human Relations*, 37, 8, 565– 88.

Coase, R. (1960) The problem of social cost, *Journal of Law and Economics*. 15, 1, 1– 44.

Douglas, M. and Wildavsky, A. (1982) *Risk and Culture: The Selection of Technological and Environmental Dangers*, Berkley, CA, University of California Press.

Earl, M. J. (1996) (ed.) *Information Management: The Organizational Dimension*, Oxford, Oxford University Press.

Fairley, R. (1994) *Risk management in software projects*, IEEE Software, May, 57–67.

Giddens, A. (1990) *The Consequences of Modernity,* Cambridge, Polity Press.

Hanseth, O. and Braa, K. (2001) Hunting for the treasure at the end of the rainbow. Standardizing corporate IT infrastructure, *The Journal of Collaborative Computing.* 10, 3- 4, 261– 92.

Hart, O. (1995), *Firms, Contracts, and Financial Structures*, Oxford, Oxford University Press.

Heidegger, M. (1959), *Gelassenheit,* Tuebingen, Neske.

Heidegger, M. (1978) *The question about technology, in Basic Writings*, London, Routledge.

Herbst, P. (1974) *Socio-Technical Systems,* London, Tavistock.

Jaeger, C.C., Renn, O., Rosa, E.A. and Webler, T (2001) *Risk, Uncertainty, and Rational Action,* London, Earthscan.

Kahneman, D. and Tversky, A. (1979) Prospect theory: An analysis of decision under risk, *Econometrica*, 47: 263– 91.

Keil, M., Cule, P.E., Lyytinen, and Schmidt, R.C. (1998), A framework for identifying software project risks, *Communications of the ACM*, 41, 11, 76– 83.

Keen, P.W. (1991) *Shaping the Future: Business Redesign through Information Technology, Boston*, Harvard Business School Press.

Latour, B. (1999) *Pandora's Hope: Essays on the Reality of Science Studies, Cambridge, Mass.*, Harvard University Press.

Leavitt, H.J. (1964) *Applied organization change in industry: Structural, technical and human approaches,* in New Perspectives in Organization Research, Chichester, Wiley: 55– 71.

Loewenstein, G.F., Hsee, C.K. , Weber, E.U. and Welch, N. (2001) Risk as feelings, *Psychological Bulletin*, 127, 2, 267– 86.

Lyytinen, K. Mathiassen, L. and Ropponen, J. (1998) Attention shaping and software risk – A categorical analysis of four classical risk management approaches, *Information Systems Research*, 9, 3: 233– 55.

McFarlan, F.W. (1981) Portfolio approach to information systems, *Harvard Business Review*, 59, 5, 142– 50.

Malone, T.W., Benjamin, R.I. and Yates, J. (1987) Electronic markets and electronic hierarchies, *Communications of the ACM*, 30, 484– 97.

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

Mumford, E. (1996), Risky ideas in the risk society, *Journal of Information Technology*, 11, 321– 31.

Perrow, C. (1984) *Normal Accidents: Living with High-Risk Technologies*, New York, Basic Books.

Power, M. (2003) *The Invention of operational risk*, Discussion paper 16, CARR-LSE. June.

Power, M. (1997) *The Audit Society – Rituals of Verification*, Oxford, Oxford University Press.

Renn, O. (1998), Three decades of risk research: Accomplishments and new challenges, *Journal of Risk Research*, 1, 1, 49– 71.
Schumpeter, J.A. (1976) *Capitalism, Socialism and Democracy*, London, Routledge.

Shiller, R.J. (2003) *The New Financial Order – Risk in the 21st Century*, Princeton, Princeton University Press.

Steinmueller, W.E. (1996) *Technology infrastructure in information technology industries*, in M. Teubal, D. Foray, M. Justman and E. Zuscovitch (eds.) Technological Infrastructure Policy: An International Perspective, Dordrecht, Kluwer.

Suchman, L.A., (1987) *Planning and Situated Action*, Cambridge, Cambridge University Press.

Thompson, J. (1967) *Organizations in Action*, New York, McGraw-Hill.

Tversky, A. and D. Kahneman (1974) Judgement under uncertainty: Heuristics and biases, *Science*, 185: 1124– 31.

Weill, P. and Broadbent, M. (1998) *Leveraging the New Infrastructure: How Market Leaders Capitalize on Information*, Boston, Harvard Business School Press.

Williamson, O.E., (1975) *Markets and Hierarchies: Analysis and Anti-trust Implications*, New York, The Free Press.

Winner, L., (1977) *Autonomous Technology: Technics-out-of-control as a Theme for Political Thought*, Cambridge, Mass., The MIT Press.

CARR Discussion Paper Series

Risk Regulation and Interest Accommodation: Pharmaceuticals' licensing in the European Community
Jurgen Feick DP 25

Decentralisation of Economic Law – An Oxymoron
Myriam Senn DP 28

Regulatory Experiments
Javier Lezaun and Yuval Millo DP30

Coming Soon

Digital Technologies and the Duality of Risk
Claudio Ciborra DP 26

From Risks to Second-order dangers in Financial Markets: Unintended consequences of risk management systems
Boris Holzer and Yuval Millo DP29

Modernisation, Partnership and the Management of Risk
Peter Miller and Liisa Kurunmaki DP 31

Available now in print from http://www.lse.ac.uk/collections/CARR/documents/discussionPapers.htm

The Role of Civil Society Organisations in Regulating Business.
Bridget M. Hutter and Joan O'Mahony DP 26

The Battle for Hearts and Minds? Evolutions in organisational approaches to environmental risk communication
Andy Gouldson, Rolf Lidskog & Misse Wester-Herber DP24

Creation of a market network: the regulatory approval of Chicago Board Options Exchange (CBOE)
Yuval Millo DP23

The Interaction of 'Civil' and Public International Regulation: Lessons from the Energy and Biodiversity Initiative
Stephen Tully DP22

Access to Justice within the Sustainable Development Self-Governance Model
Stephen Tully DP21

Justifying Non-Compliance. A Case Study of a Norwegian Biotech Firm
Filippa Corneliussen DP20

The Impact of Regulations on Firms. A Study of the Biotech Industry
Filippa Corneliussen DP19

Reforming the UK Flood Insurance Regime. The Breakdown of a Gentlemen's Agreement
Michael Huber DP 18

Mapping the Contours of Contemporary Financial Services Regulation
Julia Black DP 17

The Invention of Operational Risk
Michael Power DP 16

Precautionary Bans or Sacrificial Lambs? Participative Risk Regulation and the Reform of the UK Food Safety Regime
Henry Rothstein DP 15

Regulating Parliament: the regulatory state within Westminster
Robert Kaye DP 13

Business History and Risk. Terry Gourvish
Business Risk and Antitrust: comparative perspectives
Tony Freyer
The Risks of Working and the Risks of Not Working: historical perspectives on employers, workers, and occupational illness
Joseph Melling DP 12

The Open Method of Co-ordination and the European Welfare State
Damian Chalmers and Martin Lodge DP 11

Drivers and Drawbacks: regulation and environmental risk management systems
Marius Aalders DP 10

Conceptualising Insurance: risk management under conditions of solvency
Michael Huber DP 9

Social Licence and Environmental Protection: why businesses go beyond compliance
Neil Gunningham, R.t Kagan & Dorothy Thornton DP 8

Neglected Risk Regulation: the institutional attenuation phenomenon
Henry Rothstein DP 7

Mass Media and Political Accountability
Tim Besley, Robin Burgess and Andrea Pratt DP 6

Embedding Regulatory Autonomy: the reform of Jamaican telecommunications regulation 1988-2001
Lindsay Stirton and Martin Lodge DP 5

Critical Reflections on Regulation
Julia Black DP 4

The New Politics of Risk Regulation in Europe
David Vogel DP 3

The EU Commission and National Governments as Partners: EC regulatory expansion in telecommunications 1979-2000
Mark Thatcher DP 2

Regulating Government in a 'Managerial' Age: towards a cross-national perspective
Christopher Hood and Colin Scott DP 1

Is Regulation Right? Robert Baldwin
Business Risk Management in Government: pitfalls and possibilities Christopher Hood and Henry Rothstein
Risk Management and Business Regulation
Bridget Hutter and Michael Power DP 0