Maurizio Cavallari

Risk, Security and Organizational Aspects

Informatica & Organizzazioni

FrancoAngeli

Maurizio Cavallari

Risk, Security and Organizational Aspects

FrancoAngeli

The present book has been double peer reviewed

Contents

The author wishes to thank prof. Leslie Willcocks, prof. James Backhouse and prof. Edgar Whitley of the London School of Economics, and prof. Richard Baskerville of Georgia State University. Their scholar works and research have been of most importance for the education of the author. Since the meetings in the early 90's for EU projects, and through the studies and interactions in the last years, their influence has been a cornerstone in author's development of the academic thought.

1. Methodological Matters

1.1. The Purpose

Risk and Security matters are commonly characterized as being part of every day life, organizations, online, personal and business environments (Luhmann, 1993). They feature almost every human activity and they represent an important step in the evolution of human beings (Adams, 1995) (Ritchie & Brindley, 2007).

The purpose of this book is to investigate major research findings about risk and security from a social point of view (Sandaman, 1988), taking into account important contributions from social scholars and research into science, technology and society (Gallivan *et al.*, 2005), in order to arrive to the definition of organizational issues (Jasperson *et al.*, 2005).

The arriving point is the impact of the mentions dimensions (i.e. risk and security) into organizations (Wynne, 1982), for a variety of composed aspects, operational risk, market risk, information risk, safety on the workplace and the like.

In the Information Systems (IS) field, researchers have successfully identified a number of key factors influencing individual adoption of new Information Technologies (IT) which relate directly to risk and security (Volti, 2001) (Venkatesh *et al.*, 2003).

However, extant research sheds little light on the antecedents of ongoing or continued usage (Karahanna *et al.* 1999), the relationship between individual and institutional concepts of risk and security is also problematic, and at first glance, it appears that extant theory is of little use in terms of understanding, perceiving and evaluating the mentioned concepts (Gallivan *et al.*, 2005).

1.2. The Methodology

This section presents an overview of the methodological matters that guided the study of the present monograph. It comments interpretivism, comments on the possible role of theory in this study and discusses the research strategy of the author itself as the antecedent, and including some discussion and speculation of previous research findings that proved to be particularly useful.

Myers argues that a "research method is a strategy of inquiry which moves from the underlying philosophical assumptions to research design and data collection" (Myers, 1997). A research strategy is chosen according to the fit, between it, and the purpose of the study and the nature of the research question posed (Marshall & Rossman, 2006).

Broadly speaking, one must decide what philosophical perspective will underpin the study and one must choose a qualitative, quantitative or mixed strategy.

1.3. Philosophical Perspective

Philosophical perspectives are also known as paradigms, and are defined by Guba and Lincoln as "basic belief systems based on ontological, epistemological and methodological assumptions" and described as "axiomatic systems… differ[ing] from one another on matters much more fundamental than the locale in which the inquiry is conducted, the format of the inquiry report, or the nature of the methods used" (Guba & Lincoln, 1994).

We intend for the purpose of this monograph here a "paradigm" as a basic belief system or a worldview that guides the researcher.

The emphasis is on the paradigms, their assumptions, and the implications of those assumptions for research. In the research timeline, authors have criticized the over-quantification and the received view of knowledge, noting such issues as the theory-laden and value-laden nature of facts and the relationship between the inquirer and the object of the inquiry (Willcocks & Whitley, 2009).

The paradigms most commonly discussed are: positivism, post-positivism, critical theory, and constructivism.

Prior to research into risk and security organizational issues, those paradigms must be then examined with regard to ontology (what is the form and nature of reality), epistemology (what is the nature of the relationship between the knower and what can be known), and methodology (how can

the inquirer go about finding out whatever he/she believes can be known) (Guba & Lincoln, 1994).

The main philosophical perspectives or paradigms discussed in the subject of this work are positivist, interpretivist and critical (Chua 1986) (Orlikowski & Baroudi 1991).

Positivism continues to dominate (Orlikowski & Baroudi 1991) (Walsham 1995) (Davison et al., 2004) but interpretivism has been gaining steady ground (Lindgren, 2004) (Rescher, 2000).

The aim of interpretivism is to gain understanding rather than to be able to make predictions (Orlikowski & Baroudi, 1991). Interpretive studies generally attempt to achieve this understanding of phenomena through the meanings that people assign to them (Walsham, 1995).

More specifically, interpretive research aims to develop a richer understanding the complex world of lived experience from the point of view of those who live it.

The ontological assumptions of interpretivism (which is sometimes refer to as constructivism) can be labeled as relativist: "realities are apprehendable in the form of multiple, intangible mental constructions, socially and experientially based, local and specific in nature… and dependent for their form and content on the individual persons or groups holding the constructions" (Guba & Lincoln, 1994). Interesting contributions by Winograd and Flores and, more recently, by Davison, and Baskerville and Myers points to shed light on the perceptions of individuals and how these perceptions are shaped by the experiences of those individuals, which are local, specific and dynamic, and others, represented in discourse (Winograd & Flores, 1986) (Davison et al., 2004) (Baskerville & Myers, 2002).

1.4. The Theory Baseline

In the interpretivist tradition, the goal is not to develop testable theory but to grasp the "complex world of lived experience" (Gregor, 2006). Theory is a way of seeing and not seeing and can be seen as an initial guide to design and data collection, as part of process of collection and analysis and as final product (Walsham, 2006).

As Clarke states, "The study of new phenomena depends on a framework being developed that identifies and describes key elements and their inter-relationships, and enables an appreciation of their impacts, and their implications for various actors. Only then does the location and application of suitable bodies of theory become feasible" (Clarke, 2008).

Thus, this monograph finds its foundations within an integrative framework drawn from a variety of theoretical sources.

These include theories of Risk, Rational Action and Human Factor (the social construction of interaction), theories of Organizational Behavior and Security (theory of reasoned action and theory of planned behavior) as well as theories from the IS field itself (theories of technology acceptance and continuance).

This framework is used to describe key elements and their inter-relationships and allows an appreciation of their impacts and implications for various actors, in particular for organizations.

1.5. Qualitative and Quantitative Methods

Qualitative methods are believed to "come more easily to the human as instrument" by the opinion of Guba and Lincoln and qualitative data are seen as "a source of well-grounded, rich descriptions and explanations of processes in identifiable local contexts" (Guba & Lincoln, 1997, 2005), see also (Miles & Huberman, 1994). Thus, they are fundamentally well-suited for locating the meaning people place on the events, processes, and structures of their lives (Baskerville, 2001) (Silverman, 2005).

However, qualitative research is becoming increasingly fragmented, qualitative data analysis is now a vast field (Atkinson & Delamont, 2005) (Maxwell, 2004) and data analysis methods are not well formulated (Miles and Huberman, 1994, 2002).

Probably for that reason, qualitative research attracts also critics. For instance, Gable identifies three major weaknesses of qualitative research: (1) the inability to manipulate independent variables, (2) the risk of improper interpretation, and (3) the lack of power to randomize (Gable, 1994), see also (Marshall & Rossman, 2006) and (Myers, 1997).

Quantitative approaches to research are not contemplated in the present monograph (Vose, 2008).

2. Risk and Security: Subtle Definitions

2.1. Risk

With respect to the purpose of this monograph it is very useful to start from the very general concepts in order to arrive to the organizational aspects.

Humanity has been facing risks throughout its whole history, but nowadays risks show completely new features. This is due to the fact that the world is more and more interdependent. Past research identify three relevant trends to explain the unfolding, new characteristics of today's risks (Rosa, 1998):

- globalized industrial production,
- international division of labor, and
- global availability of consumer goods.

As a consequence of these trends, in fact, for the first time in history, more and more people throughout the world tend "to share a common set of risks. No one could escape a nuclear holocaust, ozone depletion, the consequences of monoculture and species extinction" (*ibidem*).

In this process, a key role is played by scientific and technological innovation. Innovation, in fact, has dramatically reduced many "old" risks (such as infant mortality due to infections) that our ancestors were used to cope with daily; but, on the other hand, each innovation seems to foster new, unintended risks. Our modern world has to face "technologically induced uncertainty" (Jaeger et al., 2001).

A risk is a chance of something bad or dangerous occurring and, hence, should be avoided. Avoiding risks at all is, however, impossible; risks are endemic to our life, both from a personal and professional standpoint (Thompson & Bloom, 2000), so cope with risk is a life long activity. Un-

certainty and risk are not exactly the same concepts (Fiegenbaum and Thomas, 1988). In fact certain risks, however, are not regarded in that sense: dealing with stocks in electronic markets can drive to gains also, so risk actually is a twofold dimension. Both gain and loss are at risk in a way that the *àlea* (Latin word for "uncertain event").

The above-mentioned authors point out three key differences between modern societies and the past ones, with regard to risks and uncertainty. These differences are here summarized in the following table:

Table 1 – Risk/Timeline Matrix

	Past Risks	Today's Risk
Risk type/origin	Proximate, specific	Eco-systemic
Risk impact	Circumscribed	Global
Risk awarness	Local	International

Source: Elaboration of relevant literature

Jaeger refers to Giddens and Beck to state that "the spirit of our age is the universal concern with hazards in contemporary world, the vulnerability of the environment, and of the human species itself" as we live in the, so called, risk society (Jaeger et al., 2001) (Giddens, 1990). The same authors give us a view of adopting risk as the imprimatur of our age, as we are forced to rethink the expectations of progress that were typical of the Western thought since the "Enlightenment", and as Beck says, "the dark sides of progress increasingly come do dominate the social debate" (ibidem).

Normally, humans can be confident that tomorrow they will wake up and they will find the essential features of their material and social context unchanged. This confidence is essential for self-identity building, and then collective life (with its rules, expectations, and bonds) must ensure a sufficient degree of regularity to guarantee what Giddens calls "ontological security" (Giddens, 1990, 1991).

Thus, today's socio-technical risks, far from being problems regarding merely what is specifically at stake each time, are literally threats to ontological security, just like eclipses resulted in dreadful, ontological derangements in pre-scientific societies, when major risks and uncertainties came from the natural world.

As a consequence, "worries about risks are not just individual problems, but problems of a growing collective consciousness" (Jaeger et al., 2001). That's why we deem that risk is a matter that needs rooting in sociological analysis.

As research suggests, we shall use, in order to understand the exposed, broad-bound, concept of risk sociological imagination, investigation and tools to seek answers to Kant's two key questions: "How did things get this way? How can we understand what needs to be done about them?" (Giddens, 1991).

The key elements of risk management, from an organizational perspective, can be pointed out as follows:

- risk perception;
- risk identification;
- risk quantification;
- risk mitigation/control;
- risk financing;
- rare events.

2.1.1. Risk Perception

Understanding risk is hence a fundamental point to managers and people make good choices. The criticality of an effective approach to risk management is becoming increasingly recognized. For instance, Chapman and Ward argue that poor risk management is a most decisive factor (Chapman & Ward, 2003). Thus, risk management is a core capability area of every human and organization and represents one of the most critical factors in ensuring successful management. Unfortunately, human abilities to objectively estimate probabilities of future events while deriving those from past experience are notably limited (Papadaki & Furnell, 2010). Such limits apply when managers attempt to make quantitative estimates related to impacts of many, partially interacting risk factors (Ritchie & Brindley, 2007). Thus, despite the fact that decisions and actions about activities where risk is an issue, are generally intended as to be based on structured risk assessment methods, in practices, and in organizations especially, these decisions and actions appear to be the consequences of risk perception.

Risk perception takes into account an estimation of the frequency of incidents or adverse events, which occurred in the past as well as the damage caused by those. All risk concepts refer to "uncertainty" and are hence intrinsically based on a distinction between what is certain and someway objectively assessable (truth) and something conceivable and possible, but uncertain (possibility). Uncertainty is a subjective construct, thus, "it exists only in the mind" (Papadaki & Furnell, 2010). Thus, within organizational

context, the conception of risk assessment fails in meeting the actual behavioral phenomenon of risk taking (Fishbein & Ajzen, 1975) (Fishbein, 2007).

Risk perception relies then on a subjective estimation of the expected frequency of a certain type of event carrying, both, a potentially negative effect, and a possible consequence in terms of future loss.

Correspondingly, risk perception is depending on a personal evaluation of the probabilities that a person generate in his own mind, which represents his/her own "uncertain convincement" about the occurrence of future events and their consequences.

We can conclude that risk perception depends on a variety of antecedents such as the individual experience, knowledge, personal attitudes, mind openness and the complexity of organization values and rules that formed and developed the definition of the individuals' beliefs and feelings (ibidem).

2.1.2. Risk Identification

In many cases (e.g., when walking across a road) risk identification is just a matter of paying attention. This is true also in business settings, where even inexperienced people can identify several situations as risky, on the basis of common sense.

In seek of a definition of risk in a precise, identifiable, way, despite the wide range of meanings and connotations that this word features in common usage, we find Mergolis and Renn, they identify three fundamental elements to be considered together to understand the idea of risk, (Mergolis, 1996) (Renn, 1992):

- **possibility**: humans perceive a risk if they think that some outcome is possible.
- **uncertainty**: there is a risk if a possible future event can't be predetermined with certainty.
- **impact**: there is a risk only if a possible but uncertain future state of the world can impact human reality and stakes.

In addition, there is a fourth element: their conception of risk implies that human beings can try to anticipate the future and to improve their possibilities; this idea is, of course, incompatible with fatalistic views. The worst risks, of course, are the unpredictable ones. Research into risk identi-

fication cite the case of asbestos exposure: as long as people were unaware of the risks associated with airborne asbestos fibres, companies producing, buying and using asbestos were unable to evaluate both, risk of health damages, and the legal consequences of their choices.

But many other types of risks may be less apparent and identifying them may require specific experience and know-how.

As a result, when associations between asbestos exposure and some fatal pathologies became evident, there was an explosion of litigations that destroyed not only asbestos producers, but also companies that had just become owners, through acquisition, of other companies that had previously used asbestos in their productive cycles (the recent italian dramatic case of Eternit of Casale Monferrato – Alessandria, is very eloquent about the matter).

As academic literature demonstrates, "liabilities also may be inherited, which makes mergers and acquisitions problematic these days" (Junkui & Jaafari, 2003).

A company, then, should strongly engage in understanding the risks it's involved in. The worst risks are those which reveal at the very moment the bad chance occurs.

2.1.3. Risk Quantification

After a risk is identified, the second step is to quantify its magnitude.

Again, lack of experience in the specific field, and/or lack of analysis of the actual situation with respect to similar situations already occurred, can have fatal consequences.

We can adopt, with Rosa, the following definition of Risk:

"A situation or event in which something of human value (including humans themselves) has been put at stake and where the outcome is uncertain" (Rosa, 1998).

Key features of the definition above are the following:

- risk is defined as an ontological state of the world;
- human understanding of risk is an epistemological matter, involving "perception, investigation, judgment, evaluation, and claims";
- the definition embeds the conventional probabilistic definition of risk "as the probability of an occurrence or event multiplied by the value of the outcome of that event";
- this notion of risk implies that human beings anticipate the consequences of the various possible outcomes, evaluate their desirabil-

ity, and choose. “The notion of risk adds incentives to make causal connections between present actions and future outcomes”.

Different risk perspectives can then be distinguished on the basis of how each perspective addresses the four following questions:

1. conceptualization of uncertainty: “what concept of possibility is used?” (e.g., probability);
2. scope of consequences: “what types of outcomes/consequences are considered?” (e.g., undesirable consequences)
3. combination rules: “how are the concepts of possibility and outcome combined?”
4. actor involved in making decisions: “who is the actor that judges the three questions above?” (e.g. an individual, or an institution).

In the following sections of this book, these four questions will be used to provide the framework for distinguishing and evaluating different perspectives on the issue of risk.

Research into risk and economics involved in it, cites Federal Mogul’s 1998 acquisition of a Manchester company. This company had used asbestos in previous years; Federal Mogul was aware of it at the time of the acquisition, and set aside $ 2.1 billion to cover the claims (Rodengen, 1998).

But the sum was nowhere near enough, and Federal Mogul in 2002, had to seek bankruptcy protection for the asbestos liability inherited (Ewg, 2002).

A clear example of insufficient or inaccurate quantification of economic risk for the organization.

2.1.4. Risk Mitigation and Control

When the risk exposure has been assessed (i.e., identified and quantified), a subject can take control of the situation by considering the different choices available (Junkui & Jaafari, 2003).

In many cases, it is possible either to entirely avoid the risk (e.g. by not crossing the road at all, or by renouncing the acquisition), or to choose among a full range of risk levels, each with different cost-benefits trade-offs.

Here, tactics for mitigating risk exposure come into play. Two types of activities are possible:

- loss prevention measures, which include all the activities aimed at

making bad outcomes impossible or less probable (e.g., regular inspections of the electrical wiring);

- loss reduction measures, which include all the activities aimed at reducing the magnitude of losses, when losses occur (e.g., sprinklers don't reduce the probability of fire, but if fire occurs, they reduce the damage).

2.1.5. Risk Financing

Risk mitigation, of course, has a cost.

In many cases, a way to minimize this cost is to shift the risk to a third party. As Rosa excellently describes: "The problem here, of course, is that if one is fully insured against a loss, then one has no incentive to take (privately costly) actions to reduce one's risk exposure […]. This is generally the trade-off that you will find in your personal and professional risk financing decisions – increased investment in risk elimination reduces the premiums you pay per dollar of coverage, but the down side is that you are exposed to more risk" than that to which are exposed fully insured people (Rosa, 1998).

2.1.6. Rare Events

When a very bad outcome occurs, despite all loss prevention/loss reduction measures previously provided, catastrophe planning must quickly come into play.

The difference between the loss reduction measures exposed above and loss reduction strategies that must be activated in case of disaster is the following: loss reduction measures are provided previously, to face possible and "standard" bad outcomes in the future, whereas loss reduction strategies and catastrophe planning are the consequence of the "cultural" response to disaster, after the catastrophe has occurred.

Good catastrophe planning can result in dramatic loss reduction. As an example, Crocker cites how Johnson&Johnson managed the terrible problem that occurred when an unidentified individual put poison in several bottles of a Johnson&Johnson medicine, causing the death of a person. Johnson&Johnson "didn't attempt to deflect blame (after all, they hadn't adulterated the capsules) or otherwise temporize. They immediately recalled all the capsules from store shelves – even those that were clearly untainted - and then designed the generation of tamper-proof containers still in use to-