

Summer 6-19-2015

Risk, Human Behavior, and Theories in Organizational Studies

Maurizio Cavallari

Dept. S.E.Gest.A, Università Cattolica (Milano), Italy, maurizio.cavallari@unicatt.it

Marco De Marco

Facoltà di Economia, Università Telematica Nettuno (Roma), Italy

Cecilia Rossignoli

Dept. di Economia Aziendale, Università di Verona (Verona), Italy

Nunzio Casalino

Dept. Strategie di Impresa e Innovazione Tecnologica, Università G. Marconi (Roma), Italy

Follow this and additional works at: <http://aisel.aisnet.org/whiceb2015>

Recommended Citation

Cavallari, Maurizio; Marco, Marco De; Rossignoli, Cecilia; and Casalino, Nunzio, "Risk, Human Behavior, and Theories in Organizational Studies" (2015). *WHICEB 2015 Proceedings*. Paper 55.

<http://aisel.aisnet.org/whiceb2015/55>

This material is brought to you by the Wuhan International Conference on e-Business at AIS Electronic Library (AISeL). It has been accepted for inclusion in WHICEB 2015 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Risk, Human Behavior, and Theories in Organizational Studies

Maurizio Cavallari^{1*}, Marco De Marco², Cecilia Rossignoli³, Nunzio Casalino⁴

¹Dept. S.E.Gest.A, Università Cattolica (Milano), Italy

²Facoltà di Economia, Università Telematica Nettuno (Roma), Italy

³Dept. di Economia Aziendale, Università di Verona (Verona), Italy

⁴Dept. Strategie di Impresa e Innovazione Tecnologica, Università G. Marconi (Roma), Italy

Abstract: The present paper regards risk, threats and organizational issues that are associated with human behavior; e.Business is no exception^[2]. Organizational actors in e.Business organizations make security decisions with a wide variety of meanings^[3]: information systems interactions, access to physical premises, behavior within the workplace, utilization of tools and work instruments, are just a few examples of the realm of security decisions that are made within all organizations, and e.Business organizations in particular. The way in which the risk is perceived greatly influences any decision. The aim of the present paper is to conjugate general risk theories in terms of human behavior and system security (as opposed to system risk) in order to identify a common baseline of risk and behavior, that will lead eventually lead to a structured framework that will contribute to the discipline of organizational studies.

Keywords: e.Business, eBusiness, risk, human behavior, organization, organizational studies, security, perception, threats

1. INTRODUCTION

Research into risk and the organizational issues associated with it, agree on differentiating risks and threats as Beckhouse et al.^[2] and D'Arcy et al.^[11] state. Scholars and commentators, like Dourish et al.^[16], Karat^[25], Karat et al.^[26], Mitnick^[31] and Schneier^[36], define the boundaries of the threat, risk and organizational action; where risk is the probability of an event, and threat is the potential harmful outcome of that risk to the organization.

Organizational actors in e.Business organizations make security decision in a wide variety of meanings. Information systems interactions, access to physical premises, behavior within the workplace, utilization of tools and work instruments, are just a few examples of the realm of security decisions that are made within all organizations, and e.Business organizations in particular. We argue in the present paper that risk is always associated with a specific threat. In some authors' opinion, like in Roth et al.^[35], Karat^[25] and Karat et al.^[26], with which we agree, the variety of theories about human behavior, in a particular situation of risk that involves an action or decision by the user and that is subject to "unpredictable" risk, is particularly significant, and could involve the whole organization. Therefore, understanding how users perceive risk and make security decisions is of great importance in understanding organizational security issues and how user interaction impacts risk.

The aim of the present paper is to conjugate general risk theories in terms of human behavior and system security (as opposed to system risk), like in Fishbein and Ajzen^[19] and in D'Arcy et al.^[11], in order to identify a common baseline for to risk and behavior, which will lead eventually to a structured framework that will contribute to the discipline of organizational studies, with particular emphasis on e.Business organizations^[11]-^[19]. For this reason, when issues and arguments are addressed to "organizations" in the present work, they should be perceived to pertain to the e.Business organizations, as in Beckhouse^[3].

* Corresponding author. Email: maurizio.cavallari@unicatt.it

2. RISK

For the purpose of this paper, it is useful to begin with general concepts in order to arrive at organizational aspects.

Humanity has been facing risks throughout history. However risks exhibit completely new features, as demonstrated by Jaeger et al.^[23] and Ritchie and Brindley^[33]. This is because the nations of the world have become more and more interdependent. Past research^[23] has identified three relevant trends that explain the unfolding new characteristics of today's risks, as also in Renn^[32] and Rosa^[34]:

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

The authors summarize their research from a meta-theoretical framework into three key points. They are “*reconstructed realism*”, “*external world of realism*”, and “*ontological realism*”.

They suggest that risk represents a situation in which human concern about a certain outcome depends in part on the uncertainty of the outcome itself.

By understanding that knowledge of reality differs from objective reality, people may overcome limitations in the actual situation that they recognize, Dhillon^[12].

Risk perception is no exception. The researchers who were mentioned above, like Jaeger et al.^[23], Rosa^[34] and Renn^[32], state that human limitations preclude convergence of risk humans' understanding of it.

As a consequence of these trends, more and more people throughout the world tend “*to share a common set of risks*, for the first time in history. *No one could escape a nuclear holocaust, ozone depletion, the consequences of monoculture and species extinction*”, as in Crocker^[10]. In this process, scientific and technological innovations play key roles. Innovation has dramatically reduced many previous risks (such as infant mortality due to infections) that our ancestors coped with daily. However, each innovation seems to foster new, unintended risks. Our modern world faces “*technologically induced uncertainty*”, as in Dhillon^[12] and Jaeger et al.^[23]. A risk is a chance that something bad or dangerous will occur and should be avoided. However, avoiding all risk is impossible. Risks are endemic in our lives, from both a personal and a professional standpoint. Therefore, coping with risk is a life long activity, as stated by Fiegenbaum and Thomas^[18]. In a case-study based research, Baskerville et al.^[4] provide an excellent insight into the balance between prevention paradigm and response paradigm approaches to information security management.

Uncertainty and risk are not exactly the same concepts, following aforementioned authors' opinion^[18]. However, certain risks are not regarded in that sense, such as dealing with stocks in electronic markets that may produce. Therefore, risk is actually two-d dimensional.

The abovementioned authors^[18] point out three key differences between risks and uncertainty in modern and past societies. These differences are summarized in the following table:

Table 1. Risk/Timeline matrix

	Past Risks	Current Risks
Risk type/origin	Proximate, specific	Eco-systemic
Risk impact	Circumscribed	Global
Risk awareness	Local	International

Jaeger et al.^[23] refers to Giddens^{[21]-[22]} to contribute with the statement 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. 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

western thought since the “Enlightenment”. As Dourish et al. ^[16] say, “*the dark sides of progress increasingly come to dominate the social debate*”. Normally, humans can be confident that they will awaken tomorrow and find that the essential features of their material and social contexts are unchanged.

This confidence is essential for self-identity building. Collective life (with its rules, expectations, and bonds) must ensure that there is a sufficient degree of regularity to guarantee what Giddens calls “*ontological security*” ^{[21]-[22]}. Thus, today’s socio-technical risks, instead of formerly being problems regarding what specifically is at stake each time, are literally threats to ontological security, like the eclipses that caused dreadful, ontological derangements in pre-scientific societies, when major risks and uncertainties arose from the natural world. As a consequence, adhering to Jeager et al. opinion we can say that, “*worries about risks are not just individual problems, but problems of a growing collective consciousness*” ^[23]. That is why we deem risk to be a matter that needs rooting in sociological analysis. In order to understand the exposed, broad concept of risk regarding sociological imagination, we shall use, as research by Giddens ^[22] suggests, 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?*”.

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

- risk perception,
- risk identification,
- risk quantification,
- risk mitigation/control,
- risk financing, and
- rare events (dealing with).

2.1 Risk management

Understanding risk is essential if managers and individuals are to make good choices. Criticality in an effective approach to risk management is increasingly recognized, in organizational action. For instance, Chapman and Ward ^[9] argue that poor risk management is a most decisive factor.

Thus, risk management is a core capability area of every individual and organization and represents an essential factor in ensuring successful management. Unfortunately, the human ability to objectively estimate the probability of a future event while deriving those probabilities from past experiences is notably limited ^[5].

2.1.1 Risk perception

Ongoing research into risk management and performance, like the contribution by Ritchie and Brindley ^[33], suggests that vulnerabilities are very relevant to an understanding of how people behave and perceive risk. Past experiences are relevant in evaluating decisions, and are especially important when critical choices will be made, as D’Arcy et al. ^[11].

Researchers have been developing powerful tools to neutralize possible distortions that lead to erroneous risk estimation. Employing these instruments in the assessment and evaluation processes can be useful.

Important aspects to understand are how to control and mitigate risk with good approximation, how future programs may succeed or fail, and how to minimize possible losses.

Decisions in situations of uncertainty occur every day, especially in the work environment. Because personal behavior may influence the correct application of these techniques or instruments, their application to reduce risks may encounter be limited consistently. In the case of management decisions, this can occur when relevant decisions are implemented ^[5]. Such limits apply when managers attempt to make quantitative estimates of the impacts of many partially interacting risk factors ^[33]. This is crucial for risk perception as everyone needs to manage and mitigate risk. Frequently, risk is under valued. This implies a consistency distortion in

the evaluation process, as in Misra et al.^[30]. Thus, despite the fact that decisions and actions that involve activities for which risk is an issue are generally intended to be based on structured risk assessment methods, they often appear in practice to be the results of risk perception (especially in organizations).

Risk perception takes into account an estimation of the frequency of incidents or adverse events that occurred in the past, as well as the damage caused previously. All risk concepts refer to “uncertainty” and are intrinsically based on the distinction between what is certain and what is, in some way, objectively assessable (truth), and what it is possible, but uncertain (possibility). Uncertainty is a subjective construct. Thus, “*it exists only in the mind*” as defined by Michell^[29]. Thus, within an organizational context, the conception of risk assessment fails to meet the actual behavioral phenomenon of risk taking, as in Fishbein and Ajzen^[19] and Fishbein^[20]. Risk perception relies on a subjective estimation of the expected frequency of a certain type of event, both a potentially negative effect and future loss that it could cause. Correspondingly, risk perception depends on a personal evaluation of the probabilities. It represents what he or she believes will occur in the future and the consequences.

We can conclude, speculating from past research findings by Chapman and Ward^[9], and by Crocker^[10], that risk perception depends on a variety of antecedents, such as individual experience, knowledge, personal attitude, mind openness, and the complexity of organizational values and rules that form and develop the individual beliefs and feelings.

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 also is true in business settings, where even inexperienced people can identify several situations as being risky, on the basis of common sense.

In seeking a precise, identifiable definition of risk, in view of the term’s wide range of meanings and connotations in common usage, Mergolis^[28] and Renn^[32] identified three fundamental elements to consider in order to understand the concept of risk:

- Possibility: humans perceive a risk if they think that some negative outcome is possible.
- Uncertainty: there is a risk if a possible future event cannot be pre-determined with certainty.
- Impact: there is 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 attempt to anticipate the future and improve possible outcomes. This idea is incompatible with fatalistic views.

The worst risks are unpredictable. Research into risk identification cites the case of asbestos exposure. As long as people were unaware of the risks that are associated with airborne asbestos fibers, companies that were producing, buying, and using asbestos were unable to evaluate both the risk of health damage and the legal consequences of their choices. However, many other types of risks may be less apparent, and identifying them may require specific experience and knowledge. As a result, when it became evident associations that there was a link between asbestos exposure and fatal pathologies there was an explosion of litigation that destroyed not only asbestos producers, but also companies that had just become owners by acquisition of other companies that had previously used asbestos in their productive cycles. Academic literature demonstrates, in a clear argument by Junki Yao and Jaafari^[24], that “*liabilities also may be inherited, which makes mergers and acquisitions problematic these days*”. A company should endeavor to understand the risks of activities in which it is involved. The worst risks are those that are revealed at the very moment at which the negative result occurs.

2.1.3 Risk quantification

After identifying a risk, the next step is to quantify its magnitude.

Magnitude depends on a series of factors, such as the type of approach (how will I cover it and how will people deal with it?). This is difficult to quantify. For that reason a methodological approach is necessary to define risk quantification. Again, lack of experience in a specific field, and/or lack of analysis of the actual situation relative to similar situations that have already occurred can have fatal consequences.

We can adopt the following definition of risk, given by Rosa^[34]:

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

The key features of the definition are the following:

- Risk is defined as an ontological state of the world.
- Human understanding of risk is an epistemological matter that involves “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”*^[34].
- This notion of risk implies that human beings anticipate the consequences of various possible outcomes, evaluate their desirability, and choose. *“The notion of risk adds incentives to make causal connections between present actions and future outcomes.”*^[34].

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

- conceptualization of uncertainty: what concept of possibility is used? (e.g., probability);
- scope of the consequences: what types of outcomes/consequences are considered? (e.g., undesirable consequences);
- combination rules: how are the concepts of possibility and outcome combined?;
- 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 paper, the four questions that appear above will provide the framework for distinguishing and evaluating different perspectives on the issue of risk.

Research into risk and the economics involved in it refers to Federal Mogul’s 1998^[17] acquisition of a Manchester company. This company had used asbestos in previous years; Federal Mogul was aware of this at the time of the acquisition, and set aside \$2.1 billion to cover the claims. However, the sum was nowhere nearly enough and, in 2002, Federal Mogul had to seek bankruptcy protection for the asbestos liability that it had inherited^[17]. This is an example of insufficient or inaccurate quantification of economic risk for the organization.

2.1.4 Risk mitigation and control

When risk exposure has been assessed (i.e., identified and quantified), a subject can take control of the situation by considering the different choices available to it, according to Junki Yao and Jaafari^[24].

In many cases, it is possible either to avoid the risk entirely (e.g., by not crossing the road at all or by renouncing the acquisition) or to choose from a full range of risk levels, each of which offers cost-benefit trade-offs. Here, tactics for mitigating risk exposure come into play. The following activities are possible:

- loss prevention measures, which include all the activities that seek to make bad outcomes impossible or less probable (e.g., regular inspections of electrical wiring);
- loss reduction measures, which include all the activities that seek to reduce the magnitude of losses, if they occur (e.g. sprinklers do not reduce the probability of fire; however, if a fire occurs).

2.1.5 Risk financing.

Risk mitigation has a cost. In many cases, the method that is used to minimize this cost is to shift the risk to a third party. As Rosa^[34] 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”*.

Cost is a central problem when we are dealing with risks. There is a trade-off between the cost of insuring against risks and the will to support the risk without paying a specific amount of money. The correct amount of money that a single organization must pay to ensure that the probability of risk will be reduced to zero is one of the most debated questions in academic literature, as Beckhouse et al.^[2], Beckhouse^[3], Baskerville^[4], Downland and Furnell^[14], Downland et al.^[15], Chapman and Ward^[15], Mergolis^[28], Renn^[32] and Rosa^[34].

2.1.6 Rare events.

When there is a very bad outcome, despite all loss prevention/loss reduction measures that had been provided, catastrophe planning must quickly commence.

The difference between the loss reduction measures discussed above and loss reduction strategies that must be activated in the case of a disaster is the following: loss reduction measures are provided in order to deal with possible and “standard” bad outcomes in the future, whereas loss reduction strategies and catastrophe planning are consequences of a “cultural” response to disaster after the catastrophe has occurred.

Good catastrophe planning can result in dramatic loss reduction. As an example, Crocker^[10] cites how Johnson & Johnson managed the terrible problem that occurred when an unidentified individual added poison to several bottles of a Johnson & Johnson medicine, thereby causing someone's death. 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 today. This is a textbook loss-reduction strategy—timely, aggressive, and (while costly in the short run) effective”*.

2.2 Approaches to risk.

Central to modern decision-making, the study of risk has been widely developed in several disciplines, such as natural sciences, engineering, economics, and other social sciences.

Many approaches have been developed to study risk. They include:

- decision analysis,
- quantitative risk assessment,
- psychometrics,
- insurance and portfolio investment,
- natural hazards,
- game theory,
- risk communication,
- social movements and resource mobilization, and
- bounded rationality.

These approaches have many different features. However, they share the underlying assumption of rationality. This is captured in their basic concepts and assumptions, according to Mergolis^[28] and Michell^[29].

2.3 Sharing high risks

An interesting and insightful example of the problems that may arise in the process of risk financing has been provided by Crocker^[10]. As that author demonstrates, the market in the field of insurance can result in something quite different from the invisible, “wise” hand of classical economics.

In other words, past research by Ritchie and Brindley^[33], claims that shifting risks to a third party is a process that may need political attention and design, other scholars like Mergolis also agree^[28].

As was seen above, risks are normally considered to be something to avoid or, at least, to mitigate. Thus, people who perceive a risk are ready to pay a cost for effective loss prevention and loss reduction.

Health insurance systems do exactly this. They provide loss reduction or, more precisely, they guarantee that a loss will not exceed a certain threshold. In exchange, they receive money.

The premium or fee that an insurance company demands, is based on its probability calculations. The company must determine what the annual health expenses of its insured population will be.

That is the point. Will the insured population's health expenses match the (well-known) average expenses of the general population? It would if health insurance was mandatory for all persons and a single company provided the health insurance service for all the country's citizens. In the US, however, health insurance is now mandatory (cfr. Obamacare, healthcare reform, APACA, PPACA), and there are hundreds of health insurance companies. In that situation, of course each insurance company's nightmare is that it will insure too many high-risk people and, consequently, to be forced to pay more for health expenses claims than it received from its clients, in terms of premiums or fees. This situation is called adverse selection. The fear of adverse selection has a deep impact on the insurance field in the US and causes, as the author claims, market failures.

European health insurance legislation is rather different. However it differs primarily in the coverage that the State provides to individuals and families. The Italian State guarantees assistance, which changes the impact of risk, that is moderated by a retroaction to the entire Italian population. In this system, those who are healthy share the risk and pay for those who are unfortunate and experience health problems. The latter benefit from the sharing of risk and cost with the more healthy individuals, through contribution to the State health system. This social system makes a lot sense. Because of this sharing of risk, the answer to the previously answered question is yes that the health expenses of those who are “covered” do match the (well-known) average expenses of the general population.

2.4 A significant example

Crocker's^[10] argument is that the health insurance market in the US can be divided into the following three parts: large employer groups, small groups, and individuals.

The first group is made up of large firms, which usually provide employer-sponsored coverage for their employees. The second group is made up of small firms, which sometimes provide employer-sponsored coverage—but often do not. The third group is made up of the millions of people who, for several reasons, cannot rely on employer-sponsored coverage. These people must apply individually for coverage.

Individuals who cannot rely on employer-sponsored coverage tend to belong to the weakest sectors of the population: unemployed individuals, unskilled workers, and their families. Many of these persons, especially if they are young and in good health, do not apply for individual health insurance in order to avoid expense.

As a result, “insurance companies fear that those applying for coverage are disproportionately composed of the high risk or high cost group.”^[10] In other words, if a low-income person decides to apply for individual coverage, that person may have a reason to believe that he or she will incur sizable medical bills in the future.

That is why adverse selection is a problem that tends to affect individual and small group markets, whereas large groups are exempt from it.

In fact, in large firms “employees [...] pay average premiums based on the total expected cost of the group; a particular person’s expected medical care costs are not factored into the premium he or she pays”^[10], whereas in small group and individual markets the pooling of risk occurs over much smaller groups, and consequently, the statistical variance of the expected costs is much larger.

This situation has several negative outcomes:

- Companies tend to compete for lower risk individuals. They charge very high premiums for those who are classified as “high risk” or simply refuse to issue or renew policies to such applicants.
- In order to avoid adverse selection, companies adopt refined selection mechanisms to detect high-risk people. These mechanisms are very expensive, and risk selection costs negatively affect the entire market—even low-risk people have to pay for risk selection.
- As a consequence, premiums are much higher than they should be. As many as 40 million Americans cannot afford them and remain uninsured.

Every year a great number of uninsured people must face direct health expenses that they cannot afford. This leads to the creation of debt and other severe social problems. That is why, as Crocker ^[10] asserts, a great percentage of uninsured people “is not only bad for the uninsured individual but for the general economy as well”. With this insightful example, we can mention that the process of risk shifting that is typical of the insurance market is shaped by asymmetric information. Applicants often know much more about their own probable future health expenses than insurance companies do. For example, if a person knows that cancer runs in his or her family, he or she will probably try to conceal this information from the company when applying for insurance coverage. When there is asymmetric information in a market, the market cannot be competitive. Inefficiency will result. As a consequence, we can summarize the author’s discussion ^[10] by saying that risk financing is a matter of dimension of risk groups. If the dimension of a risk group is risky *per se*, companies will try to defend against the risk by adopting selection mechanisms—and higher premiums. Thus general market inefficiencies will ensue.

2.5 The organization of risk

Crocker ^[10], the previously mentioned researcher suggests that the government pay the annual insurance company premiums of the most expensive one to three percent of individuals.

In this way, the responsibility for actual (not merely assumed) high health costs would be shifted from individual companies to all the members of a society.

If the cost of adverse selection was redistributed, insurance companies would no longer have an incentive to use and develop risk selection mechanisms and the inefficiency present in the small group and individual insurance markets would be greatly reduced. This would also enable people to purchase health insurance policies, rather than being denied coverage. Companies would probably continue to use those selection methods to continue to reduce their risks with the remaining population. Many of these risks, as we have noted, are known only after the fact.

Let us consider an example of such a policy in which the government acts as a reinsurer. New York created a subsidized health insurance program for low-income individuals and small firms. The state decided to pay for medical bills claims that exceeded certain thresholds. Enrollment in the program began in 2011. As a result, premiums for individuals were already about 50 percent less in 2013 than in the regular non-subsidized market and small firm premiums were 15-30 percent lower.

We can draw as a general conclusion that, when markets contain risks, such as in health insurance markets, market failure is very likely to be caused by information asymmetry and the potential for adverse selection. Risk can also cause a the failure of markets to form. If the government acts to take care of, or to

remove, the worst risks in such markets, the inefficiency in those markets would be greatly reduced, and markets that could not function otherwise would be able to function^[18].

This possible solution can be applied to a great variety of organizational situations, including dealing with reputational risk. Market risks and the price system also represent a domain that can benefit from the proposed speculations as well as information security risks, as in Chapman and Ward^[9], and in Crocker^[10].

3. HUMAN BEHAVIOR AND RISK

In recent years, we have seen an increase in the number of security threats that affect end users of Information Technology(IT) systems. Many incidents, such as spyware, malware, phishing, and denial of service, have made users much more aware of online threats.

The threats have impacted end-users and non-IT functions in organizations, as users proactively interpret their human/machine system relationship with greater respect for their (risk) information system security, (ISS), as in Cavusoglu et al.^[8]. However, good protection cannot be gained by default. We often find that security technologies are badly utilized (e.g., poor choice of passwords, poor antivirus protection, or security policies that are ignored), as D'Arcy et al.^[11]. This is a key point in understanding how users deal with these situations. Passwords that consumers used are often simply the first name of a child, a personal nickname, or a date of birth. That is dangerous in the case of an attack. They increase the risk probability as they enable hackers to penetrate systems much more easily than with greater password security. Free online defense software (antivirus protection), in much the same way, is more exposed to bugs. Generally, updates must be purchased and users unwilling to spend money for improved security measures. This relationship has proven to be true, in research findings by Beckhouse et al.^[2], Cavallari^{[5]-[6]-[7]}, Cavusoglu et al.^[8], Roth et al.^[35], Whitley and Galliers^[41], that suggest that knowledge of the real impact of risk is perceived based on a personal level of risk perception.

3.1 Human – Machine interaction

In some cases this is due to the carelessness of the end user. However, it can also be due to the nature of the technology and, as we discovered in previous research, the dynamics of human behavior and especially of machine interaction.

Greater awareness is still necessary, as there is strong evidence that users do not understand security risks very well – or – think that they understand security, but find it difficult to apply, as in Siponen and Vance^[37].

This attitude is common. We divide individuals who have this mindset into two groups. The first group consists of people who understand technological devices and innovations, but have no awareness of the extent of their exposure to a threat. They consider this to be an outside problem and feel that there is no need to cover it in the best possible way. This attitude risks a considerable loss in money and reputational risk, as Fiegenbaum and Thomas^[18], Roth et al.^[35], Siponen et al.^[38] state. It places users into situations where they are more exposed to future attacks. On the other hand, the other group is aware of the risks and security issues, but finds it difficult to apply consistent procedures. This is paradoxical because they realize that the problem is persistent and relevant, but they are unable to address it. This is dangerous for organizations. Consequently, a great deal of effort is continually spent for consultants and technical experts, to help organizations to avoid security problems.

3.2 Security awareness

Recent empirical investigation from Siponen et al.^[38] into compliance and systems security, show the level of security awareness and usage, even though constantly increasing, is still lacking.

However, it still has a long way to go, especially for security of applications. We must look at the problems posed by poor presentation of security functionality within end-user applications. After conducting a few experiments to demonstrate the importance of making security usable, we must examine the difficulties that can

occur in finding, understanding, and using application-level security features. Personal productivity applications have been used in practical examples to demonstrate various problems as reported by Beckhouse et al.^[2]

It is useful for a user to have protection that does not require thinking about it. In some cases, the protection can be completely invisible. However, this relies on the illegibility of default settings. A single default level of security is not sufficient if expected if the protection must meet the needs of everyone. There are many cases in which it is necessary to make choices and decisions. Nevertheless, the operation of security should be as invisible as possible, and it should be automatic when it is visible, as Spagnoletti and Za^[39] suggest.

Normally, when security is visible, what is provided to users is unlikely to captivate them. A good example that is familiar to many people are pop-up dialogs that ask the user if he or she wants to trust a particular digital certificate (i.e. encryption public key and digital identification).

Human work and behavior are constantly exposed to risk and attacks. It is widely recognized that, in a world that has a high level of innovation and sophisticated technology, criminals, hackers, and terrorists constitute malicious threats that are inflicting significant damage to users, as in Adams and Blandford^[1], Karat^[25], and Schneier^[36]. Not many users actually know what a certificate is. Thus the user must personally decide whether or not to trust an unknown digital piece (certificate) to enter a particular site. It is well known that people do not use more than a small percentage of security functions that are available to them. However, if there are serious threats, as indicated, security should be visible and utilized, Beckhouse^[3], Ritchie and Brindley^[33].

Although much security-related functionality is presented in a seemingly nice context of a graphical user interface, it can quickly disappear. For example, a number of simple check boxes or low, medium, and high settings can become complicated, if it is necessary to understand the functionality of what they control, as argued by Warkentin and Willison^[40].

Many users remain as baffled as if there was a command line interface. It is clear that organizations and domestic users will suffer, as they do not have adequate IT support or a help desk, Siponen et al.^[38]. It is obvious that they are denied the safety that they need because they are not experts.

3.3 Compliance

As Siponen and Vance^[37] described in their work, risk is related to the absence of compliance. This dearth implies a greater possibility to fall afoul of a violation of security barriers at the expense of developing and implementing organizational security policies and practices, as in Dameri^[13]. We need to evaluate, in the best way possible, the right level of compliance and policies that guarantee an adequate level of risk mitigation. A noncompliance effect will influence users to violate security policies. For that reason, we take this into account when we create and develop organizational security policies and risk assessment practices. The possible effects of noncompliance vary depending on the context and culture, but an adequate level of skill is fundamental to compliance in an IT system. Using security reflects the complexity of the security concepts involved. If one organization adopts encryption tools, such as Pretty Good Privacy (i.e., PGP for email), employees must have knowledge of concepts, such as encryption, public and private keys, digital signatures. Studies of the usability of security-oriented tools have been undertaken by Dowland and Furnell^[14].

Dowland et al.^[15] specifically looked at the usability and friendliness of the PGP utility.

Those authors considered aspects of human behavior and the impact of the Internet connection firewall, which has become Windows Firewall in Windows products.^[15] They demonstrated that the security functionality was inadequate and that the user would gain little from it.

A common factor in the above-mentioned issue is that the target was a security-oriented tool. In any case, security systems lie within more general end-user applications, which can greatly affect their usage. Although

word processors, web browsers, and email clients should have some security functionality, it can be lost on many end users^[14]. In the same direction we also find evidences from Roth et al.^[35].

If organizations don't understand how to implement and use the protection, what is the point of having it? Security features must be found, understood, and deployed effectively. This seems easy, but common problems can arise, as demonstrated by Siponen et al.^[38].

4. ORGANIZATIONAL THEORY AND PARADIGM SHIFT

It is constantly noted that organizational behavior is the “weakest link” in system security, because it can compromise systems, fall victim to social engineering, and ignore technology issues and security policies, as in Warkentin and Willison^[40].

Researchers like Dhillon^[12] have suggested a possible paradigm shift that involves human behavior (HB) and risk. Human behavior focuses on individuals, whereas security (i.e., the reciprocal of risk) as a whole is concerned with the entire organization, and not just the information system, as in Cavusoglu et al.^[8]. This distance is not particularly relevant for task-oriented problems. The rationalist-functionalist paradigm that was derived from March and Simon^[27] might suggest that an individual is a simple component in a broad-range information system. Functionalism is far behind modern conceptions of organizations and the corresponding information systems. Management information system study largely concerns the functioning of an organization. However, security concerns task-orientation very little, as argued by Adams and Blandford^[1] and Dourish et al.^[16]. The main qualities of tasks are that they are goal-oriented and within the time and activity constraints. System security does not exhibit those properties. Security management is a high level objective that has nothing to do with goal-orientation. It is a continuing process that has no time boundaries, as research findings from Misra et al.^[30]. If it is true that end users' and certain kinds of end-user behavior constitute the weakest link of a system security chain, it is appropriate to investigate the problem in searching for a framework of reference from both an individual and an organizational point of view. In fact, many authors like Dhillon^[12] and Siponen and Vance^[37], propose a top-down view of organizational/policy-directed security. However, our proposition of further analysis is bottom-up and addressed to the end user as a member of the organization and, moreover, its culture, as also stated by Beckhouse et al.^[2], along with Fiegenbaum and Thomas^[18] in two different works on two different matters that produced the same findings.

5. CONCLUSIONS

The results of the speculation in the present paper, which is based on findings of previous research, by Adams and Blandford^[1], Baskerville^[4], Dowland et al.^[15], Misra^[30] and Siponen et al.^[38], lead to the proposal of a theoretical framework that is intended to provide a robust baseline in defining the relationship between risk (and system security) and human behavior in an organizational point of view.

First and foremost, a solid theoretical framework can be found in the Contingency Model of Strategic Risk Taking. It was not originally proposed for complex risk-taking decisions by organizations (e.Business organizations), but is considered to be adapted to it^[6]. The commented study identifies a set of fundamental variables and relates them to the proposed framework. This framework takes into account the nature of the relationship between the variables referring to the individuals and the ones referring to risk-taking behavior, and consider them to build the interaction between multiple variables and the level of risk adversity/risk awareness^[14]. The contingency model is summarized by the following formal representation, which was adapted and enhanced by the authors of the present paper (1):

$$R_s = \sum_{1}^n \sum_{r}^n (E_r + I_r + O_r + P_r + DM_r) \quad (1)$$

Where:

- R_s = Strategic risk taking,
- E_r = General environmental risk indicators,
- I_r = Industry risk indicators,
- O_r = Organizational risk indicators,
- P_r = Problem risk indicators, and
- DM_r = Decision-Maker risk indicators.

We can take advantage of solid scientific literature concerning non-computer decision-making. Also, further development for research could be derived from the mentioned model and empirical evidence of the model's adaptation to system security^[6] should be verified in the future.

The other theoretical framework that can be adopted in evaluating Human Behavior security problems and decision-making is the work of Misra et al.^[30], the "Strategic Modeling Technique for Risk Assessment." The proposed modeling technique is particularly useful and valuable, because it proposes a new conceptual modeling approach by considering and evaluating, with a systemic view, the dependencies between the actors in a system and analyzes the motivations and interrelations behind the different entities and activities that characterize that system itself^[1]. The model identifies a set of risk components and defines the risk management process. The value and re-usability of the model relies on its new technique for modeling risk analysis using the concept of actor-dependency. However, it appears that the extension of the scope of the mentioned model to the domain of risk assessment in information systems^[6] is even more consistent. This can be of great help in the research of organizational studies. Thus, the modeling approach has some limitations. For example, the proposed model cannot be used while implementing existing systems. Nevertheless, although it can be of assistance only in the designing phase, the proposed model constitutes a milestone in the field.

Combining several contributions and the solid base of frameworks in organizational studies and non-computer decision-making can lead to an extremely powerful set of conceptual tools for analyzing and interpreting Risk problems in (e.Business) organizations in regard to human behavior from a systemic point of view.

REFERENCES

- [1] Adams A. and Blandford, A.. (2005). Bridging the gap between organizational and user perspectives of security in the clinical domain. *International Journal of Human-Computer Studies*, 63, 175-202.
- [2] Backhouse, J., Bener, A., Chauvidul, N., Wamala, F., Willison, R.. (2005). *Risk Management in Cyberspace, Trust and Crime in Information Societies*. Mansell, R., Collins, B., (Eds.) Edward Elgar, Cheltenham, UK Northampton.
- [3] Backhouse, J.. (2001). *Assessing Certification Authorities: Guarding the Guardians of Secure E-Commerce?*. *Journal of Financial Crime*, 9(3): 217-226.
- [4] Baskerville, R., Spagnoletti, P., Kim, J.. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information & Management* 51: 138–151.
- [5] Cavallari, M.. (2012). Analysis of evidences about the relationship between organisational flexibility and information systems security. *Information Systems: Crossroads for Organization, Management, Accounting and Engineering*. In De Marco, M., Te'eni, D., Albano, V., Za, S.. Heidelberg: Springer, D, 439-447,.

- [6] Cavallari M.. (2008). Human computer interaction and systems security-an organisational appraisal. In: De Marco M., Casalino N., *Interdisciplinary Aspects of Information Systems Studies*, Springer Heidelberg, 261-268.
- [7] Cavallari M.. (2013). The Determinants of Knowledge Transfer: The Study of a Refined Model. In: Spagnoletti P, *Organizational Change and Information Systems Working and Living Together in New Ways. Lecture Notes in Information Systems and Organisation*, Heidelberg: Springer, D., 257-265.
- [8] Cavusoglu, H., Cavusoglu, H., and Raghunathan, S.. (2004). Economics of IT Security Management: Four Improvements to Current Security Practices. *Communications of the Association for Information Systems* (14), 65-75.
- [9] Chapman, C.B., and Ward, S.C.. (2003). *Project Risk Management: Processes, Techniques and Insights*. 2nd ed., Wiley, UK.
- [10] Crocker, K. J.. (2003). Risk and Risk Management, in: *The Economics of Risk*. Meyer, D. J. (Ed.), Upjohn Institute for Employment Research, Michigan USA.
- [11] D'Arcy, J., Hovav, A., and Galletta, D.. (2009). User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research* 20(1):79-98.
- [12] Dhillon, G.. (1997). *Managing Information System Security*, London: Macmillan.
- [13] Dameri, R. P., (2008). Using an enterprise information management system to enhance IT compliance and information value, in *2nd European Conference on Information Management and Evaluation, ECIME 2008*.
- [14] Dowland, P. S., Furnell, S. M.. (2008). *Security Concepts, Services, and Threats*, Artech House Publishers.
- [15] Dowland, P. S., Furnell, S., Thuraingham, B. M., Wang, X. S.. (2005). Security Management, Integrity, and Internal Control in Information Systems. IFIP Tc-11 WG 11.1 and WG 11.5 Joint Working Conference, *IFIP Advances in Information and Communication Technology*, Springer-Verlag New York,.
- [16] Dourish, P., Grinter, R.E., Delgado de la Flor, J., and Joseph, M.. (2004). Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal Ubiquitous Computing*, 8(6): 391-401.
- [17] Federal Mogul. (2002). *Wheeling & Dealing in Asbestos Liability*, Environmental Working Group, www.ewg.org/sites/asbestos/federalmogul.php.
- [18] Fiegenbaum, A. and Thomas, H.. (1988-03). Attitudes toward risk and the risk-return paradox: prospect theory explanations. *Academy of Management Journal*, 31(1): 1988,85-106.
- [19] Fishbein, M., and Ajzen, I.. (1975). *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*. Reading, MA, Addison-Wesley.
- [20] Fishbein, M.. (2007). A Reasoned Action Approach: Some Issues, Questions, and Clarifications, in *Prediction and Change of Health Behavior: Applying the Reasoned Action Approach*. In I. Ajzen, D. Albarracín, and R. Hornik (eds.), Hillsdale, NJ: Lawrence Erlbaum & Associates, 281-296.
- [21] Giddens, A.. (1990). *The Consequences of Modernity*. Stanford CA, Stanford University Press.
- [22] Giddens, A.. (1991). *Modernity and Self-Identity, Self and Society in the Late Modern Age*. Cambridge, Polity Press.
- [23] Jaeger, C. C., Renn, O., Rosa, E. A., Webler, T.. (2001). *Risk, Uncertainty, and Rational Action*. Earthscan, London.
- [24] Junkui Yao, F. J., and Jaafari, A.. (2003). Combining Real Options and Decision Tree: An Integrative Approach for Project Investment Decisions and Risk Management. *Journal of Structured & Project Finance*, 9(3):53-70.
- [25] Karat, C.-M.. (1989). Iterative Usability Testing of a Security Application, in *Human Factors*.
- [26] Karat, J., Karat, C.-M., Brodie, C., and Feng, J.. (2005). Privacy in information technology: Designing to enable privacy policy management in organizations. *International Journal of Human-Computer Studies*, 63, 153-174.
- [27] March, J. G. and Simon, H. A.. (1958). *Organizations*.
- [28] Mergolis, H.. (1996). *Dealing with Risk: Why the Public and the Experts disagree on Environmental Issues*. Chicago IL, University of Chicago Press.
- [29] Michell, J.. (1999). *Measurement in Psychology*. Cambridge UK, Cambridge University Press.

- [30] Misra, S.C., Kumar, V., and Kumar, U.. (2007). A Strategic modeling technique for information security risk assessment. *Information Management & Computer Security*, 15(1): 64-77.
- [31] Mitnick, K.D.. (2003). *The Art of Deception*. John Wiley & Sons, New York.
- [32] Renn, O.. (1992). Concepts of Risk: A Classification, *Social Theories of Risk*. S. Krimsky and D. Golding (Eds.), Praeger, Westport, CT, 53-79.
- [33] Ritchie, B. and Brindley, C.. (2007). An emergent framework for supply chain risk management and performance measurement. *Journal of the Operational Research Society*, 58(11):1398-1411.
- [34] Rosa, E. A.. (1998). Metatheoretical Foundations for Post-Normal Risk. *Journal of Risk Research*, 1:15-44.
- [35] Roth, V., Straub, T., and Richter, K.. (2005). Security and usability engineering with particular attention to electronic mail. *International Journal of Human-Computer Studies*, 63, 51-63.
- [36] Schneier B.. (2006). *Beyond Fear, thinking sensibly about security in an uncertain world*. J. Wiley and Sons NY.
- [37] Siponen, M. T. and Vance, A.. (2010). Neutralization: New Insight into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly* 34(3): 487-502.
- [38] Siponen, M. T., Pahlila, S., and Mahmood. (2010). Compliance with Information Security Policies: An Empirical Investigation. *IEEE Computer*, 64-71.
- [39] Spagnoletti, P., Za, S.. (2013). Securing virtual enterprises: Requirements and architectural choices, *International Journal of Electronic Commerce Studies*, 4(2): 295-304.
- [40] Warkentin, M. and Willison, R.. (2009). Behavioral and Policy Issues in Information Systems Security: The Insider Threat". *European Journal of Information Systems* 18(2):101-105.
- [41] Whitley, E. A. and Galliers, R. D.. (2009). Vive les differences?: developing a profile of European information systems research as a basis for international comparisons. *European journal of information systems*, 16(1): 20-35.