The current issue and full text archive of this journal is available at
www.emeraldinsight.com/0968-5227.htm

Formulating information systems risk management strategies through cultural theory

Aggeliki Tsohou, Maria Karyda and Spyros Kokolakis
Department of Information and Communication Systems Engineering, University of the Aegean, Samos, Greece
Evangelos Kiountouzis
Department of Informatics, Athens University of Economics and Business, Athens, Greece

Abstract

Purpose – The purpose of this paper is to examine the potential of cultural theory as a tool for identifying patterns in the stakeholders' perception of risk and its effect on information system (IS) risk management.

Design/methodology/approach – Risk management involves a number of human activities which are based on the way the various stakeholders perceive risk associated with IS assets. Cultural theory claims that risk perception within social groups and structures is predictable according to group and individual worldviews; therefore this paper examines the implications of cultural theory on IS risk management as a means for security experts to manage stakeholders perceptions.

Findings – A basic theoretical element of cultural theory is the grid/group typology, where four cultural groups with differentiating worldviews are identified. This paper presents how these worldviews affect the process of IS risk management and suggests key issues to be considered in developing strategies of risk management according to the different perceptions cultural groups have.

Research limitations/implications – The findings of this research are based on theoretical analysis and are not supported by relevant empirical research. Further research is also required for incorporating the identified key issues into information security management systems (ISMS).

Originality/value – IS security management overlooks stakeholders' risk perception; for example, there is no scheme developed to understand and manage the perception of IS stakeholders. This paper proposes some key issues that should be taken into account when developing strategies for addressing the issue of understanding and managing the perception of IS stakeholders.

Keywords Risk management, Information control, Data security, National cultures

Paper type Research paper

1. Introduction

The importance of information systems (IS) for the operation of organizations nowadays is widely recognized, while security is one of the major concerns of IS management. A commonly used security management methodology is risk management, which is recommended by ISO (ISO/IEC 17799, 2005), while Computer Security Institute (2005) emphasizes that risk management aspects of computer security have become important concerns to today's organizations. It is also recognized that risk management is affected by organizational elements, including social and cultural aspects (Karyda *et al.*, 2004). Whitman *et al.* (2001) point out that while some security issues may be common to most organizations, others are "[i]diosyncratic to

Information Management & Computer Security
Vol. 14 No. 3, 2006
pp. 198-217

0968-5227
DOI 10.1108/09685220610670378

individual organizations or industry groups". Thus, there is not one security solution that is suitable for all organizations. Perhaps the major problem facing researchers and managers in the area of risk, is that risk itself is an abstract concept (Frosdick, 1997; Gerber and von Solms, 2005). While hazards and their aftermath can be identified, risk depends on a complex interplay of a number of social variables, which are ultimately combined by human judgment. The identification and estimation of risk is both a human and a social activity. Risk perception has been well explored in the scientific literature, but, to the best of our knowledge, not in the IS security context. Therefore, there are several reasons for returning to this theme. Firstly, it is undoubtedly true that a number of risk management activities are based on the way the various stakeholders perceive risks associated with IS assets. Secondly, IS security management treatment neglects risk perception, i.e. there is no scheme developed to understand and manage the perception of IS stakeholders. Finally, the concept of risk provides a plausible basis for associating risk management activities with cultural theory approaches to risk (as they are outlined in next section), in order to create a taxonomy, which takes into account the stakeholders' different perceptions and worldviews. The purpose of this paper is to examine the potential of cultural theory as sensitizing tool for identifying patterns in the stakeholders' perception of risk and its effect on the strategies for IS risk management.

The paper is organized in six sections. In Section 2, we describe the process of risk management while in Section 3 we define the research area and problems addressed in this paper. Section 4 is dedicated to a detailed analysis of the theoretical framework, so as to inform the reader of the basic theoretical elements that support the proposed risk management framework. This theoretical framework consists of a theory derived from anthropology-cultural theory (Douglas, 1978) and its theoretical elements. Section 5 supports the introduction of cultural theory in the field of IS risk management, examines its impact on the risk management processes and presents key issues that should be considered by security experts in developing risk management strategies addressing the issue of managing stakeholders' different perceptions associated with IS security. Finally, the conclusions and issues that require further investigation are presented in Section 6.

2. The risk management process

According to the Institute of Risk Management (2002), there is a variety of views and descriptions of the processes that risk management involves, the way it should be conducted and what is aimed at. Drawing from Frosdick (1997), NIST: 8000 (2002) and ISO/IEC 27001 (2005), this paper adopts a model for the risk management process which includes three risk management stages: initiation, risk analysis and risk mitigation (Figure 1).

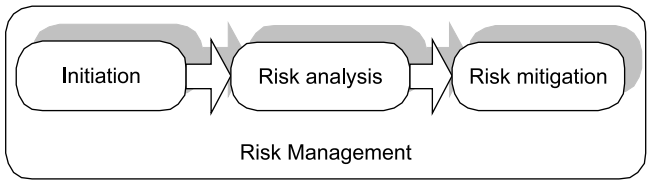

Figure 1.
The overall process of risk management

The stage of initiation aims mainly at:

- defining the context of the risk management process;
- at setting the scope of the analysis; and
- at establishing the risk management team.

During this stage the appropriate risk management methodology is also selected. Risk analysis-or risk assessment, since these terms are considered synonymous, comprises of three processes: risk identification, risk estimation and risk evaluation (Frosdick, 1997). Risk mitigation, the final stage of the risk management process, involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls that have been identified during the risk analysis process (NIST: 800-30, 2002). Risk mitigation includes also the processes of monitoring and evaluating the effectiveness of risk controls (ISO/IEC 27001, 2005).

2.1 Risk analysis

The stage of risk analysis involves the processes of risk identification, risk estimation and risk evaluation (Frosdick, 1997) as shown in Figure 2. Risk identification refers to the process of identifying risks that pose threats to the assets that need to be safeguarded. Therefore, it is necessary, at this phase, to identify the assets to be protected, associate possible threats to these assets and identify their vulnerabilities (Gerber and von Solms, 2005). Risk identification is followed by risk estimation which is the process of quantifying-putting values on – the risks that have been identified. Commonly, risks are quantified by measuring the probability of their occurrence (P) and estimating their possible business impact or cost (C); thus in the risk analysis process, risk is calculated as $R = P \times C$ (Baskerville, 1991). Finally, during the risk evaluation process, options for the treatment of the risks are identified and the level of tolerance is determined. Possible options include risk transfer (transfer risk to third parties), risk acceptance (no control of the risk), risk avoidance (if applicable, the asset is not exposed to the risk) and risk reduction (selection of appropriate control measures) (ISO/IEC 27001, 2005).

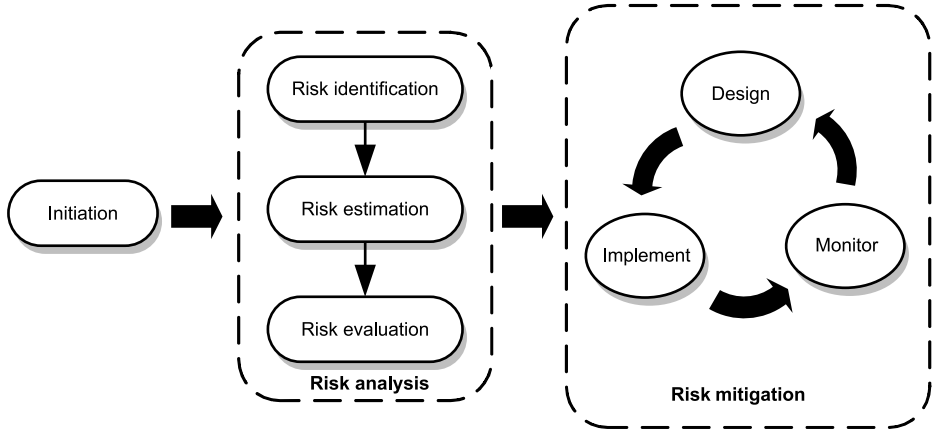

Figure 2.
The risk management stages

2.2 Risk mitigation

Risk mitigation follows the risk analysis stage as shown in Figure 1. According to ISO/IEC 27001 (2005) three tasks are included in the stage of risk mitigation:

(1) design;

(2) implement; and

(3) monitor (Figure 2).

These three tasks are individually discussed in more detail in the following.

2.2.1 Design. The process of risk mitigation includes the specification of security objectives and the establishment of security policies and processes relevant to controlling risk. Currently applied countermeasures and policies, if any, are identified and evaluated in comparison to the results of risk analysis (e.g. emergence of new risks). If required, additional control measures are specified and designed, accompanied by the timeframe over which they should be implemented.

2.2.2 Implement. The task of implementation involves the application of the selected control measures and procedures. It also includes management of recourses required for implementing these measures (people, time, money, operations). Security awareness programs are also included in this process, aiming at fostering an appropriate risk and security culture.

2.2.3 Monitor. The process of monitoring follows the implementation of the selected countermeasures. Its purpose is to ensure that the control measures are operating effectively and as intended. It includes:

- processes for the prompt detection of errors and security incidents;
- mechanisms that examine whether documented procedures are being followed; and
- reviews aiming at the evaluation of implemented controls' efficiency.

It also includes the reassessment of the level of residual risk, after taking into account possible changes that might occur to the organizational processes or the business objectives.

3. The critical role of stakeholders' perceptions for the risk management process

By and large, end-users of IS are not aware of the security measures. For most of them the IS is a tool to perform their job responsibilities as efficiently as possible; IS security is viewed as a hindrance rather than a necessity (Hansche, 2001). In order to achieve stakeholders' compliance to the security measures that have been produced from the stages of risk analysis and risk mitigation, security awareness programs are introduced. Furthermore, given the fact that end-users should be responsible for themselves, as well as for the organization, against security breaches, training employees about the IS security threats is another preventive measure adopted by organizations. However, awareness and training are not the only social factors affecting the stakeholders' perceptions on threats. According to Siponen (2000) stakeholders very often fail to apply the information security guidelines in the way they were intended even though they are aware of them.

Risk management, as described in the previous sections, involves a number of human activities which are based on the way the various stakeholders perceive risk

associated with IS assets. Risk identification and risk estimation is both a human and social activity. Different people (end-users, stakeholders, etc.) place different emphasis on different risks. Their concerns may stem from personal experience, from what they have seen or heard in the mass-media (newspapers, radio, TV, etc.) or from they have been told by friends. Many factors may influence the way risk is perceived; some of them include the familiarity with the source of danger, the ability to control the situation, and the dreadfulness of the results. For example, even though the actual risk of getting involved in an airplane crash is very small, many people are still afraid to fly (Torbjorn, 2004). A striking example of risk perception differentiations can be found in Deery (1999); his study revealed that young novice drivers perceive risks of specific driving situations at a lower level compared to other groups of drivers, since they perceive hazards less holistically and concentrate on the danger rather than on the difficulty of making appropriate actions to avoid an accident. Strong differentiations are also identified when referring to personal and general risks. People tend to consider general risks as higher than the personal ones (Torbjorn, 2004). Finally, people tend to make different estimates when they rate the same risks for themselves, their family and people in general. Sjoberg (2000) presents an enlightening study where 15 hazards were all ranked at a lower level by participants, when they were associated to themselves compared to when associated with their family or with people in general.

Therefore, people's ranking of threats may not coincide with that of IS security professionals. In essence, much of the people's knowledge of the world comes from perceived stimuli-signs, signals and images. According to Slovic *et al.* (1980) a signal value is produced by hazardous events. The process of cognition transforms such signals and forms different parts of each individual's gestalt, or indeed as part of a group gestalt. Kasperson (1992) argues that cognitive transformation is predictable and may be likened to filtering through a range of amplifiers-groups interested in the risk. As the work of Bella (1987) on communication distortion indicates, such groups will distort aspects of the risk in support of their beliefs and values. Hence, a link with cultural theory is established, since the cultural theorists would claim that the process of cognitive distortion within each group is predictable according to group and individual worldviews (Smallman and Weir, 1999).

4. Theoretical framework

Cultural theory was proposed by Douglas (1978) and Douglas and Wildavsky (1982). The basic postulate of cultural theory is that the way people socially interact impinges on the systems of symbols they use to understand the world. Therefore, the concepts people use to understand the world are related to the social constraints or structures they are exposed to (Ney and Molenaars, 1999). Cultural theory provides explanations on how and why individuals formulate their perceptions of concepts such as risk and threat. According to cultural theory these perceptions are not formed independently of the social context (Tansey and O'Riordan, 1999). Douglas and Wildavsky (1982) claim that the values and worldviews intertwined in certain social and cultural contexts – which are called cultural biases – shape individuals' perceptions and evaluations of risks. Individuals are embedded in a social structure which acts like a filter and shapes their values, attitudes and worldviews (Rippl, 2002). Risk perceptions therefore, reflect the way society is perceived and alternative views about risks and the world flow from different patterns of social structure. Cultural theory has extensively been applied in

studies related to risk perception, and more specifically in ecology and health-related risks (Langford *et al.*, 2000; Finucane and Holup, 2005; Marris *et al.*, 1996; Lima and Castro, 2005). Moreover, it has been applied in the analysis of political issues (Ney and Molenaars, 1999), risk behavior (Douglas, 1992) and industrial safety (Gross and Rayner, 1985).

4.1 Perspectives of cultural theory

Two different perspectives of cultural theory have been applied, named the stability and the mobility view,, respectively, (Langford *et al.*, 2000; Tansey and O'Riordan, 1999). These two differ both epistemologically and methodologically; a differentiation that is of high significance for the research process and for the research approach followed (see below).

According to the first perspective of the cultural theory, the "stability" view, individuals are consistent in a cultural bias. They are expected to attach themselves to social structures with the same type of cultural bias in all areas of their life (e.g. work, social life). It is therefore implied that individuals conform to this bias over time and regardless of the social context. As a consequence, a methodology for applying cultural theory may include "measuring" an individual's cultural bias, independently of a specified time or context (Langford *et al.*, 2000). Such a strategy is adopted by Dake (1991), who developed a cultural biases questionnaire. Rippl (2002) also adopts the same perspective of the theory and develops a new instrument based on Dake's work.

The second perspective of the theory-the "mobility" view, postulates that it is possible for individuals to attach themselves to social structures with different types of cultural bias and in different areas of their lives. Therefore, individuals might conform to different cultural biases according to specific contexts and/or adopt different biases over time. Since, cultural biases are regarded as context dependent, they cannot be "measured" without reference to a specific context and timeframe. For this reason, the proponents of this perspective advocate the application of qualitative methods, such as participant observation and focus groups (Langford *et al.*, 2000).

4.2 The grid/group typology

Regardless of the adopted perspective of the theory, the inextricable component of cultural theory is the grid/group typology – also referenced as the grid/group scheme. The typology provides a heuristic device for the application of cultural theory (Douglas, 1992); however, it is often confused and coincided with the theory within which it is embedded (Tansey and O'Riordan, 1999; Boholm, 1996). Furthermore, this typology has been very influential in different contexts and at a different aggregation levels.

The grid/group typology relies on the distinction between the concept of cultural bias and the concept of social relations, highlighted by Douglas (1978), who describes cultural bias as the "shared values and beliefs" whereas social relations, as "patterns of interpersonal relations". Thompson *et al.* (1990) use the term "way of life" or "worldview" which is strongly associated to the grid/group scheme, as "a combination of social relations and cultural bias".

The grid/group typology identifies four different cultural groups with distinct "ways of life". The typology lies on two dimensions, namely the grid and the group dimension. Thompson *et al.* (1990) claim that:

> ... group refers to the extent to which an individual is incorporated into bounded units. The greater the incorporation, the more the individual's choice is subject to group determination...

In short, the group dimension refers to whether an individual is member of bonded social units, how absorbing the group's activities are on the individual (Torbjorn, 2004) and the extent to which group boundaries represent constraints to the free movement of individuals in and out of a group. Thompson *et al.* (1990) claim that:

> ... grid denotes the degree to which an individual's life is circumscribed by externally exposed prescriptions. The more binding and extensive the scope of these prescriptions, the less life is open to individual negotiation...

To summarize, the grid dimension refers to the degree to which a social context is regulated and restrictive in regard to the individuals' behavior (Torbjorn, 2004).

The two dimensions provide a framework of four types of "ways of life" or worldviews, as shown in Figure 3, namely: hierarchy (high grid-high group), egalitarianism (high group-low grid), fatalism (low group-high grid) and individualism (low group-low grid). The characteristics of each worldview are explained in the following.

Marris *et al.* (1996) claim that hierarchists, meaning individuals whose worldview corresponds to high grid-high group, are characterized by strong group boundaries and binding prescriptions. These individuals' position in the world is defined by a set of established classifications, based on criteria such as age, gender, or race. These demarcations are considered unquestionable and are justified on the grounds that they enable harmonious life (Douglas and Wildavsky, 1982; Langford *et al.*, 2000; Thompson *et al.*, 1990). Hierarchical cultures emphasize the importance of establishing and preserving the "natural order" of the society. Hierarchists mostly fear things that disrupt this social order, such as social disturbance, demonstrations and crime. Another important facet of this worldview is that people who share it show a great deal of faith in expert knowledge (Torbjorn, 2004). Hierarchical individuals trust rules and

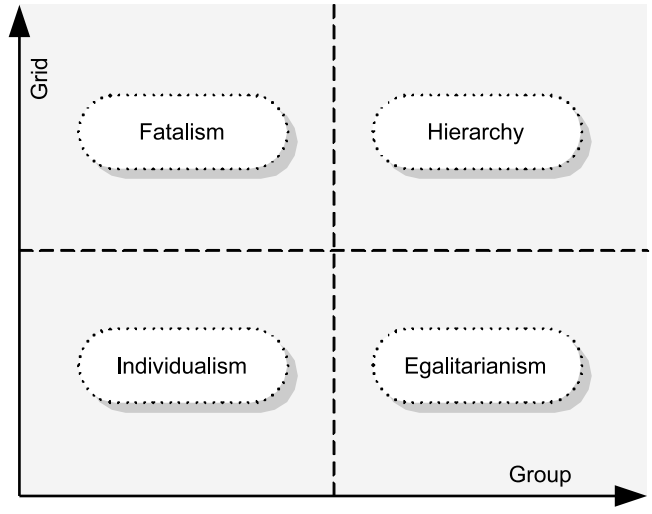

Figure 3.
The four worldviews according to the grid/group typology

regulations and believe that institutional order and experts will be able to tackle all types of problems (Lima and Castro, 2005). Hierarchical organizations are structured according to the belief that everyone must know one's place, though that place might vary with time (Altman and Baruch, 1998). Another noticeable characteristic of members of hierarchic groups is that when they cheat, steal or overlook procedures, they operate according to the same criteria and values that apply to their formal work – they act as a group in an orderly, disciplined and co-ordinated way, with respect for their own rules, limits and precedents (Mars, 1996). Finally, hierarchists are characterized by slow adaptability to change and over-dependence on regular ways of doing things (Mars, 1996).

Egalitarians, people who can be positioned in the high group-low grid quadrant, are also characterized by high degree of the group dimension, but, contrary to hierarchists, their lives are not prescribed by role differentiation. Instead, egalitarians share the idea that individuals should negotiate their relationship with others and that no person is granted authority by virtue of his or her position (Marris *et al.*, 1996; Langford *et al.*, 2000). They also believe that leadership must be charismatic (Altman and Baruch, 1998). Egalitarians are characterized by intense sense of equality; therefore, they mostly fear developments that may increase the inequalities among people. Compared with hierarchists, they tend to be skeptical to expert knowledge, because they suspect that experts and strong institutions might misuse their authority (Torbjorn, 2004). Since, they dislike others deciding for their life and actions, egalitarians prefer to have information provided to them, based upon which they can make their own personal choices (Finucane and Holup, 2005).

Individualists, people with low group-low grid worldview, are bound neither by group integration nor by prescribed roles, and assert that all boundaries are subject to negotiation (Karyda *et al.*, 2005; Langford *et al.*, 2000). They barely feel responsible towards other members of society and regard the allocation of power as a matter of own responsibility, not depended on position or status (Langford *et al.*, 2000). They do not accept enforcements based on ancestry or past, since each person is responsible for oneself (Altman and Baruch, 1998). Individualists are especially concerned for the maintenance of freedom to continue life and business as usual, and they believe that carrying on through the same paths pursued thus far is the answer (Lima and Castro, 2005). They are also particularly afraid of things that might obstruct their individual freedom (Torbjorn, 2004). Mars (1996) claims that individualists are reluctant to accept rules or to follow defined instructions or procedures, especially in the case these appear to obstruct their current autonomy, such as, for instance, maintenance and administrative procedures and manual instructions. They tend to build short term and instrumental relationships with their superiors. Individualism is also associated with corner cutting, rule breaking and cheating, which means that people who share this worldview have a propensity to cheat, convert materials to their own use, short cut procedures for ease of operation and exploit ambiguities. When they have the choice, individualists prefer to choose short-term personal advantages over long-term corporate consequences. Individualist tendencies are also linked to a high propensity for risk taking (Mars, 1996).

Finally, fatalists, with a low group-high grid worldview, believe, like hierarchists, that their autonomy is restricted by social distinctions but in contrast to them, they feel excluded from membership in the institutions responsible for setting the rules, and

tend to see themselves as "outsiders" (Douglas and Wildavsky, 1982; Langford *et al.*, 2000; Thompson *et al.*, 1990). They believe that the sphere of individual autonomy is minimal and there is little room for personal negotiations (Altman and Baruch, 1998). They also believe that social classification should be based on ancestry (Altman and Baruch, 1998). Fatalists usually take small part in social life; surprisingly they feel tied and regulated by these social groups although they do not belong to them. This fact makes this worldview quite indifferent concerning the concept of risk; what fatalists fear and what not is mostly decided by others. These individuals would rather be unaware of dangers, since they assume that they are unavoidable anyway (Torbjorn, 2004). Concerning the type of work they prefer, most of the times, they attach themselves to jobs characterized by high degree of routine (Mars, 1996).

4.3 Applications of cultural theory

The different perspectives of cultural theory, described above, have resulted in a plurality of methodological approaches for applying the theory to the study of risk. Specifically quantitative methods, qualitative methods and mixed methodologies have been used.

The efforts to apply the theory quantitatively began with Dake (1991) and Dake and Wildavsky's (1991) examination of how individuals' values or biases interact with risk perception. Dake and Wildavsky (1991) claim that the cultural theory is capable to "predict and explain what kind of people will perceive which potential hazards to be how dangerous". They developed and used a quantitative questionnaire that includes a series of agree/disagree statements to which the interviewee must respond, aiming at finding factors that are predictors of risk perception. For example, interviewees were asked whether they agree with the statement "The police should have the right to listen to private phone calls when investigating crime". Positive responses were indicators of a hierarchical worldview. Another example refers to the statement "A person is better off if he or she doesn't trust anyone" indicating a fatalist worldview. According to their study, cultural adherence was found to be the best risk perception predictor. Sjöberg (1997, 1998, 2000) reproduces the quantitative approach of the theory-testing framework developed by Dake, aiming to test the explanatory power of the grid/group typology, but his studies did not confirm Dake's findings.

Studies using qualitative methods such as participant observation and focus groups have also provided empirical support for the application of cultural theory (Rayner, 1986, 1992; Rayner and Cantor, 1987). Rayner (1992) uses a range of methodologies to explore the different institutional contexts that co-exist in a complex organization – a hospital. He also explores how these contexts intervene to the construction of associated risks, identifies the different contexts that corresponded to each of the four quadrants of the grid/group typology and describes how these influence individuals' attitudes towards risk. His goal is not to demonstrate how individuals belong to the "hierarchical" or the "individualist" type, but to provide evidence that the culture within which social actors operate enables some forms of behaviour and at the same time constrains others.

Langford *et al.* (2000) applied cultural theory in the examination of risk perceptions concerning environmental threats, using a mixed methodology. Specifically, they employed a quantitative approach (questionnaire survey) and a qualitative approach (focus groups) in the same study, in order to associate risk perceptions to the four worldviews. Their study reveals some interesting differences among the cultural types which broadly support the four types of social organization provided by cultural

theory. For example, their study supported that the worldviews characterized by high grid dimension were related to perceptions of power and authority, while the group dimension was related to differentiation of beliefs about whether collective action can bring a solution to the environmental issues examined. Finally, their study resulted in a broad distinction between the opposing grid/group worldviews; hierarchists and individualists on the one hand and egalitarians and fatalists on the other.

Furthermore, Smallman and Weir (1999) discuss the critical role of communication and the theory of the social amplification of risk perception in order to develop a framework explaining communications behaviour during crisis. They use cultural theory in order to examine the influence of culture on communication flow and direction and the notion of cultural distortion during crisis.

Although cultural theory proposes a useful theoretical framework, it has been criticized because it has not been fully supported by substantive empirical studies (Marris *et al.*, 1996). The efforts to test the theory quantitatively (Dake, 1991, 1992; Dake and Wildavsky, 1991; Sjöberg, 1997, 1998, 2000) have been problematic, since they do not provide sufficient support of the cultural theory's capability to predict risk perception (Torbjorn, 2004). Moreover, researchers have not presented sufficient evidence confirming cultural theory's predictions. According to Torbjorn (2004), most of the researchers have reported that the theory explains only a part of the variance of human risk perception instead of being capable of predicting human attitudes towards risk depending on risk perception. However, since risk perception has not been explored in the field of IS security, we argue that cultural theory can provide interesting insights for the management of stakeholders' perceptions by security experts.

5. Strategies for IS risk management informed by cultural theory

5.1 Cultural theory in the field of IS risk management

Cultural theory was developed for the study of cultures and the social organizations in which these are embedded. According to Altman and Baruch (1998) Cultural theory has been applied to a variety of institutions, themes and areas. This paper applies cultural theory in the field of IS risk management. IS consist of:

- the information that is being stored or in any way processed;
- the hardware and software used for processing the information; and
- a social system that is formed by the actions and relations among the IS users.

Under this perspective, IS are characterized not only by their technical dimension, but also by their social facet (Karyda *et al.*, 2005). Walsham (1993) explores the introduction of IS in several organizations. His study reveals the critical role social context has for the designing, implementing and evaluating IS. Consequently, social context is a critical aspect of IS and cannot be overlooked by the process of risk management. IS security experts, in particular, should employ the appropriate methods and techniques for managing, among other things, the users' beliefs and perceptions with regard to IS security.

Cultural theory has extensively been applied in risk perception studies and advocates that the factors that influence the way risk is perceived are rooted in the social context. In this paper, we attempt to use cultural theory as a tool for analysis and for providing the theoretical framework to associate social context with specific IS risks and security management practices. Other researches have noted a linkage between

cultural theory and risk management (Rayner, 1984; Lima and Castro, 2005; Marris *et al.*, 1996) but there is a lack of a clear framework for this association. This paper argues that by identifying the different worldviews shared by the users, security experts will be in place to make an informed selection of the appropriate strategies for applying security management in different cases.

5.2 The impact of the four types of cultural bias on risk management

This section describes how the four types of cultural bias of the grid/group typology can be associated with IS risk management and presents their impact on the process of IS risk management. Tables I-III summarize the following analysis.

As described in Section 2 (Figure 1), the process of risk management commences with the stage of initiation. At this stage, identifying stakeholders' cultural bias is a task of high significance, because it affects the effectiveness of the risk management method that is selected. Hierarchists value an interventionist and regulatory approach to risk management, based on institutional advice provided by experts (Lima and Castro, 2005; Marris *et al.*, 1996) and universally accepted safety standards (Marris *et al.*, 1996), because they prefer mechanisms that draw on the experience of experts, rather than rely on their own incomplete knowledge; therefore they expect risk management decisions to rely on security experts' analyses and on widely accepted security standards. Egalitarians tend to support decision-making processes that encourage public participation (Marris *et al.*, 1996). For example, among the various security analysis methods, SBA Scenario (DFS, 2005) relies on users participating and expressing their views. Individualists prefer methods that are based on economic factors, and in particular cost-benefit analysis (Langford *et al.*, 2000; Marris *et al.*, 1996). Fatalists feel that decisions are beyond their control and feel obliged to accept whatever is imposed upon them (Langford *et al.*, 2000) and therefore tend to be indifferent to the selection of risk management methods.

For example, in the case of a risk analysis review for a large social security organisation with a strong hierarchist culture, the authors emphasized on the strict application of a formal risk analysis method (CRAMM) that has been a standard in the UK. On the other hand, in the case of a risk management review for a private oil company, where individualists formed the majority, emphasis was placed on the financial implications of unresolved risks, and therefore a cost-benefit analysis approach was followed.

	Types of cultural bias			
Initiation tasks	Hierarchy	Egalitarianism	Individualism	Fatalism
Selection of risk management method	Selection of methods based on experts decisions and widely accepted security standards (Lima and Castro, 2005; Marris *et al.*, 1996)	Selection of methods that encourage stakeholders' participation (Marris *et al.*, 1996)	Selection of methods based on cost-benefit analysis (Marris *et al.*, 1996; Langford *et al.*, 2000)	Users tend to accept whatever is imposed on them (Torbjorn, 2004; Marris *et al.*, 1996; Langford *et al.*, 2000)

Table I.
Initiating risk management according to users' cultural bias

Risk analysis tasks	Types of cultural bias			
	Hierarchy	Egalitarianism	Individualism	Fatalism
Risk identification Risk estimation Risk evaluation	Threats with regard to social order prevail for users (Torbjorn, 2004; Marris *et al.*, 1996; Langford *et al.*, 2000)	Users mostly fear threats related to their sense of equity or threats that may increase inequalities (Torbjorn, 2004; Marris *et al.*, 1996; Langford *et al.*, 2000) Users expect to be informed about risk analysis (Finucane and Holup, 2005) Level of tolerance against threats can be negotiated	Users mostly fear threats to their personal freedom (Torbjorn, 2004; Marris *et al.*, 1996; Langford *et al.*, 2000) The level of tolerance against possible threats is expected to be justified by using cost-analysis criteria	Users do not pursue awareness of risk (Torbjorn, 2004)

Table II.
Performing risk analysis according to users' cultural bias

At the risk analysis stage, identifying the stakeholders' cultural bias is also highly significant, since each bias is associated with specific fears. As previously said, hierarchists mostly fear of risks that disturb social order (Langford *et al.*, 2000; Marris *et al.*, 1996; Torbjorn, 2004). Security experts should therefore expect that users with this bias would consider security threats such as hacking and computer crime as most severe. IS users will very likely expect that these risks will be treated with low tolerance.

Egalitarians, on the other hand, mostly fear whatever threats their sense of equity or whatever may increase the inequalities amongst people, such as a denial of service attack. At the same time, they are suspicious to anybody in a position of authority, including specialised experts, they dislike concentration of power and are particularly sensitive to environmental threats and threats that derive from institutions that are perceived as inequitable (Langford *et al.*, 2000; Marris *et al.*, 1996; Torbjorn, 2004). According to Finucane and Holup (2005) egalitarians expect that they will be provided with full access to information on which they can base their own risk analysis and they fear anything that may obstruct their ability to negotiate (Marris *et al.*, 1996). Therefore, the results of a risk analysis, including tolerability levels, are expected to be negotiable by individuals who adopt this worldview.

Individualists are chiefly worried of threats to their personal freedom (e.g. denial of service attacks, communications infiltration) (Langford *et al.*, 2000; Lima and Castro, 2005; Torbjorn, 2004). They accept the validity of cost-analysis methods (Langford *et al.*, 2000; Lima and Castro, 2005), and would therefore prefer that security experts justify the resulting tolerability level with cost-analysis criteria.

Finally, fatalists will very likely regard risk analysis as a meaningless task, since they believe that risks cannot be controlled and feel powerless towards change, which is always regarded as being imposed from the outside (Torbjorn, 2004; Marris *et al.*, 1996; Langford *et al.*, 2000).

Table III.
Risk mitigation according to users' cultural bias

Risk mitigation tasks	Types of cultural bias			
	Hierarchy	Egalitarianism	Individualism	Fatalism
Design	Security experts should select countermeasures and policies that do not alter the users' standard workflow	Security experts should expect resistance to controls that result from their analyses	Security experts should expect reluctance to accept rules from the users' side	Security controls should be embedded in users' tasks
Implementation	Informative awareness programs should be designed	Awareness programs should place emphasis on the justification of security measures. Awareness programs should be based on the appropriate communication means	Awareness programs should emphasize on positive incentives to promote users' compliance with security rules and policies	Awareness programs should seek to bolster users' commitment to the organisation
Monitoring	Security experts should anticipate a tendency to cheat as a group in an orderly, disciplined and co-ordinated way from the users (Mars, 1996)	Security experts should expect limited adherence of rules from users who feel threatened by security controls	Security experts should expect a higher predisposition to risk taking procedure bypassing from the users' side users are expected to choose short-term personal advantage over long-term corporate benefit (Mars, 1996)	Security experts should expect limited breach of security

For example, in the case of a risk analysis review for a non-governmental health organization, where egalitarianism was identified as the prevailing stance, the group of experts involved, including one of the authors, encouraged an open discussion of risks within the organization, so as to reach a consensus on risks that should be mitigated and risks that the organization was willing to live with. In the case of a government body, on the other hand, hard evidence had to be provided, in order to persuade hierarchists in the organization that environmental hazards and unintended operation errors were equally hazardous with attacks launched by terrorist groups and the organized crime.

Different biases, as identified by cultural theory, have also an impact on the risk mitigation process (Figure 2). During the design stage, security experts should take into account stakeholders' biases, before selecting the appropriate countermeasures and policies to be applied in a specific organization. Hierarchists are characterized by low adaptability to change (Mars, 1996); therefore, countermeasures that significantly alter their standard workflow should be avoided, in order to avoid negative reaction. Egalitarians are very likely to have limited trust on experts (Langford *et al.*, 2000; Marris *et al.*, 1996; Torbjorn, 2004) and consequently might fail to fully comply with security controls imposed by security experts. Individualists are characterized by a reluctance to accepting rules (Mars, 1996), especially if these rules are perceived as obstructing their freedom. Security experts should therefore be aware, when confronted with such a situation, that such security measures, e.g. access control and authorization mechanisms will be regarded with suspicion. Finally, since fatalists usually prefer occupying posts with routine tasks (Mars, 1996), security experts can expect that these individuals will very likely follow security controls that are embedded in the routine of their jobs.

During the implementation stage (Figure 2) security experts would benefit from identifying users' cultural bias in designing the appropriate awareness programs. Hierarchists have a disposition to follow the rules and trust experts in general (Marris *et al.*, 1996); therefore awareness programs developed for individuals sharing this bias would better be structured following an informative approach. On the opposite, egalitarians have more difficulties in accepting role differentiations (Langford *et al.*, 2000; Marris *et al.*, 1996); therefore security experts should avoid justifying security controls based solely on their expertise. Awareness programs should emphasize on the rationale of selecting the security measures, and should follow a form of discourse or communication process. Awareness programs often provide information about the responsibilities of stakeholders and rely on their sense of responsibility and obligation towards their colleagues, their boss and the organisation, for the compliance with these responsibilities (Leach, 2003). This motivation is pointless for individualists, since they feel responsible only to themselves (Altman and Baruch, 1998; Langford *et al.*, 2000) and they mostly built short-term relationships with their superiors (Mars, 1996). Therefore, awareness programs addressed to these individuals should emphasize more on positive incentives, e.g. economic rewards, for following security practices. Finucane and Holup (2005) pinpoint the individualists' belief that people should receive material reward for their work. Finally, since fatalists tend to consider themselves as outsiders of the organisation they work for (Langford *et al.*, 2000; Marris *et al.*, 1996) as a result awareness programs addressed to them should put more effort in bolstering their commitment to the organisation.

At the monitoring stage, security experts should formulate their strategy after taking into account the specific characteristics of the different stakeholders' cultural bias. It is important for security experts to know that hierarchists are expected to break rules or act contrarily to a policy, as a group in an orderly, disciplined and co-ordinated way (Mars, 1996). Egalitarians are expected to break rules if they feel that these rules generate inequalities or if they are not convinced for their purpose. At this stage it is also important for security experts to be aware of the fact that individualists have a tendency to risk taking and a propensity to bypassing procedures. They are expected to choose short-term personal advantage over long-term corporate benefit (Mars, 1996). Finally, individuals whose worldviews tends to fatalism are not expected to breach security controls for their personal gain, since they believe they have little or no power to influence the course of events in their favour (Langford *et al.*, 2000).

For example, in the case of a private company in the area of mobile communications, where two of the authors acted as security consultants, the proposed awareness program aimed at fostering individual responsibility for security, because the users' worldview was predominately egalitarian. On the contrary, when confronted with an organization where fatalists prevail, detailed and unambiguous security procedures should be provided to the users.

5.3 Formulating context sensitive risk management strategies

Summarizing the previous sections we can argue that cultural theory may be useful in providing a tool for the analysis of the IS risk management social context and the stakeholders' perceptions. It should be noted that different cultural biases coexist in organizations, reflecting the different subcultures. Nevertheless, in most cases there is one type of cultural bias that prevails, or is more relevant with regard to security, than the others.

To begin with, the security expert should study the IS's social context, decide what the type(s) of cultural bias that he or she has to deal with are and, finally, adjust the IS risk management process accordingly. As described in Section 3, two distinct perspectives of the theory have been applied; the stability and the mobility view. The adoption of one perspective that is most appropriate for an IS security context has not been explored in this paper and is an issue that requires further research. Moreover, these social types can be explored either by quantitative or by qualitative methods or by mixed methodologies; an issue that is strongly affected by the adopted perspective of the theory. In this paper we state that, independently of the adopted perspective and the methodology used for the theory's practice, the grid/group model can be used by security experts for the management of users' perceptions of risk.

Based on the preceding analysis we can formulate four distinct strategies for IS risk management. These strategies would be developed on the basis of the different cultural bias IS users might share, according to the grid/group typology. The security expert can adjust the process of risk management by adopting the appropriate strategy, in order to manage the stakeholders' perceptions of risk, according to the social context of the IS risk management. Some of the key issues that must be considered in developing risk management strategies to offset each type of cultural bias are shown in Figure 4.

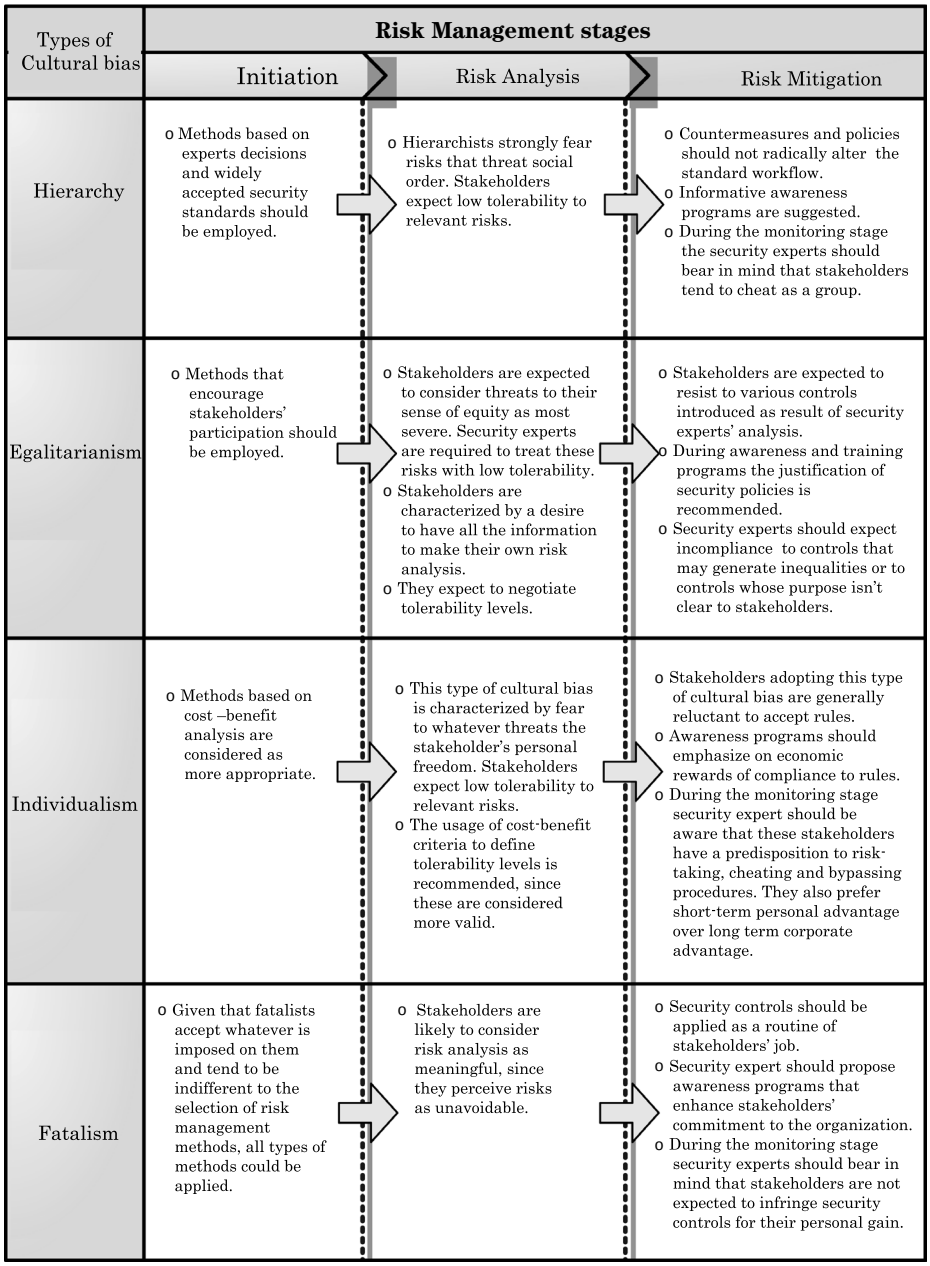

Figure 4.
Key issued to be considered in developing IS risk management strategies

6. Conclusions and further research

Risk management is a common practice applied by security experts for the protection of IS. Many researchers (Gerber and von Solms, 2005; Pfleeger, 2000) have pointed that the risk management process can be improved, if certain social factors that influence the process and the outcome of risk management are taken into account. These factors include the social context of security controls' application and the stakeholders' perceptions with regard to IS risks. Security experts are therefore called to manage not only technical IS security issues, but also social issues and threats (Trompeter and Eloff, 2001). Relevant approaches that attempt to manage these factors, exist; such as the design and implementation of awareness programs (Cresson Wood, 1995, 1997; Hansche, 2001; Peltier, 2005), but there is no scheme developed for the understanding and management of the perception of IS stakeholders.

In this paper we examined cultural theory as a sensitizing tool for identifying patterns in the stakeholders' perception of risk and we have presented its effect on the strategies for IS security management cultural theory has been applied to a variety of institutions, themes and areas (Altman and Baruch, 1998) and has been connected by various researchers to risk management (Lima and Castro, 2005; Marris *et al.*, 1996; Rayner, 1984), but not in the IS security context. Our analysis provides a framework for this association, which results in the identification of context sensitive risk management strategies.

The preceding analysis has allowed us to comprehend the role that cultural biases play with regard to security management and to formulate security strategies accordingly. The next step would be to transcribe these findings from the strategic to the operational level, so as security experts can employ practices that address cultural biases in the area of IS security management.

Another issue of further research includes the decision of the most appropriate perspective of the theory for the IS security context and the proper methodology as well. Notwithstanding, empirical research of the strategies' application and success should be conducted to support the validity of the proposed framework. Moreover, these strategies suggest factors that should be taken into account by security experts, in order to understand and manage the IS stakeholders' perceptions of risk. Since, these factors critically affect the process of risk management, they could be incorporated into an information security management system (ISMS), as this is specified by ISO/IEC 27001 (2005). In this standard, the ISMS is defined as part of the management system, which establishes, implements, operates, monitors, maintains and improves information security. The way the outlined strategies can be included into an ISMS is not obvious and should be further researched.

References

Altman, Y. and Baruch, Y. (1998), "Cultural theory and organizations: analytical method and cases", *Organization Studies*, Vol. 19 No. 5, pp. 769-85.

Baskerville, R. (1991), "Risk analysis: an interpretive feasibility tool in justifying information systems security", *European Journal of Information Systems*, Vol. 1 No. 2, pp. 121-30.

Bella, D. (1987), "Organizations and systematic distortion of information", *Journal of Professional Issues in Engineering*, Vol. 113 No. 4, pp. 360-70.

Boholm, A. (1996), "Risk perception and social anthropology: a critique of cultural theory", *Ethnos*, Vol. 61 Nos 1/2, pp. 64-84.

Computer Security Institute (2005), *CSI/FBI Computer Crime and Security Survey*, CSI Inc., Miamai, OK.

Cresson Wood, C. (1995), "Information security awareness raising methods", *Computer Fraud & Security Bulletin*, Vol. 1995 No. 6, pp. 13-15.

Cresson Wood, C. (1997), "Policies alone do not constitute a sufficient awareness effort", *Computer Fraud & Security*, Vol. 1997 No. 12, p. 14.

Dake, K. (1991), "Orienting dispositions in the perception of risk: an analysis of contemporary worldviews and cultural biases", *Journal of Cross-cultural Psychology*, Vol. 22 No. 1, pp. 61-82.

Dake, K. (1992), "Myths of nature: culture and the social construction of risk", *Journal of Social Issues*, Vol. 48 No. 4, pp. 21-37.

Dake, K. and Wildavsky, A. (1991), "Individual differences in risk perception and risk-taking preferences", in Garrick, B.J. and Gekler, W.C. (Eds), *The Analysis, Communication, and Perception of Risk*, Plenum Press, New York, NY, pp. 15-24.

Deery, H. (1999), "Hazards and risk perception among young novice drivers", *Journal of Safety Research*, Vol. 30 No. 4, pp. 225-36.

DFS (2005), *SBA Security: SBA-Scenario*, Swedish Information Processing Society, available at: www.dfs.se/products/sbaeng/method/ (accessed 27 September 2005).

Douglas, M. (1978), "Cultural bias", Occasional Paper No. 35, Royal Anthropological Institute of Great Britain and Ireland.

Douglas, M. (1992), *Risk and Blame: Essays in Cultural Theory*, Routledge, London.

Douglas, M. and Wildavsky, A. (1982), *Risk and Culture: An Assay on the Selection of Technological and Environmental Dangers*, University of California Press, Berkeley, CA.

Finucane, M. and Holup, J. (2005), "Psychosocial and cultural factors affecting the perceived risk of genetically modified food: an overview of the literature", *Social Science & Medicine*, Vol. 60, pp. 1603-12.

Frosdick, S. (1997), "The techniques of risk analysis are insufficient in themselves", *Disaster Prevention and Management*, Vol. 6 No. 3, pp. 165-77.

Gerber, M. and von Solms, R. (2005), "Management of risk in the information age", *Computers and Security*, Vol. 24 No. 1, pp. 16-30.

Gross, J. and Rayner, S. (1985), *Measuring Culture*, Columbia University Press, New York, NY.

Hansche, S. (2001), "Designing a security awareness program: part I", *Information Systems Security*, Vol. 9 No. 6, pp. 14-22.

Institute of Risk Management (2002), *A Risk Management Standard*, AIRMIC, ALARM, IRM, , available at: www.theirm.org/ (accessed 4 October 2005).

ISO/IEC 17799 (2005), *Information Technology – Security Techniques – Code of Practice for Information Security Management*, ISO/IEC, Geneva.

ISO/IEC 27001 (2005), *Information Technology – Security Techniques – Information Security Management Systems – Requirements*, ISO/IEC, Geneva.

Karyda, M., Kokolakis, S. and Kiountouzis, E. (2004), "Information systems security and the structuring of organisations", *Proceedings of the 7th International Conference on the Social and Ethical Impacts of Information and Communication Technologies (ETHICOMP 2004), Syros, Greece*, pp. 451-61.

Karyda, M., Kiountouzis, E. and Kokolakis, S. (2005), "Information systems security: a contextual perspective", *Computers and Security Journal*, Vol. 24 No. 3, pp. 246-60.

Kasperson, R. (1992), "The social amplification of risk: progress in developing an integrative framework", in Krimsky, S. and Golding, D. (Eds), *Social Theories of Risk*, Chapter 6.Vol. 6, Praeger, London, pp. 153-78.

Langford, I., Georgiou, S., Bateman, I., Day, R. and Turner, R. (2000), "Public perceptions of health risks from polluted coastal bathing waters: a mixed methodological analysis using cultural theory", *Risk Analysis: An International Journal*, Vol. 20 No. 5, pp. 691-705.

Leach, J. (2003), "Improving user security behaviour", *Computers and Security*, Vol. 22 No. 8, pp. 685-92.

Lima, M. and Castro, P. (2005), "Cultural theory meets the community: worldviews and local issues", *Journal of Environmental Psychology*, Vol. 25 No. 1, pp. 23-35.

Marris, C., Langford, I. and O'Riordan, T. (1996U), "Integrating sociological and psychological approaches to public perceptions of environmental risks: detailed results from a questionnaire survey", Centre for Social and Economic Research on the Global Environment, University of East Anglia, Norwich.

Mars, G. (1996), "Human factor failure and the comparative structure of jobs: the implications for risk management", *Journal of Managerial Psychology*, Vol. 11 No. 3, pp. 4-11.

Ney, S. and Molenaars, N. (1999), "Cultural theory as theory of democracy", *Innovation*, Vol. 12 No. 4.

NIST: 800-30 (2002), *Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology*, NIST, Dallas, TX.

Peltier, T. (2005), "Implementing an information security awareness program", *Information Systems Security*, Vol. 14 No. 2, pp. 12-37.

Pfleeger, S. (2000), "Risky business: what we have yet to learn about risk management", *Journal of Systems Software*, Vol. 53, pp. 265-73.

Rayner, S. (1984), "Disagreeing about risk: the institutional cultures of risk management and planning for future generations", in Halden, S. (Ed.), *Risk Analysis, Institutions, and Public Policy*, Associated Faculty Press, New York, NY, pp. 150-69.

Rayner, S. (1986), "Management of radiation hazards in hospitals: plural rationalities in a single institution", *Social Studies of Science*, Vol. 16, pp. 573-91.

Rayner, S. (1992), "Cultural theory and risk analysis", in Krimsky, S. and Golding, D. (Eds), *Social Theories of Risk*, Praeger, Westport, CT, pp. 83-116.

Rayner, S. and Cantor, R. (1987), "How fair is safe enough? The cultural approach to societal technology choice", *Risk Analysis*, Vol. 7, pp. 3-10.

Rippl, S. (2002), "Cultural theory and risk perception: a proposal for a better measurement", *Journal of Risk Research*, Vol. 5 No. 2, pp. 147-65.

Siponen, M. (2000), "A conceptual foundation for organizational information security awareness", *Information Management & Computer Security*, Vol. 8 No. 1, pp. 31-41.

Sjöberg, L. (1997), "Explaining risk perception: an empirical evaluation of cultural theory", *Risk, Decision and Policy*, Vol. 2 No. 2, pp. 113-30.

Sjöberg, L. (1998), "World views, political attitudes and risk perception", *Risk: Health, Safety and Environment*, Vol. 9 No. 2, pp. 137-52.

Sjoberg, L. (2000), "Factors in risk perception", *Risk Analysis*, Vol. 20 No. 1.

Slovic, P., Fischoff, B. and Lichtenstein, S. (1980), "Facts and fears: understanding perceived risk", in Schwing, R.C. and Albers, W.A. (Eds), *Societal Risk Assessment. How Safe is Safe Enough?*, Plenum, London, pp. 181-216.

Smallman, C. and Weir, D. (1999), "Communication and cultural distortion during crises", *Disaster Prevention and Mangement*, Vol. 8 No. 1, pp. 33-41.

Tansey, J. and O'Riordan, T. (1999), "Cultural theory and risk: a review", *Health Risk Society*, Vol. 1 No. 1.

Thompson, M., Richard, E. and Wildavsky, A. (1990), *Cultural Theory*, Westview Press, Boulder, CO.

Torbjorn, R. (2004), "Explaining risk perception: an evaluation of cultural theory, Norwegian university of science and technology",Vol. 85, Norwegian University of Science and Technology, Department of Psychology, Trondheim.

Trompeter, C. and Eloff, J. (2001), "A framework for the implementation of socio-ethical controls in information security", *Computers and Security*, Vol. 20 No. 5, pp. 384-91.

Walsham, G. (1993), *Interpreting Information Systems in Organizations*, Wiley, Chichester.

Whitman, M., Towsend, A. and Aalberts, R. (2001), "information systems security and the need for policy", in Dhillon, G. (Ed.), *Information Security Management: Global Challenges in the New Millennium*, Idea Group Publishing, Harshey, PA.

Further reading

ISO/IEC (2000), *Information Technology-Code of Practice for Information Security Management*, ISO/IEC 17799, Geneva.

About the authors

Aggeliki Tsohou is currently a PhD student at the University of the Aegean, Department of Information and Communication Systems Engineering. She holds a BSc in Informatics and an MSc in Information Systems, both acquired from Athens University of Economics and Business. Her research interests include information systems security management, risk assessment and risk management.

Maria Karyda is currently a postdoctoral researcher at the Information and Communication Systems Security Laboratory of the University of the Aegean. She obtained a BSc in Informatics, an MSc in Information Systems and a PhD in Information Systems Security from the Athens University of Economics and Business, Greece. Her research interests include organizational aspects of information systems security management, the use and application of security policies and security culture and awareness.

Spyros Kokolakis is a Lecturer at the Department of Information and Communication Systems Engineering at the University of the Aegean, Greece. He received a BSc in Informatics from the Athens University of Economics and Business in 1991 and a PhD in Information Systems from the same university in 2000. His current research interests include information systems security management, risk analysis, and security policies design and implementation. He is a member of IEEE and ACM. Spyros Kokolakis is the corresponding author and can be contacted at: sak@aegean.gr

Evangelos Kiountouzis is a Professor of Information Systems at the Department of Informatics of the Athens University of Economics and Business, Greece. He studied Mathematics at the University of Athens, Greece, and received a PhD in Informatics from the University of Ulster, UK. His professional and research interests focus on information systems analysis and design methodologies and on information systems security management. He is the author of several books on the topics of information systems and information systems security management and he has published numerous papers in international conferences and journals.