Development of a Framework for Analyzing Individual and Environmental Factors Preceding Attitude toward Information Security

Ruben Mancha
University of Texas at San Antonio

Glenn Dietrich
University of Texas at San Antonio

Follow this and additional works at: http://aisel.aisnet.org/amcis2007

Recommended Citation
http://aisel.aisnet.org/amcis2007/178

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2007 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
Development of a Framework for Analyzing Individual and Environmental Factors Preceding Attitude toward Information Security

Ruben Mancha  
The University of Texas at San Antonio  
ruben.mancha@utsa.edu

Glenn Dietrich  
The University of Texas at San Antonio  
glenn.dietrich@utsa.edu

Abstract

The purpose of this study is to explore the relations between environmental and personal factors affecting accepted peer influence as a determinant of the individual attitude toward information security. Interactional psychology offers a research framework in which the individual attitude related to security is considered a result of an interaction between the person and the situation. While research on information systems security using the organizational and group levels of analysis is common in the literature, research considering the implications of the individual characteristics and attitude on organizational information security is novel. Our primary interest is to present the theoretical framework, proposed model and suggested methodology to approach this research framework.

Keywords: Security, personality, peer influence, attitude, organizational security awareness, organizational norm

Introduction

Information security systems rely on different organizational, environmental, technical and individual factors. Security depends on the awareness and capabilities of the organization to create policies and proactively verify their implementation. The political and social environment also impact organizational security through legislative mandates and public opinion. Technology, as a facilitator, has a vital role in the assurance of information security. Ultimately information security relies on the behavior of the people that manage and use the information and on the factors that condition their behaviors.

Although the evident relevance of the human component on obtaining adequate levels of organizational information security, the study of the reciprocal interaction of technology, work environment and security can not be found in the IS literature (Gonzalez and Sawicka 2002). This topic is secondarily discussed in research regarding different aspects of organizational security.

The purpose of the present study is to fill the perceived gap by exploring personality dimensions and attempting to describe how they moderate the relation among organizational security awareness, organizational norm and accepted peer influence. Accepted peer influence is considered an antecedent of attitude toward information security. We attend to an individual level of analysis.
The present research contributes to the body of knowledge of Information Systems by proposing a model that links personality theory and the topic of information security. We support the idea that norm affects attitude in a process mediated by the level in which the individual perceives as rewarding the generally accepted view. This is backed by research testing Fishbein and Aizen’s (1975) model of attitude-behavior (Liska 1984, Sample and Warland 1973, Guagnano et al. 1995).

Our research offers another important contribution as it transgresses from a multidisciplinary interaction toward an interdisciplinary integration of the Information Systems and the Psychology disciplines. The contribution also extends to the managerial world as our research attempts to clarify the complex interplay between the employees’ personal characteristics, the work environment, and information security. The gained knowledge on the influence of personality on the individual accepted influence and attitude toward security would help managers to understand how to manipulate the organizational security environment to assure the optimal information security.

The rest of the paper is organized as follows. The next section briefly discusses previous work on the personal and environmental factors affecting security and adjoining topics. This is followed by an explanation of the theoretical framework and the research assumptions. The proposed research model is then presented and described. Next, the suggested methodology for a quantitative study design is presented. Finally the conclusions and limitations are discussed.

**Previous work**

There is limited empirical research in information security systems centered on the study of the interaction between individual characteristics, individual behavior, technology, and work environment (Gonzalez and Sawicka 2002). Nevertheless, a review of the literature indicates that the mentioned topic is secondarily and partially discussed in other areas of information security research. We have also to mention that, as in the case of the studies on computer abuse, the tripartite: human factors, environmental factors, and behavior are frequently approached from the perspective of security violations (Straub 1990).

Two articles were found to undertake a similar approach to the one we present. In the following paragraphs we discuss existing similarities and the main differences among our study and those articles.

Gonzalez and Sawicka (2002) discuss compliance and the relevance of human factors in information security, focusing on the perception of risk and its effects on compliance. They described a causal loop diagram and applied dynamical simulation to its study. Our research converges with the one by Gonzalez and Sawicka (2002) in that we also consider an interdisciplinary approach to information security systems and integrate individual and environmental factors for their simultaneous study. However, our proposal diverges from the former on two main aspects: (1) we consider personality as a factor that moderates the personal cognitive response affecting the individual compliance, and (2) the present research attends to a quantitative study with the purpose of verifying the validity of a variance model.

Personality and compliance were studied by Shropshire et al. (2006) in research where two of the five dimensions of personality: conscientiousness and agreeableness were hypothesized to be positively related to IT security-compliant behavior. Our research differs from Shropshire et al. (2006) in the following aspects: (1) we attend to the individual acceptance of influence seeking a favorable reaction of third parties; and (2) our model considers the personality dimensions as attribute variables moderating the relation between the environmental factors and the accepted peer influence. Also the purpose of Shropshire et al. (2006) is to “propose a method for identifying individuals who are most likely to commit IT security infractions based on various dimensions of their personality”. We instead attend to the verification of the relations proposed in a variance model; with the purpose of extending our knowledge on the interaction between environmental and personal factors, the accepted peer influence, and the attitude toward information security.

Once we have stated the few different research approaches to individual factors affecting information security found in the literature, we will introduce in the following sections the theoretical framework of our study and the variance model that we want to test.

**Theoretical framework**

In this study we want to verify the proposition that individual and environmental factors affect attitude in a process mediated by the accepted peer influence.
The proposed research approach is supported by the framework given by the interactionist model of personality research (Endler and Magnusson 1976, Terborg 1981). This model describes actual behavior as “a function of continuous process of multidirectional interaction […] between the individual and the situation encountered” (Terborg 1981). We consider attitude, precedent construct of Behavior and Intentional Behavior (Fishbein and Aizen 1975, Aizen 1988, 1991), as the mediating variable being affected by those environmental and personal factors.

Interactional psychology acknowledges that people vary in cognition, abilities and motivation, and that situations vary on cues, rewards and opportunities (Terborg 1981). Within this frame we begin our model considering two dimensions of personality: conscientiousness and agreeableness. We also consider two concepts that characterize the security environment in the organization: subjective norm and security awareness.

The model presented in figure 1 describes the proposed moderating effect of the personal factors on the accepted peer influence, and the assumed mediating effect of the accepted peer influence between the environmental factors and the attitude toward security. Accepted peer influence is defined as the level in which an individual accepts influence from the organization with the expectation of receiving a reward. The nature of the reward will be characterized in the next section.

![Figure 1. Interactionist model of individual attitude toward security mediated by the accepted peer influence](image)

Research on the Theory of Planned Behavior (Fishbein and Aizen 1975, Aizen 1988, 1991) and other studies considering the relation between attitude and behavior (Liska 1984, Sample and Warland 1973) support the relations, or the interest on the study of the relation, considered in the model. Our model attempts to increase the knowledge on the Theory of Planned Behavior by considering precedents that condition the cognitive deliberation that results in the attitude, and by integrating potential preceding independent and attribute variables of attitude.

| Table 1. Five personality dimensions (Carver and Scheier 1988, McCrae & Costa 1997) |
|---------------------------------|------------------------------------------|
| **Factor** | **Defining labels** |
| Extraversion | Assertiveness, open expression of impulses, confident assurance, happiness |
| Agreeableness | Warmness, docile compliance, considerate |
| Openness | Fantasy, ideas, values, aesthetics |
| Conscientiousness | Persistence, responsibility, planfulness, will to achieve |
| Neuroticism | Emotional disorganization, fearfulness, concern |

The vast research on personality and personality assessment seems to agree on the existence of five main personality dimensions (Digman 1990, McCrae and Costa 1987, Costa and McCrae 1992, Goldberg 1990, Carver and Scheier 1988) or
superordinate factors (Carver and Scheier 1988). At the same time there exists disagreement on the nature of the superordinate factors, as they are composed for several traits that represent “blends of factors” subject to connotative interpretations (Carver and Scheier 1988). The authors’ different characterizations of the dimensions rely on the types and number of traits or the measurement instruments each author considers. The general model of five personality dimensions is presented in table 1. We characterize each dimension attending to some defining labels. For further detail on the nature of the superordinate factors consider Digman (1990) and Carver and Scheier (1988).

Two of the dimensions are considered relevant for this research: conscientiousness and extraversion.

Now that the framework has been presented we will define and discuss the constructs and the relations proposed in the model.

**Research model**

The model is presented below in figure 2. In the remainder of this section we will define the constructs, describe the relations among them, and state the hypotheses to test.

![Proposed model of interactional characterization of the attitude toward security](image)

**Figure 2. Proposed model of interactional characterization of the attitude toward security**

Organizational security subjective norm is defined as the individual’s perception of whether people important to the individual in the organization think the behavior should be performed. This construct can be viewed as social norm (Aizen 1988, 1991) in organizational settings.

Organizational security awareness is defined as the level in which the users in an organization are aware of the security mission of the organization (Siponen 2000). The security mission is presented to the employee as security guidelines or procedures.

The first construct derived from a personality dimension is agreeableness. It is defined as the individual tendency of being concerned with the maintaining of relationships (Costa and McCrae 1985, Carver and Scheier 1988). It has also been related with altruism, nurturance, caring, and emotional support (Digman 1990). We find support in the literature to add to the mentioned list of traits: conformity (Fiske 1949), and friendly compliance (Digman and Takemoto-Chock 1981).
The second construct derived from a personality dimension is conscientiousness. It is defined as the individual purposeful striving toward goals, and also as responsibility and planfulness (Carver and Scheier 1988).

Accepted peer influence is defined as the level in which an individual accepts influence from other individuals in the organization and determines her / his attitude toward security, with the expectation of receiving an intrinsic or an extrinsic reward. Accepted peer influence should not be considered as a degree of action in accordance with the imposed norm. It should be understood as the degree in which the individual includes personal beliefs in the value system, in acceptance of external influence, or with the expectation of a reward (Kelman 2006).

Attitude toward security is defined, following the original work of Fishbein and Aizen (1975) and Aizen (1988, 1991), as the individual’s positive or negative feelings about performing the behavior of securing the information. Behavioral intention and behavior correspond with the homonym constructs of the Theory of Planned Behavior (Fishbein and Aizen 1975, Aizen 1988, 1991).

We will now define the relations proposed in the model:

Two environmental factors: organizational security awareness and organizational security subjective norm are considered constructs affecting the level of accepted peer influence. We propose to assess the following formal relations: (R1) organizational security subjective norm affects the level of accepted peer influence, (R2) organizational security awareness affects the level of accepted peer influence, and (R3) organizational security subjective norm affects attitude toward security. The study of the relation (R3) will allow us to test the assumed mediation of level of accepted peer influence between organizational security subjective norm and attitude toward security.

We also propose the following moderating relations in the model: (M 2R1) the construct agreeableness acts as a moderator of the relation between the organizational security subjective norm and the level of accepted peer influence, (M 1R1) the construct conscientiousness acts as a moderator of the relation between the organizational security subjective norm and the accepted peer influence, and (M 1R2) the construct conscientiousness acts as a moderator over the relation between organizational security awareness and the accepted peer influence.

The level of accepted peer influence, as the level of cognitive acceptance of an external influence, is related to the attitude toward information security. To justify this relation we have to consider that accepted peer influence underlies in its construction a change on beliefs, more or less profound depending on their level of integration in the personal value system (Kelman 2006). The relation between beliefs and attitude is also supported in the models by Fishbein/Aizen (Liska 1984).

The Theory of Planned Behavior (Fishbein and Aizen 1975, Aizen 1988, 1991), and related research on the relation among attitude and behavior (Sample and Warland 1973, Terry and Hogg 1996), have demonstrated the validity of the relations between attitude toward the behavior, intentional behavior, and actual behavior. Two other constructs: level of identification and level of internalization (Kelman 1958, 2006), although not considered as part of this first study, are reflected in the model, defined, and proposed to relate to the attitude toward security. Perceived group norm, also social norm, has been found to predict individual attitude (Terry and Hogg 1996, Aizen 1988, 1991), justifying the relation (R3) between organizational security subjective norm and accepted peer influence.

The operationalization of the personality constructs should consider alternative and supplemental dimensions to assure the completeness of the measurements. The adjective check list (Piedmont et al. 1991) can be considered as the measurement instrument with those purposes.

The hypotheses can be formally expressed as:

H1. The degree of organizational security subjective norm is positively related to the accepted peer influence.

H2. The degree of organizational security awareness is positively related to the accepted peer influence.

H3a. The personality attribute conscientiousness positively moderates the relation between organizational security subjective norm and accepted peer influence.

H3b. The personality attribute conscientiousness positively moderates the relation between organizational security awareness and accepted peer influence.

H4. The personality attribute agreeableness positively moderates the relation between organizational security subjective norm and accepted peer influence.
We have included other two constructs in the model as directions for future research. We will briefly discuss their importance and the previous studies that justify their consideration. Their proposed relations to the other constructs in the model have also been represented. Level of identification and level of internalization have been adapted to the nature of the model from Kelman (1958), and are defined here as:

Level of identification is the degree in which an individual accepts influence because he/she wants to establish or maintain a satisfying self-defining relationship to another person or group (Kelman 1958, 2006).

Level of internalization is defined as the level in which an individual accepts influence in order to maintain the congruence of actions and beliefs, because of the content of the induced behavior (Kelman 1958, 2006).

Level of identification and level of internalization define two dimensions of attitude. Level of identification refers to the extent in which a person considers the adoption of the induced behavior as extrinsically rewarding. Level of internalization represents the degree in which the individual considers the adoption of the induced behavior as intrinsically rewarding. We justify the relevance of those two constructs in the model as they can be considered properties of attitude. Research demonstrates that attitude effects are dependent on attitude properties (Liska 1984), including the manner of attitude formation (Fazio and Zanna 1978), and the intensity of the attitude (Liska 1984). We justify that attitudes formed through identification differ in nature from those formed through internalization. We also argue that intrinsically rewarding behaviors have different intensity than extrinsically rewarding behaviors.

In this section we have defined the constructs, discussed the model and the proposed relations between the constructs, and formally presented the hypotheses we want to test. In the following section we will briefly mention the research methodology.

Proposed research methodology

We propose a research design within the explained interactional framework as a quantitative study. The subjects must use in their daily work-related tasks an information system with access to organizational data. All the work-scales complying with this requirement should be equally considered. Specific data regarding the subjects’ work position and the size of the organization will be gathered.

We consider as the ideal sample size no less than 200 subjects from different types of organizations, attending to data analysis and validity constraints. The superordinate factors of personality conscientiousness and agreeableness can be characterized for the participants using an adjective check list (ACL). This personality assessment allows the recovery of the five superordinate factors of personality when appropriate markers are used (Piedmont 1991).

The development of two questionnaires is required to assess organizational security subjective norm and organizational security awareness. Organizational security awareness should be computed as an aggregate indicator from the individual responses within each organization considered. Information about the nature of the existing security guidelines should be obtained from the personnel responsible of information security, and contrasted with the results. Two questionnaires should be created to assess the individual level of accepted peer influence and attitude toward security.

We anticipate the use of two multiple regression techniques to analyze the data: moderated multiple regression (MMR) and hierarchical multiple regression (HMR). MMR is frequently used to test moderation effects (Stone-Romero and Liakhovitski 2002) and HMR to test for mediating effects (Stone-Romero and Rosopa 2004).

The use of HMR to validate the assumed-mediating effect of accepted peer influence on attitude toward security should acknowledge some limitations due to the non-experimental nature of the design considered (Stone-Romero and Rosopa 2004). Causal inferences should not be concluded using this regression strategy. The use of this design is justified attending to the exploratory nature of the study.

Threats to validity

We perceive a priori the possibility of different threats to validity acting in the proposed design. In the following paragraphs we explain the most important ones and consider some possible actions to minimize their effect.
The nature of sample will depend on the number and type of organizations that will become part of the study. Information about the type and size of organization will be gathered to study a possible selection threat on the sample. Another threat to consider relevant to internal validity is the ambiguous causal precedence. We can only base the validity of the proposed temporal occurrence on previous research on similar models (Liska 1984, Sample and Warland 1973, Fishbein and Aizen 1975), as the proposed non-experimental design does not allow us to infer causality.

Construct validity is another threat to consider, especially for the constructs: accepted peer influence, organizational security subjective norm, and organizational security awareness. Construct confounding should be studied in each case. We are also aware of a possible mono-method bias’ internal threat. The use of negatively worded items could be used to minimize it.

Content validity might be a problem in the newly created questionnaires (although content validity problems are not expected with the personality variables using in their assessments ACL). Positively and negatively worded questions should be used to reduce acquiescence response bias.

The use of pre-tests should be considered to assess reliability of the questionnaires and general aspects of construct validity.

The limited generalizability of the results is also considered a threat in the proposed study design. To reduce it we would suggest following the recommendations given by Shadish, Cook and Campbell (2002) to assess external validity using grounded theory. We also suggest the consideration of a sample size not inferior to 200 subjects, based on the directions given by Stone-Romero and Liakhovitski (2002) to increase the statistical power of the HMR methodology.

Conclusions and limitations

In this paper we have presented a theoretical model that accounts for environmental and individual factors to explain the individual level of attitude toward security. Two dimensions of personality: agreeableness and conscientiousness are expected to positively moderate the effect of the organizational security subject norm and the organizational security awareness on the level of accepted peer influence. At the same time, the accepted peer influence has been justified as a assumed mediator on the attitude toward security.

We have described a non-experimental design for the study and analyzed its main limitations as directions for future research.

The contribution of the paper is not limited to the model proposed. We have made use of a theoretical framework that should be explored further in the study of the relation among individual and organizational factors affecting information systems generally, and information security particularly. We have also included in the model and characterized two constructs as properties of attitude (Liska 1984): level of internalization and level of identification. We encourage the scholars in the Information Systems discipline to conduct studies considering those two or similar constructs in order to increase our understanding on the nature of the attitude toward information security behaviors and, more generally, toward the use of information systems.

References


Fiske, D. W. "Consistency of the factorial structures of personality ratings from different sources," Journal of Abnormal and Social Psychology (44), 1949, pp 329-44


