Association for Information Systems
AIS Electronic Library (AISeL)

WISP 2012 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

Winter 12-15-2012

Conceptualization of Constructs for Shaping Information Security Behavior: Towards a Measurement Instrument

Waldo Rocha Flores
Royal Institute of Technology, waldorf@ics.kth.se

Matus Korman
Royal Institute of Technology

Conceptualization of Constructs for Shaping Information Security Behavior: Towards a Measurement Instrument

Waldo Rocha Flores[1]
Industrial Information and Control Systems, Royal Institute of Technology,
Stockholm, Sweden

Matus Korman
Industrial Information and Control Systems, Royal Institute of Technology,
Stockholm, Sweden

ABSTRACT

The development of new means to attack information systems by attacking humans accessing the systems has increased the attention given to risks related to human or social aspects of information security. However, the effect of organizational key constructs proposed in organizational and individual behavior literature on information security has not been rigorously examined. Therefore it is important to develop measurement instruments and validate them properly to empirically capture the phenomena with reliable results. In this paper we attempt to conceptualize seven constructs and their sub-dimensions toward developing a measurement instrument. This attempt is carried out through specifying the nature of each construct's conceptual domain and surveying content domain experts on the relevance, comprehensiveness and clarity of the identified dimensions of the construct. Based on the survey results we provide a set of validated constructs and dimensions that can be used to formally specify future measurement models for investigating how organizations can influence information security behavior.

Keywords: Information security; information security behavior; construct conceptualization.

[1] Corresponding author. waldorf@ics.kth.se

INTRODUCTION

The increased effectiveness and robustness of technical security components has made it more difficult to successfully attack an organization's computer systems using purely technical means. Many attackers have therefore started to attack the humans accessing and using the computers through attacks that exploit human social weaknesses (e.g., social engineering) (Applegate 2009). This development has increased the attention given to risks related to human or social aspects of information security. The research domain is however still rather immature and extant socio-technical information security approaches criticized as lacking not only theoretically grounded methods, but also empirical evidence on their effectiveness (Puhakainen and Siponen 2010). Furthermore, there is a deficit in the literature on studies investigating the effect of key organizational constructs proposed in organizational and individual behavior literature related to information security (Hu et al. 2012). We therefore believe that studies to identify important organizational and individual constructs to shape employee behavior are needed. This paper reports on our first results of the development of an instrument to measure the organizational impact on information security behavior. The instrument includes the following organizational and individual constructs that were identified through a previously conducted research study: Information Security Leadership, Organizational Structure, Information Security Process, Security Knowledge Transfer, Perceived Learning Oriented Environment, Perceived Social Information Security Culture, and Perceived Employee Awareness (Rocha Flores and Ekstedt 2012).

To assure the validation of the measurement instrument, the conceptual domain of the included constructs are first defined as recommended by literature (MacKenzie et al. 2011). This important stage of instrument development has, unfortunately, often been neglected. This has led

to a significant amount of trouble later in the validation process and triggered a sequence of events that undermines construct validity. This paper therefore argues that the development of a measurement instrument that follows a formal and rigorous process is critical for reliable empirical results, and addresses the inadequate attention given in the literature concerning construct conceptualization in the construct validation process. The purpose of the study is threefold. Firstly, we attempt to specify the nature of the constructs' conceptual domain, i.e., identify the type of property the construct represents, and the entity to which it applies. Secondly, we attempt to identify the relevance and comprehensiveness of the identified construct's dimensions by surveying content domain experts. Finally, we provide a set of validated constructs and dimensions whose definitions have been tested for unambiguity. In doing so, we attempt to fill a gap in the existing literature by providing a set of constructs that have undergone a conceptualization process. This set can be used in future studies to investigate how organizations can influence information security behavior. The rest of the paper unfolds as follows. In the next section, we present the preliminary conceptualization of the included constructs and related dimensions. Section three presents the method for collecting survey data on the proposed conceptualization. Section four presents and discusses results of the survey, and section five summarizes and concludes the paper.

CONSTRUCT CONCEPTUALIZATION

While there have been many instruments developed to measure the influence of individual factors on compliance behavior, there are few that capture the influence of organizational and individual constructs in combination. Further, little attention has been given to the conceptualization process. According to (MacKenzie et al. 2011), an adequate definition of the construct domain is of crucial importance to the validity of the study, particularly content

validity. A critical first step to achieving this is to develop a precise and detailed conception of the target construct and its theoretical context. The construct, as well as the conceptual domain to which the construct belongs (the property to which the construct refers and the entity to which the construct applies) need to be formally specified. It is also suggested to consider the conceptual theme of the construct in terms of necessary and sufficient attributes or characteristics, and stability over time, across situations and cases when defining the constructs. Finally, the construct needs to be defined in unambiguous terms. Once the constructs have been clearly defined, it is important to step back and evaluate the construct dimensionality, i.e., whether there are multiple sub-dimensions of per focal construct and how they related to the focal construct and to each other. In this study, seven focal constructs with multiple dimensions used in the conceptualization process are presented in table 1, together with their property, entity and preliminary set of dimensions. As mentioned in the previous section, these constructs were identified in a research study that was previously conducted (Rocha Flores and Ekstedt 2012).

Table 1. Focal constructs and their conceptual domain

Construct	**Property**	**Entity**	**Dimensions**
Information Security Leadership	Action	Person	Articulate Security Vision,
			Provide Appropriate Role Model,
			Foster Employee Cooperation towards Common Goals,
			Set High Performance Expectations
Organizational Structure	Intrinsic characteristic	Organization	Existence of Formal Information Security Unit,
			Existence of Senior-Level Information Security Executive,
			Existence of Information Security Steering Committee,
			Well-defined Information Security Responsibility Structure
Information Security Process	Process	Organization	Continuous Information Security Planning,
			Information Security Performance

			Monitoring
Security Knowledge Transfer	Process	Persons	Formal Training on Information Security Policies, Formal Awareness Training on General Information Security Threats, Informal Knowledge Sharing Arrangements Use of IT for Knowledge Transfer
Perceived Learning Oriented Environment	Perception	Person	Perceived Support When Performing Security-related Tasks, Verbally Given Feedback when Learning Information Security, Vicarious Experience
Perceived Social Information Security Culture	Perception	Person	Social Relationships, Shared Security Goals
Perceived Employee Awareness	Perception	Person	Perceived Information Security Policy Perceived General Security Awareness

RESEARCH DESIGN

After the constructs were preliminarily conceptualized, a pilot test was performed to get opinions on the survey material. The purpose was to get feedback on the preliminary categorization, its understandability and on the definitions of the constructs. We approached three groups for the pilot in three rounds. The first group included three IT professionals, the second included three academic experts within conceptual modeling and research methodology, and the third group contained three academics with general competence in information security. The pilot participants were asked to complete the survey, and give us comments on the quality of the survey instrument. Each respondent was interviewed after completing the survey to find out how the survey could be improved. Between each round the instrument was revised and after the third round we found the survey quality to be satisfying.

Selection of Content Domain Experts

A thorough selection of experts based on expert criteria is important in order to assure reliability and quality of the study (Weiss and Shanteau 2003). The experts were identified from

scientific articles from searches in professional societies' databases such as the IEEE and in pure indexing databases such as SCOPUS. The search criteria involved combinations of topic-words such as "socio-technical information security", "information security governance", "information security", and "information security management" with research area limitations such as "knowledge sharing" and "IT governance". The resulting selections of articles were then manually screened, based on title and abstract (if sufficient) or full content (if necessary) to determine whether the authors should be invited to participate or not. The searches were limited in time to the past three years, i.e. only publications from 2008 and onward were selected. In all, 120 content experts were invited to participate. We decided on the number of respondents based on the following three reasons: Firstly, the study is of exploratory nature. Secondly, we also collected qualitative data on opinions and having too many respondents would make is difficult to analyze the data (Kvale 1986). Thirdly, in the process of collecting data for validating relevance and comprehensiveness of included variables, a minimum of three experts are advised while it is indicated that using more than ten is probably unnecessary (Lynn 2006).

The Survey

As the experts consulted in this study were geographically widely spread, an e-mail survey was used (Mangione 1995). Invitations to respond to an electronic survey were sent in September to a sample of content domain experts. The survey was hosted by a widely used internet-based application (SurveyMonkey) and open for answering during ten days. A reminder was sent to non-responding participants in order to increase the response rate (Blaxter et al. 2010). The survey consisted of five pages of which the first provided an introduction to the survey, and guidance for answering the questions. The second page included questions used to assess background information of respondents. The following pages of the survey consisted of

seven questions utilized in order to obtain information regarding the degree of association the experts believe each dimension has to its focal construct. For each dimension the respondents were asked to assess their degree of association to its focal construct using a five-point Likert scale ranging from 1 to 5, where 1 = not associated, 2 = somewhat associated, 3 = quite associated, 4 = highly associated, and 5 = very highly associated. The survey also included questions about the comprehensiveness of the dimensions, i.e. if there is any important dimension missing to capture the construct domain, and the understandability of the dimensions, i.e. if the dimensions are named improperly and should therefore be renamed. For each construct the respondents were asked to give qualitative opinions on the given set of dimensions in order to assure that all dimensions related to the constructs have been taken into account.

Analysis

SPSS 19.0 was used to analyze the survey data. As a first step we checked for outliers and non-normality. Then means, standard deviation, maximum and minimum values were calculated. Inspired by Stalmeijer et al. (2008), we initially decided to eliminate from the questionnaire the dimensions that were rated below 3.5 and after considering the experts' comments on why they believed the dimension is not relevant to its construct. However, if a dimension rate both was close to the threshold and there is strong theoretical evidence for the importance of the dimension, we decided to keep the dimension. Furthermore, there were some cases where the experts both commented on dimension names and suggested changes. In these cases the dimensions were modified, accordingly. We believe that in some cases our dimensions were not formulated clearly enough, as the experts believed them to be somewhat less relevant, unlike indicated by the theoretical background. Those specific dimensions were kept in the model. Finally, we also included new dimensions based on the experts' comments.

RESULTS AND DISCUSSION

In total, 18 experts completed the survey section regarding the organizational constructs (15%), and 16 completed the survey regarding the individual constructs (12.5%). After ten days we were satisfied with the number of completed surveys and thus choose to close the survey. The descriptive results indicate that the experts in general believed the included dimensions to be relevant and thus associated the constructs as proposed, with ratings varying between 2.9 and 4.5 (Table 2).

Table 2. Descriptive results (1 = not associated; 5 = highly associated)

Constructs and Dimensions	**Min**	**Max**	**Mean**	**SD**
Information Security Leadership				
Articulate Security Vision	3	5	4,5	0,71
Provide Appropriate Role Model	2	5	3,9	0,8
Foster Employee Cooperation Towards Common Goals	2	5	3,9	0,96
Set High Performance Expectations	1	5	2,9	1,35
Organizational Structure				
Existence of Formal Information Security Unit	2	5	3,6	1,09
Existence of Information Security Executive	1	5	3,6	1,34
Existence of Information Security Steering Committee	1	5	3,1	1,18
Well-defined Information Security Responsibility Structures	2	5	4,2	0,99
Strategic Information Security Process				
Continuous Information Security Planning	2	5	4,1	1,21
Information Security Performance Monitoring	2	5	4,2	0,94
Security Knowledge Transfer				
Formal Training on Information Security Policies	2	5	3,8	1,1
Formal Awareness Training on General Information Security Threats	2	5	3,7	1,07
Informal Knowledge Sharing Arrangements	1	5	3,5	1,1
Use of IT for Knowledge Transfer	1	5	3,3	1,19
Perceived Employee Awareness				
Perceived Information Security Policy Awareness	2	5	4,1	1,06
Perceived General Security Awareness	3	5	3,9	0,72
Perceived Learning Oriented Environment				
Perceived Support When Performing Security-related Tasks	2	5	3,9	0,89
Verbally Given Feedback	1	5	3,3	0,87
Vicarious Experience	2	5	3,4	1,09
Perceived Social Information Security Culture				
Social Relationships	1	5	3,7	1,3
Shared Security Goals	1	5	3,8	1,21

Qualitative Suggestions and Modifications to the Proposed Conceptualization

Among the organizational constructs and dimensions, Set High Performance Expectations ended up with a score of 2.9, which is below the chosen threshold (3.5). In addition, 27.8% of the respondents meant that the dimension was not associated with its construct, which created an obvious polarization between the negative answers as compared to the majority of slightly positive answers (38.9%) and an equal amount of mid-scale answers (27.8%). On the contrary, it was argued that clear and concrete objectives should be defined based on acceptable risk criteria, which in context of the study we see upon as a form of security performance expectations. In addition, a proposition to include Punishment of Non-compliance was made. Based on those inputs and our further judgment, we decided to replace the construct called Set High Performance Expectations with Perform Regulatory Actions so as both to cover the act of articulating expectations seen as an integral part of leadership (Podsakoff et al 1990), and include the use of contingent reward (i.e., punishment and rewards aimed at achieving compliance). The dimension Existence of Information Security Steering Committee ended up with a score of 3.1 and one respondent noted that the existence of a formal information security unit or steering committee might not be feasible for smaller organizations. Taking the comment into consideration, we revised the three closely related constructs named Existence of (Formal) Information Security {Unit, Executive, Steering Comittee}, only retaining the first. At the same time, a construct named Information Security Liaisons was added so as to reflect the function of coordinating information security efforts across the organization (Kayworth and Whitten 2010). Based on the expert feedback received, the Strategic Information Security Process dimension was broadened by a construct named Risk Assessment. Finally, given both the threshold closeness and the considerably tenable view of IT as a significant contributor to knowledge

transfer in corporate environments (Gold et al. 2001), we decided to retain the construct Use of IT for Knowledge Transfer despite it having received a score of 3.3 (0.2 below the threshold).

Among the individual constructs and dimensions (as opposed to the organizational ones), constructs named Verbally Given Feedback and Vicarious Experience ended up below the threshold, scoring 3.3 and 3.4, respectively. According to several respondents, terms used to describe the individual constructs and dimensions were difficult to grasp, while the connection to information security was not obvious. Admitting this difficulty as a possible bias factor, the closeness of the construct scores to the chosen threshold (0.2 and 0.1, respectively) while considering the availability of a strong theoretical background in favor of the dimensions' relevance to the construct (Warkentin et al. 2011), we finally decided to also retain these two constructs.

SUMMARY AND CONCLUSIONS

The purpose of the study was threefold. Firstly, we have attempted to specify the nature of the construct's conceptual domain. Secondly, we have surveyed content domain experts on the relevance, comprehensiveness and clarity of the identified constructs' dimensions. Finally, based on the quantitative survey results and qualitative suggestions we provided a set of validated constructs and dimensions that can be used to formally specify a measurement model that investigates how organizations can achieve resilient information security behavior. In doing so, we have attempted to fill a gap in the information security literature by providing a set of organizational and individual constructs, that has been conceptualized, and can be used in future empirical models. The revised conceptualization of constructs and dimensions are depicted in table 3. See table 1, for the constructs conceptual domain (related properties and entities).

In the next phase of the research, empirical data will be collected using the key informant methodology in which respondents will be chosen based on their position, experience and professional knowledge. Data will be collected from two key-informants per organization – one respondent from the security organization, and one with a role that includes regular utilization of information technology products and services, e.g. computers, Internet access, electronic mail, etc. (at least ten respondents per organization). Hypotheses will be tested using structural equation modeling. Items to capture the constructs will be generated, and the content validity of the items will be assessed. After formally specifying a measurement model, empirical data will be collected from convenience samples through two pilot surveys. To measure behavior while being under an attack, we are currently conducting several experiments. Quantitative data is being collected through several case studies using a scenario-based survey and unannounced phishing experiments. As a scenario-based survey is planned to be used for measuring information security behavior in the empirical study, the usefulness of a scenario-based survey to assess information security behavior will be evaluated by comparing the results from both methodology approaches. Finally, the validated research model will be set to the test through collection of data from Swedish organizations.

Table 3. Revised set of constructs and dimensions with definitions

Construct or dimension	**Definition**
Information Security Leadership	*The information security leader's actions to motivate employees to adopt a security-savvy behavior.*
Articulate Security Vision	The information security leader's actions to articulate a security vision so that all employees can easily and clearly understand the aim of information security efforts is in the organization.
Provide Appropriate Role Model	The information security leader's actions to both show a reasonable level of mastery, and make it clear for each employee what role s/he plays in the organization's information security efforts, what are his/her responsibilities and whom to turn to in case of a concern.
Foster Employee Cooperation Towards	The information security leader's actions to portray information security efforts as business-supportively protective and collective

Common Goals	(as opposed to purely individual); promote understanding and cooperation as a means of achieving and maintaining effective information security.
Perform Regulatory Actions	The information security leader's actions to set expectations, as well as provide contingent reward (i.e., punishing non-compliance and negligence while rewarding success stories and exemplary behavior).
Organizational Structure	*A set of static organizational characteristics, which in context of this study, should support governance of information security.*
Existence of Formal Information Security Unit	The existence of a formal organizational unit responsible for handling information security matters within the organization (e.g., coordinating incident responses, providing support to employees or providing advice upon an information security concern.)
Information Security Liaisons	The existence of top-down coordinated (vertical) cooperation on information security within the organization (e.g., each significant department or organizational unit having a manager responsible for coordinating information security efforts).
Well-defined Information Security Responsibilities	The existence, accessibility and proper distribution of clear descriptions of information security responsibilities to all relevant employees in the organization.
Strategic Information Security Process	*A formal and systematic effort (a set of activities) with the purpose of managing information security.*
Risk Assessment	A formal and systematic effort aimed at maintaining an actual picture of assets, threats, weaknesses, existing countermeasures and finally risks, with regards to information security.
Information Security Planning	A formal and systematic effort aimed at planning for information security (e.g., acquisition of countermeasures, training and education, exercises.)
Information Security Performance Monitoring	A formal and systematic effort aimed at monitoring the state of information security, as well as the performance of information security efforts and countermeasures (e.g., structures, rules or systems) in the organization.
Security Knowledge Transfer	*A process of capturing and sharing knowledge about information security among organizational members through formal and informal information flows.*
Formal Training on Information Security Policies	Formal activities as a result of a systematic effort aimed at training employees on compliance with actual information security policies in the organization.
Formal Awareness Training on General Information Security Threats	Formal activities as a result of a systematic effort aimed at training employees on general information security threats (e.g., threats relevant while browsing the Internet, using e-mail for correspondence, or telephone communication).
Informal Knowledge Sharing Arrangements	Informal activities and arrangements (e.g., meetings, seminars or workshops) aimed at sharing knowledge and experience regarding information security matters.
Use of IT for	The utilization of IT resources (e.g., IT solutions and/or devices) in

knowledge transfer	order to aid spreading, sharing and maintenance of information security awareness and knowledge in the organization.
Perceived Learning Oriented Environment	*Employee's perception of the support, possibilities and encouragement of learning within the organizational environment.*
Perceived Support When Performing Security-related Tasks	The individual perception of the availability of support when performing a work task (e.g., situational support from colleagues or a superior).
Verbally Given Feedback when Learning Information Security	The individual perception of verbal feedback being provided regarding information security while performing work tasks etc. (e.g., informal verbal warning, coaching, dialogues or discussions).
Vicarious Experience	The process of observation- and imitation-based learning from colleagues, co-motivated through seeing a colleague successfully perform a task.
Perceived Social Information Security Culture	*The employee's individual perception of shared beliefs and values among colleagues in the work environment.*
Social Relationships	The employee's individual perception of the quality (e.g., richness and friendliness) of social relationships at the workplace.
Shared Security Goals	The employee's individual perception of security goals being shared at the workplace (i.e., the employee and his/her colleagues share the same goals regarding information security).
Perceived Employee Awareness	*The employee's individual perception of both his/her general knowledge about information security and his/her cognizance of the information security policy, at an employee.*
Perceived Information Security Policy Awareness	The employee's individual perception of his/her own cognizance of the actual information security policy in the organization.
Perceived General Security Awareness	The employee's individual perception of his/her own awareness of general information security phenomena such as value of assets, threat exposure given circumstances, vulnerabilities and risks.

REFERENCES

Applegate, S. D. 2009. "Social Engineering: Hacking the Wetware!," *Information Security Journal: A Global Perspective* (18:1), pp. 40-46.

Blaxter, L., Hughes, C., and Tight, M. 2010. *How to Research*, 4th edn. Maidenhead: McGraw-Hill/Open University Press.

Hu, Q., Dinev, T., Hart, P., and Cooke, D. 2012. "Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture," *Decision Sciences* (43:4), pp. 615-660.

Kvale, S. 1986. *Interviews. An introduction to qualitative research interviewing*, Thousand Oaks, CA: Sage Publications.

Lynn, M. R. 2006. "Determination and Quantification of Content Validity," *Nursing Research* (35:6), pp. 382-386.

MacKenzie, S. B., Podsakoff, P. M., and Podsakoff, N. P. 2011. "Construct measurement and validation procedures in MIS and behavioral research: integrating new and existing techniques," *MIS Quarterly* (35:2), pp. 293-334.

Mangione, T. W. 1995. *Mail Surveys: Improving the Quality*, Thousand Oaks, CA: Sage Publications.

Puhakainen, P., and Siponen, M. 2010. "Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study," *Management Information Systems Quarterly* (34:4), pp. 757-778.

Rocha Flores, W., and Ekstedt, M. 2012. "A Model for Investigation Organizational Impact on Information Security Behavior," In *Seventh Annual Workshop on Information Security and Privacy (WISP) 2012*.

Stalmeijer, R. E., Dolmans, D. H. J. M., Wolfhagen, I. H. A. P., Muijtjens, A. M. M., and Scherpbier, A. J. J. A. 2008. "The development of an instrument for evaluating clinical teachers: involving stakeholders to determine content validity.," *Medical teacher* (30:8), pp. 272-277.

Weiss, D. J., and Shanteau, J. 2003. "Empirical assessment of expertise.," *Human factors* (45:1), pp. 104-116.

Bonini, C. P. 1963. *Simulation of Information and Decision Systems in the Firm*, Englewood Cliffs, NJ: Prentice-Hall.