Association for Information Systems
AIS Electronic Library (AISeL)

WISP 2012 Proceedings

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

Winter 12-15-2012

A Model for Investigating Organizational Impact on Information Security Behavior

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

Mathias Ekstedt
Royal Institute of Technology

A Model for Investigating Organizational Impact on Information Security Behavior

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

Mathias Ekstedt
Industrial Information and Control Systems, Royal Institute of Technology,
Stockholm, Sweden

ABSTRACT

The increased amount of attacks targeting humans accessing and using computers has made it significantly important to understand human and organizational behavior in attacks and how resilient behavior can be achieved. This paper presents a research model that attempts to understand how organizational and human factors complement each other in shaping information security behavior. The model was developed through an inductive approach, in which content domain experts were interviewed to gain a deeper understanding of the phenomena. Common patterns that were identified in the interviews were then combined with data collected through surveying the literature. Specifically, the research model includes constructs related to the organization and promotion of information security, constructs related to perceptions of information security awareness and the social conditions within an organizational setting, and individual constructs related to an individual's perceptions of attitude, normative beliefs, and self-efficacy. Implications for continuing research and how the model will be tested empirically are discussed.

Keywords: Organization of information security; information security risks; organizational structures; information security awareness

[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 computer systems using purely technical means. Many attackers have therefore started to attack the humans accessing and using the computer systems (Applegate 2009) . This development has increased the attention given to risks related to human or social aspects of information security. In organizational settings, typical risks against employees include the risk of being deceived to comply with a malicious request, e.g. execute malware on the computer or reveal sensitive information (Mitnick and Simon 2002). Numerous papers have therefore focused on describing important concepts and solutions to cope with these risks. The research domain is however still rather immature, and the extant socio-technical information security approaches have been criticized as lacking not only theoretically grounded methods, but also empirical evidence on their effectiveness (Puhakainen and Siponen 2010): only one paper examines organizational measures that are theory-based and evaluate their effectiveness empirically trough actual socio-technical attacks (Workman 2008). Related research has usually focused on investigating individual perceptions of external cues and properties that determine policy compliance and based their analyses on a variety of theories including theory of planned behavior (Bulgurcu et al. 2010), general deterrence theory (Lee et al. 2004), and learning theory (Warkentin et al. 2011). Other related research have largely focused on success rates of certain types of socio-technical attacks, e.g. (Dodgejr et al. 2007), or analyzing characteristics that explain an individual’s susceptibility to these attacks, e.g. (Pattinson et al. 2012). However, the effect of key organizational constructs proposed in organizational and individual behavior literature, on information security has not been rigorously examined (Hu et al. 2012). We therefore argue that there is a need for more studies linking key organizational and individual constructs to develop a better understanding of theoretical relationship between constructs on different levels in an organization. We further believe that it is important to investigate factors related to actual behavior while being under an attack, in addition to studies on how compliant employees are to specific policies, or estimating success probabilities for an attack. The purpose of this study is twofold. Firstly, we are interested in getting a deeper understanding of how factors complement each other in shaping information security behavior. Secondly, we suggest a research model that includes both organizational and individual constructs to investigate how organizations can shape this behavior. We attempt to fulfill this purpose through a combined method approach of conducting semi-structured interviews with content experts and surveying the literature. The result is the main contribution of the paper and is presented as a preliminary research model which includes a set of organizational and individual constructs that potentially could shape information security behavior.

The rest of the paper unfolds as follows. The next section presents an overview of risks related to insecure behavior and influences on information security behavior. The section that follows presents the methodology for conducting the interviews. The findings from the combined method approach is then presented and discussed. The paper concludes with a summarization of this study's findings together with both the preliminary research model and a description of implications for the continuing research

SHAPING INFORMATION SECURITY BEHAVIOR

The purpose of the study is to identify important constructs for developing a research model to investigate organizational and individual constructs, and their effectiveness in shaping security behavior. However, to understand why it's important to shape information security behavior, the risks related to insecure behavior are first described.

Risks Related to Insecure Behavior

In this study, the focus is on risks that could be realized through an attack exploiting insecure behavior of an employee. Behavior that could be exploited include careless use of email, computer passwords, use and disposal of computers, portable storage drives and other hardware that can either contain sensitive information or spread malware, lack of precaution when visiting suspicious websites or installing software, or falling victim to manipulative techniques and comply to a malicious request. In this study we have examined insecure behavior related to four attacks. These attacks are now further described.

Phishing is an attack described as the marriage between technology and social engineering in which attackers use spoofed email messages to trick end-users into taking a suggested action that benefits the attacker (Nohlberg and Kowalski 2008). For instance, the attacker can convince end-users to reply with sensitive information such as user credentials or click on a malicious link where the attacker either: i) automatically introduce malware by exploiting vulnerabilities in the web browser (e.g. drive by download) or ii) persuade end-users to execute malware on their computers. Malware can also be executed through hidden scripts in attached documents.

In a *Physical intrusion* an attacker enters a target organization and try to obtain information by impersonate a legitimate party such as an employee, visitor, or service personnel using false credentials or a good story. Thus easily bypass any technical or physical defenses (Mitnick and Simon 2002). Once inside the target organization, the attacker can look for sensitive or even classified information by going through the trashes (so called dumpster diving), the office landscape (so called desktop hacking), or look over an employee's shoulder to acquire passwords or pin numbers (so called shoulder surfing).

An attacker can also use the phone to impersonate someone in a position of authority and target someone less educated in the area of security (e.g. help desk employees) to increase the information competence in the preparation for another, more valuable attack. When possible, the attacker can also use this attack method to persuade the victim to reveal sensitive information over the phone. We refer this type of attack as *Phone fraud* (Mitnick and Simon 2002).

Malware trough portable media is a practice of using a combination of technical and social attack methods. For instance, an attacker can leave a USB memory stick, or a CD with a tempting text, outside a building, to entice a victim's curiosity into using the item in their computer (Nohlberg and Kowalski 2008).

Influences on Information Security Behavior

To gain a general understating of the potential influences on information security behavior, related literature was first consolidated. This process resulted in an the understanding that a behavior can be affected by an individual's attitude towards information security, normative beliefs about information security, and perceived knowledge of the topic, i.e. self-efficacy (Bulgurcu et al. 2010). These factors can further be influenced by the shared beliefs, and relationships between employees (Hu et al. 2012), and perceptions of the organizational information security policies, practices, and procedures (Chan et al. 2005). These social structure perceptions can potentially be influenced by management actions that promote good information security practices through clear direction, and provide knowledge of what is necessary for managing information security risks (R. von Solms and B. von Solms 2006). These actions can be deployed trough security structures, processes and transferring mechanisms. Organizational structures involve the existence of responsible functions such as senior-level information security executives and a diversity of coordinating committees (Kayworth and Whitten 2010). The structure of clear and unambiguous definitions of the roles and responsibilities of the involved parties throughout the whole organization are prerequisites for effective information security. Security processes refer to the strategic- and operational decision-making and monitoring of security performance. However, even if processes and the above mentioned structures are in place, it is possible that the information security efforts are not aligned with the business strategy, environment and needs, and thus are ineffective. It is therefore crucial that also knowledge transferring mechanisms are deployed in an organization.

The theoretical linkages provide a base for exploring the impact of various socio-technical factors required to shape employee information security behavior. As this specific linkage has not been rigorously examined, a deeper understanding of the domain is first required.

RESEARCH DESIGN

In developing a research model, MacKenzie et al. (2011) suggested that after gaining a general understating of the domain, interviews using an inductive approach with content experts should be conducted. Through the interview process, common patterns emerge and the researcher then begins to search for literature which is treated as additional data, and compare this data with the emerged patterns from the interviews (Trochim and Donnelly 2006). Six semi structured interviews were utilized in order to capture rich, detailed information on content experts' views of the investigated domain in general, and factors to shape an employee's behavior when dealing with actual socio-technical attacks in particular. The number of respondents was decided due to the following reasons: i) the study is of exploratory nature, and ii) the last interview did not produce any new radical insights into the content experts' view of the domain. The latter argument is given support by the literature recommending that interview data should be collected until theoretical saturation take place and a too high number of respondents will make thorough interpretations of the interviews difficult (Kvale 1986).

Data Collection

The interviews were carried out from February 2012 to June 2012. All respondents had acquired a deep domain specific knowledge trough experience of the topic on a regular basis. Two of the respondents were academics, but both have many years of practical experience in the domain. The four practitioners were selected on recommendations, and have worked extensively within the investigated domain. The data of respondents is summarized in Table 1.

Table 1. Respondent data

Respondent	Position	Experience (Years)	Time (Hours)
1	Professor and scientist (private industry)	>15	1
2	Senior Consultant	16	1.5
3	Consultant	5	1.5
4	Head of Security (private industry)	12	2.5
5	Associate professor and practitioner	>10	2
6	Senior security researcher (private industry)	>15	1

Three of the interviews were carried out face-to-face at the expert's respective places of business, and three were carried out over telephone due to geographical concerns. The interviews were audio-recorded and transcribed. Handwritten notes were also taken the interviewer and transcribed electronically. The interviews all had the same general approach, and consisted of two main objectives: (i) to gain a deeper understanding of important concepts for shaping information security behavior and (ii) to discuss potential relationships between constructs towards developing the model to investigate antecedents of information security behavior. In terms of important constructs, we explicitly asked for opinions on constructs related to actual behavior while being under a socio-technical attack, i.e., if these affect the outcome of attacks.

Due to the complexity of acquiring data on how organizational and individual variables complement each other in shaping information security behavior effort was spent to enforce reliability of results. That is, the original layout and scope of the interviews was somewhat changed according to the focus area(s) of the respondents. For example, no answers were forced, and the respondents were allowed to discuss a particular area in greater detail. As a consequence, more time was spent on those matters the respondents perceived to be of greater importance for the topic of the study. The first part of the interview described the topic of the study and the outline of the event. The second part concerned risks that could exploit insecure behavior. The third part concerned potential constructs on both an organizational and individual level that influence information security behavior. The final part concerned potential relationship between organizational and individual constructs in order to shape information security behavior.

RESULTS AND DISCUSSSION

This section reports of the combined method approach using data from interviews and from the literature. The constructs were classified as follows. Constructs categorized as organizational constructs (See Table 2) are related to the organization and promotion of information security. Individual constructs (See Table 3) are related either to perceptions of information security awareness and the social conditions within an organizational setting (also referred to as mediators in Table 1 and Figure 1, for example) as perceived by end-users or to an individual's attributes that influence information security behavior (also referred to as motivational constructs in Figure 1 for example and comprising attitude, normative beliefs, and self-efficacy).

Five broad organizational constructs were emerged from the analysis of the combined data and presented in the Table 2 and illustrated in the research model (See Figure 1). In the following, the constructs are discussed and the sources are specified.

Table 2. Organizational constructs

Construct	**Key Aspects**
Information Security Leadership	Security Visions, Provide Role Model, Foster Cooperation Towards Common goals, Set High Performance Expectations
Organizational Structures	Formal Security Unit, CISO, Steering Committee, Well-defined Information Security Responsibilities
Information Security Processes	Information Security Planning, Performance Monitoring
Security Knowledge Transfer	Training on Policies, Threat Awareness, Informal training, IT-based training
Shared Organizational Security Knowledge	Security Awareness of Business Managers, Business Awareness of Security Personnel

The importance of leadership was acknowledged early in the interviews. Respondent 1 argued as follows.

> *"All kinds of measures can be implemented and employees can be trained, but without strong leadership to educate business unit managers and security personnel, measures will not be effective. Strong leadership gives effective operational measures."*

Trough leadership, the importance of protecting information assets should be articulated, and the leader should provide a role model for employees to follow, foster cooperation towards common goals, and set performance expectations (Podsakoff et al. 1990).

The respondents agreed that structures are needed to facilitate the deployment of security efforts, and communication between leaders, security personnel, and business representatives. The literature also acknowledge the importance of structures for deploying management actions and leadership (Van Grembergen and De Haes 2008). Key aspects of the organizational structures identified in this study are: formal security unit, an executive with information security as the main responsibility, the establishment of a committee comprised of business and security personnel, and well-defined responsibilities (Kayworth and Whitten 2010).

Formal processes to develop policies, plan the implementation of security controls (e.g. end-user training) and monitor the effectiveness of implemented controls were acknowledge as crucial. Ongoing knowledge sharing is crucial to establish understanding and alignment between business and IT managers (Van Grembergen and De Haes 2008). By using mechanisms such as security education and cross-training, shared security knowledge can be achieved among managers and employees can understand what is expected of them, and how to protect themselves from security risks. Respondent 2 and Respondent 3 shared the following.

> *"The operational personnel need to know what is expected of them. The persons at the highest level of the organization need to communicate directives to operational personnel so that they know why security measures are important, how to implement them, and why."*
>
> *"Business managers need to understand the importance of information security and understand how it can be used to support the business and not hinder it. On the other hand security mangers also need to understand the business and the end-user for developing security policies and programs that focuses on the end-users perspective."*

Capturing and transferring the security knowledge to increase end-user awareness and shape their behavior is usually conducted through formal awareness education and training programs, workshops, lectures or through IT-based training tools. However, both the experts and the literature argue that it is not enough to merely have formal knowledge transferring processes in place – the management needs to assure and monitor that the users have comprehended the knowledge for it to be truly effective (Barrett 2003). This could be done through implementing regular security exercises using weaker forms of penetration tests. These exercises reinforce the training and education programs. It also keeps the users alert, and more prepared in the occasion of an actual socio-technical attack (Nohlberg and Kowalski 2008).

Three broad constructs, working as mediators for an individual's motivation towards behaving secure (i.e. attitude, normative beliefs, and self-efficacy), were emerged from the analysis of the combined data. These are presented in the Table 3 and illustrated in the research model (See Figure 1).

Table 3. Mediators

Constructs	**Key Aspects**
Perceived Awareness	Public information policy Internet use policy Installation policy Written information policy Hardware disposal policy Communication policy Call-back policy
Perceived Social Culture	Shared Beliefs, Shared Goals, Social Relationships
Perceived Learning Environment	Perceived Support, Verbal Feedback, Vicarious experience

Policies are used as formal directives, and are crucial to manage socio-technical risks by shaping employee behavior that is conducive to the protection of information assets (Da Veiga and Eloff 2010). How effective the policy is, depends on how well the employees accept the policy, i.e. how well the policy fit to the culture of the organization. Respondent 4 shared the following.

> *"There are individuals in an organization that behave insecurely regardless of formal organizational directives. It is difficult to shape individual behavior, it is therefore important to shape an organization, and by doing so employees will be influenced by each other. For instance, by looking at how colleagues behave the behavior of a single employee can potentially be influenced".*

Respondent 5 shared the following.

> *"You can implement a thousand polices, but they will not be accepted if they don't fit to the cultural environment within the organization. Some policies might be more accepted by employees working in military and civilian government facilities, and international airports, while employees at a local construction company might strongly reject the same policy if they find it irrelevant with regards to the type of environment they work in."*

Punishment is thought to not be effective. Respondent 4 and respondent 5 shared the following.

> *"I don't believe punishment is effective. You should talk with your employees and teach them how to prevent incidents. There should be a supportive environment in the organization, not a punishment oriented."*

> *"Using disciplinary measures only creates a negative feeling which can affect the productivity and motivation of the employees. Employees complying with a request from a malicious perpetrator in good faith shouldn't be punished."*

The comments indicate that efforts should be directed to encourage employees towards security-savvy behavior. All six respondents contributed to the identification of specific policies to shape information security behavior. Polices recommended by the experts and the litterateur are described as follows. Policies can regulate that only generic information should be listed on publicly available sources, that employee Internet usage is restricted (e.g. usage of social network sites during work hours), and that additional software installation privileges are restricted (Da Veiga and Eloff 2010). Policies can also address the acceptable use and disposal of sensitive information written on paper, and the acceptable use and disposal of hardware that can contain sensitive information (Peltier 2006). Awareness of policies addressing information that can be communicated, how it can be communicated, to whom and under what conditions is also believed to influence information security behavior (Dontamsetti and Naranayan 2009). Finally, employees should be informed that whenever any questionable request is made by phone, they should call back and check that the number belongs to someone with suitable authorization (Nohlberg and Kowalski 2008). The importance of social structures, culture and an environment that encourage learning was acknowledged by the respondents. Respondent 4 and respondent 5 discussed these aspects thoroughly, and from the literature key aspects related to social culture (Chow and Chan 2008) and learning environment were identified (Warkentin et al. 2011).

SUMMARY AND CONLUSION

We attained a deeper understanding of how factors complement each other in shaping information security behavior. Furthermore, a research model that includes both organizational and individual constructs to shape this behavior is suggested (See Figure 1). To test the research model, 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 from the security organization with a role such as: Chief Information Officer, IT Manager, Chief Information Security Officer, and Security Officer, and one with a role that include regular utilization of information technology products and services, e.g. computers, Internet access, electronic mail, etc. (at least ten respondents per organization). Hypothesis related to the research model will be tested using structural equation modeling. To assure the validation of the measurement instrument, the conceptual domain of the included constructs will firstly be defined as recommended by (MacKenzie et al. 2011). Then, 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 actual behavior while being under a socio-technical 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.

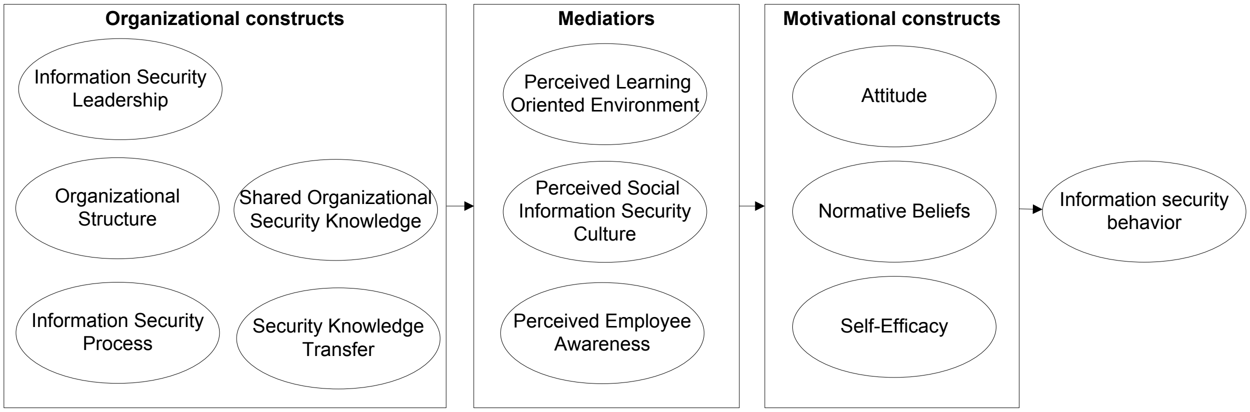
Organizational constructs
Information Security Leadership
Organizational Structure
Shared Organizational Security Knowledge
Information Security Process
Security Knowledge Transfer
Mediatiors
Perceived Learning Oriented Environment
Perceived Social Information Security Culture
Perceived Employee Awareness
Motivational constructs
Attitude
Normative Beliefs
Self-Efficacy
Information security behavior

Figure 1. Preliminary research model

REFERENCES

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

Barrett, N. 2003. “Penetration testing and social engineering: Hacking the weakest link,” *Information Security Technical Report* (8:4)Elsevier, pp. 56–64.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. “Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness,” *Management Information Systems Quarterly* (34:3), pp. 523 - 548.

Chan, M., Woon, I., and Kankanhalli, A. 2005. “Perceptions of Information Security in the Workplace-Linking Information Security Climate to Compliant Behavior,” *Journal of Information Privacy & Security* (1:3), pp. 18.

Chow, W. S., and Chan, L. S. 2008. “Social network, social trust and shared goals in organizational knowledge sharing,” *Information & Management* (45:7), pp. 458-465.

Dodgejr, R., Carver, C., and Ferguson, a. 2007. “Phishing for user security awareness,” *Computers & Security* (26:1), pp. 73-80.

Dontamsetti, M., and Naranayan, A. 2009. “Impact of the Human Element on Information Security,” In *Social and Human Elements of Information Security Emerging Trends and Countermeasures*IGI Global, pp. 27-43.

Van Grembergen, W., and De Haes, S. 2008. *Implementing Information Technology Governance: Models, Practices, and Cases*, Hersey, New York: IGI Global.

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.

Kayworth, T., and Whitten, D. 2010. "Effective Information Security Requires a Balance of Social and Technology Factors," *MIS Quartely Executive* (9:3), pp. 303-315.

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

Lee, S. M., Lee, S.-G., and Yoo, S. 2004. "An integrative model of computer abuse based on social control and general deterrence theories," *Information & Management* (41:6), pp. 707-718.

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.

Mitnick, K., and Simon, W. 2002. *The art of deception*, Indianapolis, Indiana: Wiley Publishing, pp. 368.

Nohlberg, M., and Kowalski, S. 2008. "The cycle of deception – a model of social engineering attacks, defenses and victims," In *Proceedings of the Second International Symposium of Human Aspects of Information Security & Assurance (HAISA 2008)*, pp. 1-11.

Pattinson, M. R., Jerram, C., Parsons, K., McCormac, A., and Butavicius, M. 2012. "Why Do Some People Manage Phishing Emails Better Than Others?," *Information Management & Computer Security* (20:1)Emerald Group Publishing Limited, pp. 18-28.

Peltier, T. R. 2006. "Social engineering: Concepts and solutions," *Information Systems Security* (15:5)Taylor & Francis Ltd., pp. 13–21.

Podsakoff, P. M., MacKenzie, S. B., Moorman, R. H., and Fetter, R. 1990. "Transformational leader behaviors and their effects on followers' trust in leader, satisfaction, and organizational citizenship behaviors," *The Leadership Quarterly* (1:2), pp. 107-142.

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.

von Solms, R., and von Solms, B. 2006. "Information Security Governance: A model based on the Direct–Control Cycle," *Computers & Security* (25:6)Elsevier, pp. 408-412.

Trochim, W. M. K., and Donnelly, J. P. 2006. *The Research Methods Knowledge Base* , (3rd ed,)Atomic Dog, pp. 362.

Da Veiga, A., and Eloff, J. H. P. 2010. "A framework and assessment instrument for information security culture," *Computers & Security* (29:2)Elsevier Ltd, pp. 196-207.

Warkentin, M., Johnston, A. C., and Shropshire, J. 2011. "The influence of the informal social learning environment on information privacy policy compliance efficacy and intention," *European Journal of Information Systems* (20:3)Nature Publishing Group, pp. 267-284.

Workman, M. 2008. "A test of interventions for security threats from social engineering," *Information Management & Computer Security* (16:5), pp. 463-483.