Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2009 Proceedings

Americas Conference on Information Systems (AMCIS)

2009

Identifying Factors that Influence Corporate Information Security Behavior

Santos M. Galvez
TUI University, sgalvez@tuiu.edu

Indira R. Guzman
TUI University, iguzman@tuiu.edu

Identifying Factors that Influence Corporate Information Security Behavior

Santos M. Galvez
TUI University
sgalvez@tuiu.edu

Indira R. Guzman
TUI University
iguzman@tuiu.edu

ABSTRACT

In this paper, we present a social/behavioral meta-study of good corporate information security practices. The research model combines social cognitive theory and control theory in order to explain the individual and environmental factors that influence corporate information security behavior. The model includes employees' beliefs about their abilities to competently use computer information security tools in the determination of effective information security practices within organizations. We present the definition and operationalization of constructs such as information security awareness and information security practice as the dependent variable and then support within the organization, encouragement by others, others' use as environmental factors in the information security context; and finally, self-efficacy and outcome expectations as the independent variables of the model. This research model is aimed to develop an effective audit and recommendation model for organizations that are looking to make significant improvements in their information security profiles.

Keywords

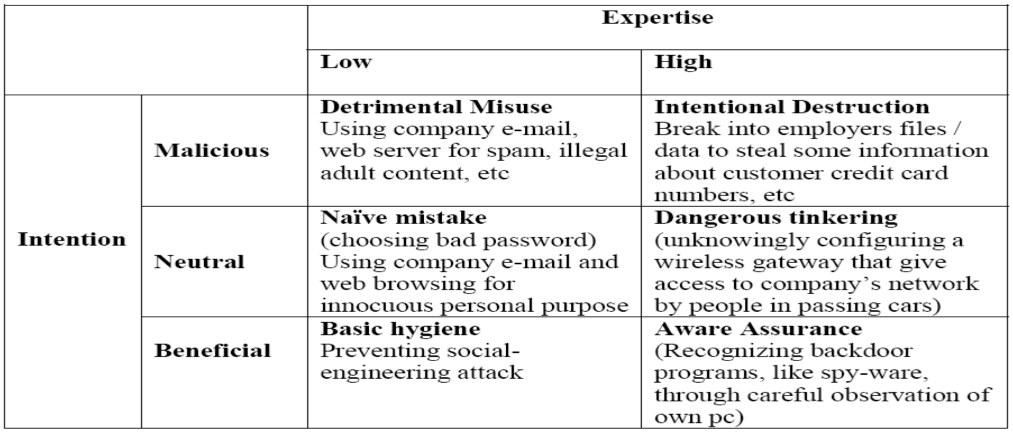
Social Cognitive Theory; Control theory; Information Security Behavior; Security Awareness and Practice

INTRODUCTION

With the emergence of the TCP/IP internet protocol worldwide in 1973, the world was "opened" to the world of Internet. Individuals, organizations and the whole society began to explore the richness and all the potentials that the new service has to offer and have been using it in all kinds of activities. Opening the world to the internet was a great opportunity for people and business; however, it is also an opportunity for thieves and hackers to get access to the information in organizations in an unauthorized way.

According to DarkReading.com (2006) web site hacking costs are substantial. For instance, in cases where stolen IDs and passwords were used, the average loss per incident was $1.5 million; a recent survey by the Yankee Group indicates that more than half of companies rate their Internet downtime costs at more than $1,000 per hour; Finally, in a study published in 2004, the Aberdeen Group found that the cost of Internet based business disruptions was about $2 million per incident. These figures are just the tip of the iceberg in representing the costs associated with the intentional destruction of computer related activities.

There is an extensive variety of information security risks such as viruses, worms, denial-of-service attacks, spoofing, stolen passwords, social engineering, software exploitation, trojan horses, and authority and authorization violations that can have a very negative impact on the regular operations of an organization (Chen, Shaw, Yang, 2006). As security threats have grown, the need to protect organizational data has became a corporate crucial need. Although some of these attacks can be originated externally, most of them are directly or indirectly originated by internal employees (Dhillon and Backhouse, 2000). For example, the most dangerous method and perhaps the easiest way of obtaining information is social engineering. Arief and Besnard (2005) refer to this as "weaknesses in wetware" which they refer to as human users. As they note, "the aim is to trick people into revealing passwords or other information that compromises a target systems' security" (p. 5). This kind of social engineering takes advantage of a basic human impulse toward helping other people, what psychologists and sociologists call prosocial behavior (Stanton & Stam, 2006). Many times, the problem is not the technology, but the users who use it. Despite the occurrence of high technical security infrastructure employees use the systems in a way that they can break the security systems (Taneja, 2006). Therefore, it is important to understand the factors that influence information security behavior. According to Stanton, Stam, Mastrangelo and Jolton (2005), behavior of employees about information security can be designed as a two dimensional structure with "intentionality" and "technical expertise" of the employees to perform the behavior represented as the two dimensions of the map (Table 1). The employee's behavior toward computer systems can be malicious, neutral or favorable to the organization. In addition, they can be classified into two categories, high technology expertise and low technology expertise. Most of the end users of the IS can be categorized as low expertise. Therefore, they need to get trained to improve the security usage of the information system.



		Expertise	
		Low	**High**
Intention	**Malicious**	**Detrimental Misuse** Using company e-mail, web server for spam, illegal adult content, etc	**Intentional Destruction** Break into employers files / data to steal some information about customer credit card numbers, etc
	Neutral	**Naïve mistake** (choosing bad password) Using company e-mail and web browsing for innocuous personal purpose	**Dangerous tinkering** (unknowingly configuring a wireless gateway that give access to company's network by people in passing cars)
	Beneficial	**Basic hygiene** Preventing social-engineering attack	**Aware Assurance** (Recognizing backdoor programs, like spy-ware, through careful observation of own pc)

Table 1. Two Factor Taxonomy of Security Behavior Adopted from Stanton (2005) and taken from Taneja (2006).

According to Chen, Shaw and Yang (2006), the lack of security knowledge and awareness on the part of the users of information systems is a major security problem within organizations. Information security threats could be minimized if internal users of the information systems of an organization performed effectively information security practices (Ryan, 2006) or what we can call security behavior. While there are different theories in the literature used to study and predict human behaviors such as Theory planned behavior , we chose to focus on Social cognitive theory (Bandura, 1977) that looks at the environmental and individual's cognitive factors that influence behavior. In addition we also include Control theory (Ouchi, 1977; Eisenhardt, 1985) which focuses on the perceived outcomes due to certain behaviors. In other words, this model will allow us to explain which factors (influence from others, individuals cognitive factors about his/her confidence or the perceived of compliance with security policies) mostly influence individuals to perform security practices within organizations.

In the following sections of this paper, we first discuss social cognitive theory (SCT). SCT serves as the foundation for understanding: (a) environmental or situational characteristics, for example social pressures including encouragement by others, other's use, and support to use information security tools; (b) cognitive personal factors including computer self-efficacy, outcome expectations as well as demographic characteristics; and (c) information security behavior defined information security practice (ISP) as defined and operationalized by Ryan (2006). Based on Control Theory and the work performed by Boss (2007) we include some mandatory aspects (in contrast with voluntary ones) that could influence security behaviors.

A set of propositions are then offered based on the SCT model. Finally, the implications of the implementation of this model, and the strengths and limitations of this approach, are discussed.

According to Chen, Shaw and Yang (2006), the lack of security knowledge and awareness on the part of the users of information systems is a major security problem within organizations. Information security threats could be minimized if internal users of the information systems of an organization performed effectively information security practices (Ryan, 2006).

RESEARCH QUESTIONS

This study addresses the following research questions:

- How do environmental factors influence security behavior?
- How do cognitive factors influence security behavior
- How does security awareness affect the information security behavior?
- How do control factors (specification and evaluation) influence security behavior?

LITERATURE REVIEW

Social cognitive theory is defined as human behavior relationship between environment, personal factors, and behavior (Bandura, 1977; 1997). Individuals choose the environments in which they exist and are influenced by those environments. Behavior is affected by environment, which in turn are affected by behavior. Finally, behavior is influenced by personal factors of the individual, and in turn, behavior affects those same factors (Compeau and Higgins, 1995). According to this theory, an individual's behavior is uniquely and reciprocally determined by each of these three factors: environmental influences such as social pressures or unique situational characteristics, cognitive and other personal factors including personality and demographic characteristics and finally, behavior (Compeau and Higgins, 1995, p.190).

According to Bandura (2002) social cognitive theory adopts agentic perspective. There are three modes of agency very well differentiated by the theory. One of them is personal agency which is implemented individually; Proxy agency is when people influence others to act on their behalf with the purpose of secure desired outcomes. Collective agency is when people exercise through group of actions. However, in this study, we focus on personal agency or individualism within the information security context. In fact, SCT has many dimensions, but in this research we are concerned with the role of cognitive factors in individual behavior, similarly to Compeau and Higgins (1995) but applied to information security context.

We start defining information security behavior (Information security practice at work) as the dependent variable of our model. We then define the independent variables of our model within the information security context.

The dependent variable: Information Security Behavior

ISP - Information Security Practice at work

In the information security business, there are a number of different security models proposed by professionals and organizations (Berghel,2007). These models such as time-based security, principle of least privilege, defense in depth, baseline security, perimeter hardening, intrusion detection, and intrusion prevention are trying to minimize real or potential vulnerabilities and threats. The difference between these models is the strategy against vulnerabilities and threats for example time-based security (TBS) uses time as the primary measure of risk. The safety margin increases with advance warning, so as long as the advance warning exceeds the sum of the detection and response times the information is protected. On the other hand, the principle of least privilege (POLP) relies on controls. This strategy varies inversely with the degree of control given to the application or user. Currently, there are different well known organizations that promote specific security standards, such as the Control Objectives for Information and related Technology (COBIT), the Federal Information System Controls Audit Manual (FISCAM), the Certified Information Systems Auditors (CISA), the BSI 7799/ISO 17799/ISO 27001 standards for best practices. These standards map to government legislation or mandates such as the Health Insurance Portability and Accountability (HIPAA) (Berghel, 2007). The Information Security Organization (ISO) standards take the form of guidance and recommendations intended to serve as a single reference point for identifying the range of controls needed for most situations where information systems are used (Veiga and Eloff, 2007). The ISO/IEC 27000 series is an information security standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) as ISO/IEC 17799:2005 and then renumbered ISO/IEC 27002:2005. As stated by Veiga and Eloff (2007), ISO 17799 has gradually gained recognition as an essential standard for information security where ISO27001 (2005) is regarded as part two of ISO/IEC 17799 and proposes an approach of continuous improvement through a process of establishing, implementing, operating, monitoring, reviewing, maintaining and improving the organization’s information security management (ISO, 2005; IEC, 2005). Since these security policies should be implemented within organizations, employees who follow them are actually the ones who effectively perform security practices. Ma and Pearson (2005) empirically validated seven of the ten constructs from the guidelines and practices within the most accepted and security standards by information technology professionals: ISO/IEC 17799: 2005 and BS 7799. Based on the analysis of these constructs, Ryan (2006) came up with an ISP scale that includes items that evaluate information security practices of the users from the same nine views that were used in the ISA scale. The operationalization of this ISP construct as presented in Ryan’s work include items like these:

On business computer systems…

- I log off when I leave a computer system
- All of my computer sessions require a unique user-id and password

- I backup my data on reliable media (disks, CDRW, etc)
- I test the restorability of back-up files that I have created
- I check that virus protection software is enabled and updated
- I check for new versions of virus protection software
- As I surf the Web, I allow browsers to accept cookies from Web sites (R)
- I allow software to save user-ids and passwords for faster return visits (R)
- I encrypt confidential files with passwords
- I look for "https://" before I make Internet financial transactions

The independent variables

ISA - Information Security Awareness

According to Goodhue and Straub, 1991; Straub and Welke, 1998; Dhillon and Backhouse, 2001; Hu et al., 2006 information security is a socio-technological problem that requires thorough understanding of the weakest link in the defense against security threats: human behavior and attitudes about using these security technologies. According to the Department of Trade and Industry's 2004 Information Security Breaches Survey reports that humans are the weakest link in the chain of security control (Chen et al., 2006). Therefore, one of the preventive measures suggested by Timms, Potter, & Beard (2004) was to create a security-aware culture which will have the mission of educating staff about different security risks and their responsibilities. Within the IS literature, the concept of awareness has been defined for example as "technology awareness" by Deniv and Hu (2007), as "user's raised consciousness of and interest in knowing about technological issues and strategies to deal with them" (p.391). For example, in a document of the National Institute of Standards and Technology, Lisa Lindholm defines security awareness as "an individual responsibility and sufficient understanding to comply with policies"[1] . She also indicates that security awareness is the best ROI for information security programs. According to Siponen (2000), ISA is used to refer to a state where individuals in an organization are aware of their security mission, as well as ideally devoted to it. Information security awareness is very important as the security techniques or procedures, but the processes can be misused, misinterpreted or not used by individuals in that way losing their real efficacy (e.g. Hoffer and Straub, 1989; Goodhue and Straub, 1989; Ceraolo, 1996; Straub, 1990; Straub and Welke, 1998). Finally, based on a literature review, Chen et al. (2006) defines ISA as a focus on attention to security when individuals recognize IT security concerns and respond accordingly. These definitions do not imply only being informed about security issues, but actually being responsive about them which therefore can be considered as a behavioral factor. It is important to mention that this definition also implies a cognitive behavior. The increase of security awareness should minimize individual's related faults toward security threats and increase the efficiency of the security techniques and procedures against security threats in an organization. For this study, therefore, we define ISA as user's increased consciousness of and interest in knowing about security issues and the strategies to deal with them. ISA is one of the information security behaviors.

In order to operationalize this variable, we found three ways of measuring awareness in the IS literature: One of Disiv and Hu (2007), another from Chen et al. (2006) and finally one from Ryan (2006). We propose to use the approach of Ryan (2006) because that is the one that is more explicitly directed to information security. Ryan (2006) analyzed initially a series of 12 attributes of the ISA construct grouped into demographic, technology, policy and threat-context views. He ended up with 9 ISA views: technology, threat-context, user authentication, formal policy, physical, access control, information policy, encryption, and security management. The operationalization of this ISA construct include items like the following:

With respect to information technology and its security, I am aware…

- Virus protection software can identify and remove known viruses (+)
- Virus protection software requires frequent updates (+)
- Firewall software can block network attacks (+)
- Personal firewall software can block logical port access to/from a computer (+)
- Acceptable Use Policy strongly suggests keeping passwords safeguarded (+)

Following the literature, information security awareness is the basis of information security behavior, we thus propose,

Proposition 1: The higher the information security awareness, the higher the information security practice.

[1] http://csrc.nist.gov/organizations/fissea/2006-conference/Lindholm-FISSEA2006.pdf

Bandura stated that the major cognitive forces guiding behavior are outcomes and self-efficacy. Regarding, outcomes individuals usually assume behaviors they believe will end up in valued outcomes. Self-efficacy influences choices about which behaviors to undertake (Compeau and Higgins, 1995).

Cognitive forces

Self Efficacy in Information Security (InfoSec)

According to Bandura (1977), self-efficacy is the individual perception or belief that one has the capability to perform a particular behavior and for having sufficient skills to perform given tasks, where the individual would also tend to do the tasks successfully (Compeau and Higgins, 1995; Ryan, 2006). Compeau and Higgins (1995) developed and validated for the first time a construct to understand the impact of self-efficacy on individual reactions to computing technology named 'computer self efficacy' (CSE). The authors initially developed a theoretical model based on social cognitive theory (Bandura, 1986) that includes the new measure of CSE. Then they tested their model in a sample of 1020 knowledge workers in Canada, concluding that self-efficacy plays an important role in shaping individuals' feelings and behaviors towards computer use. Individuals with high self-efficacy used computers more, derived more enjoyment from their use, and experienced less computer anxiety (Compeau and Higgins, 1995). Affect and anxiety also had a significant impact on computer use. The authors present a follow up study of the one published in 1995. They test a subset of the model tested in the 1995 paper but using longitudinal data gathered from 394 end users over a one-year interval. The results confirm that both self efficacy and outcome expectations impact on an individual's affective and behavior reactions to information technology. This later study uses the scales from the 1995's paper confirming reliability of the instrument. It also provides the instrument as it was used in the study. The authors conclude that both self-efficacy and outcome expectations impact on an individual's affective and behavioral reactions to IT. Self efficacy is a strong and significant predictor of affect, anxiety and use one year later. Self-efficacy beliefs regulate human functioning through cognitive, motivational, affective and decisional processes (Bandura, 2002).

SCT has proven to be a powerful mechanism for explaining, predicting, and governing behavior and has been broadly used by researches. For example, Havelka (2003), used data from students enrolled in the MIS course at a large Midwestern university (approximately 15,000 students) to test software self-efficacy and computer anxiety among students with different demographic predictors such as academic majors, years of experience using computers, amounts of computer coursework, etc. The author concludes that students from different business majors have different levels of self-efficacy, and a negative relationship between software self-efficacy and computer anxiety. Other researchers, Hayashi, et al. (2004) conducted a field experiment to test a proposed integrative research model. The model is based on CSE, Technology acceptance model, Expectation-Confirmation model (ECM) and End-user computing theories. It is used to assess the intention of online learners who continue using the e-learning system as a vehicle to assimilate IT skills. La Rose and Eastin (2004) proposed and tested a new model of media attendance based on SCT. The present media usage as an explicit media consumption behavior (specifically, the use of the Internet) that is determined by the anticipated outcomes that go after that consumption. In another research, SCT has helped understand physical activity behavior among college students (Suminski & Petosa, 2006). The authors found that the Web has been shown to be a good method for bringing behavior-change programs because of its low cost and popularity among large numbers of people .

In this study, the construct of CSE is adapted to the information security context as it was done by Ryan (2006). CSE is defined as the individual perception or belief that one has the capability to perform information security behaviors and for having sufficient skills to perform security tasks, where the individual would also tend to do the tasks successfully. The security tasks refer specifically to the ability to install and set-up security software at the user level. If end users are able to confidently install and set up basic security software in their computers, this will influence their actual information security practices.

The survey items that measure this construct include questions developed by Compeau and Higgins (1995) but adapted to the installation and set up of security software as done by Ryan (2006). Some of the questions are the ones listed below.

In your opinion, could you install and set-up security software…
… if there was no one around to tell me what to do as I go?
… if I had never used another application like it before?
… if I had only manuals for reference?
… If I had used similar applications before to obtain the same goal?

We thus propose,

Proposition 2: The higher the individual's computer self-efficacy in information security, the higher the information security practice.

Outcome Expectations in Information Security (InfoSec)

Outcome expectations have been considered by many IS researchers, i.e. Davis (1989), Thompson (1991) and Robey (1979) as individuals are more likely to undertake behaviors they believe will result in valued outcomes than those they do not see as having favorable consequences. In information security, these relationships and expectations may significantly vary because users may not see immediate outcomes of favorable consequences of being secure; instead they would see faster the consequences of not being secure when an attack is already a reality in the network. Following the original model of Compeau and Higgins (1995) in included both of the relationships: the potential influence of computer self efficacy in InfoSec and outcome expectations, as well as the one between outcome expectations and information security practice at work. The outcome expectations should be measured based on survey items that measure for example usefulness as presented by Davis (1989), Pavri's (1988) beliefs construct and Thompson, et al.'s (1991) construct reflecting the expected consequences of using security measures. Respondents would be asked to indicate how likely they thought it was that each of these outcomes would result from their use of information security tools. Thus, we suggest that:

Proposition 3a: The higher the individual's computer self-efficacy in information security, the higher the outcome expectations in information security.

Proposition 3b: The higher the outcome expectations in information security, the higher the information security practice.

Mandatoriness

Following the literature in information security that refers to the importance of security control (Boss, 2007), we include in our model the variable of Mandatoriness as a cognitive factor (Bandura, 1977). Boss (2007) took control theory (Ouchi, 1977; Eisenhardt, 1985) to "provide insight on why individuals take cyber-precautions within the work environment and the impact of management policies and procedures on individual compliance" (p.20). Accordingly, this construct measures individual's perceptions that compliance with existing security policies and procedures is required within organization. Boss included four items measured on a 7-point Likert scale that were adapted from the conceptualization of mandates discussed in Chae & pool (2005) and explicitly stated in Hartwick & Barki (Hartwick & Barki, 1994) regarding the required use of a system. The items include questions such as the ones listed below.

Please indicate the degree to which you agree or disagree with the following statements regarding your organization :

- I am required to secure my system according to the organization's documented policies and procedures.
- It is expected that I will take an active role in securing my computer from cyber-attacks (hacking, virus infection, data corruption, etc.).
- Regulatory compliance requirements (FERPA, HIPAA, Sarbanes-Oxley etc.) emphasize the need for me to follow the organization's IT security policies, procedures and guidelines to the best of my ability.

We thus propose,

Proposition 4: The higher the perceived mandatoriness, the higher the information security practice.

Environmental Factors

Following the main theory that drives this conceptual paper, social cognitive theory posits that an ongoing reciprocal interaction between three forces (cognitive, environmental and behavioral). Following the model presented by Compeau and Higgins (1995), we propose to evaluate the environmental factors (the social external factors) that could influence security behavior. We discuss encouragement by others, others' use and support of the organization to use information security tools.

Encouragement by others

According to SCT behavior in a given situation is affected by environmental or situational characteristics. Encouragement of others within the individual's reference group can be expected to influence both self efficacy and outcome expectations. Therefore, encouragements of use of information security tools represented by verbal persuasion (i.e. training) by the people to whom an individual looks to obtain guidance on behavioral expectations will influence actual ISP.

The type of questions to be used to measure encouragement by others would include questions such as those asking

To what the extent the use of information security tools was encouraged by others in the individual's reference group, including:

- their peers in their work organization
- their peers in other organizations
- their friends
- their manager
- their subordinates.

We thus propose,

Proposition 4a: The higher the encouragement of information security practices (use) by members of the organization, the higher the individual's computer self efficacy in information security.

Proposition 4b: The higher the encouragement of information security practices (use) by members of the organization, the higher the individual's outcome expectations in information security.

Others' use

Users either new or old are strong influenced by the behavior of others. They usually build their security attitudes and set their own security behaviors according to:

- The values and attitudes showed in the behavior of senior management.
- The company's values and the coworkers' behaviors
- The interest of the company to show good security putting in place systems to monitor security behavior, reward good behavior, and respond to bad behavior.

In the case when there are a lot of inconsistencies between the formal statements in the policy and what the person observes in practice around them, users will follow the procedures based on what they see instead of what they are told(Leach, 2003).

"Encouragement of use is one source of influence on self-efficacy and outcome expectations" (Compeau and Higgins, 1995). The actual behavior of others with respect to the use of information security tools is a further use of information used in forming self-efficacy and outcome expectations. Knowing that other people put into practice information security behaviors such as password management may positively influence individual's password security practice. Following Compeau and Higgins' work, participants would be asked to indicate, on a five-point scale, the extent to which (1) their peers in their work organization, (2) their peers in other organizations, (3) their family, (4) their friends, (5) their manager, (6) other management, and (7) their subordinates actually used information security tools.

Proposition 5a: The higher the use of IS tools by others within the organization (the reference group), the higher the individual's CSE in information security.

Proposition 5b: The higher the use of IS tools by others within the organization (the reference group), the higher the individual's outcome expectations in information security.

Support:

All organizations no matter the size have to have trust on their staff every day and in every operational task that they perform. Therefore, good security training targeted how to improve user's security behaviors could significantly reduce the size of the security-related overhead .That is why the primary objective of the company is to influence its users' security behavior to drive down the level of security and severity of the security incidents that it experiences. Poor security behavior determines the level of security incidents that the company suffers. Thus, companies have a plan ready to make security improvements by having a strong security culture (Leach, 2003).

"Support of the organization for IS tools can also be expected to influence individuals' judgments of self efficacy" (Compeau and Higgins, 1995). The availability of assistance to individuals, who require support to use information security tools, should increase their ability and therefore ISP. Following Compeau and Higgins' work, drawn from Thompson, et al. (1991), participants would be asked the extent to which assistance was available in terms of security tools selection such as antivirus, firewalls, etc. and specialized instruction. They also rated (on the same scale) the extent to which their coworkers were a source of assistance in overcoming difficulties and their perception of the organization's overall support for computer users. Thus, we propose:

Proposition 6a: The higher the support for information security in the organization, the higher the individual's CSE in information security.

Proposition 6b: The higher the support for information security in the organization, the higher the individual's outcome expectations in information security.

Organizational Control Factors

According to Boss (2007), control is in essence utilized primarily to achieve specific objectives within an organizational setting. Formal controls are usually implemented to achieve a certain outcome or to encourage specific behaviors. In this case, we refer to the procedures and policies implemented within organizations. Following Boss' work we include Specification and Evaluation as two variables that measure the perceptions of the individuals about the organizational control factors that are in place.

Specification

Boss (2007) defined the construct specification to measure individual perceptions about the existence of corporate policies and/or procedures that deal with information security. The construct is a four item measured on a 7 – point Likert scale. The items were adapted from elements of control specification in Kirsch's (1996) Behavioral Control Composite Measure (adapted from Daft & Macintosh (1981)) and the Cardinal (2001) Formalization Measure (Adapted from Aiken & Hage (1968), Dewar & Werbel (1979), and Hell (1968)) that include questions such as:

Please indicate the degree to which you agree or disagree with the following statements

- I am familiar with the organization's IT security policies, procedures, and guidelines
- I am required to know a lot of existing written procedures and general practices to secure my computer system
- There are written rules regarding security policies and procedures at the organization.
- The organization's existing policies and guidelines cover how to protect my computer system.

Thus, we propose:

Proposition 7: The higher the individual's perception of security specifications in organizations, the higher the perceived mandatoriness.

Evaluation

According to Boss(2007) this construct measures the individual perceptions that managers examine, organize and analyze collected data to reach a conclusion regarding individual compliance with the given policies and procedures. The construct is measured on a 7-point Likert scale. Items were adapted from Cardinal (2001) Frequency of Performance Appraisal measure (adapted from Abbey (1982)) and general control literature (Eisenhardt, 1985). Boss operationalized the variable including questions such as the following.

Please indicate the degree to which you agree or disagree with the following statements.

- Managers in my department frequently evaluate my security behaviors
- Managers regularly examine data relating to how well I follow security policies and procedures
- Managers formally evaluate me and my colleagues regarding compliance with security policies
- Managers assess whether I follow organizational security procedures and guidelines

Thus, we propose:

Proposition 8: The higher the individual's perception of evaluation, the higher the perceived mandatoriness.

Based on the preliminary review of social cognitive theory and its implication in the information security context, as well as the organizational control factors we present a total of 8 propositions represented in the graphic research model in figure 1. We hope that this model can be used to collect empirical data and evaluate the weight and importance of environmental factors and organizational control factors on actual security practices.

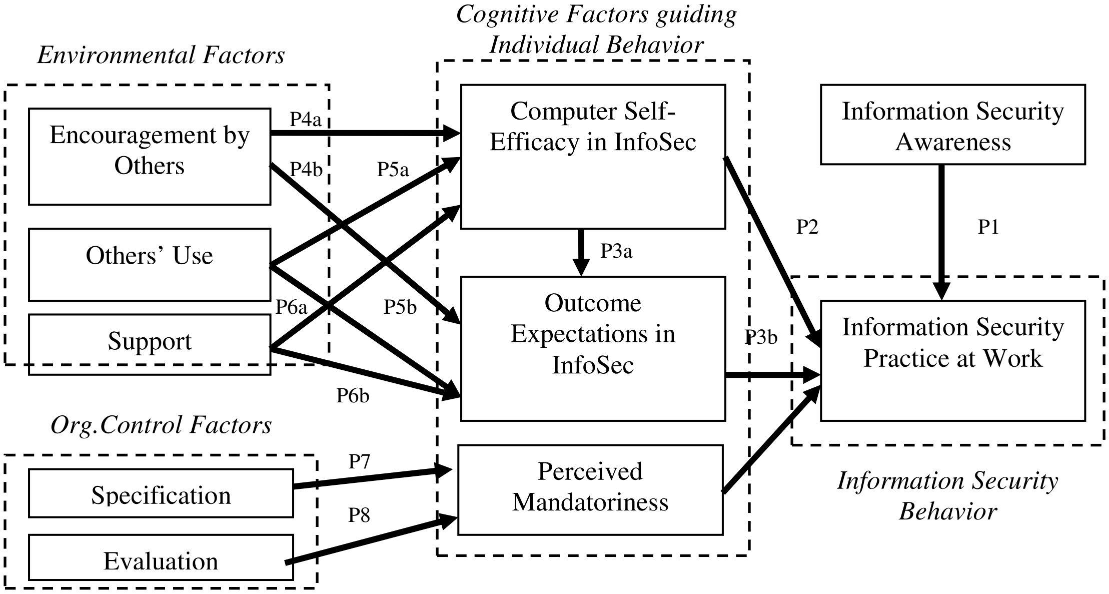

Cognitive Factors guiding Individual Behavior
Environmental Factors
Encouragement by Others
Others' Use
Support
P4a
P4b
P5a
P6a
P5b
P6b
Computer Self-Efficacy in InfoSec
P3a
Outcome Expectations in InfoSec
Perceived Mandatoriness
Org.Control Factors
Specification
Evaluation
P7
P8
P2
P3b
Information Security Awareness
P1
Information Security Practice at Work
Information Security Behavior

Figure 1. Research Model of Corporate Information Security Behavior

(adapted from Compeau and Higgins, 1995; Ryan, 2006; Boss 2007)

DISCUSSION

This paper presented a review of the literature on information security and the applications of two well known theories in the literature, SCT applied to the information security context and security control (the influence of organizational measures). We provided the definitions of ISA and ISP and then linked those constructs with environmental and individual factors. Ryan (2006) defined the three constructs ISA, ISP and self efficacy in information security context but did not link these constructs under SCT. Boss (2007) took the organizational control measures but did not take environmental factors and cognitive factors that SCT includes. Previous empirical research on SCT highlights the importance of this theory in IS. We believe that much of the successful security practices are driven by the socio cognitive reactions of the individuals to the environmental factors defined as well as the individual capabilities to maintain, install and set up basic security tool under security policies. Because of the compliance component in information security and recent regulations such as SOX and HIPPA we think that organizational factors play also a very important role. Previous literature has shown that SCT can predict the behavior of the individuals that might be impacted by environmental and personal factors. In this paper, our proposed model is aimed to explain employees' beliefs about their abilities to competently use computer information security tools in the determination of effective information security practices within organizations. The main contribution of our study is the presentation of a model of corporate information security behavior that can lead to develop effective auditing tools to follow profiles and also make recommendations for organizations that are looking for significant improvements in their information security.

REFERENCES

1. Agarwal, R., Sambamurthy, V., & Stair, R. (2000). The Evolving Relationship between General and Specific Computer Self-Efficacy: An Empirical Investigation. *Information Systems Research*, 11(4), 418-430.
2. Arief, B. and D. Besnard (2005). Technical and Human Issues in Computer-Based Systems Security. Centre for Software Reliability, School of Computing Science, University of Newcastle upon Tyne. Retrieved November 28, 2007 from, http://www.dirc.org.uk/publications/techreports/papers/5.pdf
3. Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review,* 84, 191-215.
4. Bandura, A. (1997). *Self-efficacy: The exercise of control.* New York: W.H. Freeman and Company.
5. Bandura, A. (2002). Social Cognitive Theory in Cultural Context. *Applied Psychology: An International Review*, 51(2), 269-290.
6. Berghel, H. (2007). Better-Than-Nothing Security Practices. Communications of the ACM, 50(8), 15-18.
7. Boss, R. S. (2007). *Control, Perceived Risk And Information Security Precautions: External and Internal Motivations for Security Behavior*. University of Pittsburgh.
8. Chen, C.C., R S Shaw, and S.C. Yang. (2006). Mitigating Information Security Risks By Increasing User Security Awareness: A Case Study Of An Information Security Awareness System. Information Technology, Learning, and Performance Journal, 24(1), 1-14.
9. Compeau, D. R. and C. A. Higgins (1995). "Application of social cognitive theory to training for computer skills." Information Systems Research 6(2): 118.
10. Compeau, D. R. and C. A. Higgins (1995). "Computer self-efficacy: Development of a measure and initial test." *MIS Quarterly 19*(2): 189.
11. DarkReading.com (2006). How Much Does a Hack Cost? Retrieved December 1, 2007 from, http://www.darkreading.com/document.asp?doc_id=101631
12. Dhillon, G., & Backhouse, J. (2000). Information system security management in the new millennium. *Communications of the ACM, 43*(7), 125-128.
13. Dhillon, G. and Backhouse, J. (2001) "Current Direction in IS Security Research: Towards Socio-Organizational Perspectives," *Information Systems Journal*, 11, 127-153.
14. Dinev, T., & Hu, Q. (2007). The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies *. Journal of the Association for Information Systems, 8(7), 386.
15. Eisenhardt, K. M. (1985). Control: Organizational and economic approaches. *Management Science, 31*(2), 134-149.
16. Goodhue, D.L. and Straub, D.W. 1991. Security concerns of system users: A study of perceptions of the adequacy of security, *Information & Management* 20, 13-27.
17. Havelka, D. (2003). "Predicting software self efficacy among business students: A preliminary assessment." *Journal of Information Systems Education* 14(2): 145.
18. Hayashi, A., C. Chen, et al. (2004). "The Role of Social Presence and Moderating Role of Computer Self Efficacy in Predicting the Continuance Usage of E-Learning Systems." *Journal of Information Systems Education* 15(2): 139.
19. Hu, Q., Hart, P., and Cooke, D. (2006) "The Role of External Influences on Organizational Information Security Practices: An Institutional Perspective," Proceedings of the 39th Hawaii International Conference on Systems Science (HICSS 39), January 4-7, Hawaii, USA. CD-ROM, IEEE Computer Society.
20. John, L. (2003). Improving user security behavior. *Computer & Security*, 22(8).
21. LaRose, R., & Eastin, M. S. (2004). A Social Cognitive Theory of Internet Uses and Gratifications: Toward a New Model of Media Attendance. *Journal of Broadcasting & Electronic Media 48*(3):
22. Lee, C.-C., H. K. Cheng, et al. (2007). "An empirical study of mobile commerce in insurance industry: Task-technology fit and individual differences." *Decision Support Systems* 43(1): 95.
23. Lindholm, l. (2006). Security Awareness. Retrieved, 2008, from the World Wide Web: http://csrc.nist.gov/organizations/fissea/2006-conference/Lindholm-FISSEA2006.pdf
24. Marakas, G. M., M. Y. Yi, et al. (1998). "The multilevel and multifaceted character of computer self-efficacy: Toward clarification of the construct and an integrative framework for research." *Information Systems Research* 9(2): 126.

25. Marakas, G. M., R. D. Johnson, et al. (2007). "The Evolving Nature of the Computer Self-Efficacy Construct: An Empirical Investigation of Measurement Construction, Validity, Reliability and Stability Over Time." *Journal of the Association for Information Systems* 8(1): 15.
26. Ouchi, W. G. (1977). Relationship between Organizational-Structure and Organizational-Control. *Administrative Science Quarterly, 22*(1), 95-113.
27. Reed, K., D. H. Doty, et al. (2005). "The Impact of Aging on Self-efficacy and Computer Skill Acquisition." *Journal of Managerial Issues* 17(2): 212.
28. Ryan, James Emory (2006) A comparison of information security trends between formal and informal environments. Ph.D. dissertation, Auburn University, United States -- Alabama. Retrieved October 22, 2007, from ProQuest Digital Dissertations database. (Publication No. AAT 3225287).
29. Sheng, Y. P., J. M. Pearson, et al. (2003). "Organizational culture and employees' computer self-efficacy: An emperical study.*" Information Resources Management Journal* 16(3): 42.
30. Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. Information Management & Computer Security, 8(1), 31.
31. Smith, S. M. (2005). "The Digital Divide: Gender and Racial Differences In Information Technology Education." *Information Technology, Learning, and Performance Journal* 23(1): 13.
32. Stanton, J. M., & Stam, K. R. (2006). *The Visible Employee: Using Workplace Monitoring and Surveillance to Protect Information Assets - Without Compromising Employee Privacy or Trust*. Medford, NJ: Information Today, Inc.
33. Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of End User Security Behaviors. *IEEE International Conference on Systems, Man and Cybernetics,* 2501-2506.
34. Straub, D. W. and Welke, R. J. 1998. Coping with Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly,* 22, 4, 441-469.
35. Suminski, R. R., & Petosa, R. (2006). Web-Assisted Instruction for Changing Social Cognitive Variables Related to Physical Activity. *Journal of American College Health Journal of American College Health J1 - Journal of American College Health, 54*(4), 219-225.
36. Taneja, A. (2006). Determinants of adverse usage of Information Systems Assets: A study of antecendents of is exploit in organizations.
37. Thatcher, J. B. and P. L. Perrewe (2002). "An empirical examination of individual traits as antecendents to computer anxiety and computer self-efficacy." MIS Quarterly 26(4): 381.
38. Torkzadeh, G., J. C.-J. Chang, et al. (2006). "A contingency model of computer and Internet self-efficacy." Information & Management 43(4): 541.
39. Vara, V. (2007). Ten Things Your IT Department Won't Tell You. *Wall Street Journal*, pp. R1.