Association for Information Systems
AIS Electronic Library (AISeL)

ICIS 2007 Proceedings

International Conference on Information Systems (ICIS)

December 2007

The Last Line of Defense: Motivating Employees to Follow Corporate Security Guidelines

Laurie Kirsch
University of Pittsburgh

Scott Boss
Bentley College

THE LAST LINE OF DEFENSE:

MOTIVATING EMPLOYEES TO FOLLOW CORPORATE SECURITY GUIDELINES

Information Privacy and Security

Scott R. Boss
Department of Accountancy
Bentley College
Waltham, MA
781-891-2353
sboss@bentley.edu

Laurie J. Kirsch
Katz Graduate School of Business
University of Pittsburgh
Pittsburgh, PA
412-648-7276
lkirsch@katz.pitt.edu

Abstract

Information security has become increasingly important to organizations. Despite the prevalence of technical security measures, individual employees remain the last line – and frequently the weakest link – in corporate defenses. When individuals choose to disregard security policies and procedures, the organization is at risk. How, then, can organizations motivate their employees to follow security guidelines? Using an organizational control lens, we build a model to explain individual information security precaution-taking behavior. Specific hypotheses are developed and tested using a field survey. We examine elements of control and introduce the concept of "mandatoriness" which we define as the degree to which individuals perceive that compliance with existing security policies and procedures is compulsory or expected by organizational management. We find that the acts of specifying policies and evaluating behaviors are effective in convincing individuals that security policies are mandatory. The perception of mandatoriness is effective in motivating individuals to take security precautions.

Keywords: Information security, Control, Mandatoriness

THE LAST LINE OF DEFENSE:

MOTIVATING EMPLOYEES TO FOLLOW CORPORATE SECURITY GUIDELINES

Introduction

The topic of information systems security has received a great deal of attention in the popular media and in trade journals over the past ten years. For example, Ken Dunham, director of the Rapid Response Team at iDefense, is convinced that "There's a well-developed criminal underground market that's connected to the mafia in Russia and Web gangs and loosely affiliated mob groups around the world" (Naraine 2006, p. 1). The risks of having poor security are generally well documented (Straub and Welke 1998) and include identity theft, data loss, and appropriation of computer and telecommunications resources. Alarmingly, the threat of attack is continuing to grow. A recent Internet study shows that there has been a marked increase in data theft and the creation of malicious code developed specifically to steal confidential information (Symantec Corporation 2007). Cyber criminals are continuing to refine their attack methods to remain undetected and to create global, cooperative networks to support the ongoing growth of criminal activity (Symantec Corporation 2007). Accordingly, many companies view security as one of their top concerns (Dale and The Associated Press 2006). There is evidence, however, that despite the efforts of organizations to secure their systems and data, they are still exposed to potential hackers in increasing numbers (Swartz 2005) and individuals either do not view security as a top priority or do not realize that they are at risk (Frieze et al. 1987).

Information security refers to all necessary measures that assure that systems will behave as expected and produce reliable results (Garfinkel et al. 2003; Ross 1999).[1] Corporations typically address the issues of computer security through technical means, using centralized firewalls and other software to try to protect corporate data. However, to achieve secure systems and data requires more than a focus on the technical issues; it also requires management attention (Dutta and McCrohan 2002) to design effective information security policies and motivate individual behavior to follow those policies (National Cyber Security Alliance 2005). Unfortunately, though extensive corporate measures are often put in place to protect data and systems, employees themselves often bypass extant information security policies, exposing organizations to data loss and cybercrime (Dhillon 2001). Thus, organizations face a dilemma of how to promote security policies and procedures to individual employees in the most effective way.

The purpose of this research is to examine this dilemma. The specific research question addressed is: How can organizations motivate individuals to take precautions in accordance with extant policies and procedures? The theoretical lens to examine this question is organizational control, which is defined broadly as any attempt to motivate individuals to behave in a manner consistent with organizational objectives (Jaworski 1988; Ouchi 1979). Following the suggestions of Kirsch (2004), in this study, control is examined at a granular level to better understand which specific elements of control encourage individuals to take precautions in a work environment. This study also investigates the role of individual perceptions of the mandatoriness of the controls as a significant part of the control process.

The paper proceeds as follows: The relevant literatures are reviewed, a model is developed and hypotheses are stated for testing. The research design and methodology are then discussed followed by a description of the results. The study concludes with a discussion of limitations of the study, areas for future research, and the implications of this research.

---

[1] Information security is differentiated from computer security by focusing more on behavioral aspects of security while computer security encompasses information security in addition to the other aspects of security such as technical aspects, physical security, system security, networking issues, etc. (McDaniel, G., and IBM Corporation *IBM dictionary of computing* McGraw-Hill, New York, 1994, pp. xi, 758 p, Ross, S.T. *UNIX system security tools* McGraw-Hill, New York, 1999, pp. xviii, 444 p.)

Background Literature, Model Development, and Hypotheses

Information security has been a concern to practitioners and theoreticians for decades (Dhillon 2001; GRIDtoday 2006; Hughes and DeLone 2007; Pearson and Weiner 1985). With the increasing use of interconnected networks to integrate all aspects of businesses and to reach outside organizational walls through the Internet, organizations are exposed to potential attacks in new ways that are often misunderstood (Whitman 2003). Typically, to deal with the exposure that comes with Internet connectivity, organizations implement a wide array of technical safeguards such as firewall software and hardware and intrusion detection devices (Dhillon and Backhouse 2000; Dutta and McCrohan 2002). Technical solutions are often the focus of corporate security efforts because they are the easiest to implement and centrally control, but they are not always the most effective (Dhillon and Backhouse 2000). While a system can be securely defended through technical means, if a single user shares a password or opens an e-mail containing a new virus that is not included in the anti-virus software, the technical safeguards are easily breached. On the other hand, behavioral solutions, such as educating individuals about security measures and informing others of penalties for disregarding security policies, have been found to be more effective than technical approaches (Straub 1990) but also more difficult to effectively implement. Though many studies consider these behavioral solutions (Dhillon and Backhouse 2001; Straub and Welke 1998), they are typically viewed as secondary to technical means of preventing cyber attacks (Chin 1999; Ives et al. 2004; Mercuri 2002). Very few studies look directly at the role that behavioral policies and procedures play in the process of encouraging employees to secure assets (Hone and Eloff 2002; Kankanhalli et al. 2003; Kotulic and Clark 2004).

When individuals are not motivated to follow the policies and procedures designed to protect both individuals and organizations, security fails (Campbell 2000; CERT Coordination Center 2004; Coren 2005). One area that has received scant attention in the Information Systems (IS) research literature is the role that individual compliance plays in preventing cyber-attacks. Specifically, how individuals take precautions, how they are motivated to take precautions, and the impact of corporate security policies on individual precaution-taking behavior have not been extensively researched. The accounting literature recognizes information security as a control system (Dopuch et al. 1982), but the IS literature has underdeveloped conceptualizations of how these control systems work in the realm of information security. Therefore, in this study, we used the control literature as a foundation for conceptualizing and exploring individual precaution-taking behavior.

Control

In Ouchi's (1978; 1979; 1980) seminal works, he argued that there are three modes of control: outcome (where the individual is evaluated and rewarded based on results achieved), behavioral (where the individual is evaluated and rewarded based on following prescribed behaviors), and clan (where social norms determine the desired behavior and individuals are rewarded or sanctioned by the group). However, some researchers have found these control modes complex and difficult to both study and measure (Kirsch et al. 2002; Snell 1992). Kirsch (2004) notes that there are inconsistencies and overlaps in the definitions and argues that to further our understanding, research is needed that examines control at a more granular level: what she calls the elements of control: specification, evaluation, and reward (Kirsch 2004).[2]

Specification refers to the formalized statement of a required behavior or outcome (Kirsch 2004). Formalized statements articulate desired behaviors or outcomes and are typically codified as organizational policies and procedures. These policies theoretically allow the controller to align the desired behavior or outcome and with organizational goals with the intent of achieving a specified objective (Kirsch 2004; Lorange and Scott-Morton 1974). For example, a well specified information security policy could be "Report/forward any suspicious e-mails (ones that request personal or organizational data, called "phishing") to the IS security personnel for investigation,"

[2] Following Eisenhardt (1985), Kirsch (2004) uses "measurement" instead of "specification." However, we feel the term "specification" better captures the meaning of this element since it emphasizes "… articulating specific behaviors and outcomes … common norms and values" (Kirsch 2004, p. 377). Kirsch also includes "roles and relationships" as a control element. Since this study only examines formal behavioral controls, where the control relationship typically manifests itself as a superior-subordinate dyad, the relationship element was dropped from our model.

or "Employees are to regularly update their computers with the latest security patches provided by (vendor)." Well specified policies give clear direction to the individual with the goal of achieving the desired behavior or outcome.

Evaluation is the sifting and organization of collected data with the intent of assessing individuals' compliance with specified behaviors or outcomes (Jaworski 1988; Kirsch 2004). Those involved in evaluation have the responsibility to determine whether the desired outcome has been achieved or whether the individual has exhibited the required behaviors by following the documented policies. Evaluation involves the use of formal documentation and information exchange to assess current status and make adjustments as necessary (Jaworski 1988; Kirsch 2004; Ouchi 1980). For example, an IS or security auditor can evaluate individual behaviors by examining server logs to verify that individuals have downloaded the latest security patches or examine e-mail logs and compare them to IS security e-mails to verify that phishing e-mails were forwarded to the appropriate personnel.

Finally, *reward* is based on individuals following the prescribed behavior (Chow et al. 1995; Eisenhardt 1985; Kirsch 2004), where individuals are rewarded based on following a prescribed behavior or meeting a target outcome. Eisenhardt (1985) notes that in the organizational literature, the reward for compliance with organizational control is often implicit; reward is a natural extension of specification and evaluation. Agency theory, where contracting is specifically involved within the agency relationship, makes rewards explicit (Eisenhardt 1985).

The examination of the elements of control has the potential to provide us with a deeper understanding of the effectiveness of control in different settings, thus this research focuses on specification, evaluation, and reward. In particular, these elements can be applied to the security environment to provide insight on the impact of management policies and procedures on individual compliance. With the changing nature of security threats (American National Standards Institute 2005; National Cyber Security Alliance 2005), it is difficult to stay current with the different types of attacks organizations face. Understanding how organizations specify information security policies, evaluate individuals, and reward them based on their level of compliance can help us to develop and implement policies in a more effective manner. Moreover, it is important to recognize that specification, evaluation, and reward are independent. For example, because a security policy is specified does not necessarily mean that adherence to the policy is evaluated or rewarded. This idea is explored in more detail as specific hypotheses are developed.

The examination of the elements of control directly applies to security for two reasons. First, security policies and procedures are often specified and administered by technical managers with no "line" responsibility for the individuals who must follow those policies. This means that specified controls, even if evaluated and rewarded, might be seen as optional as those enforcing compliance have no direct authority over those they seek to control. Second, security policies and procedures (specification) are put in place to regulate the behaviors of individuals to achieve (or prevent) a particular outcome (Eisenhardt 1985; Kirsch 2004). These policies can be seen, collectively, as a recipe that will endeavor to ensure a secure system not only at the present time, but also in the future. The result is that while policies are directed, in a general way, at the individual, how the individual follows those policies has implications for the entire organization.

Mandatoriness

Mandatoriness is here defined as the degree to which individuals perceive that compliance with existing security policies and procedures is compulsory or expected by organizational management. Prior research on control often implies that controls in place are perceived as mandatory or that individuals are compliant with policies and procedures implemented by management (Eisenhardt 1985; Harrison and McKinnon 1999). For example, most worm viruses are spread by individuals opening files received in e-mails that infect the host computer and mail replicas of the virus to e-mail addresses in the user's address book. Despite the best efforts of IS security personnel and the use of anti-virus filters, new viruses inevitably arrive in individuals' e-mail. If individuals were always compliant with security policies that specify, "Employees are not to open suspicious/unexpected e-mail attachments, from either unknown or trusted individuals" these worm viruses would not be a threat as they would never be executed. Evidence in the news and other reports shows us that the exact opposite is often the result. For example, the "I Love You" virus that infected computers in 2001 disrupted the communications of hundreds of thousands of computers and caused losses estimated in the billions of dollars (Chertoff 2001). To examine individual attitudes toward controls, this research explicitly considers the role of perceived mandatoriness in individual response to organizational controls.

Some IS literature has discussed mandatory versus voluntary systems, but is not always consistent in the discussion or definition of a mandatory system. The IS literature classifies a mandatory system in terms of being declared mandatory by management (Karahanna and Straub 1999), or non-mandatory because alternatives to the technology exist (Taylor and Todd 1995). A stronger conceptualization of mandatory systems is used by Hartwick & Barki (1994) and Venkatesh & Davis (2000) who define mandatory as the individual's perceptions of "required use" by managers. Approaching this from a control perspective, we use Kirsch's (2004) conceptualization of control elements discussed earlier. Control specification evokes a general level of obedience from individuals (Feldman 1998; Milgram 1974; Prakash and Rappaport 1975). Further, the propensity of individuals to perceive that a policy or set of policies is mandatory depends on whether management evaluates the individual's compliance with the prescribed policy. [3]

Precaution Taking

The ultimate goal of implementing security policies and procedures is that individuals within organizations will follow those policies and take precautions. Without individual action, security policies are meaningless as they have no influence on the overall security of systems within the organization. In this study, precaution taking is defined as the degree to which individuals perceive they take measures to secure their computers and deal with information security in accordance with prescribed corporate security policies and procedures as well through individual, proactive actions. Thus, in addition to following prescribed security policies and procedures, individuals should be generally aware of security threats. This general awareness can be enhanced through the formation and communication of formal information security policies (Straub 1990; Straub and Welke 1998)

Model Development & Hypotheses

Controls are often implemented within organizations for security purposes (American National Standards Institute 2005) with the goal of motivating individuals to comply with the desired behavior. A critical aspect of exercising control is the specification of desired behaviors or outcomes, often in the form of formal documented procedures (Eisenhardt 1985; Kirsch 2004). For example, a security policy might state, "Employees are to log off their computers when not at their desks." This policy addresses two possible concerns: the issue of accountability in that someone might use the "available" computer and thus not be held accountable for their actions, and to limit the amount of time a hacker has to attack a specific "active" user. The classic, if somewhat disturbing, obedience studies done by Milgram (1974) found that directives from a perceived authority resulted in the majority of individuals complying with those directives, suggesting that the directives were viewed as mandatory. Subsequent research has supported these findings over the past 30 years (Feldman 1998; Schneider et al. 2005), showing that the act of specifying a desired behavior leads to perceptions of mandatoriness on the part of individuals. The specification of a information security policy is the first step in signaling to the individual that the policy is mandatory. Therefore we predict that:

H_1: Specification of a set of security policies will be positively associated with the individual's perceived mandatoriness of that set of security policies.

According to the old business adage "That which is measured improves," the simple act of formulating and communicating policy to an organization is rarely enough to motivate action (Lim et al. 2002; Luft 1994). Individuals need to perceive that compliance with extant policies is important to management and that management views compliance with the policy as mandatory. One way management signals the importance of a policy is by assessing whether it is being followed. Evaluation is an essential part of control and can be characterized as the analysis of collected data that allows management to determine individual compliance (Kirsch 2004). If

[3] Mandatory controls are difficult to cognitively differentiate from punishment, which was originally included in the theoretical model. Of specification, evaluation, reward, and punishment, the first three (specification, evaluation, and reward) are consistent with Kirsch (2004) and Eisenhardt (1988) while punishment is not typically addressed in this literature. Analysis of the data shows that respondents were unable to differentiate between punishment and mandatoriness in this study. Rather than discard punishment completely from the study we chose to combine the punishment and mandatoriness items together to create a single mandatoriness construct consisting of Mand01, Mand03, Mand04, Punish01 (Mand05), Punish02 (Mand06), Punish03 (Mand07), and Punish04 (Mand08).

management either never or only infrequently evaluates compliance, those policies will most likely be disregarded by employees. Evaluation of individual compliance thus results in the perception that a policy is mandatory, suggesting that:

H_2: Evaluation of compliance with security policies will be positively associated with the individual's perceived mandatoriness of the established set of security policies.

Reward is the final factor that signals to the individual that a control is mandatory. If policies are stated, data gathered, individuals evaluated, but there is no consequence for either compliance or non-compliance, individuals will soon decide that the control is not important to management and thus not mandatory, regardless of management declarations (Straub and Welke 1998). The consequence of a reward for compliance with a policy is enough to signal to employees that a policy is mandatory (Frederickson and Waller 2005; Luft 1994). Thus we predict that:

H_3: Reward for compliance with security policies and procedures will be positively associated with the individual's perceived mandatoriness of the established set of security policies.

The additional costs of time and effort required to comply with security policies and procedures make it easy to ignore requirements that are not considered to be mandatory. Lim et al. (2002) found that only 60 percent of employees accept Internet usage policies at face value, suggesting that there are doubts at the individual level regarding how they view extant policies. Specifying a policy with subsequent evaluation and reward are not enough to motivate individuals to follow policy. On the other hand, management expectations have a strong effect on individual behavior (D'Aquila 2001): the compliance expectations of managers will influence the behavior of their employees. This suggests that if individuals perceive security policies to be mandatory, they are more likely to adhere to those policies. We therefore predict that:

H_4: Perceived mandatoriness of an information security policy will be associated with an increased likelihood that individuals will take security precautions.

The theoretical model representing these assertions and their relationships is shown below in Figure 1. Controls for computer self efficacy (CSE) (Compeau and Higgins 1995), the degree to which people feel comfortable using a computer, and apathy, or the lack of motivation or enthusiasm (Charlton and Birkett 1995), were also included as control variables. It is reasonable to assume that how competent individuals feel with computers (CSE) should increase their perceptions that they can follow policies, and that a lack of motivation to pay attention to security (apathy) will likely reduce the precautions taken by individuals.

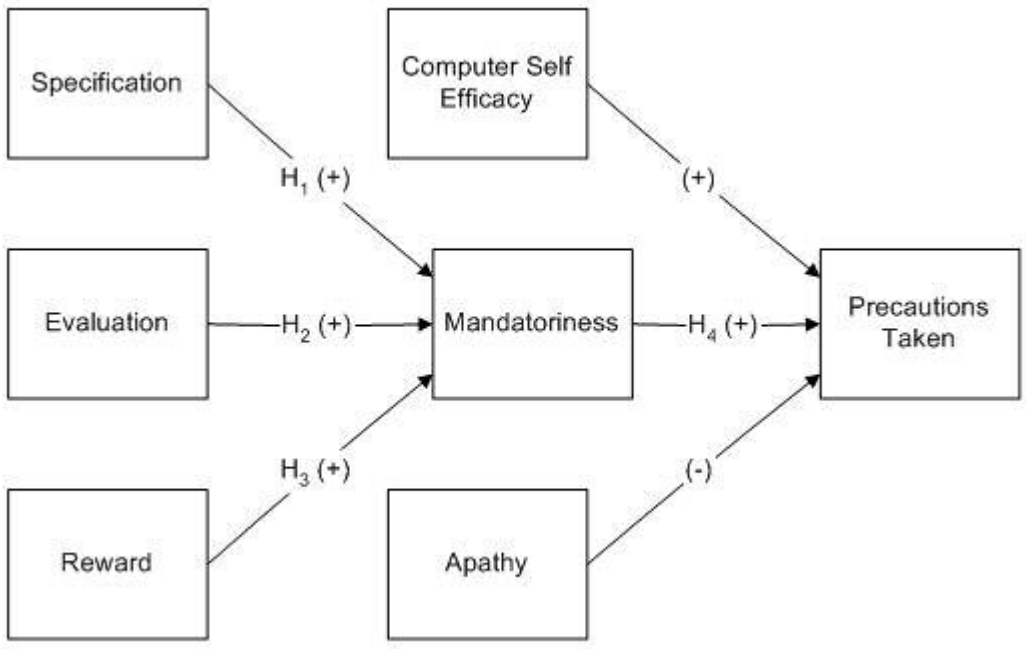

Figure 1 – Research Model

Research Design and Methodology

To test the hypothesized relationships, questionnaires were developed to measure the constructs described in the research model. Instruments were developed from extant literature (Cardinal 2001; Eisenhardt 1985; Kirsch 1996; National Cyber Security Alliance 2005) and adapted to the security context. A pre-test was conducted in July 2005 with 28 MBA students to provide qualitative assurance about a measure's content validity, construct validity, and reliability. As a result of the pre-test the questionnaire was modified to eliminate confusing language and to refine the constructs in the model.

After securing approval from our Institutional Review Board, the study was pilot tested in October 2005 at a large public institution on a population of approximately 180 individuals within the Information Systems Department (ISD) to further refine the measures. Of the population, 80 individuals participated in the survey. Analysis of the data obtained from the pilot test showed general support for the research model.

Data Collection

The main data collection took place in May 2006 at a large, U.S. medical center located in the southeastern United States (SEMC). The organization employs approximately 4,750 people, of whom approximately 3,900 are female and 850 are male. Those targeted for participation were individuals who use computers on a daily basis, including clerical support staff, professional services, technical services, nurses and nursing services, physicians, and management. The organization has historically been technically oriented and has recently integrated their information systems with their medical records, resulting in almost all employees having to utilize a computer on a daily basis. Additionally, HIPPA regulations require information security training for hospital employees which made this site a good choice for data collection.

The data were gathered through a web-based survey which was available to employees for a period of approximately three weeks. Individuals were contacted initially by e-mail informing them that SEMC was conducting a security study and would like their participation. Usernames and a link to the questionnaire URL were provided in the initial e-mail. Reminder e-mails were sent to individuals who had not yet filled out the survey throughout the collection period. Once the survey was complete, incentive awards for participation were distributed through a random drawing.

The population of potential respondents, described above, was approximately 3,500 people, of which 1698 valid responses were obtained (approximately 49 percent). The sample included personnel from all areas of the organization with staff nurses and office/clerical personnel having the highest number of responses. The full breakdown of the sample by organizational area is detailed in Table 1.

Table 1 – Respondent Position Descriptions and Frequencies

Position	n	%
Office and Clerical	381	22.7
Support Services	53	3.2
Professional Services	161	9.6
Technical Services	194	11.5
Staff RN	476	28.3
Other Nursing Services	126	7.5
Physician	37	2.2
Coordinator	81	4.8
Team Leader, PDS	10	0.6
Manager	112	6.7
Director	40	2.4
Administration	11	0.7
Total	1682*	100.0

*Note: 15 respondents (0.9% of the total data set) did not indicate their position when completing the survey.

Respondents' education ranged from some high school to post-graduate degrees, with 93 percent having at least some college education. The sample consisted of 1471 females (87 percent) and 226 males (13 percent) which generally reflects the population of SEMC. The ages of the respondents ranged from 21 to 78 years old. Descriptive statistics for the sample are shown below in Table 2.

Table 2 – Respondent Demographic Characteristics

Characteristic (Years)	Mean	SD	Org Mean	Min	Max	n
Job Tenure	8.29	8.18	8.42	0.2	47	1696
Computer Expertise (Self Reported)	13.34	6.56	--*	1.0	40	1660
Age	41.82	10.87	42.68	21.0	78	1696

*Note: The organization does not collect comprehensive information regarding employee computer expertise.

To assess the possibility of non-response bias, the extrapolation method described by Armstrong and Overton (1977) was used to examine "waves" of respondents. The last "wave" of 184 respondents (those who responded after the last reminder e-mail was sent) was compared with the first 184 responders of the survey, the rationale being that the last wave (approximately 11 percent of responders) would not have participated at all without the additional stimulus of reminders, emails, and extensions. These responders would then be the most similar to non-respondents if non-response bias exists and they are significantly different than the first group of responders. The extrapolation was done by performing t-tests comparing the first wave respondents construct scores with the last wave respondent scores. All construct differences were insignificant with the exception Computer Self Efficacy ($p<0.01$) showing that those who responded later felt that, on average, had less confidence in their abilities to use computers to accomplish tasks. This is to be expected as those who put off taking a mandatory on-line survey would be those with the least confidence in their abilities in working with a computer.

We used two procedures to identify subjects whose responses indicated "deviance" and were thus unsuitable for inclusion in our survey. Deviance was identified as either a participant who failed to respond to a large number of questions, or those who did not provide consistent responses. Respondents who exhibited either of these characteristics were, likely, not paying complete attention when completing the survey, thus their responses are suspect and were removed from the response data.

The majority of the missing variables were distributed equally across the data; however, 20 cases had a disproportionate percentage (more than 40 percent) of missing values where the mean number of missing responses per case was 3.74. These cases were dropped from the data set. Other deviant cases were identified through the use of reverse coded items in the scales. By assessing the extent to which an individual scored reverse coded items in the same direction as those that were not, we are able to detect individuals who may not have been taking the survey seriously. Those respondents who answered the same answer throughout the survey (for example a respondent who answered "5" to all questions) for "Likert-type" questions are suspect, the reason being that even a minimal amount of attention to the survey would have resulted in at least one different answer. There were 25 cases that met these criteria and were subsequently dropped. Overall, 45 cases in total were removed from the dataset resulting in a total of 1671 cases in the final dataset.

Reliability and Validity Analysis

There are three standard processes for assessing reliability of scales. Chronbach's coefficient alpha (Nunnally 1978; Nunnally and Bernstein 1994) where alpha scores exceed 0.70 are considered reliable. A second process is the measure of internal consistency developed by Fornell and Larcker (1981) and preferred in PLS analysis (Chin 1998). The goal of this analysis, similar to Chronbach's alpha, is to achieve a score greater than 0.70. A final test of scale reliability involves examining whether items have item loading of at least 0.70 from PLS which demonstrates that the items share more variance with the construct than error variance (Carmines and Zeller 1979).

An initial reliability analysis was performed using all three tests (Chronbach's alpha, internal consistency, loading examination) and did not indicate that any items from the scales should be dropped with the exception of items in the apathy scale. Apathy items 1 to 4 were dropped because of a low Chronbach's alpha score and low loading scores. As a result of dropping the problematic items, Chronbach's Alpha increased from 0.54 to 0.79 and internal consistency increased from 0.47 to 0.90.

To ensure high content validity of the measures, measures from extant literature were adapted, where possible, for the survey. Comments and feedback from experienced researchers were obtained throughout the instrument development process and pre-test and pilot-study results were carefully analyzed. Initial assessments of convergent and discriminant validity were conducted using factor analysis with Varimax rotation. The analysis showed that items from the mandatoriness, reward, and CSE scales were cross loading on several of the factors identified. To address these issues, low loading items were dropped one at a time and the factor analysis was re-run and examined for additional cross-loading items.

As a result, mandatoriness item 2, reward item 1, and CSE items 1-3 were dropped resulting in the items loading cleanly over seven constructs and shows a clear separation of items along construct lines with Eigenvalues greater than 1.0 as seen in Table 3 (with factors loading lower than 0.40 suppressed). This suggests a high level of construct validity.

Table 3 – Factor Analysis Results

	Factor						
Variable	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Spec01				0.75			
Spec02				0.67			
Spec03				0.75			
Spec04				0.75			
Eval01			0.86				
Eval02			0.87				
Eval03			0.88				
Eval04			0.86				
Reward02					0.69		
Reward03					0.89		
Reward04					0.88		
Mand01		0.68					
Mand03		0.72					
Mand04		0.66					
Mand05		0.75					
Mand06		0.72					
Mand07		0.75					
Mand08		0.79					
Precaut01						0.74	
Precaut02						0.78	
Precaut03						0.78	
CSE4	0.79						
CSE5	0.85						
CSE6	0.90						
CSE7	0.85						
CSE8	0.78						
CSE9	0.82						
CSE10	0.82						
Apathy05							0.89
Apathy06							0.89
Eigenvalues	4.99	4.62	3.66	2.77	2.29	2.28	1.70
% Variance	16.66	15.39	12.19	9.23	7.63	7.61	5.67

A second reliability analysis was performed to re-check the reliability of the scales. Table 4 (below) provides the relevant reliability statistics for each item (the loadings and residual variance) and for each scale (internal consistency and Chronbach's alpha) after the problematic items were removed.

Table 4 – Reliability and Validity Analysis					
Variable	**Loading**	**Internal Consistency**	**Chronbach's Alpha**	**AVE**	**Square Root of AVE**
Spec01	0.83				
Spec02	0.75				
Spec03	0.88				
Spec04	0.89				
Specification		0.90	0.89	0.70	0.84
Eval01	0.93				
Eval02	0.95				
Eval03	0.95				
Eval04	0.95				
Evaluation		0.97	0.96	0.89	0.95
Reward02	0.92				
Reward03	0.75				
Reward04	0.78				
Reward		0.86	0.81	0.67	0.82
Mand01	0.84				
Mand03	0.84				
Mand04	0.80				
Mand05	0.80				
Mand06	0.78				
Mand07	0.77				
Mand08	0.81				
Mandatoriness		0.93	0.91	0.65	0.81
Pre01	0.89				
Pre02	0.84				
Pre03	0.86				
General Precautions		0.90	0.83	0.75	0.86
CSE04	0.79				
CSE05	0.86				
CSE06	0.90				
CSE07	0.85				
CSE08	0.77				
CSE09	0.84				
CSE10	0.84				
CSE		0.94	0.93	0.70	0.84
Apathy05	0.91				
Apathy06	0.91				
Apathy		0.90	0.79	0.82	0.91

This reliability analysis indicates that all of variable meet the accepted minimum for both a traditional analysis (Cronbach Alpha > 0.70 (Nunnally 1978)) as well as PLS analysis (AVE > 0.50 (Chin 1998)) after the cross-loading variables were removed. Additionally, the control variables (CSE and apathy) also met the generally accepted levels after modification.

Item discriminant validity is tested by examining the correlation coefficients of each of the item with each of the constructs. The items should correlate highly with their intended construct, but not with unintended constructs. Acceptable discriminant validity is shown when the correlations with their intended construct exceed their correlations with all other constructs. As shown below in Table 5, this condition holds for all items (item correlations relating to the intended construct are in bold) suggesting that the scales have a high degree of discriminant validity.

Table 5 – Item Discriminant Validity					
	Specification	**Evaluation**	**Reward**	**Mandatoriness**	**Precautions Taken**
Spec01	**0.84**	0.36	0.04	0.53	0.38
Spec02	**0.79**	0.48	0.22	0.46	0.38
Spec03	**0.86**	0.40	0.04	0.62	0.35
Spec04	**0.87**	0.50	0.14	0.60	0.41
Eval01	0.49	**0.94**	0.37	0.48	0.37
Eval02	0.48	**0.95**	0.37	0.49	0.38
Eval03	0.48	**0.95**	0.35	0.49	0.37
Eval04	0.51	**0.95**	0.33	0.54	0.39
Reward02	0.18	0.41	**0.78**	0.25	0.20
Reward03	0.06	0.27	**0.89**	0.07	0.11
Reward04	0.10	0.27	**0.88**	0.13	0.13
Mand01	0.59	0.44	0.11	**0.83**	0.51
Mand03	0.58	0.35	0.02	**0.82**	0.46
Mand04	0.56	0.34	0.06	**0.79**	0.47
Mand05	0.55	0.47	0.18	**0.81**	0.38
Mand06	0.49	0.51	0.24	**0.79**	0.39
Mand07	0.48	0.44	0.19	**0.79**	0.37
Mand08	0.49	0.43	0.17	**0.83**	0.41
Precaut01	0.42	0.34	0.09	0.54	**0.86**
Precaut02	0.38	0.35	0.23	0.40	**0.87**
Precaut03	0.38	0.34	0.11	0.44	**0.86**

Convergent validity is demonstrated when the average variance extracted (AVE) by a construct's items is at least 0.50 (Chin and Gopal 1995). An examination of Table 4 (above) shows that all constructs meet this criterion. Discriminant validity is assessed by comparing the correlations between two constructs with the square root of AVE of each construct. Correlations between two constructs that are greater than the square root of AVE are indicative of poor discriminant validity between the constructs involved. Table 6 shows that the square root of AVE score (in bold along the diagonal) was larger than the correlations between any two related constructs. The final survey scales can be seen in Appendix 1.

Table 6 – Construct Discriminant Validity					
	Specification	**Evaluation**	**Reward**	**Mandatoriness**	**Precautions Taken**
Specification	**0.84**				
Evaluation	0.52**	**0.95**			
Reward	0.13**	0.37**	**0.82**		
Mandatoriness	0.66**	0.53**	0.18**	**0.81**	
Prec. Taken	0.46**	0.40**	0.17**	0.53**	**0.86**

Results

The research hypotheses were tested by examining the size and significance of structural paths using PLS analysis techniques. PLSGraph software was utilized to do principal component analysis, path analysis, and regression to simultaneously evaluate both theory and data (Wold 1982). The percentage of variance is shown below in Figure 2, with 49 percent of the variance being explained in the relationships between the control elements and mandatoriness and 36 percent of the variance being explained between mandatoriness, the control variables, and precautions taken.

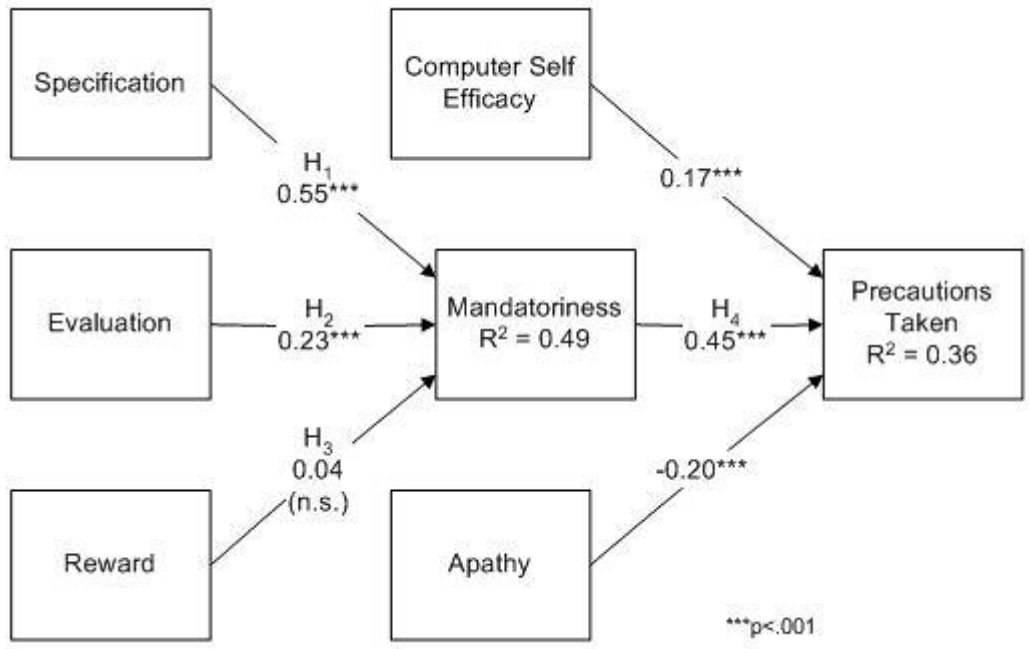

Figure 2 – PLS Results

All of the proposed hypotheses, with one exception, were supported. Specification significantly influences perceptions of mandatoriness (β=0.55, p<.001), as proposed in Hypothesis 1. Evaluation significantly influences mandatoriness (β=0.23, p<.001), as proposed in Hypothesis 2. Finally, mandatoriness significantly influences the dependent variable, precautions taken (β=0.45, p<.001), as predicted in Hypothesis 4. The control variables also had a significant influence on the dependent variable with both computer self-efficacy (β=0.17, p<.001) and apathy (β=-0.20, p<.001) contributing to the overall explanatory power of the model. Hypothesis 3 (the effects of reward on mandatoriness) was not supported.

Common Method Bias

A common problem in social science research is common method bias. Common method bias is defined as the "variance (in a study) that is attributable to the measurement method rather than to the constructs the measures represent" (Podsakoff et al. 2003) and is estimated to have affected a significant number of studies over the years (Cote and Buckley 1987). Podsakoff et al. (2003) note that there are both procedural and statistical remedies to control for common method bias.

The procedural methods used in this study include subjecting the questionnaire to rigorous review by peers. Additionally, the uses of both a pretest and pilot test have improved the study and provide more consistent and unbiased scales. In this way we controlled for item characteristic effects and item context effects. Likewise, the questionnaire was designed so that criterion and predictor variables were separated. Finally, the respondents were guaranteed anonymity for their participation, and the steps taken to ensure that anonymity was maintained were reviewed by the Institutional Review Board at our organization. These methods controlled for measurement context effects.

Podsakoff et al. (2003) provide a decision tree to select statistical remedies for common method bias based on the type of study and circumstances of that study. For this study it is recommend that the single-common-method-factor approach and the multiple-specific-method-factors approach be used to show any common method bias, specifically common rater effects, that might be present in the study. To do this questions that could cause common rater effects were identified, specifically those that emphasize social desirability as there is a strong cultural and legislative emphasis on information security at the target site. The IS department at the hospital regularly emphasizes security

and the HIPPA and Sarbanes-Oxley legislation require that ongoing security training be performed on an ongoing basis. The results of this analysis showed that none of the relationships changed in any significant way with t-statistics changing by less than one for any relationship, and the significance levels remaining the same for all relationships. We thus conclude that common method bias is not a significant factor in this study.

Discussion and Implications

The results of this research emphasize the need for managers to focus on behavioral solutions in addition to the technical ones in the context of information security. As predicted, the specification of a policy significantly predicts individual perceptions of mandatoriness. Further, specification has indirect effects on precautions taken, mediated by individual perceptions of mandatoriness. Second, the perception that the evaluation of a desired behavior in itself contributes to perceptions that the policy is mandatory as well as indirectly motivating individuals to take precautions. These results suggest that specification of a policy is a mental construct where the simple act of codifying required behavior and then evaluating the behaviors themselves effects behavioral change as well as conveying a sense of mandatoriness. The results suggest that the specification of information security policies and evaluation for non-compliance with those policies both contribute to perceptions of mandatoriness.

The significance of apathy in the model shows that individuals do not necessarily pay attention to security, further emphasizing that the attitudes toward information security are not as strong as they should be considering the seriousness of the issue. One reason for the apathy may be the absence of line authority by those who enforce the policies over those required to follow them. This implies that line management in addition to IS or security management personnel within the organization need to emphasize the importance of security on a regular basis to overcome these effects. Additionally, the significance of computer self efficacy emphasizes the need to train all members of the organization on how to use a computer. As individuals feel more confident in using the computer to complete their work, they will be more likely to take precautions with the computer.

The results do not support the prediction that the effects of using reward as an incentive to follow mandatory guidelines (the security policy) impact individual perceptions of mandatoriness (Hypothesis 3). This is contrary to what is typically discussed in the literature where rewards are used as incentive to change behaviors (Eisenhardt 1988; Luft 1994). The reason for the lack of support may be a result of the differences in context between what is typically seen in the literature and the security context. The literature findings usually reflect situations where rewards are used as incentives for individuals to go above and beyond their current compensation level (Luft 1994) for doing their jobs (endeavoring to keep their computer systems secure) and does not appear to have the desired impact. Other explanations for this finding may either be that the rewards themselves are too distant from the act of securing the computer, or that organizations do not typically engage in rewarding precaution-taking behavior. These results require further research to provide more insight to this finding. Regardless, rewards were not found to impact individual perceptions of mandatoriness.

A final implication for managers is that their approach to security is a key issue. When security is viewed (either explicitly or implicitly) as something that is "above and beyond" individuals' job descriptions, it is unlikely that much thought will be given to their part in information security. The results show that managerial attention is needed to craft meaningful information security policies and to motivate individuals to follow them. Managers should emphasize the specification of policies and evaluation of those policies for non-compliance, while giving less emphasis to reward. Likewise, top managerial support is necessary for these policies to be effective (Knapp et al. 2006)

Conclusions

Before discussing the conclusions, there are several limitations to this study that should be noted. First, the use of a single respondent to measure both the dependent and independent variables can be problematic and could lead to common method bias. While this is a concern, the study deals with perceptions that are best measured by a single source. Further both procedural and statistical remedies were applied and do not indicate the presence of common method bias. Second, the use of the same set of data to both obtain the measurement model and to assess the structural model may methodologically lead to an over-fit model, however given the volume of data this may not be an issue. Third, this study focused only on formal behavioral controls. It is likely that the presence of a strong security culture (clan control or subjective norms) or outcome controls explain some of the variance that was not

captured in this study. The examination of both clan control and the effects of subjective norms on mandatory situations should be the topic of future studies. Likewise, future research should include the relationships element of control as the security phenomenon is examined in terms of different relationships to help us better understand how control works within organizations and how subjective norms affect the relationship.

This research offers several contributions to the literature. First, it looks at a topic that is under-researched: the behavioral aspects of information security. Given the attention security is currently receiving in the media and by academic groups, this research is both timely and important. Second, security is examined from a managerial control perspective, which adds to research that studies security from a technical perspective. This study has also allowed us to focus on and test the elements of control (Kirsch 2004) in the context of information security. Our study of specification, evaluation, and reward complements research that investigates control as a more global construct, and it demonstrates the validity of examining these elements individually and collectively to show their influence.

Finally, this study explicitly introduced to the control literature the concept of mandatoriness. To the best of our knowledge, prior studies have not examined whether individuals perceive controls to be mandatory. Yet these perceptions are likely to influence whether individuals act in accordance with those controls. This study has shown that while the specification and evaluation aspects of information security policies are integral to whether an individual view them as mandatory, the impact of these efforts should be assessed. Additionally the "mandate" provided by the implementation of controls may not be strengthened to the degree anticipated by offering rewards for compliance. Further apathy regarding information security leads individuals not to take security precautions. Finally, managerial investment in computer training and education will ultimately protect the organization as individuals with high computer self efficacy better understand what they need to do to protect corporate computer assets. These findings offer insights into how to structure security controls and the implications of management actions on providing a secure corporate environment.

When the individual is the last line of defense in information security, it is logical that organizations should craft strong computer policies and procedures and do all they can to motivate individuals to comply. This research shows us that the process of implementing information security policies goes beyond crafting the policy and telling individuals in the organization that the policies are mandatory. More care needs to be taken at the management level to implement policies and then follow up through training and evaluation to motivate employees to effect a more secure computer environment.

Appendix – Survey Scale Items

Specification: Items adapted from (Kirsch 1996) and Cardinal (2001)	
Spec01	I am familiar with the organization's IT security policies, procedures, and guidelines.
Spec02	I am required to know a lot of existing written procedures and general practices to secure my computer system.
Spec03	There are written rules regarding security policies and procedures at the organization.
Spec04	The organization's existing policies and guidelines cover how to protect my computer system.
Evaluation: Items adapted from Cardinal (2001) and Eisenhardt (1985)	
Eval01	Managers in my department frequently evaluate my security behaviors.
Eval02	Managers regularly examine data relating to how well I follow security policies and procedures.
Eval03	Managers formally evaluate me and my colleagues regarding compliance with security policies.
Eval04	Managers assess whether I follow organizational security procedures and guidelines.
Reward: Items adapted from (Kirsch 1996) and Cardinal (2001)	
Reward01	My pay raises and/or promotions depend on whether I follow documented security policies and procedures.
Reward02	I will receive personal mention in oral or written reports if I comply with security policies and procedures at this organization.
Reward03	I will be given monetary or non-monetary rewards for following security policies and procedures.
Reward04	Tangible rewards are tied to whether I follow the organization's IT security policies, procedures, and guidelines.
Mandatoriness: Items adapted from (Kirsch 1996) and Cardinal (2001) and conceptualizations in Chae and Pool (2005) and Hartwick and Barki (1994)	
Mand01	I am required to secure my system according to the organization's documented policies and procedures.
Mand03	There is an understanding that I will comply with organization security policies and procedures.
Mand04	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.
Mand05	I will be sanctioned for not complying with documented security policies and procedures.
Mand06	Senior management will be notified if I do not follow the organization's IT security policies, procedures, and guidelines.
Mand07	There are specific punishments tied to whether I follow security policies and procedures.
Mand08	Failure to secure my system by following the organization's IT security policies, procedures, and guidelines can have repercussions on my career.
Precautions Taken: Items developed from professional security standards and from general information security best practices published by the National Cyber Security Alliance (2005)	
Precaut01	I pay attention to computer security during my daily routine.
Precaut02	I keep aware of the latest security threats so I can protect my system.
Precaut03	My system is as secure as I can make it.
Computer Self Efficacy (CSE): Items taken from Compeau and Higgins (1995). The questions relate to the following statement: "I could complete my job using the software package . . ."	
CSE04	... if I had seen someone else using it before trying it myself.
CSE05	... if I could call someone for help if I got stuck.
CSE06	... if someone else helped me get started.
CSE07	... if I had a lot of time to complete the job for which the software was provided.
CSE08	... if I had just the built-in help facility for assistance.
CSE09	... if someone showed me how to do it first.
CSE10	... if I had used similar packages like this one before to do the job.
Apathy: Items developed to reflect the lack of motivation or enthusiasm regarding information security.	
Apathy05	Paying attention to security takes too much time.
Apathy06	I'm too busy to be bothered by information security concerns.

References

American National Standards Institute "ISO ICS 35 Information Technology," 2005.

Armstrong, J.S., and Overton, T.S. "Estimating Nonresponse Bias in Mail Surveys," *Journal of Marketing Research* (14:3) 1977, pp 396-402.

Campbell, C.M. "Hacking rises despite increased security spending," Network World, Inc., 2000.

Cardinal, L.B. "Technological innovation in the pharmaceutical industry: The use of organizational control in managing research and development," *Organization Science* (12:1), Jan-Feb 2001, pp 19-36.

Carmines, E.G., and Zeller, R.A. *Reliability and validity assessment* Sage Publications, Beverly Hills, Calif., 1979, p. 70.

CERT Coordination Center "2004 E-Crime Watch Survey Shows Significant Increase in Electronic Crimes," Carnegie Mellon University, Pittsburgh, PA, 2004.

Chae, B., and Poole, M.S. "Mandates and technology acceptance: A tale of two enterprise technologies," *Journal of Strategic Information Systems* (14:2), Jun 2005, pp 147-166.

Charlton, J.P., and Birkett, P.E. "The Development and Validation of the Computer Apathy and Anxiety Scale," *Journal of Educational Computing Research* (13:1) 1995, pp 41-59.

Chertoff, M.J. "Statement of Michael Chertoff Assistant Attorney General, Criminal Division, U.S. Department Of Justice before the Subcommittee on Crime Committee on the Judiciary U.S. House of Representatives," in: *Subcommittee on Crime Committee on the Judiciary U.S. House of Representatives*, Washington DC, 2001.

Chin, S.K. "High-confidence design for security," *Communications of the ACM* (42:7), Jul 1999, pp 33-37.

Chin, W.W. "The partial least squares approach for structural equation modelling," in: *Modern methods for business research,* G.A. Marcoulides (ed.), Lawrence Erlbaum, Mahwah, N.J., 1998, pp. viii, 437 p.

Chin, W.W., and Gopal, A. "Adoption Intention in GSS - Relative Importance of Beliefs," *Data Base for Advances in Information Systems* (26:2-3), May-Aug 1995, pp 42-64.

Chow, C.W., Hirst, M., and Shields, M.D. "The effects of pay schemes and probabilistic management audits on subordinate misrepresentation of private information: An experimental investigation in a resource allocation context," *Behavioral Research in Accounting* (7) 1995, pp 1-15.

Compeau, D.R., and Higgins, C.A. "Computer Self-Efficacy - Development of a Measure and Initial Test," *MIS Quarterly* (19:2), JUN 1995, pp 189-211.

Coren, M. "Experts: Cyber-crime bigger threat than cyber-terror," Cable News Network LP, LLLP, Atlanta, GA, 2005.

Cote, J.A., and Buckley, M.R. "Estimating Trait, Method, and Error Variance - Generalizing across 70 Construct-Validation Studies," *Journal of Marketing Research* (24:3), Aug 1987, pp 315-318.

D'Aquila, J.M. "Financial accountants' perceptions of management's ethical standards," *Journal of Business Ethics* (31:3), Jun 2001, pp 233-244.

Dale, M., and The Associated Press "Verizon could offer settlements over blocked e-mails," Pittsburgh Post Gazette, Pittsburgh, PA, 2006.

Dhillon, G. "Violation of safeguards by trusted personnel and understanding related information security concerns," *Computers & Security* (20:2) 2001, pp 165-172.

Dhillon, G., and Backhouse, J. "Information system security management in the new millennium," *Communications of the ACM* (43:7), Jul 2000, pp 125-128.

Dhillon, G., and Backhouse, J. "Current directions in IS security research: towards socio- organizational perspectives," *Information Systems Journal* (11:2), Apr 2001, pp 127-153.

Dopuch, N., Birnberg, J.G., and Demski, J.S. *Cost accounting: accounting data for management's decisions*, (3rd ed.) Harcourt Brace Jovanovich, New York, 1982, pp. x, 726 p.

Dutta, A., and McCrohan, K. "Management's role in information security in a cyber economy," *California Management Review* (45:1), Fall 2002, pp 67-+.

Eisenhardt, K.M. "Control: Organizational and economic approaches," *Management Science* (31:2), Feb 1985, pp 134-149.

Eisenhardt, K.M. "Agency-Theory and Institutional-Theory Explanations - the Case of Retail Sales Compensation," *Academy of Management Journal* (31:3), Sep 1988, pp 488-511.

Feldman, R.S. *Social psychology*, (2nd ed.) Prentice Hall, Upper Saddle River, N.J., 1998, pp. xxii, 618 p.

Fornell, C., and Larcker, D.F. "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research* (18:1) 1981, pp 39-50.

Frederickson, J.R., and Waller, W. "Carrot or stick? Contract frame and use of decision-influencing information in a principal-agent setting," *Journal of Accounting Research* (43:5), Dec 2005, pp 709-733.

Frieze, I.H., Hymer, S., and Greenberg, M.S. "Describing the crime victim: psychological reactions to victimization," *Professional Psychology: Research and Practice* (18:4) 1987, pp 299-315.

Garfinkel, S., Spafford, G., and Schwartz, A. *Practical UNIX and Internet security*, (3rd ed.) O'Reilly, Beijing ; Sebastopol, CA, 2003, pp. xxix, 954 p.

GRIDtoday "IT Security Spending to Hit $61 Billion for 2006, says Info-Tech," Tabor Communications Inc., San Diego, CA, 2006.

Harrison, G.L., and McKinnon, J.L. "Cross-cultural research in management control systems design: a review of the current state," *Accounting Organizations and Society* (24:5-6), Jul-Aug 1999, pp 483-506.

Hartwick, J., and Barki, H. "Explaining the Role of User Participation in Information-System Use," *Management Science* (40:4), Apr 1994, pp 440-465.

Hone, K., and Eloff, J.H.P. "Information security policy - what do international information security standards say?," *Computers & Security* (21:5) 2002, pp 402-409.

Hughes, L.A., and DeLone, G.J. "Viruses, worms, and Trojan horses - Serious crimes, nuisance, or both?," *Social Science Computer Review* (25:1), Spr 2007, pp 78-98.

Ives, B., Walsh, K.R., and Schneider, H. "The domino effect of password reuse," *Communications of the ACM* (47:4), Apr 2004, pp 75-78.

Jaworski, B.J. "Toward a Theory of Marketing Control: Environmental Context, Control Types, and Consequences," *Theory of Marketing Control* (52), July 1988, pp 23-39.

Kankanhalli, A., Teo, H.H., Tan, B.C.Y., and Wei, K.K. "An integrative study of information systems security effectiveness," *International Journal of Information Management* (23:2), Apr 2003, pp 139-154.

Karahanna, E., and Straub, D.W. "The psychological origins of perceived usefulness and ease-of-use," *Information & Management* (35:4), Apr 1999, pp 237-250.

Kirsch, L.J. "The Management of Complex Tasks in Organizations: Controlling the Systems Development Process," *Organization Science* (7:1), JAN-FEB 1996, pp 1-21.

Kirsch, L.J. "Deploying common solutions globally: The dynamics of control," *Information Systems Research* (15:4), Nov 8 2004, pp 374-395.

Kirsch, L.J., Sambamurthy, V., Ko, D.G., and Purvis, R.L. "Controlling information systems development projects: The view from the client," *Management Science* (48:4), APR 2002, pp 484-498.

Knapp, K.J., Marshall, T.E., Rainer, R.K., and Ford, F.N. "Information security: management's effect on culture and policy," *Information Management & Computer Security* (14:1) 2006, pp 24-36.

Kotulic, A.G., and Clark, J.G. "Why there aren't more information security research studies," *Information & Management* (41:5), May 2004, pp 597-607.

Lim, V.K.G., Teo, T.S.H., and Loo, G.L. "How do I loaf here? Let me count the ways," *Communications of the ACM* (45:1), Jan 2002, pp 66-70.

Lorange, P., and Scott-Morton, M.S. "A Framework for Management Control Systems," *Sloan Management Review* (16:1), Fall 1974, pp 47-56.

Luft, J. "Bonus and Penalty Incentives Contract Choice by Employees," *Journal of Accounting & Economics* (18:2), SEP 1994, pp 181-206.

McDaniel, G., and IBM Corporation *IBM dictionary of computing* McGraw-Hill, New York, 1994, pp. xi, 758 p.

Mercuri, R.T. "Security watch - Computer security: Quality rather than quantity," *Communications of the ACM* (45:10), Oct 2002, pp 11-14.

Milgram, S. *Obedience to authority; an experimental view*, (1st ed.) Harper & Row, New York,, 1974, pp. xvii, 224 p.

Naraine, R. "Return of the Web Mob," in: *eWeek.com*, Ziff Davis Media, New York, NY, 2006.

National Cyber Security Alliance "Top Ten Cybersecurity Tips," National Cyber Security Alliance, Washington DC, 2005.

Nunnally, J.C. *Psychometric theory*, (2d ed.) McGraw-Hill, New York, 1978, pp. xv, 701 p.

Nunnally, J.C., and Bernstein, I.H. *Psychometric theory*, (3rd ed.) McGraw-Hill, New York, 1994, pp. xxiv, 752 p.

Ouchi, W.G. "Transmission of Control through Organizational Hierarchy," *Academy of Management Journal* (21:2) 1978, pp 173-192.

Ouchi, W.G. "Conceptual-Framework for the Design of Organizational Control Mechanisms," *Management Science* (25:9) 1979, pp 833-848.

Ouchi, W.G. "Markets, Bureaucracies, and Clans," *Administrative Science Quarterly* (25), March 1980, pp 129 - 141.

Pearson, F.S., and Weiner, N.A. "Toward an Integration of Criminological Theories," *Journal of Crime and Criminology* (76:1), Winter 1985, pp 116-150.

Podsakoff, P.M., MacKenzie, S.B., Lee, J.Y., and Podsakoff, N.P. "Common method biases in behavioral research: A critical review of the literature and recommended remedies," *Journal of Applied Psychology* (88:5), Oct 2003, pp 879-903.

Prakash, P., and Rappaport, A. "Informational Interdependencies - System Structure Induced by Accounting Information," *Accounting Review* (50:4) 1975, pp 723-734.

Ross, S.T. *UNIX system security tools* McGraw-Hill, New York, 1999, pp. xviii, 444 p.

Schneider, F.W., Gruman, J.A., and Coutts, L.M. *Applied social psychology : understanding and addressing social and practical problems* SAGE Publications, Thousand Oaks, Calif., 2005, pp. xiii, 449 p.

Snell, S.A. "Control-Theory in Strategic Human-Resource Management - the Mediating Effect of Administrative Information," *Academy of Management Journal* (35:2), Jun 1992, pp 292-327.

Straub, D.W. "Effective IS Security: An Empirical Study," *Information Systems Research* (1:3), Sep 1990, pp 255 - 273.

Straub, D.W., and Welke, R.J. "Coping with systems risk: Security planning models for management decision making," *MIS Quarterly* (22:4), Dec 1998, pp 441-469.

Swartz, J. "2005 worst year for breaches of computer security," in: *USA Today*, Gannett Co. Inc., 2005.

Symantec Corporation "Symantec Reports Rise in Data Theft, Data Leakage, and Targeted Attacks Leading to Hackers' Financial Gain," 2007.

Taylor, S., and Todd, P. "Assessing IT usage: The role of prior experience," *MIS Quarterly* (19:4), Dec 1995, pp 561-570.

Venkatesh, V., and Davis, F.D. "A theoretical extension of the Technology Acceptance Model: Four longitudinal field studies," *Management Science* (46:2), Feb 2000, pp 186-204.

Whitman, M.E. "Enemy at the gate: Threats to information security," *Communications of the ACM* (46:8), Aug 2003, pp 91-95.

Wold, H.O.A. (ed.) *Soft Modeling: The basic design and some extensions*. North Holland Press, Amsterdam ; New York, New York, 1982.