European Journal of Information Systems (2009) 18, 151–164

www.palgrave-journals.com/ejis/

If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security

Scott R. Boss[1], Laurie J. Kirsch[2], Ingo Angermeier[3], Raymond A. Shingler[4] and R. Wayne Boss[5]

[1]Department of Accountancy, Bentley University, U.S.A.; [2]Joseph M. Katz Graduate School of Business & College of Business Administration, University of Pittsburgh, U.S.A.; [3]Spartanburg Regional Medical Center, U.S.A.; [4]Spartanburg Regional Medical Center, U.S.A.; [5]Leeds School of Business, University of Colorado at Boulder, U.S.A.

Correspondence: Scott R. Boss, Department of Accountancy, Bentley University, 175 Forest Street, Waltham, MA 02452, U.S.A.
Tel: +781 891 2353;
Fax: +781 891 2896;
E-mail: sboss@bentley.edu

An earlier version of this paper was presented in Montreal, Quebec, Canada at the International Conference on Information Systems, 2008.

Abstract
Information security has become increasingly important to organizations. Despite the prevalence of technical security measures, individual employees remain the key link – 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, thus if individuals believe that management watches, they will comply.
European Journal of Information Systems (2009) **18,** 151–164. doi:10.1057/ejis.2009.8; published online 31 March 2009

Keywords: information security; control; mandatoriness

Received: 8 April 2008
Revised: 15 August 2008
2nd Revision: 18 January 2009
Accepted: 23 February 2009

Introduction

Information systems (IS) security has received a great deal of attention and coverage in the popular media and trade journals over the past 10 years and, 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). The typical institutional response to the threat of compromise is to focus primarily on the *systems'* components (hardware and software) of information security (Hu *et al.*, 2007), where information security refers to all necessary measures that assure that systems will behave as expected and produce reliable results (Ross, 1999; Garfinkel *et al.*, 2003). However, to achieve secure systems and data requires more than a focus on systems solutions. Secure systems require management attention to design effective information security policies (Dutta & McCrohan, 2002) and motivated individuals to follow those policies (National Cyber Security Alliance, 2005). Unfortunately, employees are often resistant to security policies (Hu *et al.*, 2007) and bypass them, thus exposing their organizations to data loss and cybercrime (Dhillon, 2001).

When individuals are not motivated to follow security policies and procedures designed to protect both individuals and organizations, security fails (Coren, 2005). Thus, organizations face the challenge of how to promote security policies and procedures for individual employees in the most effective way. 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. Moreover, the concept of *mandatory* controls, where participation is not optional or where compliance is required by the organization, is not typically discussed in the control or security literatures. The assumption, although not stated specifically, is that controls would not be specified if they were not important enough to be mandatory (Chae & Poole, 2005). Although this assumption may be correct, the continuing issues regarding information security indicate that not all members of an organization regard information security policies and procedures as mandatory and therefore do not comply with the security policies.

The objective of this research is to examine how organizations motivate individuals to take precautions in accordance with extant policies and procedures, and to understand the role of individual perceptions 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. The specific research questions to be addressed are 'What factors affect the perception of mandatoriness?' and 'To what degree does mandatoriness affect compliance behavior'? To examine our research questions, we turn to the literature on organizational control, which explores the processes managers use to direct, motivate, and encourage individuals to behave in a manner consistent with organizational objectives (Ouchi, 1979; Jaworski, 1988; Cardinal, 2001). A control perspective has been applied to many contexts, including sales (Eisenhardt, 1985), research & development (Cardinal, 2001), and management of start-up firms (Cardinal *et al*., 2004). In addition, several researchers have applied a control perspective to the study of custom and outsourced IS development (Kirsch, 1996, 2004; Choudhury & Sabherwal, 2003; Nidumolu & Subramani, 2003). The organizational control perspective is also appropriate for this context of information security because we are interested in understanding the circumstances under which individual behavior reflects control mechanisms put in place by managers to secure IT assets, and whether individuals' perceptions of mandatoriness affects their behavior.

Our paper proceeds as follows: The next section discusses the relevant literature and develops our model with specific hypotheses. The following section examines our research design and methodology including model validation. Finally, results are presented and the implications of this research are discussed.

Background literature, model development, and hypotheses

This study investigates the role of individual perceptions of the mandatoriness of the controls as a significant part of the information security process. Consistent with other IS researchers, we take a behavioral view of control that encompasses all attempts that managers take to ensure individuals' behavior in a desired fashion (Kirsch, 1996; Choudhury & Sabherwal, 2003). Control researchers often use Ouchi's (1979) seminal work on control to differentiate behavior, outcome, and clan control modes. Managers exercise behavior and outcome control by specifying desired behaviors for employees to follow and rewarding them for doing so (behavior control), or articulating desired targets for employees to achieve and basing rewards on whether employees achieved these targets (outcome control) (Cardinal, 2001). Clan control is exercised when individuals share values and norms and behave in a manner that is consistent with those shared values and norms (Birnberg & Snodgrass, 1988). Control modes are exercised via specific mechanisms that include financial incentives, detailed project plans, peer pressure, socialization practices, and meetings (Kirsch, 1997).

Much of the empirical work on control in the IS literature has examined the antecedents of control or the control process itself (e.g., Kirsch, 1996, 1997, 2004; Choudhury & Sabherwal, 2003). In contrast, we are interested in understanding the effects of controls in place, beginning with the relationship between control and mandatoriness. Rather than studying control modes or mechanisms, however, we turn to Kirsch's (2004) conceptualization of control elements which, in turn, were derived from work by Eisenhardt (1985). Extant control literature can be complex and difficult to both study and measure (Snell, 1992; Kirsch *et al*., 2002). Kirsch (2004, 1997) notes that there are inconsistencies and overlaps in the definitions of control modes, and that mechanisms can be used to exercise multiple modes of control. Therefore, she 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 (which Kirsch (2004) calls measurement), evaluation, and reward. An evaluation of security at the elemental level will give us a clearer picture of the impacts of control elements on the individual (Kirsch, 2004). Further this approach will give us a deeper understanding of the impact of mandatoriness on individual behaviors.

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 individuals, how each individual follows those policies is to some degree discretionary and may vary widely, but the implications for the entire organization are serious.

The examination of the elements of control, therefore, has the potential to provide insight on the impact of management policies and procedures on individual compliance. With the changing nature of security threats (National Cyber Security Alliance & McAfee Corporation, 2008), it is difficult for the individual to stay current with the different types of attacks that either the organizations or individual might face. The level of compliance, additionally, can signal to management the degree to which the policy has been successfully implemented and its effectiveness. 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.

We argue that understanding how organizations specify information security policies, as well as evaluate and reward individuals for their compliance behavior, has a direct impact on the degree to which the individual believes that the controls are mandatory. In the next sections, we develop these ideas, beginning with an exploration of the concept of mandatoriness.

Mandatoriness

Our concept of 'mandatoriness' is rooted in prior studies of 'mandates' and 'mandatory systems' found in many technology acceptance and implementation studies. This literature often views mandates as directives or orders (Brown *et al*., 2002; Chae & Poole, 2005). Hartwick & Barki (1994) and Venkatesh & Davis (2000), for example, define mandatory as the individual's perceptions of 'required use' by managers, and Karahanna & Straub (1999) observe that a mandatory system is one that is declared mandatory by management. A non-mandatory system, on the other hand, is one in which alternatives to the technology exist (Taylor & Todd, 1995). Most studies in IS characterize mandates in three ways: as a black box where individuals either react positively or negatively to the mandate, as a one-time decision to obey or reject, and as 'orders from management' when the mandate may stem from other sources such as legal or regulatory bodies (Chae & Poole, 2005).

There have been numerous empirical studies of technology acceptance and implementation. However, many of these studies focus on situations in which the individual has some discretion in adopting the technology or system (e.g., the adoption of spreadsheets), thus focusing on voluntary rather than mandatory adoption (Rawstorne *et al*., 1998; Venkatesh & Davis, 2000). Recent work by Malhotra and colleagues (Malhotra & Galletta, 2005; Malhotra *et al*., 2008) has extended the work on voluntary usage by offering a more complex view of volitional behavior. In their study of voluntary acceptance and usage of a communication and collaboration system, Malhotra & Galletta (2005) introduce psychological attachment model, in which they integrate three forms of commitment from social influence theory (Kelman, 1958, 1961) – internalization, identification, and compliance – with UTAUT concepts of perceived usefulness and perceive ease-of-use to explain attitudes and behavioral intentions of adoption and usage. They argue that internalization, identification, and compliance represent different forms of commitment to adopt and use a system. Malhotra *et al*. (2008) draw on organismic integration theory (Ryan & Deci, 2000; Deci & Ryan, 2002), which argues that individuals are totally volitional and therefore initiate all behaviors. In their empirical study, Malhotra *et al*. distinguish among behaviors that are volitional (i.e., an individual perceives himself as the origin of his behavior), mandatory (i.e., an individual perceives that his behavior is in compliance with an external authority), or introjected (i.e., an individual feels coerced to act in a manner that is counter to personal values).

In contrast, some scholars have focused their attention solely on the concept of mandates and mandatory systems. For example, Markus (1983) describes how some users accepted, and some resisted, the implementation of a financial system whose use was mandated by management. More recently, Sussman & Siegal (2003) examine the adoption of advice received in mediated contexts such as e-mail. Though use of e-mail is not explicitly mandated by management, the authors suggest that the adoption of e-mail is not voluntary for knowledge workers in contemporary organizations. How the individual reacts to a mandate is usually along a continuum where they interpret the degree to which they believe a policy is mandatory or voluntary and act accordingly (Brown *et al*., 2002). Mandates are often subject to interpretation because a mandate is not generally a simple directive. A mandate is often accompanied with rules and regulations, which describe the desired outcome and how the outcome is to be achieved. How the mandate and these documents are interpreted can result in a wide variance of actual compliance (Chae & Poole, 2005).

This research on mandates and mandatory systems shows us that there is often a great deal of give and take based on the individual interpretation of the directive. Therefore we define 'mandatoriness' in the context of our study, as the degree to which individuals perceive that compliance with existing security policies and procedures is compulsory or expected within the organization. In the next section, we explicitly consider the role of mandatoriness in individual response to the elements of control: specification, evaluation, and reward.

The elements of control

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 (Eisenhardt, 1985; Das & Teng, 1998). Further, when management implements a control, they send a signal that compliance is expected by individuals in the organization as there would not typically be requirements to behave in a certain way if management did not feel that the directive was important enough to be mandatory.

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). 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 with organizational goals with the intent of achieving a specified objective (Lorange & Scott-Morton, 1974; Kirsch, 2004). Well-specified policies give clear direction to the individual with the goal of achieving the desired behavior or outcome. 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 (many systems are set to require a password to unlock after 10–15 min of activity) 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. Likewise, another well-specified information security policy could be 'Report/forward any suspicious e-mails (ones that request personal or organizational data, called 'phishing') that are not caught by the organization's spam filter to the IS security personnel for investigation.'

Control research suggests that establishing uniform performance criteria throughout the company enhances performance (Nidumolu & Subramani, 2003). The classic 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 (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 an information security policy is the first step in signaling to the individual that the policy is mandatory. Therefore we predict that:

H1: *Specification of a set of security policies will be positively associated with the individual's perceived mandatoriness of that set of security policies.*

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. 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. Evaluation can also be more hands on where security or management personnel physically examine individuals' computers to check for compliance.

The old business adage 'That which is measured improves,' indicates that the simple act of formulating and communicating policy to an organization is rarely enough to motivate action (Luft, 1994; Lim *et al*., 2002). Individuals need to perceive that compliance with extant policies is important to management. This importance can be manifested in many ways but, regardless of the way this is expressed, management needs to indicate that they view compliance with the policy as mandatory. One way management signals the importance of a policy is by checking to see if it is being followed (Dopuch *et al*., 1982). Evaluation is an essential part of control and can be characterized as the analysis of collected data that allows management to determine compliance (Kirsch, 2004). If 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:

H2: *Evaluation of compliance with security policies will be positively associated with the individual's perceived mandatoriness of the established set of security policies.*

The *reward* element of control is the notion that individuals are rewarded based on following a prescribed behavior or meeting a target outcome (Chow *et al*., 1995; Kirsch, 2004). Eisenhardt (1985) notes that in the organizational literature, the rewards are often implicit, whereas agency theory, in which contracting is specifically involved within the agency relationship, makes rewards explicit.

We posit that rewards signal to the individual that a control is mandatory. Control theory ties rewards to individuals behaving in certain ways, thus compliance with the expected behaviors will bring rewards to the individuals (Eisenhardt, 1985; Kirsch, 1997). If policies are stated, data gathered, individuals evaluated, but there is no reward for either compliance or lack of a reward for non-compliance, individuals will soon decide that the policy is unimportant and thus not mandatory, regardless of management declarations (Straub & Welke, 1998). The consequence of a reward for compliance with a policy is an additional signal to employees that a policy is mandatory (Frederickson & Waller, 2005). Thus we predict that

H3: *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.*

Precaution taking

The ultimate goal of implementing security policies and procedures is to secure the organizations digital property. Without at least tacit acceptance and some individual action, security policies are meaningless (Hu *et al*., 2007). 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 as 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 management formation and communication of formal information security policies (Straub, 1990; Straub & Welke, 1998).

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. A control system consists primarily of the process that organizations use to monitor and evaluate behavioral performance of individuals against some standard (Ouchi, 1977, 1979). How management implements this process (through specification, evaluation, and reward) may be viewed as being a hindrance to completing operational tasks (Falk & Kosfeld, 2004). A mandate that a policy is to be followed can encourage individuals to comply where a lack of requirement may signal that the control is unimportant.

As noted earlier, how individuals interpret the mandate is subject to a variance in actual compliance (Chae & Poole, 2005). Lim *et al*. (2002) found that only 60% of employees accept Internet usage policies at face value, suggesting that there are doubts at the individual level regarding the importance of information security policies. Specifying a policy with subsequent evaluation and reward is not enough to motivate individuals to follow that policy. On the other hand, management expectations have a strong effect on individual behavior (D'Aquila, 2001), thus 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

H4: *Perceived mandatoriness of an information security policy will be associated with an increased likelihood that individuals will take security precautions.*

Finally, the literature indicates that individuals respond to controls in different ways (Schnedler & Radovan, 2007). Although individuals might follow a policy if it is specified, there are others that will not. Likewise, there will be variance in the reaction of individuals in response to evaluation and reward. Information security policies are considered by most to be necessary (Kadam, 2002), but some research has shown that following the policies may reduce their work effectiveness (Falk & Kosfeld, 2004). As a result, it is likely that individuals require a mandate from management before compliance will occur. This suggests an additional mediation role of the mandate in the relationship between the control elements and taking precautions where the mandate itself is the motivation for individual compliance, thus

H5: *Perceived mandatoriness of an information security policy will mediate the relationship between the control elements (specification, evaluation, and reward) and security precautions taken.*

The theoretical model representing these assertions and their relationships is shown in Figure 1. Controls for computer self-efficacy (CSE) (Compeau & Higgins, 1995), the degree to which people feel comfortable using a computer, and apathy, the lack of motivation or enthusiasm (Charlton & Birkett, 1995), were also included as control variables. The literature suggests that in addition to specification, evaluation, reward, and mandatoriness, that CSE will have an impact on whether individuals will follow computer-related policies and procedures (Compeau & Higgins, 1995; Hasan, 2006). Thus it is reasonable to assume that how competent individuals feel in accomplishing tasks with computers should also increase their perceptions that they can take measures to secure their computers and follow policies. Likewise, the apathy literature indicates that individuals may disregard policies and procedures because they are too busy or just do not consider information security to be important (Macaulay & Cook, 1994). Thus, the lack of motivation will likely reduce the precautions taken by individuals.

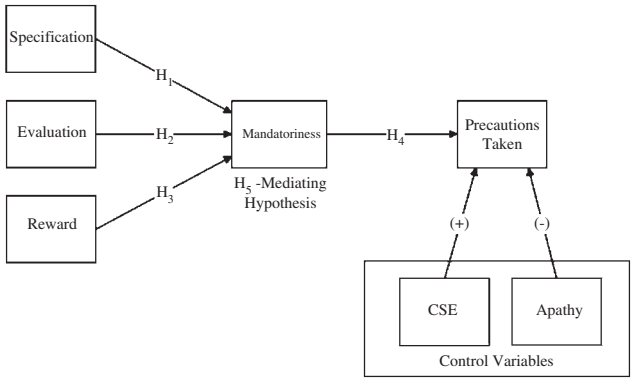

Figure 1 Research model.

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 (Eisenhardt, 1985; Kirsch, 1996; Cardinal, 2001; National Cyber Security Alliance, 2005) and adapted to the security context. All of the constructs were deemed to be reflective as the items themselves are essentially interchangeable and have equal weight in determining the construct itself (Petter *et al*., 2007). A pre-test was conducted with 28 MBA students to provide qualitative assurance about a measure's content validity, construct validity, and reliability.

The study was pilot tested at a large public institution on a population of approximately 180 full-time employees of the Information Systems Department 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 at a large medical center located in the southeastern United States (Southeastern Museums Conference, SEMC). The organization employs approximately 4750 people, of whom approximately 3900 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 IS with their medical records, resulting in almost all employees having to utilize a computer on a daily basis. Additionally, federal 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 3 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 3500 people, of which 1698 valid responses were obtained (approximately 49%). The full breakdown of the sample by organizational area, which generally reflects SEMCs' overall composition, is detailed in Table 1.

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

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.

To assess the possibility of non-response bias, the extrapolation method described by Armstrong & Overton (1977) was used to examine 'waves' of respondents. The last 'wave' of 184 respondents was compared with the first 184 responders, the rationale being that the last wave (approximately 11% of responders) would not have participated at all without the additional stimulus of reminders, emails, and extensions. The extrapolation was done by performing t-tests comparing construct scores between the first and last wave respondents. All construct differences were insignificant with the exception of CSE ($P<0.01$) 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 online survey would most likely be those with the least confidence in their abilities in working with a computer.

Due to missing data and other deviant responses (e.g., answering '5' to every question), 45 cases were removed, resulting in a total of 1671 cases in the final data set.

Reliability and validity analysis

There are three standard processes for assessing reliability of reflective scales. Cronbach's coefficient alpha (Nunnally & Bernstein, 1994) where alpha scores that exceed 0.70 are considered reliable. A second process is the measure of internal consistency developed by Fornell & Larcker (1981) and preferred in partial least squares (PLS) analysis (Chin, 1998). The goal of this analysis, similar to Cronbach's alpha, is to achieve a score greater than 0.70. A final test of scale reliability involves examining whether items have an item loading of at least 0.70 from

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.

PLS which demonstrates that the items share more variance with the construct than error variance (Carmines & Zeller, 1979).

An initial reliability analysis was performed using all three tests and did not indicate that any items from the scales should be dropped with the exception of items in the apathy scale. Apathy items 1–4 were dropped because of a low Cronbach's alpha score and low loading scores. As a result of dropping the problematic items, Cronbach'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, reward item 1, and CSE items 1–3 were dropped resulting in the remaining items loading cleanly over seven constructs and shows a clear separation of items along construct lines with eigenvalues greater than 1.0 which suggests a high level of construct validity. A second reliability analysis was performed to re-check the reliability of the scales. As seen in Table 3, all variables meet the accepted guidelines, with Cronbach's alpha, loadings, and internal consistency measuring >0.70.

Item discriminant validity is tested by examining the correlation coefficients of each item with each construct. 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 4, 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.

Convergent validity is demonstrated when the average variance extracted (AVE) by a construct's items is at least 0.50 (Chin & Gopal, 1995). An examination of Table 4 shows that all constructs meet this criterion.

Table 3 Reliability and validity analysis

Variable	*Loading*	*Internal consistency*	*Cronbach's alpha*	*AVE*
Spec01	0.83			
Spec02	0.75			
Spec03	0.88			
Spec04	0.89			
Specification		0.90	0.89	0.70
Eval01	0.93			
Eval02	0.95			
Eval03	0.95			
Eval04	0.95			
Evaluation		0.97	0.96	0.89
Reward02	0.95			
Reward03	0.69			
Reward04	0.73			
Reward		0.85	0.81	0.64
Mand01	0.90			
Mand02	0.90			
Mand03	0.88			
Mand04	0.82			
Mandatoriness		0.90	0.91	0.77
Pre01	0.89			
Pre02	0.85			
Pre03	0.85			
General precautions		0.90	0.83	0.75
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
Apathy05	0.90			
Apathy06	0.91			
Apathy		0.90	0.79	0.82

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 5 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 A.

Table 4 Item discriminant validity

	Specification	*Evaluation*	*Reward*	*Mandatoriness*	*Precautions taken*
Spec01	**0.81**	0.39	0.11	0.45	0.29
Spec02	**0.78**	0.46	0.22	0.38	0.27
Spec03	**0.85**	0.47	0.12	0.53	0.28
Spec04	**0.84**	0.49	0.18	0.49	0.29
Eval01	0.51	**0.88**	0.35	0.38	0.27
Eval02	0.48	**0.88**	0.34	0.33	0.26
Eval03	0.50	**0.91**	0.37	0.40	0.28
Eval04	0.46	**0.86**	0.31	0.39	0.27
Reward02	0.22	0.39	**0.78**	0.30	0.15
Reward03	0.13	0.29	**0.85**	0.16	0.12
Reward04	0.14	0.29	**0.86**	0.16	0.10
Mand01	0.52	0.40	0.21	**0.82**	0.35
Mand02	0.48	0.39	0.25	**0.84**	0.39
Mand03	0.42	0.30	0.15	**0.82**	0.28
Mand04	0.45	0.33	0.20	**0.84**	0.27
Precaut01	0.33	0.27	0.08	0.40	**0.83**
Precaut02	0.27	0.25	0.18	0.28	**0.83**
Precaut03	0.27	0.25	0.10	0.30	**0.83**

Table 5 Construct discriminant validity

	Specification	*Evaluation*	*Reward*	*Mandatoriness*	*Precautions taken*
Specification	**0.84**				
Evaluation	0.55**	**0.95**			
Reward	0.19**	0.39**	**0.80**		
Mandatoriness	0.56**	0.43**	0.24**	**0.88**	
Precautions taken	0.34**	0.30**	0.15**	0.39**	**0.86**

**$P<0.01$.

Results

The research hypotheses were tested by examining the size and significance of structural paths using PLS analysis techniques with PLS-Graph v3. 00. The percentage of variance is shown in Figure 2, with 42% of the variance being explained in the relationships between the control elements and mandatoriness and 40% of the variance being explained between mandatoriness, the control variables, and precautions taken.

All of the proposed hypotheses, with one exception, were supported. Specification significantly influences perceptions of mandatoriness ($\beta=0.56$, $P<0.001$), as proposed in H1. Evaluation significantly influences mandatoriness ($\beta=0.14$, $P<0.001$), as proposed in H2. Finally, mandatoriness significantly influences the dependent variable, precautions taken ($\beta=0.48$, $P<0.001$), as predicted in H4. Hypothesis H3 (the effects of reward on mandatoriness) was not supported.

The control variables also had a significant influence on the dependent variable with both CSE ($\beta=0.17$, $P<0.001$) and apathy ($\beta=-0.20$, $P<0.001$) contributing to the overall explanatory power of the model. To examine the substantive impact of the control variables to the overall model, we compared the variance explained (R^2) by the control variables alone ($R^2=0.18$) with the variance explained by the whole model to determine an effect size (f^2) using the following formula: $(R^2_{full}-R^2_{selected})/(1-R^2_{full})$ (Cohen, 1977; Mathieson *et al.*, 2001). The effect size of the control variables in this model is large ($f^2=0.36$) indicating a substantial significant ($P<0.001$) effect on precautions taken.

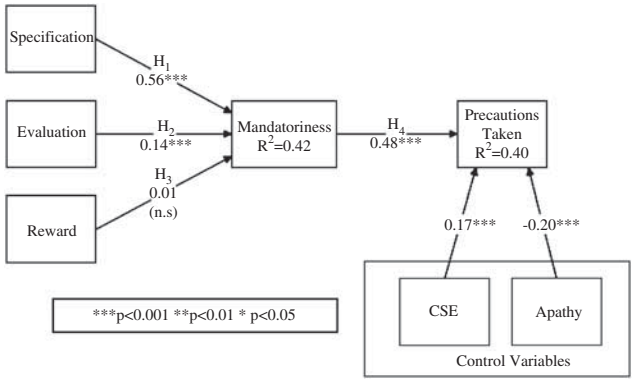

Figure 2 PLS results.

Table 6 Mediation analysis

	Step 1 DV = Mandatoriness	*Step 2 DV = Precautions taken*	*Step 3 DV = Precautions taken*
Specification of polices	0.47***	0.25***	0.13***
Evaluation performed	0.13***	0.15***	0.12***
Rewards given	0.10***	0.04	0.01
Mandatoriness			0.26***
Adjusted R^2	0.34***	0.14***	0.18***

***$P > 0.001$.

Mediation hypothesis

To test for mediation effects stated in H5 we use regression models and first regress the control elements (specification, evaluation, reward) on mandatoriness, second regress the control elements on the dependent variable (precautions taken), and third regress the control elements and mandatoriness on the dependent variable. For mediation to be shown, there must be a significant relationship between the control elements and mandatoriness (Step 1), a significant relationship between the control elements and the dependent variable (Step 2), and there must be a significant relationship between mandatoriness and the dependent variable (Step 3). If all of these hold, the effects of the control variables in Step 3 need to be smaller than the effects in Step 2 (Baron & Kenny, 1986). Other researchers have recommended that Step 2 be optional as it is likely that mediation would cause the effect of the independent variable on the dependent variable to disappear (Kenny *et al*., 1998; Shrout & Bolger, 2002). The results of the mediation analysis are shown in Table 6.

After following the steps we see that, using regression analysis, specification and evaluation, are partially mediated by mandatoriness providing some support for H5.

Common method bias

A potential problem in social science research is common method bias. 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, including subjecting the questionnaire to rigorous review by peers and using both a pre-test and pilot test, have improved the study and provide more consistent and unbiased scales. Likewise, the questionnaire was designed so that criterion and predictor variables were separated and the respondents were guaranteed anonymity for their participation.

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 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.

An additional adaption of this method was proposed by Liang *et al*. (2007). To perform this test, the indicators of all constructs are reflectively associated with the method factor with the results showing the variance explained by the construct and by the method factor (bias). As shown in Appendix B although all of the method loadings were significant, the average substantive explained variance for an indicator is 0.71 and the average common method-based variance is 0.01 showing a ratio of substantive variance to method variance of 71:1. Additionally, the structural model shows different levels of significance for the path coefficients. We therefore conclude that common method bias is not a significant factor in this study.

Discussion and implications

Of the five hypotheses tested: H1, H2, and H4 are supported; H5 is partially supported; and H3 is not supported. This research also highlights the importance of both apathy and CSE as important variables that influence information security behaviors, even though the effects of these constructs were not hypothesized.

These results indicate that mandatoriness and its antecedents significantly impact individual precaution-taking behaviors. 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 was supported 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.

A primary contribution of this research has been to explicitly introduce the concept of mandatoriness in the information security context and model it in an organizational control framework. In addition, we measure mandatoriness and assess its impacts. The results of this study show that when individuals view a policy to be mandatory they will take precautions as required. To date, much of the IS literature has treated a mandate as a one-time choice or a declaration, and assumed that individuals accepted directives as mandates. This research shows that the concept of something being 'mandatory' goes beyond this relatively simple view and that individual perceptions of mandatoriness vary, thus allowing us to more fully explore the concept. This research has theoretical implications for the control literature by providing a point from which to build additional theory about mandatoriness and mandates.

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 (H3). This is contrary to what is typically discussed in the literature where rewards are used as incentive to either change or encourage specific 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 compliance with expected behaviors, but it may be that in the security realm individuals feel that the rewards would be to encourage them to go above and beyond management expectations (Luft, 1994). When it comes to security expectations, however, there is relatively little the individual can do to exceed expectations. 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. Additionally, this research focused primarily on the positive 'reward' aspects as noted in the control literature (Kirsch, 2004). Other literature (such as general deterrence theory (Blumstein, 1978)) differentiates between punishment and reward and focuses on the effects of punishment in organizational and individual settings. Future research should explore these distinctions especially as they relate to mandatoriness and compliance with proscribed behaviors.

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. The significance of CSE, in turn, may indicate that precaution taking is also a function of individual comfort with computers and individual's confidence in their own ability to utilize the computer to accomplish tasks. Given the strong effects demonstrated in this study by variables that we controlled for, we recommend that future research investigate the theoretical linkages between both apathy and CSE with information security.

Management implications

There are also several implications for managers that this research has highlighted. 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 individuals have the ability to bypass technical security solutions, it is important that management recognize the key position of the individual in their security efforts. The effects of the control variables, apathy and CSE, also have strong managerial implications. As apathy negatively impacts individual precaution-taking behaviors, it is important that line managers 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 CSE emphasizes the need to train all members of the organization in computer use. 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 insignificant impact of rewards in the security context may also indicate that endeavoring to keep computer systems secure may be considered by most individuals as 'part of the job' instead of an activity that would require additional effort and thus be worth the reward. As such rewards do not appear to have the desired impact. Management should focus on the specification and evaluation of information security policies rather than introducing an additional incentive policy to motivate employees.

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.

Limitations and 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. Although 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, this study focused only on formal specification, evaluation, and reward. It is likely that the presence of a strong security culture (as manifested in informal modes of control or subjective norms) might explain additional variance, and should be the topic of future studies as well as incorporating other aspects such as punishment or other theoretical lenses such as those used in the theory of planned behavior (Ajzen, 1985) to more effectively understand the effects of control on security. Finally, this study used individuals that are employed in the health-care industry and, given the nature of the industry and the implementation of federal health privacy laws; it could be argued that this group is more accepting of formal controls than those in a different setting, therefore affecting the generalizability of the study. A comparison of these scores with scores obtained from the IS department used in the pilot test ($n = 80$) show approximately the same results, both in terms of effect and direction. This suggests that the results are not dependent on the industry of the respondents. However, it could be that IS professionals are just as security aware, or more so, as those in the health-care industry. Future research could investigate the model in different settings to strengthen its generalizability.

This research offers several contributions to the literature. First, it looks at a topic that is underresearched: 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, the major contribution of this study is the explicit introduction to the control literature of 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 although the specification and evaluation aspects of information security policies are integral to whether an individual views 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 CSE 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.

About the authors

Scott R. Boss (Ph.D., University of Pittsburg), is Assistant Professor of Accountancy at Bentley University, U.S.A. His research concentrates on information security and control at both the individual and group levels. He has presented papers at many conferences and is active in several professional groups.

Laurie J. Kirsch (Ph.D., University of Minnesota), is Professor of Business Administration at the University of Pittsburgh, U.S.A. Her research explores the management of IS projects and initiatives. She has published her work in leading scholarly journals, has served on numerous editorial boards, and is active in several professional groups.

Ingo Angermeier, President/CEO of Spartanburg Regional Healthcare System, has more than 35 years' experience in teaching hospitals and multi-specialty group practices. He has served as Assistant Dean and Professor in two medical schools, published more than two dozen papers in professional journals, and lectured widely throughout the United States.

Raymond A. Shingler is the CIO/VP of Support Services at Spartanburg Regional Healthcare System in Spartanburg, South Carolina. His responsibilities include data and voice systems and system-wide support services. Previously, he served as the VP/CIO at Peninsula Regional Medical and Director of IT at Salisbury University, Salisbury, Maryland.

R. Wayne Boss is Professor of Management in the Leeds School of Business at the University of Colorado, Boulder Campus. Dr. Boss is the editor of the *Organization Development and Change Newsletter* for the Academy of Management and serves on the editorial boards of several major professional journals.

References

AJZEN I (1985) From intentions to actions: a theory of planned behavior. In *Action Control, from Cognition to Behavior* (KUHL J, and BECKMANN J, Eds), pp 11–39, Springer-Verlag, Berlin, NY.

AMERICAN NATIONAL STANDARDS INSTITUTE (2005) *Iso ics 35 Information Technology*. American National Standards Institute, Washington DC.

ARMSTRONG JS and OVERTON TS (1977) Estimating nonresponse bias in mail surveys. *Journal of Marketing Research* **14(3),** 396–402.

BARON RM and KENNY DA (1986) The moderator mediator variable distinction in social psychological-research – conceptual, strategic, and statistical considerations. *Journal of Personality and Social Psychology* **51(6),** 1173–1182.

BIRNBERG JG and SNODGRASS C (1988) Culture and control – a field-study. *Accounting Organizations and Society* **13(5),** 447–464.

BLUMSTEIN A (1978) Introduction. In *Deterrence and Incapacitation: Estimating the Effects of Criminal Sanctions on Crime Rates* (BLUMSTIEN A, COHEN J and NAGIN D, Eds), National Academy of Sciences, Washington DC.

BROWN SA, MASSEY AP, MONTOYA-WEISS MM and BURKMAN JR (2002) Do I really have to? User acceptance of mandated technology. *European Journal of Information Systems* **11(4),** 283–295.

CARDINAL LB (2001) Technological innovation in the pharmaceutical industry: the use of organizational control in managing research and development. *Organization Science* **12(1),** 19–36.

CARDINAL LB, SITKIN SB and LONG CP (2004) Balancing and rebalancing in the creation and evolution of organizational control. *Organization Science* **15(4),** 411–431.

CARMINES EG and ZELLER RA (1979) *Reliability and Validity Assessment*. Sage Publications, Beverly Hills, CA.

CHAE B and POOLE MS (2005) Mandates and technology acceptance: a tale of two enterprise technologies. *Journal of Strategic Information Systems* **14(2),** 147–166.

CHARLTON JP and BIRKETT PE (1995) The development and validation of the computer apathy and anxiety scale. *Journal of Educational Computing Research* **13(1),** 41–59.

CHIN WW (1998) The partial least squares approach for structural equation modeling. In *Modern Methods for Business Research* (MARCOULIDES GA, Ed), pp 295–336, Lawrence Erlbaum, Mahwah, NJ.

CHIN WW and GOPAL A (1995) Adoption intention in gss – relative importance of beliefs. *Data Base for Advances in Information Systems* **26(2–3),** 42–64.

CHOUDHURY V and SABHERWAL R (2003) Portfolios of control in outsourced software development projects. *Information Systems Research* **14(3),** 291–314.

CHOW CW, HIRST M and SHIELDS MD (1995) 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,** 1–15.

COHEN J (1977) *Statistical Power Analysis for the Behavioral Sciences*. Academic Press, New York.

COMPEAU DR and HIGGINS CA (1995) Computer self-efficacy – development of a measure and initial test. *MIS Quarterly* **19(2),** 189–211.

COREN M (2005) *Experts: Cyber-Crime Bigger Threat than Cyber-Terror*. Cable News Network LP, LLLP, Atlanta, GA.

D'AQUILA JM (2001) Financial accountants' perceptions of management's ethical standards. *Journal of Business Ethics* **31(3),** 233–244.

DAS TK and TENG BS (1998) Between trust and control: developing confidence in partner cooperation in alliances. *Academy of Management Review* **23(3),** 491–512.

DECI EL and RYAN RM (2002) *Handbook of Self-determination Research*. University of Rochester Press, Rochester, NY.

DHILLON G (2001) Violation of safeguards by trusted personnel and understanding related information security concerns. *Computers & Security* **20(2),** 165–172.

DOPUCH N, BIRNBERG JG and DEMSKI JS (1982) *Cost Accounting: Accounting Data for Management's Decisions*. Harcourt Brace Jovanovich, New York.

DUTTA A and MCCROHAN K (2002) Management's role in information security in a cyber economy. *California Management Review* **45(1),** 67–87.

EISENHARDT KM (1985) Control: organizational and economic approaches. *Management Science* **31(2),** 134–149.

EISENHARDT KM (1988) Agency-theory and institutional-theory explanations – the case of retail sales compensation. *Academy of Management Journal* **31(3),** 488–511.

FALK A and KOSFELD M (2004) *Distrust – The Hidden Cost of Control*. National Bureau of Economic Research, Cambridge, MA.

FORNELL C and LARCKER DF (1981) Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research* **18(1),** 39–50.

FREDERICKSON JR and WALLER W (2005) Carrot or stick? Contract frame and use of decision-influencing information in a principal-agent setting. *Journal of Accounting Research* **43(5),** 709–733.

GARFINKEL S, SPAFFORD G and SCHWARTZ A (2003) *Practical Unix and Internet Security*. O'Reilly, Beijing, Sebastopol, CA.

HARTWICK J and BARKI H (1994) Explaining the role of user participation in information-system use. *Management Science* **40(4),** 440–465.

HASAN B (2006) Delineating the effects of general and system-specific computer self-efficacy beliefs on is acceptance. *Information & Management* **43(5),** 565–571.

HU Q, HART P and COOKE D (2007) The role of external and internal influences on information systems security – a neo-institutional perspective. *Journal of Strategic Information Systems* **16(2),** 153–172.

JAWORSKI BJ (1988) Toward a theory of marketing control: environmental context, control types, and consequences. *Theory of Marketing Control* **52,** 23–39.

KADAM A (2002) Writing an information security policy. *Network Magazine*. Indian Express Group, Mumbai, India.

KARAHANNA E and STRAUB DW (1999) The psychological origins of perceived usefulness and ease-of-use. *Information & Management* **35(4),** 237–250.

KELMAN HC (1958) Compliance, identification, and internationalization: three processes of attitude change? *Journal of Conflict Resolution* **2(1),** 51–60.

KELMAN HC (1961) Processes of opinion change. *Public Opinion Quarterly* **25(1),** 57–78.

KENNY DA, KASHY DA and BOLGER N (1998) The handbook of social psychology. In *The Handbook of Social Psychology* (GILBERT DT, FISKE ST and LINDZEY G, Eds), pp 233–265, McGraw-Hill, Boston, NY.

KIRSCH LJ (1996) The management of complex tasks in organizations: controlling the systems development process. *Organization Science* **7(1),** 1–21.

KIRSCH LJ (1997) Portfolios of control modes and is project management. *Information Systems Research* **8(3),** 215–239.

KIRSCH LJ (2004) Deploying common solutions globally: the dynamics of control. *Information Systems Research* **15(4),** 374–395.

KIRSCH LJ, SAMBAMURTHY V, KO DG and PURVIS RL (2002) Controlling information systems development projects: the view from the client. *Management Science* **48(4),** 484–498.

LIANG HG, SARAF N, HU Q and XUE YJ (2007) Assimilation of enterprise systems: the effect of institutional pressures and the mediating role of top management. *MIS Quarterly* **31(1),** 59–87.

LIM VKG, TEO TSH and LOO GL (2002) How do I loaf here? Let me count the ways. *Communications of the ACM* **45(1),** 66–70.

LORANGE P and SCOTT-MORTON MS (1974) A framework for management control systems. *Sloan Management Review* **16(1),** 47–56.

LUFT J (1994) Bonus and penalty incentives contract choice by employees. *Journal of Accounting & Economics* **18(2),** 181–206.

MACAULAY S and COOK S (1994) Performance management as the key to customer service. *Industrial and Commercial Training* **26(11),** 3–8.

MALHOTRA Y and GALLETTA D (2005) A multidimensional commitment model of volitional systems adoption and usage behavior. *Journal of Management Information Systems* **22(1),** 117–151.

MALHOTRA Y, GALLETTA DF and KIRSCH LJ (2008) How endogenous motivations influence user intentions: beyond the dichotomy of extrinsic and intrinsic user motivations. *Journal of Management Information Systems* **25(1),** 267–299.

MARKUS ML (1983) Power, politics, and mis implementation. *Communications of the ACM* **26(6),** 430–444.

MATHIESON K, PEACOCK E and CHIN WW (2001) Extending the technology acceptance model: the influence of perceived user resources. *Database for Advances in Information Systems* **32(3),** 86–112.

MILGRAM S (1974) *Obedience to Authority; an Experimental View*. Harper & Row, New York.
NATIONAL CYBER SECURITY ALLIANCE (2005) *Top Ten Cybersecurity Tips*. National Cyber Security Alliance, Washington DC.
NATIONAL CYBER SECURITY ALLIANCE AND MCAFEE CORPORATION (2008) *Mcafee-ncsa Online Safety Study*. National Cyber Security Alliance and McAfee Corporation, Washington DC.
NIDUMOLU SR and SUBRAMANI MR (2003) The matrix of control: combining process and structure approaches to managing software development. *Journal of Management Information Systems* **20(3)**, 159–196.
NUNNALLY JC and BERNSTEIN IH (1994) *Psychometric Theory*. McGraw-Hill, New York.
OUCHI WG (1977) Relationship between organizational-structure and organizational control. *Administrative Science Quarterly* **22(1)**, 95–113.
OUCHI WG (1979) Conceptual-framework for the design of organizational control mechanisms. *Management Science* **25(9)**, 833–848.
PETTER S, STRAUB D and RAI A (2007) Specifying formative constructs in information systems research. *MIS Quarterly* **31(4)**, 623–656.
PODSAKOFF PM, MACKENZIE SB, LEE JY and PODSAKOFF NP (2003) Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of Applied Psychology* **88(5)**, 879–903.
RAWSTORNE P, JAYASURIYA R and CAPUTI P (1998) An integrative model of information systems use in mandatory environments. In *International Conference on Information Systems* pp 325–330, Association for Computing Machinery, Helsinki, Finland.
ROSS ST (1999) *Unix System Security Tools*. McGraw-Hill, New York.
RYAN RM and DECI EL (2000) Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *American Psychologist* **55(1)**, 68–78.
SCHNEDLER W and VADOVIC R (2007) *Legitimacy of Control*. Institute for the Study of Labor (IZA), Bonn, Germany.
SCHNEIDER FW, GRUMAN JA and COUTTS LM (2005) *Applied Social Psychology: Understanding and Addressing Social and Practical Problems*. Sage Publications, Thousand Oaks, CA.
SHROUT PE and BOLGER N (2002) Mediation in experimental and nonexperimental studies: new procedures and recommendations. *Psychological Methods* **7(4)**, 422–445.
SNELL SA (1992) Control-theory in strategic human-resource management – the mediating effect of administrative information. *Academy of Management Journal* **35(2)**, 292–327.
STRAUB DW (1990) Effective is security: an empirical study. *Information Systems Research* **1(3)**, 255–273.
STRAUB DW and WELKE RJ (1998) Coping with systems risk: security planning models for management decision making. *MIS Quarterly* **22(4)**, 441–469.
SUSSMAN SW and SIEGAL WS (2003) Informational influence in organizations: an integrated approach to knowledge adoption. *Information Systems Research* **14(1)**, 47–65.
SYMANTEC CORPORATION (2007) *Symantec Reports Rise in Data Theft, Data Leakage, and Targeted Attacks Leading to Hackers' Financial Gain*. Symantec Corporation, Cupertino, CA.
TAYLOR S and TODD P (1995) Assessing it usage: the role of prior experience. *MIS Quarterly* **19(4)**, 561–570.
VENKATESH V and DAVIS FD (2000) A theoretical extension of the technology acceptance model: four longitudinal field studies. *Management Science* **46(2)**, 186–204.

Appendix A

See Table A1.

Table A1 Survey scale items (All items measured on a 7 point likert-type scale)

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 Poole (2005) and Hartwick and Barki (1994)	
Mand01	I am required to secure my system according to the organization's documented policies and procedures.
Mand02	It is expected that I will take an active role in securing my computer from cyber-attacks (hacking, virus infection, data corruption, etc.).
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.

Table A1 Continued

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 & 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 am too busy to be bothered by information security concerns.

Appendix B

See Table B1.

Table B1 Common method bias analysis

Item	*Substantive factor loading* (*R*1)	$R1^2$	*Common-method factor loading* (*R*2)	$R2^2$
Spec01	0.82**	0.67	0.09**	0.01
Spec02	0.74**	0.55	0.09**	0.01
Spec03	0.87**	0.75	0.11**	0.01
Spec04	0.85**	0.72	0.11**	0.01
Eval01	0.89**	0.79	0.11**	0.01
Eval02	0.89**	0.79	0.11**	0.01
Eval03	0.91**	0.83	0.11**	0.01
Eval04	0.85**	0.72	0.11**	0.01
Reward02	0.78**	0.61	0.07**	0.00
Reward03	0.85**	0.72	0.05**	0.00
Reward04	0.86**	0.74	0.05**	0.00
Mand01	0.83**	0.69	0.10**	0.01
Mand02	0.84**	0.70	0.10**	0.01
Mand03	0.81**	0.66	0.09**	0.01
Mand04	0.83**	0.69	0.09**	0.01
Precaut01	0.86**	0.74	0.08**	0.01
Precaut02	0.82**	0.67	0.07**	0.00
Precaut03	0.81**	0.66	0.07**	0.00
Average	0.84	0.71	0.09	0.01

**$P<0.01$.