European Journal of Information Systems (2011) 20, 267–284

www.palgrave-journals.com/ejis/

The influence of the informal social learning environment on information privacy policy compliance efficacy and intention

Merrill Warkentin[1], Allen C. Johnston[2] and Jordan Shropshire[3]

[1]Department of Management and Information Systems, College of Business, Mississippi State University, Mississippi State, MS, U.S.A.; [2]Department of Management, Information Systems, and Quantitative Methods, University of Alabama at Birmingham, Birmingham, AL, U.S.A.; [3]IT Department, Georgia Southern University, Statesboro, GA, U.S.A.

Correspondence: Merrill Warkentin, Department of Management and Information Systems, College of Business, Mississippi State University, 302 McCool Hall, P.O. Box 9581, Mississippi State, MS 39762-9581, U.S.A.
Tel.: +01 662 325 1955;
E-mail: m.warkentin@msstate.edu

Received: 29 September 2009
Revised: 19 April 2010
2nd Revision: 5 July 2010
3rd Revision: 30 November 2010
Accepted: 8 December 2010

Abstract
Throughout the world, sensitive personal information is now protected by regulatory requirements that have translated into significant new compliance oversight responsibilities for IT managers who have a legal mandate to ensure that individual employees are adequately prepared and motivated to observe policies and procedures designed to ensure compliance. This research project investigates the antecedents of information privacy policy compliance efficacy by individuals. Using Health Insurance Portability and Accountability Act compliance within the healthcare industry as a practical proxy for general organizational privacy policy compliance, the results of this survey of 234 healthcare professionals indicate that certain social conditions within the organizational setting (referred to as external cues and comprising situational support, verbal persuasion, and vicarious experience) contribute to an informal learning process. This process is distinct from the formal compliance training procedures and is shown to influence employee perceptions of efficacy to engage in compliance activities, which contributes to behavioural intention to comply with information privacy policies. Implications for managers and researchers are discussed.
European Journal of Information Systems (2011) **20,** 267–284.
doi:10.1057/ejis.2010.72; published online 25 January 2011

Keywords: external cues; privacy; learning; situational support; verbal persuasion; vicarious experience

Introduction

An increasing body of legislative provisions and standards requires that the privacy and confidentiality of information about students, employees, patients, consumers, citizens, and others be protected and secured (Mercuri, 2004; Robinson, 2005; Radcliff, 2007). Many of these regulatory requirements impose significant burdens on individual employees to maintain compliant positions. Clerks, salespersons, customer service representatives, bankers, professors, doctors, nurses, government officials, and others who directly interact with the public (customers, members, students, patients, etc.) must ensure that their communication exchanges (whether in person or via various electronic means) comply with a variety of requirements governing the format, presentation, distribution, maintenance, storage, and archiving of various data and information items (Langender & Cook, 2004). See Appendix A for further information about selected regulations and standards around the world. Without vigilant compliance by each and every employee, an employer may fail to

be in compliance, thereby exposing the organization to significant liability from regulators or from lawsuits. A survey of over 200 senior managers of healthcare organizations reveals that data breaches in the U.S. alone cost the healthcare industry $6 billion annually (Horowitz, 2010).

Given the present state of privacy compliance among both public and private sector entities – as evident by the American Institute of Certified Public Accountants' (AICPA) recent ranking of privacy compliance as the second most important managerial concern with regard to technology management – it is imperative that organizations devote sufficient attention and resources to the pursuit of privacy compliant behaviour for all employees (Lacey, 2009). CIOs must focus on all aspects of handling sensitive information, and must ensure that all employees who interact with such information and with the public understand and implement the organization's policies and procedures. Unfortunately, within an organizational setting, each employee represents a source of threat to the organization's security and privacy regulation compliance and without proper compliance behaviour from each employee, compliance by the organization is unlikely (Siponen, 2001; Furnell *et al*., 2002; Warkentin & Willison, 2009).

To achieve this imperative, many organizations (1) implement formal Security Education, Training, and Awareness (SETA) programmes (Furnell *et al*., 2002; Whitman & Mattord, 2004), (2) monitor policy compliance (electronically and through behaviour observation), and (3) seek to establish an environment that is conducive to employee motivation and intentions to comply with the information privacy policies. Because even a minor security infraction dealing with personal data can have significant consequences for a business or entity (Straub & Welke, 1998; Dhillon, 2001; Willison & Backhouse, 2006), practitioners and researchers must better understand how the informal social learning environment (as opposed to formal training) can influence employee behaviours that will ensure the privacy and confidentiality of the patrons who entrusted their sensitive information to the organization (Vogt, 2005). Further, scholars suggest that without the aid of SETA programmes and other measures, the information security and privacy techniques and procedures that organizations do have in place will eventually lose their effectiveness (Goodhue & Straub, 1989; Hoffer & Straub, 1989; Straub & Welke, 1998; Siponen, 2000).

Prior literature contains many studies that investigate the components of an effective formal training programme and the impact of formal training on employees (Mathieu *et al*., 1992; Sulsky & Kline, 2007). But is an *informal* social learning environment capable of supporting, enhancing, or perhaps alternatively, diminishing the levels of compliance efficacy and intentions among employees? There is little existing insight into how the social elements of an organizational setting, also called *external cues*, influence employee compliance outcomes. Moreover, when the compliance context concerns privacy and security policy compliance, the scope of empirical studies from which to inform current research becomes even narrower. Based on this gap in both the academic and the practitioner literature, the following research question is posed:

RQ: *How does the informal social learning environment in which employees operate influence employee perceptions of information privacy policy compliance efficacy and compliance intentions?*

These *external cues* exist in any social setting in which individuals are exposed to the thoughts, actions, and verbiage of others (Bandura, 1988; Gist & Mitchell, 1992). Such cues can be defined as potential sources of influences to an individual, but outside of the direct control of the individual (Gist & Mitchell, 1992). In terms of information privacy policy compliance support, external cues include workplace-related elements of the informal social learning environment in the form of resources, experiential learning opportunities, and verbal support from peers, instructors, or managers that have the potential to influence the compliance efficacy levels and compliance intentions of those employees that operate within that environment.

Given the regulatory requirements imposed on organizations within numerous industries, and the steady diet of reports of non-compliant sanctions imposed by federal regulatory oversight committees as previously described, research in the area of employee compliance with organizational security and privacy regulations remains necessary and highly desirable. Recent studies in this area (Herath & Rao, 2009; Johnston & Warkentin, 2010), while continuing to develop our understanding of compliance motivation and behavioural factors leading to non-compliance, have yet to consider the influence of cues in the informal environment in which employees operate and within which employees are expected to develop their individual capabilities toward and intentions about compliance.

We aim to illuminate certain vagaries associated with informal social learning experiences and to clearly identify how these external cues influence the perceptual outcomes associated with the informal social learning environment. We test an application of social learning theory in a unique context involving compliance efficacy and intentions. Further, the results provide promising insights for managers who seek to cultivate a learning environment in which compliance efficacy is elevated rather than weakened.

Theoretical framework and research model

Because employee compliance with security and privacy policies and procedures is so critical, the IS security and privacy research community has established a significant

stream of high-quality research that investigates this specific domain. A large number of studies (see Appendix B) have examined the issue of compliance or non-compliance with security and privacy policies, focusing on the intention and behaviour of employees and examining factors which either hinder or facilitate compliance with security policies. These studies lead us to understand that external cues are influential elements to an individual; however, this influence has not been examined in an *informal* social learning context, and their ability to influence perceptions of compliance beliefs and intentions has not previously been established. Social learning theory (Bandura, 1977) provides a framework for understanding the relationship of external cues and compliance attitudes as it specifically relates to the outcomes of an informal learning environment to the environmental factors and cognitive processes individuals experience as part of the learning process.

Social learning theory (Bandura, 1977) is a prominent theory for describing the interaction between an individual's knowledge, experiences, the environment in which the individual operates and the individual's behaviour (Rotter, 1960; Bandura, 1968, 1977; Crittenden, 2005). Social learning theory posits that an individual's behaviour is the result of a learning process that is dependent in part on the support present within the environment (situational support) (Bandura 1977), in part on the availability of vicarious learning opportunities (vicarious experience) (Kanfer & Ackerman, 1989), and in part on the feedback obtained from others (verbal persuasion). Further, Bandura (1977, 1988) contends that the learning process is continuous and that learning outcomes can evolve as these factors of situational support, vicarious experience, and verbal persuasion change.

By examining the antecedents of compliance self-efficacy from the perspective of social learning theory, a research model is formed that provides a unique framework for understanding the influence of an informal social learning environment on individual compliance outcomes. Our privacy compliance research model, illustrated in Figure 1, suggests that external cues within an informal social learning environment influence employee self-efficacy for completing compliance actions, and ultimately, behavioural intentions to comply. The inclusion of self-efficacy as a *mediating* factor between the effects of external cues on behavioural intent is purposeful and is positioned to remain consistent with the seminal works of Bandura (1977) in articulating social learning theory.

Based upon the theoretical framework described above, the following section provides support for the relationships illustrated in Figure 1 and presents the hypotheses of the present study. The research model and its associated hypotheses are grounded in and supported by extant literature in social learning theory and policy compliance.

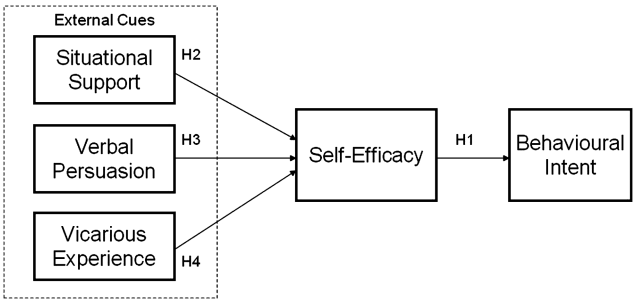

Figure 1 Privacy compliance learning model (*a priori*).

Hypotheses development

The concept of self-efficacy (Bandura, 1977) refers to one's beliefs in one's capabilities to successfully engage in (perform) a specific area of behaviour (or task). Put another way, self-efficacy is an individual's expectations of his or her ability to successfully navigate certain situations based on a perceived level of capability. Higher levels of self-efficacy are postulated to lead to approach *vs* avoidance behaviour. Self-efficacy expectations are behaviourally specific (rather than general), so each type of self-efficacy must be discussed in reference to a specific behavioural domain (a 'behavioural referent') in order to be meaningful. The concept has been applied to computer skills, learning skills, social skills, and others, such as mathematics, science, healthcare, repair, computers, and investing (Mathieu *et al*., 1993; Marakas *et al*., 1998; Torkzadeh & Van Dyke, 2002). Within the specific context of this study, self-efficacy is defined as an 'individual's judgment of his or her capability to engage in activities necessary to comply with information privacy policies, such as those stipulated by HIPAA'.

High levels of self-efficacy have been repeatedly shown to be associated with high levels of performance or achievement (Mathieu *et al*., 1993). Given that behavioural intent has also been shown to be an antecedent of actual behaviour, under the right facilitating conditions, the connection between self-efficacy and intent seems intuitive. Research grounded in the theory of planned behaviour further supports this notion, suggesting that self-efficacy mirrors perceived behavioural control in terms of its impact on behavioural intentions (Fishbein & Cappella, 2006). In fact, numerous studies support such a relationship (Hill *et al*., 1986, 1987; Carr & Sequeira, 2007). For instance, in a study of the effects of family business experiences on entrepreneurial behaviour, Carr & Sequeira (2007) draw upon the theory of planned behaviour in positioning self-efficacy as having a direct positive influence on entrepreneurial action. Their rationale was that intent will be at its highest level when individuals 'anticipate that they can perform the behaviour successfully' (Carr & Sequeira, 2007, p. 1091). Further, from a policy compliance perspective, the positive relationship between self-efficacy and behavioural intent has been demonstrated by Bulgurcu *et al*.

(2010) in their study of employee policy compliance. The works of Johnston & Warkentin (2010), Herath & Rao (2009), and Sasse *et al*. (2001) also support the role of self-efficacy in predicting policy compliance intention. Rhee *et al*. (2009) found not only that high levels of computer security self-efficacy led to increased behavioural intent to strengthen security effort, but also that self-efficacy was associated with more secure behaviours in practice. (They further suggest that future research should investigate the role of vicarious learning and other variables in strengthening security self-efficacy.) In the present study, we take a similar posture and posit that high levels of self-efficacy lead the employee to have higher levels of behavioural intent to comply with privacy policy requirements. As such, the following hypothesis is offered:

H1 *An individual's behavioural intent to comply with information privacy policy is positively influenced by his or her self-efficacy regarding the information privacy policy compliance.*

Applying a social learning theory perspective to compliance self-efficacy, Wexley & Latham (1991) determined that individuals are better prepared when they are exposed to vicarious experiences of others through observation, are provided with the opportunity to practice their newly gained knowledge, and are provided with feedback as to their performance in applying the newly acquired knowledge. These external cues of vicarious experience, situational support, and verbal persuasion have been demonstrated to directly influence levels of efficacy. It has also been suggested that the absence or poor conceived presence of any of these cues can had adverse effects on efficacy (Sulsky & Kline, 2007). By examining each cue separately, we are able to infer interesting relationships between the cue and an individual's perceptions of compliance efficacy.

Situational support

Previous research suggests that employee efficacy levels can be directly influenced by their informal social learning environment (Mathieu *et al*., 1992). Perceived levels of situational support within the learning environment, such as the presence of supportive materials, availability of help from others, support from supervisors or peers, or an adequate amount of time for task completion can influence expectations for success within the environment (Peters & O'Connor, 1980; Peters *et al*., 1988; Gist & Mitchell, 1992). For instance, Herath & Rao (2009) positioned resource availability as a direct antecedent of self-efficacy, contending that 'the presence of facilitating resources is likely to result in higher levels of self-efficacy whereas the absence of facilitating resources can represent a barrier to undertaking an action and thus, result in lower levels of self-efficacy' (p. 112). Leach (2003) further supports this reasoning and contends that the resources provided by a company in support of desired security behaviours among their employees will ultimately dictate the level of employee confidence needed to perform the desired compliance activities.

From a learning perspective, Mathieu *et al*. (1992) determined that severe constraints in situational support led to decreased levels of learning by reducing the motivation of the employees to perform well in learning opportunities or in their jobs (Phillips and Freedman, 1984). As these and other scholars espouse, unmotivated employees are less aware of and less receptive to learning opportunities (Ralls & Klein, 1991; Mathieu *et al*., 1992). As a result, the employees gain less from their learning opportunities and perceive less value from their informal social learning experiences (Mathieu *et al*., 1992). Conversely, environments that provide sufficient supportive resources, encourage employee compliance, and allow for an adequate amount of time for compliance could be perceived by employees as supportive and motivate them to actively engage compliance learning activities, thereby leading to higher levels of perceived self-efficacy. Based on this logic, the following hypothesis is offered:

H2 *An individual's perception of information privacy compliance self-efficacy is positively influenced by situational support.*

To obtain a more complete understanding of the factors that influence perceptions of information privacy compliance self-efficacy we must also look to the works of Bandura (1977, 1988) and Gist & Mitchell (1992), who suggest that organizations provide much more than mere situational support to their employees' learning efforts. Verbal persuasion and vicarious experience are also important factors leading to the successful learning. Similar to situational support, these factors are described as external cues, or factors outside of the control of the individual but within the auspices of the firm. Also similar to situational support, verbal persuasion and vicarious experience are perceptual and are evaluated at the individual level by those who have been exposed to them within the firm.

Verbal persuasion

Verbal persuasion refers to feedback or instructions which are intended to support an individual's ability to perform a given task (Bandura, 1977; Bandura & Cervone, 1986). The more supportive the feedback a person receives about accomplishing a task, the more that person is motivated to complete the task successfully (Bandura, 1986; Bandura & Cervone, 1986). Bandura & Cervone (1986) determined that the use of feedback which addresses the differential between a person's performance and that of a standard or aspiration is an effective means of modifying perceptions and attitudes.

Numerous studies have investigated the effects of verbal persuasion in various forms across various contexts. For instance, Anderson (1995) found verbally persuasive messages from a friend to be instrumental in motivating a driver to avoid driving while intoxicated. Also, Van Vianen (1999) determined verbal persuasion to be a significant factor leading to the formulation of ambition for a managerial position. Verbal persuasion is particularly effective if it is focused beyond merely supporting the individual to complete a particular task (Schunk, 1983; 1984). The more descriptive the feedback is in terms of outlining performance expectations, the more it impacts the person's feelings regarding the task (Bandura & Cervone, 1986).

In the context of this study, it is asserted that verbal persuasion within the informal social learning environment will motivate employees to be alert and engaged in learning opportunities, thereby ultimately enhancing their perceptions of compliance self-efficacy. Several recent studies support this contention, including Johnston & Warkentin's (2010) study in which it was established that persuasive messages from peers and colleagues can positively influence an individual's intention to comply with recommended security actions by stimulating the individual's perceived level of self-efficacy to successfully accomplish the recommended actions. Leach (2003) also sites verbal persuasion ('what they are told') as an influential factor, capable of strengthening an employee's efficacy toward the prevention of internal security threats. Based on this logic, the following hypothesis is posited:

H3 *An individual's perception of information privacy compliance self-efficacy is positively influenced by verbal persuasion.*

Vicarious experience

Vicarious experience, another external cue of perceived self-efficacy, refers to an individual's indirect experience with a task through observation (Bandura, 1977; Kanfer & Ackerman, 1989; Gist & Mitchell, 1992). From the early works of Bandura (1977), vicarious experience is a key element of social learning theory and has been attributed to the attainment of desired outcomes due to its direct positive impact on the efficacy levels of those in observation (Barclay, 1982). Further, vicarious experience through behavioural modelling has been established as a critical determinant of successful learning outcomes, especially when the modelling occurs in the informal, day-to-day type scenario (Manz & Sims Jr., 1981). For instance, Compeau & Higgins (1995) determined that when some employees were provided the opportunity to observe other employees interacting with a computer in their usual work setting, the self-efficacy levels of the observing employees increased significantly.

Frequently, organizations either promote or require their employees to spend some amount of time in observation of the actions of others. For new hires, especially, this time spent 'shadowing' a more experienced colleague or peer can be beneficial in helping them to gain the confidence needed to complete those tasks expected of them. Within the context of information privacy policy compliance, it is expected that employees will be motivated to perform tasks pertaining to the protection of information privacy by observing the practices of others. Recent studies support this contention, including Vroom & von Solms (2004), Leach (2003), and Workman *et al*. (2008), suggesting that the efficacy of employees to take appropriate security actions is positively influenced by what they see around them and the behaviour of others. As such, the following hypothesis is offered:

H4 *An individual's perception of information privacy compliance self-efficacy is positively influenced by vicarious experiences.*

These external cues are not controllable by the individual, but are elements of an environment, be it a workplace or any other organizational setting (Gist & Mitchell, 1992). These cues act to alter employee perceptions concerning information privacy policy compliance and the actions necessary to meet that goal. The following section describes the methods for testing the conceptual model and its associated hypotheses.

Method

Study context and sample

As a strategic objective, organizations seek to ensure a high level of compliance with emerging privacy policies, especially when they are backed by significant regulatory sanctions or legal liability. In order to test our hypotheses, we sought an organizational environment in which privacy compliance is paramount. Given the regulatory requirements imposed on patient information privacy protection, the healthcare industry serves as an excellent test bed from which to investigate the research questions posed by this study. The Health Insurance Portability and Accountability Act (HIPAA) is a U.S. regulation designed to protect the privacy and confidentiality of patient medical information. This legislation includes both security and privacy provisions (Fedorowicz & Ray, 2004; Robinson, 2005). Whereas the security component of HIPAA is intended to stipulate those mechanisms necessary to protect patient information, the privacy element addresses the issues of limitations, responsibility, and access and control. For this paper, HIPAA serves as a proxy for privacy policy to which employees must comply and to which organizations must provide appropriate formal training so as to facilitate compliance by their employees. In fact, it can be argued that HIPAA offers the ideal standardized

formalized privacy policy in widespread use as a compliance mandate for a large population of individuals (Shen *et al*., 2006).

The unit of analysis for this research project is the individual employee of a healthcare organization, termed a 'healthcare professional'. Such individuals include nearly all staff (employees) of organizations that provide healthcare services to individuals (patients). They may include medical personnel (physicians, physician's assistants, nurses, lab technicians, specialists, and other medical personnel) and administrative (non-medical) staff members (managers, clerks, insurance specialists, administrative assistants, and other non-medical personnel).

We initially contacted 11 individuals (medical and administrative professionals) in nine separate and diverse healthcare organizations. These included four senior nurses at two separate large hospitals and a large university health centre, a resident intern at a teaching hospital, an IT Director at a military base, and other administrative and medical personnel at a physical therapy facility, a mental healthcare facility, a low-income clinic, and several smaller physician clinics. Each first-level contact (or 'sampling seed') was asked to forward the invitation email to their colleagues within their divisions or departments at their organization and to ask those recipients to also forward the email to other healthcare professionals. The potential maximum number of recipients could be assumed to include all employees of the nine organizations, which numbered over 2000 at that time. The seeds of this respondent-driven sampling method (also known as snowball sampling) were diverse in terms of healthcare specialization, age, gender, geographic region, and other characteristics. However, this method has been challenged due to possible self-selection bias or bias that may arise when the topic of the survey is controversial (such as drug use) or when differences in the size of social networks is a factor (e.g. when some recipients have many more contacts than others, which could adversely affect the outcome of research in marketing trends, etc.). None of these reported biases was deemed to apply to the focus of the present study. In fact, Salganik & Heckathorn (2004) suggest that respondent-driven sampling methods can generate results which 'are asymptotically unbiased no matter how the seeds were selected' (p. 193). Recognizing that bias can result from every sampling method, we find no reason to presume that our use of the respondent-driven sampling method resulted in any unacceptable bias that would jeopardize the results.

Of the entire sampling frame described above, a total of 234 healthcare professionals responded to the survey, of which 202 responses were valid and usable for analysis. Each of the participants was initially screened using a filtering question on the survey to ensure that they indeed handled private information and were subsequently subject to HIPAA. A total of 115 (60%) of the respondents were female, while 72 (36%) were between the ages of 26 and 39. The majority of the respondents were employed in either public hospitals (37%) or private hospitals (28%), with 71% of them employed at facilities with 250 or more employees. Also, 46% of the respondents have been healthcare professionals for at least 10 years.

Prior to measure validation and model testing, the responses were analysed in order to identify response set (Rennie, 1982). A response set is the tendency among subjects to respond to questions in a particular way independently of the content of the items (Kerlinger, 1973; Andrich, 1978). No cases of response set were detected. Additionally, two tests of common methods variance were employed. First, Harman's one factor test of common methods was conducted with satisfactory results. An additional test of partial correlation was also conducted (Podsakoff & Organ, 1986). This procedure stipulates that the first factor from the principal components analysis should be introduced into the PLS model as a control variable. This is based on the assumption that the first factor is the most likely to approximate CMV (if any bias exists). If the factor produces changes in variance, than it is assumed that CMV is present (Podsakoff *et al*., 2003). As anticipated, there were no significant changes in explained variance. Thus, it appears that common methods bias is not problematic.

Measures and instrumentation

The present study involves the measurement of five latent constructs, including self-efficacy, situational support, vicarious experience, verbal persuasion, and behavioural intent. These constructs were measured as follows:

- Self-efficacy (SEFF) was measured using eight reflective scale items. The items were adopted and modified from Bandura (1977) to reflect the context of this study.
- Behavioural intent (BINT) was represented by five reflective scale items. These scale items were originally developed by Fishbein & Ajzen (1975), and have since been used to predict a range of human behaviours (see Sheppard *et al*. (1988) for a review).
- Situational support (SS) was measured using six formative scale items. The items were adapted from Peters & O'Connor (1980) for this research.
- Vicarious experience (VE) was measured via seven formative scale items. The items were modified from Bandura (1977) to fit this specific context.
- Verbal persuasion (VP) was operationalized using seven formative scale items. These measures were adapted from Bandura (1977), and adapted for this research.

Items for self-efficacy were measured using five-point Likert scales, where '1' corresponded with 'nothing' and '5' corresponded with 'a great deal'. Behavioural intent, situational support, vicarious experience, and verbal persuasion were measured using seven-point Likert scales, where '1' corresponded with 'strongly disagree' and '7'

corresponded with 'strongly agree'. Appendix C presents the complete instrument used in this study.

Following established guidelines (Jarvis *et al*., 2003; Petter *et al*., 2007), the constructs and corresponding scales used in this study were categorized as either formative or reflective. As previously indicated, situational support, vicarious experience, and verbal persuasion were identified as formative, while self-efficacy and behavioural intent were recognized as reflective. Because biases may occur when formative constructs are misspecified as reflective (MacKenzie *et al*., 2005), the constructs were classified according to the decision rules outlined by Petter *et al*. (2007). In summary, these rules concern the direction of causality among constructs and items, and the interchangeability, covariation, and nomological net of the scale items.

Content validity for all instrument scales was established through both literature review and an expert panel comprised of 12 individuals in both academia and healthcare. Particularly for formative constructs, content validity is critical, as removal of items from formative scales must be theoretically driven and must not compromise scale robustness by removing items that capture critical dimensions of the latent variables (Diamantopoulos & Winklhofer, 2001; Straub *et al*. 2004; Petter *et al*. 2007). Based on the results of the content validity tests, a final survey instrument was produced consisting of 33 items. An additional seven questions were included for collecting demographic information such as gender, age, and workplace characteristics.

Results

As suggested by Gefen *et al*. (2000), the validity and reliability of the measures were assessed prior to hypothesis testing. Because the model included formative constructs, a components-based approach to structural equation modelling was taken; the calculations were performed using the SmartPLS software package (Ringle *et al*., 2005).

Analysis of reflective measures

Tests were conducted to evaluate the convergent and discriminant validity and the reliability of reflective measures. To begin, factor loadings were used to establish convergent validity. Loadings in excess of 0.70 on their respective factors are interpreted to indicate convergent validity (Straub *et al*., 2004). A second indicator of convergence was also employed. Here, a value above 0.50 for the average variance extracted (AVE) for each construct is assumed to indicate sufficient convergence. Tests results indicate that both of these conditions have been met (see Table 1).

Discriminant validity is demonstrated when the square root of the AVE is greater than the correlations between constructs (Bollen, 1989). (The square rooted AVEs for self-efficacy and behavioural intent are 0.7688 and 0.7221, respectively; their inter-construct correlation is 0.2103.) For a second test of discriminant validity, individual items may be assumed to possess sufficient discriminant validity if they load higher on their own respective construct than on any other latent variable (Gefen *et al*., 2000; Straub *et al*., 2004). As demonstrated in Table 1, this was true for all items. Based on both tests, the measures possess sufficient discriminant validity.

Table 1 Psychometric properties of reflective measures

Construct	*Item*	*Self-efficacy*	*Behavioural intent*	*AVE*	*Reliability*
Self-efficacy	SEFF1	0.7974	0.1053	0.591	0.875
	SEFF2	0.8193	0.1169		
	SEFF3	0.8871	0.1844		
	SEFF4	0.8776	0.1711		
	SEFF5	0.9032	0.2735		
	SEFF6	0.9396	0.2211		
	SEFF7	0.8967	0.2017		
	SEFF8	0.8927	0.1203		
Behavioural Intent	BINT1	0.2655	0.9334	0.536	0.738
	BINT2	0.1243	0.8474		
	BINT3	0.2421	0.7718		
	BINT4	0.1843	0.7973		
	BINT5	0.2389	0.7647		

Reliability is established by examining the internal consistency measure for each construct. Constructs which exceeded the 0.70 level are judged to possess sufficient reliability (Fornell *et al*., 1982). As shown in Table 1, the recommended threshold for construct reliability is exceeded.

Analysis of formative measures

Alternative tests of validity and reliability were conducted on the formative constructs: situational support, vicarious experience, and verbal persuasion (Petter *et al*., 2007). In order to assess convergent and discriminant validity, patterns of correlation between items and latent variables are depicted in a modified multi-trait, multi-method (MTMM) matrix (Loch *et al*., 2003). The matrix is depicted in Table 2.

Convergent validity is assessed via examination of item-construct correlations (Chin, 1995; Diamantopoulos & Winklhofer, 2001). If items load significantly on their corresponding constructs, convergent validity is demonstrated. The results indicate that item weights are significant at a 0.05 level of significance, with the exception of four indicators, SS3, VE2, VP1, and VP5. The four non-significant items were further analysed according to prescriptions for interpreting formatively measured construct results (Cenfetelli & Bassellier, 2009).

The prescriptions developed by Cenfetelli & Bassellier (2009) distinguish between the relative and absolute contribution of an indicator to its construct. Relative contribution is the relation between an indicator and a criterion while holding other predictors constant. It is the

Table 2 Psychometric properties of formative measures

	SS1	*SS2*	*SS3*	*SS4*	*SS5*	*SS6*	*SS*	*VE1*	*VE2*	*VE3*	*VE4*	*VE5*	*VE6*	*VE7*	*VE*	*VP1*	*VP2*	*VP3*	*VP4*	*VP5*	*VP6*	*VP7*	*VP*
SS1	—																						
SS2	0.643	—																					
SS3	0.562	0.711	—																				
SS4	0.421	0.644	0.656	—																			
SS5	0.560	0.803	0.543	0.638	—																		
SS6	0.522	0.772	0.678	0.667	0.619	—																	
SS	0.661	0.902	0.761	0.712	0.802	0.789	—																
VE1	0.245	0.576	0.244	0.456	0.346	0.466	0.412	—															
VE2	0.463	0.471	0.471	0.387	0.571	0.565	0.554	0.633	—														
VE3	0.342	0.345	0.523	0.435	0.451	0.461	0.474	0.556	0.605	—													
VE4	0.385	0.457	0.536	0.516	0.343	0.345	0.517	0.702	0.564	0.542	—												
VE5	0.401	0.482	0.481	0.231	0.359	0.304	0.451	0.691	0.601	0.621	0.705	—											
VE6	0.273	0.408	0.456	0.324	0.453	0.345	0.449	0.730	0.599	0.633	0.533	0.685	—										
VE7	0.454	0.398	0.409	0.387	0.321	0.319	0.421	0.699	0.623	0.455	0.675	0.767	0.657	—									
VE	0.427	0.471	0.465	0.412	0.398	0.428	0.547	0.802	0.689	0.731	0.746	0.889	0.981	0.766	—								
VP1	0.432	0.432	0.430	0.655	0.390	0.458	0.408	0.601	0.549	0.549	0.401	0.485	0.399	0.453	0.577	—							
VP2	0.398	0.502	0.416	0.534	0.421	0.361	0.492	0.583	0.415	0.324	0.385	0.556	0.345	0.467	0.432	0.406	—						
VP3	0.476	0.574	0.602	0.503	0.502	0.403	0.596	0.621	0.487	0.463	0.532	0.513	0.487	0.546	0.534	0.598	0.656	—					
VP4	0.512	0.453	0.482	0.613	0.489	0.391	0.643	0.593	0.576	0.532	0.294	0.639	0.563	0.478	0.591	0.651	0.548	0.415	—				
VP5	0.533	0.528	0.510	0.502	0.620	0.498	0.510	0.607	0.583	0.576	0.453	0.289	0.392	0.459	0.536	0.519	0.491	0.386	0.655	—			
VP6	0.407	0.429	0.295	0.370	0.528	0.451	0.495	0.512	0.601	0.309	0.397	0.451	0.600	0.536	0.498	0.438	0.503	0.681	0.712	0.277	—		
VP7	0.565	0.436	0.420	0.491	0.471	0.514	0.361	0.539	0.723	0.384	0.380	0.578	0.587	0.630	0.520	0.673	0.487	0.436	0.590	0.475	0.627	—	
VP	0.547	0.446	0.537	0.479	0.539	0.438	0.592	0.601	0.538	0.467	0.471	0.604	0.591	0.321	0.637	0.691	0.771	0.831	0.799	0.639	0.743	0.724	—

importance of an indicator compared to other indicators of the same construct. Absolute contribution is the relation between an indicator and a criterion, ignoring other predictors. In some instances it is necessary to consider both perspectives, in order to develop a more accurate picture of an indicator's influence. For instance, an indicator may have a low or non-significant relative contribution to the construct. Despite this, it may still have an important absolute contribution. It is therefore recommended that when relative contribution (measured in terms of indicator weights) is low, absolute contribution (represented by item loadings) should also be considered.

Because four items in this study have a low relative contribution, it is necessary to consider their unique relations with their associated constructs. The absolute contributions for SS3, VE2, VP1, and VP5 are significant. Their values are 0.721, 0.761, 0.693, and 0.718, respectively. Thus, although the contributions of the indicators are relatively low compared to other indicators, they have a strong, bivariate relation to their respective constructs (Nunnally & Burnstein, 1994). Furthermore, there did not appear to be any patterns in wording, polarity, or content among the items that would account for the differences and no conceptual issues regarding the construct definitions were salient. Thus, there was no theoretical justification for removing the items and rather than discarding the items and changing the meaning of the constructs, it was determined that the items should be retained.

Finally, evidence of discriminant validity is presented when items correlate higher with their respective construct measures than with other construct measures and their composite values (Loch *et al.*, 2003). The results of the analysis indicate an acceptable level of discriminant validity (see Table 2).

Structural model

Because the model was comprised of reflective and formative constructs, bootstrap sampling was used to test the proposed relationships among the constructs (Gefen *et al.*, 2000). Path coefficients and *t*-values were obtained through this procedure, and are depicted in Table 3. The results indicate that all paths are significant at the $\rho < 0.05$ level of confidence.

To ensure that self-efficacy mediates the relationship between each of the external cues and behavioural intent, Baron & Kenny's (1986) steps for establishing mediation were followed. First, it was established that situational support, verbal persuasion, and vicarious experience are correlated with behavioural intent. Second, it was determined that each is related to self-efficacy. Third, self-efficacy was found to be related to behavioural intent. Situational support, verbal persuasion, and vicarious experience were then entered into the model, but their paths were statistically insignificant. Thus, as shown in Table 4, there is sufficient empirical support to conclude that self-efficacy mediates the relationship between the external cues (situational support, verbal persuasion, and vicarious experience) and behavioural intent.

The model's explanatory power was considered by observing the R^2 of endogenous constructs (Chin, 1998). As shown in Figure 2, the model accounts for 60.9% of the variance in self-efficacy and 43.7% of the variance in behavioural intent. All of the hypotheses are supported. Finally, several factors were introduced as controls on self-efficacy. They include job title, organization tenure, length of career as a healthcare professional, gender, age, training recency, format of training, and total number of employees at current location. It was found that training recency and total number of employees were significant ($\beta = 0.1261$, $\rho < 0.05$ and $\beta = 0.2142$, $\rho < 0.05$, respectively).

Table 3 Path coefficients and their *t*-values

Hypothesis	*Path coefficient (β)*	*t-Value*	*Significance*	*Outcome*
H_1: SEFF → BINT	0.3763	2.037	$\rho < 0.050$	Supported
H_2: SS → SEFF	0.3431	2.762	$\rho < 0.001$	Supported
H_3: VP → SEFF	0.2809	2.664	$\rho < 0.001$	Supported
H_4: VE → SEFF	0.3145	1.992	$\rho < 0.050$	Supported

Discussion

The findings of this study provide strong evidence for understanding the influence of an informal social learning environment on employee perceptions of information privacy policy compliance efficacy and intentions.

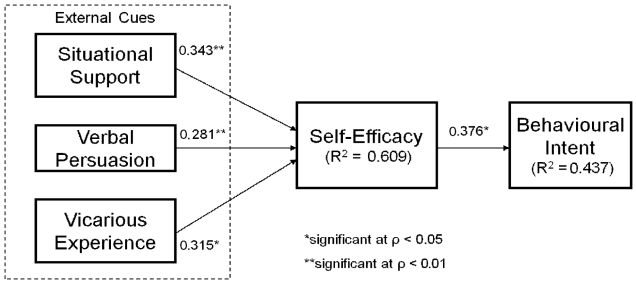

Figure 2 Privacy compliance learning model.

Table 4 Testing mediation effects of self-efficacy

External Cue	*Dependent variable: BINT*	*Dependent variable: SEFF*	*Dependent variable: BINT (SEFF included)*
SS	$\beta = 0.3121$, $\rho < 0.05$	$\beta = 0.2875$, $\rho < 0.05$	$\beta = 0.2185$, $\rho = 0.13$
VE	$\beta = 0.1463$, $\rho < 0.05$	$\beta = 0.3406$, $\rho < 0.05$	$\beta = 0.1409$, $\rho = 0.11$
VP	$\beta = 0.2846$, $\rho < 0.05$	$\beta = 0.1742$, $\rho < 0.05$	$\beta = 0.2863$, $\rho = 0.16$

The findings suggest that an employee's compliance intentions are formed in part by the direct influence of his or her compliance efficacy levels and indirectly from the external cues present within the informal social learning environment. These results can also provide guidance for both managerial and research endeavours involving employee policy compliance, in general, and information privacy policy compliance, specifically.

Managerial implications

Managers wishing to improve individual information privacy compliance should consider a programme aimed at improving employee perceptions of support for learning about policy compliance. Such a programme should focus on manipulating external cues – ambient factors which affect employee attitudes. Surprisingly, external cues are not often considered, even though they can be a cost-effective means of improving learning outcomes. For situational support, we suggest that managers provide time and materials that would signal to the individual employee the value the organization places on information privacy and compliance with information privacy policies and procedures. To enhance employee perceptions of verbal persuasion, we recommend that managers make reasonable efforts to convey the importance of the information privacy policies to the employees, as well as providing verbal feedback. Finally, to foster learning through vicarious experience, the IT managers could pair new employees with mentors, organize group learning exercises, and facilitate on-the-job training to enhance practical learning of information privacy procedures. Suggestions regarding the use of three external cues, perceived situational support, verbal persuasion, and vicarious experience, are provided in Table 5.

Table 5 Stimulating privacy compliance

External cues	*Suggested actions*
Situational support	• Provide adequate time for employees to complete activities which entail information privacy compliance • Supply all materials necessary for adhering to information privacy policies
Verbal persuasion	• Offer regular constructive feedback (both positive and negative) • Convey the importance of each employee's participation in formal information privacy training and policy compliance • Ask how the organization can improve its formal information privacy training and be prepared to field reasonable requests
Vicarious experience	• Pair experienced employees with new hires in learning exercises • Organize group learning exercises • Combine classroom training with on-the-job training to enhance practical learning of information privacy procedures

Research implications

The application of social learning theory to examine the influence of an informal social learning environment on employee compliance outcomes is unique to this study, but does provide numerous opportunities for future research in this area. For instance, while the majority of compliance research has focused on formal training outcomes, very few studies have focused on the informal aspects of a workplace and how elements within this workspace impact employee beliefs, attitudes, and perceptions related to compliance activities. As is evident from the results of this study, social learning theory provides a useful lens for conceptualizing the interactions that take place between an employee and his or her workplace environment. Also, social learning theory can be applied within the policy compliance context to determine the long-term effects of an informal social learning environment on compliance outcomes, perhaps uncovering attenuating or intensifying effects over time.

Future research directions

The present study provides strong support for establishing the antecedents of privacy regulation compliance self-efficacy by individual employees. Conducted among healthcare professionals, its findings can easily be generalized to other employees who must observe protocols to protect the privacy of other individual-level information. However, several limitations in our research offer opportunities for future research to continue this work.

Though we had over 200 respondents, they came from a handful of healthcare-related organizations and further research should be conducted within a large variety of organizations of all types throughout the country. Further, the actual link between self-efficacy and behaviour (actual compliance) should be established in this context, if possible. For example, laboratory experiments might be conducted to measure whether those professionals who report higher levels of intent will actually safeguard information more closely. Alternatively, independent measures for compliance behaviour, such as system logs or supervisory observations, could be utilized. Finally, it is possible that organizational size is an important antecedent if, for example, small facilities have smaller budgets for training, but may foster a more information-protective culture. Future research could target data collection specifically from large and small enterprises with sufficient statistical significance to explore this research question, and further information regarding organizational security budgets and organizational culture could be collected.

Conclusions

In many nations, the privacy of sensitive information is protected by a myriad of laws and restrictions, and the

job of ensuring compliance is increasingly falling on IT directors. The results of this investigation provide guidance to all managers concerned with regulatory compliance involving individual employee behaviour, especially where consumer privacy is concerned. To ensure that the staff actually complies with the privacy provisions of such regulations, managers must pursue technical and behavioural controls that have been proven to be effective in supporting the goals of such legislation.

Our findings indicate that social elements of an organizational setting (external cues) do influence employee information privacy compliance self-efficacy by manipulating the degree to which the employees perceive their informal social learning environment as either supportive or detrimental to their ability to carry out compliance activities. The study results suggest that organizations can provide a supportive work environment that facilitates high levels of compliance self-efficacy by ensuring that employees (1) are provided with the right tools and opportunities (situational support) to complete their jobs and actually protect the privacy of sensitive information, (2) are provided with adequate feedback and instruction (verbal persuasion) in support of privacy policy compliance, and (3) are given the opportunity to learn from each other (vicarious experience). The findings also indicate that these external cues also have a downstream influence on employee information privacy policy compliance intentions and that their influence is mediated by perceptions of self-efficacy.

In summary, as concerns over privacy regulations continue to shape the manner in which organizations manage consumer and employee data, managers, IT and otherwise, must ensure that their employees are properly supported in the management of sensitive data. Maximizing the effectiveness of the informal social learning environment is critical to the success of each employee and the entire organization toward compliance with privacy provisions. As such, management must consider any and all factors which may influence employee learning outcomes, including social factors critical to social learning opportunities. This study identified three social-oriented, supportive elements within organizational settings that have the potential to positively influence how employees react to learning opportunities and subsequently improve efficacy toward compliance actions. Understanding the source of employee perceptions is only a first step, but does give the organization an advantage in the compliance struggle.

About the authors

Dr. Merrill Warkentin is a Professor of MIS in the College of Business at Mississippi State University. He has published several books and over 150 research manuscripts, primarily focusing on computer security management, eCommerce, and virtual collaborative teams, in edited books, *Proceedings*, and in leading academic journals such as *MIS Quarterly*, *European Journal of Information Systems*, *Decision Sciences*, *Decision Support Systems*, *Information Systems Journal*, *Communications of the ACM*, *Communications of the AIS*, *Information Resources Management Journal*, *Journal of Organizational and End User Computing*, *Journal of Global Information Management*, and the *DATA BASE for Advances in Information Systems*. He is an Associate Editor for *European Journal of Information Systems*, the *MIS Quarterly* Special Issue on Security, *Information Resources Management Journal*, and the *Journal of Information Systems Security*. In 2009, he was the Co-Guest Editor of the *European Journal of Information Systems* Special Issue on Security. He has chaired several global conferences on computer security, including the pre-ICIS Workshop on Information Security and Privacy (WISP) and the IFIP Workshop on Information Security. He is the Vice Chair of IFIP Working Group 8.11/11.13 on Information Systems Security Research. Dr. Warkentin has also served as a consultant to numerous organizations and has served as National Distinguished Lecturer for the Association for Computing Machinery (ACM). His Ph.D. in MIS is from the University of Nebraska-Lincoln.

Dr. Allen C. Johnston is an Assistant Professor in the School of Business at the University of Alabama at Birmingham. He holds a BS from Louisiana State University in Electrical Engineering as well as an MSIS and Ph.D. in Information Systems from Mississippi State University. He has conducted research across several fronts in the area of information systems including e-commerce trust, technology adoption and diffusion, biometric systems, information technology governance, and intelligent agent design. However, the primary focus of his research has been in the area of information assurance and computer security, with a specific concentration on the behavioral aspects of information security and privacy. Johnston has over 30 articles published in journals, scholarly texts, as well as international, national, and regional conference proceedings. His works can be found in such outlets as *MIS Quarterly*, *Communications of the ACM*, *Journal of Global Information Management*, *Journal of Organizational and End User Computing*, *Journal of Information Privacy and Security*, and *DATA BASE for Advances in Information Systems*. He has also served as guest speaker and provided consultation services to numerous entities including Regions Financial Corporation, ISACA, the Birmingham Chapter of the Institute of Management Accountants, and the National Decision Sciences Institute.

Dr. Jordan Shropshire is an Assistant Professor of IT at Georgia Southern University. His research interests

include behavioral and technical aspects of information security, IT disaster recovery, technology diffusion, and measurement issues. His Ph.D. in information security is from Mississippi State University, and his undergraduate degree in business is from the University of Florida. His work has been published in several journals, including *Journal of Computer Information Systems*, *Behavior and Information Technology*, *Journal of Information Technology Management*, *Journal of Internet Banking and Commerce*, and *Information Management & Computer Security.*

References

ANDRICH D (1978) A rating formulation for ordered response categories. *Pyschometirka* **43(4),** 561–573.

ANDERSON C and AGARWAL R (2010) Practicing safe computing: a multimethod empirical examination of home computer user security behavioural intentions. *MIS Quarterly* **34(3),** 613–643.

ANDERSON RB (1995) Cognitive appraisal of performance capability in the prevention of drunken driving: a test of self-efficacy theory. *Journal of Public Relations Research* **7(3),** 205–229.

BARON R and KENNY D (1986) The moderator-mediator variable distinction in social psychological research: conceptual, strategic and statistical considerations. *Journal of Personality and Social Psychology* **51(1),** 1173–1182.

BARCLAY L (1982) Social learning theory: a framework for discrimination research. *Academy of Management Review* **7(4),** 587–594.

BANDURA A (1968) A social learning interpretation of psychological dysfunctions. In *Foundations of Abnormal Psychology* (LONGON D and ROSENHAM D, Eds), pp 293–344, Holt, Rinehart & Winston, New York, NY.

BANDURA A (1977) Self-efficacy: toward a unifying theory of behavioral change. *Psychological Review* **84(2),** 191–215.

BANDURA A (1986) *Social Foundations of Thought and Action*. Prentice-Hall, Englewood Cliffs, NJ.

BANDURA A (1988) Organizational applications of social cognitive theory. *Australian Journal of Management* **13(2),** 275.

BANDURA A and CERVONE D (1986) Differential engagement of self-reactive influences in cognitive motivation. *Organizational Behavior & Human Decision Processes* **38(1),** 92–114.

BLOOM PN, MILNE GR and ADLER R (1994) Avoiding misuse of information technologies: legal and societal considerations. *Journal of Marketing* **58(1),** 98–110.

BOLLEN K (1989) *Structural Equations with Latent Variables*. Wiley, New York, NY.

BOSS SR, KIRSCH LJ, ANGERMEIER I, SHINGLER RA and BOSS RW (2009) If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems* **18(2),** 151–164.

BULGURCU B, CAVUSOGLU H and BENBASAT I (2010) Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly* **34(3),** 523–548.

CARR J and SEQUEIRA J (2007) Prior family business exposure as intergenerational influence and entrepreneurial intent: a theory of planned behavior approach. *Journal of Business Research* **60(10),** 1090–1098.

CENFETELLI R and BASSELIER G (2009) Interpretation of formative measurement in IS research. *MIS Quarterly* **33(4),** 689–707.

CHIN W (1995) Partial least squares is to Lisrel as principal components analysis is to common factor analysis. *Technology Studies* **2,** 315–319.

CHIN W (1998) The partial least squares approach to structural equation modelling. In *Modern Methods for Business Research* (MARCOULIDES G, Ed.), pp 295–336, Lawrence Erlbaum Associates, Mahwah, NJ.

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

CRITTENDEN WF (2005) A social learning theory of cross-functional case education. *Journal of Business Research* **58(7),** 960–966.

D'ARCY J, HOVAV A and GALETTA D (2009) User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research* **20(1),** 79–98.

DHILLON G (2001) Violation of safeguards by trusted personnel and understanding related information security concerns. *Computers & Security* **20(2),** 165–173.

DIAMANTOPOULOS A and WINKLHOFER H (2001) Index construction with formative indicators: an alternative to scale development. *Journal of Marketing Research* **38(2),** 269–277.

DINEV T, BELLOTTO M, HART P, RUSSO V, SERRA I and COLAUTTI C (2006) Privacy calculus model in e-commerce – a study of Italy and the Unites States. *European Journal of Information Systems* **15(4),** 389–402.

FEDOROWICZ J and RAY A (2004) Impact of HIPAA on the integrity of healthcare information. *International Journal of Healthcare Technology & Management* **6(2),** 142–157.

FISHBEIN M and AJZEN I (1975) *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*. Addison-Wesley, Reading, MA.

FISHBEIN M and CAPPELLA JN (2006) The role of theory in developing effective health communications. *Journal of Communication* **56(s1),** s1–s17.

FORNELL C and BOOKSTEIN F (1982) Two structural equation models: LISREL and PLS applied to consumer exit-voice theory. *Journal of Marketing Research* **19,** 440–452.

FURNELL S, GENNATOU M and DOWLAND P (2002) A prototype tool for information security awareness and training. *Logistics Information Management* **15(5/6),** 352–357.

GEFEN D, STRAUB D and BOUDREAU M (2000) Structural equation modelling techniques and regression: guidelines for research practice. *Communications of AIS* **7(7),** 1–78.

GIST M and MITCHELL T (1992) Self-efficacy: a theoretical analysis of its determinants and malleability. *Academy of Management Review* **17(2),** 183–211.

GOODHUE DL and STRAUB DW (1989) Security concerns of system users: a proposed study of user perceptions of the adequacy of security measures. In *Proceedings of the 21st Hawaii International Conference on System Science* (HICSS), Kona, HA, January.

GUPTA A (2008) Prescription for change. *Wall Street Journal*, 20 October.

HERATH T and RAO HR (2009) Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems* **18(2),** 106–125.

HILL T, SMITH N and MANN M (1986) Communicating innovations: convincing computer phobics to adopt innovative technologies. In *Advances in Consumer Research* (LUTZ RJ, Ed.), pp 419–422, Association for Consumer Research, Provo, UT.

HILL T, SMITH N and MANN M (1987) Role of efficacy expectations in predicting the decision to use advanced technologies: the case of computers. *Journal of Applied Psychology* **72(2),** 307–313.

HOFFER JA and STRAUB DW (1989) The 9 to 5 underground: are you policing computer crimes? *Sloan Management Review* **30(4),** 35–43.

HOROWITZ BT (2010) Data breaches cost health care industry $6 billion annually. *eWeek Magazine*, 10 November.

JARVIS C, MACKENZIE S, PODSAKOFF P and MICK D (2003) A critical review of construct indicators and measurement model misspecification in marketing and consumer research. *Journal of Consumer Research* **30(2),** 199–218.

JOHNSTON AC and WARKENTIN M (2010) Fear appeals and information security behaviours: an empirical study. *MIS Quarterly* **34(3),** 549–566.

KANFER R and ACKERMAN PL (1989) Motivation and cognitive abilities: an integrative/aptitude-treatment interaction approach to skill acquisition. *Journal of Applied Psychology* **74(4),** 657–690.

KERLINGER F (1973) *Foundations of Behavioral Research* 2nd edn, Holt Reinhart & Winston, London, UK.

LANGENDERFER J and COOK DL (2004) Oh, what a tangled web we weave: the state of privacy protection in the information economy and recommendations for governance. *Journal of Business Research* **57(4),** 734–747.

LEACH J (2003) Improving user security behaviour. *Computers & Security* **22(8),** 685–692.

LACEY D (2009) *Managing the Human Factor in Information Security: How to Win Over Staff and Influence Business Managers*. John Wiley and Sons, New York.

LEE Y and LARSEN KR (2009) Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems* **18(2),** 177–187.

LOCH K, STRAUB D and KAMEL S (2003) Diffusing the internet in the Arab world: the role of social norms and technological culturation. *IEEE Transactions on Engineering Management* **50(1),** 45–64.

MACKENZIE S, PODSAKOFF P and JARVIS C (2005) The problem of measurement model misspecification in behavioral and organizational research and some recommended solutions. *Journal of Applied Psychology* **90(4),** 710–730.

MANZ CC and SIMS Jr. HP (1981) Vicarious learning: the influence of modeling on organizational behavior. *Academy of Management Review* **6(1),** 105–113.

MARAKAS G, YI M and JOHNSON R (1998) The multilevel and multifaceted character of computer self-efficacy: toward clarification of the construct and an integrative framework for research. *Information Systems Research* **9(2),** 126–163.

MATHIEU JE, MARTINEAU JW and TANNENBAUM SI (1993) Individual and situational influences on the development of self-efficacy: implications for training effectiveness. *Personnel Psychology* **46(1),** 125–147.

MATHIEU JE, TANNENBAUM SI and SALAS E (1992) Influences of individual and situational characteristics on measures of training effectiveness. *Academy of Management Journal* **35(4),** 828–847.

MERCURI RT (2004) The HIPAA-potamus in health care data security. *Communications of the ACM* **47(7),** 25–28.

MYYRY L, SIPONEN M, PAHNILA S, VARTIAINEN T and VANCE A (2009) What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems* **18(2),** 126–139.

NUNNALLY JC and BERNSTEIN IH (1994) *Psychometric Theory*. McGraw-Hill, New York, NY.

PAHNILA S, SIPONEN M and MAHMOOD A (2007) Employees' behavior towards IS security policy compliance. In *Proceedings of the 40th Hawaii International Conference on System Sciences*.

PETERS LH and O'CONNOR EJ (1980) Situational constraints and work outcomes: the influences of a frequently overlooked construct. *Academy of Management Review* **5(3),** 391–397.

PETERS LH, O'CONNOR EJ, EULBERG JR and WATSON TW (1988) An examination of situational constraints in air force work settings. *Human Performance* **1(2),** 133–144.

PETTER S, STRAUB DW and RAI A (2007) Specifying formative constructs in is research. *MIS Quarterly* **31(4),** 623–656.

PHILLIPS JS and FREEDMAN SM (1984) Situational performance constraints and task characteristics: their relationship to motivation and satisfaction. *Journal of Management* **10(3),** 321–331.

PODSAKOFF PM and ORGAN D (1986) Self-reports in organizational research: problems and prospects. *Journal of Management* **12(4),** 531–544.

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.

RADCLIFF S (2007) Commentary: legal effect of revealing private information in the US and abroad. *Information Systems Management* **24(4),** 343–344.

RALLS RS and KLEIN KJ (1991) Trainee cognitive ability and motivation: Effects on computer training performance. In *Proceedings of the 6th Annual Conference of Industrial and Organizational Psychology*.

RENNIE L (1982) Research note: detecting a response set to likert-style attitude items with the rating model. *Education Research and Perspectives* **9(1),** 114–118.

RHEE HS, KIM C and RYU YU (2009) Self-efficacy in information security: its influence on end users' information security practice behavior. *Computers & Security* **28(6),** 816–826.

RINGLE C, WENDE S and WILL A (2005) SmartPLS 2.0 (beta). [WWW document] www.smartpls.de.

ROBINSON T (2005) Data security in the age of compliance. *Networker* **9(3),** 24–30.

ROTTER JB (1960) Some implications of a social learning theory for the prediction of goal directed behavior from testing procedures. *Psychological Review* **67,** 301–316.

SALGANIK MJ and HECKATHORD DD (2004) Sampling and estimation in hidden populations using respondent-driven sampling. *Sociological Methodology* **34(1),** 193–239.

SASSE MA, BROSTOFF S and WEIRICH D (2001) Transforming the 'weakest link' – a human/computer interaction approach to usable and effective security. *BT Technology Journal* **19(3),** 122–131.

SCHUNK DH (1983) Ability versus effort attributional feedback: differential effects on self-efficacy and achievement. *Journal of Educational Psychology* **75(6),** 848–856.

SCHUNK DH (1984) Sequential attributional feedback and children's achievement behavior. *Journal of Educational Psychology* **76(5),** 1159–1169.

SHEPPARD B, HARTWICK J and WARSHAW P (1988) The theory of reasoned action: a meta-analysis of past research with recommendations for modifications and future research. *Journal of Consumer Research* **15(3),** 325–343.

SHEN JJ, SAMSON LF, WASHINGTON EL, JOHNSON P, EDWARDS C and MALONE A (2006) Barriers of HIPAA regulation to implementation of health services research. *Journal of Medical Systems* **30(1),** 65–69.

SIPONEN MT (2000) A conceptual foundation for organizational information assurance awareness. *Information Management and Computer Security* **8(1),** 31–41.

SIPONEN MT (2001) An analysis of the recent IS security development approaches: descriptive and prescriptive implications. In *Information Security Management – Global Challenges in the Next Millennium* (DHILLON G, Ed.), Idea Group, Hershey, PA.

SIPONEN M and VANCE A (2010) Neutralization: new insights into the problem of employee information systems security policy violations. *MIS Quarterly* **34(3),** 487–502.

STANTON JM, STAM KR, MASTRANGELO PM and JOLTON JA (2005) Analysis of end user security behaviors. *Computers & Security* **24(2),** 124–133.

STRAUB D (1990) Effective IS security: an empirical study. *Information Systems Research* **1(3),** 255–276.

STRAUB DW, BOUDREAU MC and GEFEN D (2004) Validation guidelines for IS positivist research. *Communications of AIS* **13(63),** 380–427.

STRAUB DW and WELKE RJ (1998) Coping with system risk: security planning models for management decision making. *MIS Quarterly* **22(4),** 441–464.

SULSKY LM and KLINE TJ (2007) Understanding frame-of-reference training success: a social learning theory perspective. *International Journal of Training and Development* **11(2),** 121–131.

TORKZADEH G and VAN DYKE TP (2002) Effects of training on internet self-efficacy and computer user attitudes. *Computers in Human Behavior* **18(5),** 479–494.

VAN VIANEN AE (1999) Managerial self-efficacy, outcome expectancies, and work-role salience as determinants of ambition for a managerial position. *Journal of Applied Social Psychology* **29(3),** 639–665.

VOGT N (2005) Can privacy compliance be monitored? *Journal of Health Care Compliance* **7(4),** 56–58.

VROOM C and VON SOLMS R (2004) Towards information security behavioural compliance. *Computers & Security* **23(3),** 191–198.

WARKENTIN M and WILLISON R (2009) Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems* **18(2),** 101–105.

WEXLEY KN and LATHAM GP (1991) *Developing and Training Human Resources in Organizations*. HarperCollins, New York City.

WHITMAN EM and MATTORD HJ (2004) Making users mindful of IT security; awareness training is vital to keeping the idea of IT security uppermost in employees' minds. *Security Management* **48(11),** 32–34.

WILLISON R and BACKHOUSE J (2006) Opportunities for computer crime: considering systems risk from a criminological perspective. *European Journal of Information Systems* **15(4),** 403–414.

WORKMAN M, BOMMER WH and STRAUB D (2008) Security lapses and the omission of information security measures: a threat control model and empirical test. *Computer in Human Behavior* **24(6),** 2799–2816.

Appendix A

Privacy laws and regulations

In the 21st century, IT directors, Chief Information Officers (CIOs), Chief Security Officers (CSOs), and Chief Privacy Officers (CPOs) are responsible for ensuring that their organizations are in compliance with an ever-expanding alphabet soup of governmental regulations and requirements, industry standards, and international conventions that relate to security and privacy of sensitive information (Dinev *et al*., 2006). Many organizations have placed responsibility for regulatory compliance in the hands of IT directors. In the U.S., these regulations include the Privacy Act of 1974, the Fair Credit Reporting Act of 1988, the Video Privacy Protection Act of 1988, the Children's Online Privacy Protection Act (COPPA) of 1998, the Sarbanes-Oxley Act ('SOX'), the Gramm-Leach-Bliley Act (GLBA, also known as the Financial Modernization Act of 1999), the Health Insurance Portability and Accountability Act (HIPAA) and the 'HITECH ACT' which amended it in 2009, the Family Educational Rights and Privacy Act (FERPA), the Patriot Act, California's Security Breach Notification Act (SB-1386 and 45 other similar state breach notification laws), various banking regulations, credit card company requirements, and others. (The 2009 HITECH Act reaches far beyond healthcare providers by requiring data protection practices by business partners and vendors who handle protected health information, while also adding requirements for data breach notification.) Further, publicly traded firms in the U.S. must comply with Securities and Exchange Commission (SEC) provisions, FASB, and PCAOB. The Cable Communications Policy Act of 1984 requires cable companies to obtain subscriber consent whenever they collect or distribute personal information and the Cable TV Privacy Act of 1984 prevents disclosure of subscribers' viewing habits without their prior written consent (Bloom *et al*., 1994).

Various U.S. states have enacted specific regulatory compliance mandates concerning categories of medical information, such as HIV status and mental health diagnoses, creating a complex mosaic of compliance requirements, especially for medical practices that operate across state lines (Langender & Cook, 2004). As medical diagnostic procedures are offshore outsourced, compliance with privacy mandates will be the most important risk to the development of global medical information networks (Gupta, 2008).

Canada's PIPEDA governs the collection, use, and disclosure of personal information by private entities, plus various Canadian provinces have additional privacy regulations, such as Ontario's Personal Health Information Protection Act and personal information privacy acts in Quebec, Alberta, and British Columbia.

The European Union (EU) mandates further information-related rules, some of which affect U.S. companies doing business in Europe. The EU Data Protection Directive (Directive 95/46/EC) regulates the collection, storage, and use of personal data within the European Union, requiring companies within the member states to comply with specific provisions. Other EU regulations include provisions to maintain the privacy of information in banking (Basel II and MiFID), telecommunications (Data Retention Directive 2006/24/EC), and other areas. The U.K.'s Data Protection Act (DPA) mandates eight privacy and disclosure provisions for all organizations that collect and store personal information. Many firms throughout the world also seek ISO17799 compliance status, placing further compliance burdens on CIOs.

Appendix B

Table B1 Select employee security/privacy policy compliance literature

Author (Date)	*User base/context*	*Methodology*	*Constructs*	*Description*
Boss *et al.* (2009)	Employees/ Organization (1)	Field study: data collected via surveys	Specification, evaluation, reward, mandatoriness, general precautions, computer self-efficacy, apathy	Using organizational control as a lens, a model is built to explain security precaution-taking behaviour. Results find that specifying policies and evaluating behaviours influences the perceived mandatoriness of security policies. Mandatoriness effectively motivates individuals to take security precautions.
Bulgurcu *et al.* (2010)	Employees/Multiple Organizations	Field study: data collected via surveys	Information security awareness, perceived benefit of compliance, intrinsic benefit, safety of resources, rewards, perceived cost of compliance, work impediment, perceived cost of non-compliance, intrinsic cost, vulnerability of resources, sanctions, attitude, normative beliefs, self-efficacy to comply, intention to comply	Findings suggest that employee intention to comply with information security policy is influenced by attitude, normative beliefs, and self-efficacy to comply. Employee attitude is influenced by benefit of compliance, and costs associated with both compliance and non-compliance which are beliefs about overall consequences of compliance/ non-compliance. Information security awareness positively influences attitude and outcome beliefs.
D'Arcy *et al.* (2009)	Employees/Multiple Organizations	Field study: data collected via surveys	IS misuse intention, perceived certainty, perceived severity, user awareness of … security policies, SETA programme, computer monitoring	Extends general deterrence theory by examining security countermeasures (security policies, SETA programme, computer monitoring) as antecedents to perceived certainty and severity of sanctions. Findings suggest that all three countermeasures deter IS misuse intentions. Perceived severity of sanctions (as opposed to certainty of sanctions) is most effective at deterring IS misuse.
Herath & Rao (2009)	Employees/Multiple Organizations	Field study: data collected via surveys	Punishment severity, detection certainty, perceived probability of security breach, perceived severity of security breach, security breach concern level, response efficacy, response cost, security policy compliance intention, security policy attitude, self-efficacy, subjective norm, descriptive norm, resource availability, organizational commitment	Findings suggest that organizational commitment and social influence increase compliance intentions. Policy attitudes influenced by severity of breaches, response efficacy, self-efficacy and response costs. Employees underestimate probability of security breaches.
Johnston & Warkentin (2010)	Faculty, staff and students at a large university	Experiment	Perceived threat severity, perceived threat susceptibility, self-efficacy, response efficacy, social influence, behavioural intention	Investigates the influence of fear appeals on end-user compliance with computer security recommendations. Results suggest fear appeals influence end-user behavioural intentions but not uniformly. Perceptions of self-efficacy, response efficacy, threat severity, and social influence also play a role.

Table B1 Continued

Author (Date)	*User base/context*	*Methodology*	*Constructs*	*Description*
Leach (2003)	Employee/ Organization	Conceptual	Body of knowledge, senior management and colleagues demonstrated behaviours, user's security common sense and decision-making skills, effort required for compliance and temptations not to comply, user's psychological contract with their employer, user's personal values and standards of conduct, user security behaviours	Suggests strengthening the employees' psychological contract with the organization in order to reduce the internal security threat.
Lee & Larsen (2009)	Employees/Multiple Organizations	Field study: data collected via surveys	Perceived severity, perceived vulnerability, response efficacy, self-efficacy, response cost, social influence, adoption intention	Threat and coping appraisal were found to predict adoption intentions of anti-malware software by small- and medium-sized business executives. Vendor support facilitated adoption for IS experts/IT intensive industry while IT budget facilitated adoption for non-IS experts/non-IT intensive industry groups.
Myyry *et al*. (2009)	Employees in one organization and part-time graduate students	Field study: data collected via surveys	Preconventional reasoning, conventional reasoning, postconventional reasoning, values	Applies concepts from moral reasoning and values to understand compliance with IS security policies. Preconventional moral reasoning, which focuses on fear of sanctions, had a positive influence on both hypothetical and actual compliance. Openness to change and conventional moral reasoning were negatively associated with compliance behaviour.
Pahnila *et al*. (2007)	245 Employees/ Organization (1)	Field study: data collected via surveys	Sanctions, threat appraisal, coping appraisal, normative beliefs, information quality, facilitating conditions, habits, rewards, attitude toward complying, intention to comply, actual compliance	Proposes and tests a theoretical model explaining employees' IS security policy compliance. Employees' attitude, normative beliefs and habits have significant effect on intentions to comply with security policy. Threat appraisal and facilitating conditions impact attitude but coping appraisal does not. Sanctions do not influence intentions to comply. Rewards did not influence actual compliance.
Sasse *et al*. (2001)	Employees/ Organization (1)	Field study: data collected via mixed methods (surveys, secondary data, interviews)	Memory decay, password count, use frequency, punishment, awareness, and others.	Presented examples of how undesirable user behaviour with passwords can be caused by poorly designed and implemented procedures that conflict with task demands and are inconsistent with characteristics of human memory. Findings also suggest the importance of motivation and training to address seven issues that lead to undesirable password behaviour including low probability and severity of threat, low perceived response efficacy and social issues such as trust *vs* paranoia. Findings seem to suggest that employees who feel a stronger sense of organizational commitment are more careful with their password behaviour.

Siponen & Vance (2010)	Employees/Multiple Organizations	Field study: data collected via surveys	Defence of necessity, appeal to higher loyalties, condemn the condemners, metaphor of the ledger, denial of injury, denial of responsibility, neutralization, formal sanctions, informal sanctions, shame, intention to violate IS security policy	Results suggest that neutralization theory provides an explanation for IS security policy violations. When neutralization is incorporated in the model, no effects of general deterrence theory are significant.
Stanton *et al*. (2005)	1167 Employees/ Organizations (various within the U.S.)	Field study: data collected via surveys	Password management behaviours, password sharing behaviours, organizational support of security-related behaviours	Created a taxonomy of end user security-related behaviour along two dimensions: level of technical knowledge required and intentionality of behaviour. Tested taxonomy via a survey to identify six categories of end users. Evidence that good password behaviour is related to training, awareness, monitoring and motivation.
Straub (1990)	Employees/Multiple Organizations	Field study: data collected via surveys	Deterrent certainty, deterrent severity, computer abuse, rival explanations	Findings suggest deterrence measures such as policies and guidelines about appropriate system use and penalties are effective at improving security while other alternative explanations such as motivational and environmental factors were found to be insignificant.
Vroom & von Solms (2004)	Organization level	Conceptual	Employee behaviour, organizational culture, organizational behaviour	Argues that auditing employee security behaviour is difficult. Proposes an alternative to auditing which is to create a more information security-conscious organizational culture.
Workman *et al*. (2008)	588 Employees/ Organization	Field study: data collected via surveys & secondary data	Perceived severity, vulnerability, locus of control, self-efficacy, response efficacy, response cost, subjective omission of security	Proposes and tests a threat control model to explain why users who know how to protect their systems fail to do so. Findings suggest threat assessment and coping assessment influence subjective and objective omissive behaviour. Self-efficacy and locus of control drawn from Social Cognitive Theory affect omissive behaviours.

Source: Adapted from Anderson & Agarwal (2010).

Appendix C

Table C1 Instrument items

VarName	*Instrument item*
SS1	I find that my organization's resources effectively support HIPAA compliance.
SS2	I am comfortable complying with HIPAA privacy policies within my organization.
SS3[a]	I wish I had better resources with which to aid HIPAA compliance.
SS4	I feel like I have someone to ask if I have questions about HIPAA compliance.
SS5	I feel as though I have adequate time to comply with HIPAA requirements.
SS6	I feel as though my supervisors support my HIPAA compliance actions.
VP1[a]	I tend **not** to believe others when they tell me I can comply with HIPAA.
VP2	I often get important feedback from administrators about HIPAA compliance.
VP3	Listening to others discuss HIPAA compliance gives me useful information for compliance.
VP4[a]	I learn little about HIPAA compliance from the suggestions of others.
VP5[a]	The feedback I receive from others does **not** help me comply with HIPAA.
VP6	When people I respect tell me I can comply with HIPAA, I tend to believe them.
VP7	Feedback from my peers is valuable to me.
VE1	I am able to improve my compliance with HIPAA by noticing the errors that others make.
VE2[a]	The things I learned in training do **not** help me comply with HIPAA.
VE3	When I see others not comply with HIPAA, I am able to learn how to comply with HIPAA more effectively.
VE4	I have developed confidence in my ability to comply with HIPAA by observing the mistakes that others make.
VE5	I have had meaningful opportunities to observe others comply with HIPAA.
VE6	Watching others make mistakes has taught me how to comply with HIPAA.
VE7	I have learned how to be HIPAA compliant by watching others.
BINT1	I intend to continue to protect patient privacy.
BINT2	I plan to continue to safeguard patient privacy.
BINT3	I predict that I will not continue to protect patient privacy.
BINT4	I plan to routinely observe HIPAA guidelines.
BINT5	I predict that I will observe HIPAA procedures.
SEFF1	How much can you do to protect the confidentiality of patient medical data?
SEFF2	How much can you do to ensure HIPAA compliance?
SEFF3	How much can you do to influence the privacy of patient data?
SEFF4	How much can you do to ensure that other healthcare workers follow HIPAA guidelines?
SEFF5	How much can you do to ensure patient information privacy?
SEFF6	How much can you do to control the use of patient data so that it is HIPAA compliant?
SEFF7	How much can you do to safeguard the privacy of patient records?
SEFF8	How much can you do to reduce violations of patient privacy policies?
JOBTITLE	What is your job title?
WORKFOR	Who do you work for?
TOTEMPS	About how many total employees work at your location for your employer?
CARLENG	How long have you worked as a healthcare professional (in your career)?
TENURE	How long have you worked at your current organization (employer)?
GENDER	Please indicate your gender.
AGE	What is your age?

[a]Reverse coded.