European Journal of Information Systems (2009) 18, 106–125

www.palgrave-journals.com/ejis/

Protection motivation and deterrence: a framework for security policy compliance in organisations

Tejaswini Herath[1] and H. Raghav Rao[2,3]

[1]Department of Finance, Operations and Information Systems, Brock University, Canada; [2]Management Science and Systems, School of Management, The State University of New York at Buffalo, U.S.A.; [3]Computer Science and Engineering, College of Engineering, The State University of New York at Buffalo, U.S.A.

Correspondence: Tejaswini Herath, Department of Finance, Operations and Information Systems, Brock University, St. Catharines ON L2S 3A1, Canada.
Tel: +905 688 5550, ext. 4179;
Fax: +905 378 5723;
E-mail: teju.herath@brocku.ca

Abstract
Enterprises establish computer security policies to ensure the security of information resources; however, if employees and end-users of organisational information systems (IS) are not keen or are unwilling to follow security policies, then these efforts are in vain. Our study is informed by the literature on IS adoption, protection-motivation theory, deterrence theory, and organisational behaviour, and is motivated by the fundamental premise that the adoption of information security practices and policies is affected by organisational, environmental, and behavioural factors. We develop an Integrated Protection Motivation and Deterrence model of security policy compliance under the umbrella of Taylor-Todd's Decomposed Theory of Planned Behaviour. Furthermore, we evaluate the effect of organisational commitment on employee security compliance intentions. Finally, we empirically test the theoretical model with a data set representing the survey responses of 312 employees from 78 organisations. Our results suggest that (a) threat perceptions about the severity of breaches and response perceptions of response efficacy, self-efficacy, and response costs are likely to affect policy attitudes; (b) organisational commitment and social influence have a significant impact on compliance intentions; and (c) resource availability is a significant factor in enhancing self-efficacy, which in turn, is a significant predictor of policy compliance intentions. We find that employees in our sample underestimate the probability of security breaches.
European Journal of Information Systems (2009) **18,** 106–125. doi:10.1057/ejis.2009.6; published online 21 April 2009

Keywords: security policy compliance; protection motivation; deterrence; organisational commitment

Introduction

In today's information intensive society, the secure management of information systems (IS) has become critically important. Although organisations actively use security technologies and practices, information security cannot be achieved through technological tools alone. The recent attention to security policies in academic literature points to the need for empirical investigations on security compliance and the efforts and findings of field surveys suggest that while organisations are making a considerable effort to use technology to improve security, more attention is being focused on other formal and informal control mechanisms, including policies, procedures, organisational culture, and the role individuals play in security.

An investigation of the causes of recent security incidents shows that employee negligence has led to breaches costing organisations millions of

Received: 21 February 2008
Revised: 15 August 2008
2nd Revision: 31 January 2009
Accepted: 23 February 2009

dollars in losses (Privacyrights.org, 2005, 2006). Although some insider breaches may be maliciously intended, Vroom & von Solms (2004) contend in their review of the 2001 Information Security Industry Survey that many security breaches may be the result of negligence or ignorance of security policies. Incidences of failures to prevent security breaches due to end-user negligence are indicators of the failure of IS security governance programmes that do not address individual values, beliefs, and means to encourage conformity with policies (Mishra & Dhillon, 2006).

Increasingly, many information security-related computing behaviours such as patch management and antivirus updates are being automated to reduce the task knowledge and time burdens on end-users. Tasks including the appropriate use of computer and network resources and appropriate password habits, however, have to be dealt with appropriate computer security policies. The importance of appropriate computer use policies has been emphasised for a long time, but their impact and effectiveness is far from clear. Most participants attending a panel held at ICIS 1993 (Loch *et al*., 1998) reported that although these policies are necessary, they perceived them to be ineffective. The defined policies may be crystal clear and detailed, but compliance may be lacking, particularly with regard to information security (von Solms & von Solms, 2004). Security incidents (Privacyrights.org, 2005, 2006) and field surveys (CERT/CC, 2004; Gordon *et al*., 2006) suggest that employees seldom comply with information security policies and procedures. In fact, employees may choose not to comply with security policies for reasons of convenience in their day-to-day routine.

In organisations, managers responsible for information security establish computer security policies; however, if the employees and end-users of organisational IS do not understand the importance of these practices and are not keen or willing to follow the policies, then these efforts are in vain. Policies, especially those involving information security, are viewed as mere guidelines or general directions to follow rather than hard and fast rules (von Solms & von Solms, 2004). Due to the relatively discretionary nature of adherence to these policies, organisations find the enforcement of security a challenging task. Recent surveys in the information security literature such as eCrime Survey (CERT/CC, 2004) reveal that although the policies and procedures are in place, many employees and outside contractors ignore them. A Computer Security Institute/Federal Bureau of Investigation (FBI) survey reports that organisations find enforcement of end-user policy as one of the main challenges for achieving higher levels of information security (Gordon *et al*., 2006).

In this paper, we draw upon the literature in the areas of protection motivation theory, general deterrence, and organisational behaviour to develop and test an Integrated Protection Motivation and Deterrence model of security policy compliance under the umbrella of Taylor-Todd's Decomposed Theory of Planned Behaviour (DTBP) (Taylor & Todd, 1995). Our paper makes several theoretical and empirical contributions. We draw upon protection motivation theory and incorporate an evaluation of threat appraisal and coping appraisal to identify attitudes towards security policies. We evaluate the effect of employees' organisational commitment on security policy compliance intentions. We also assess the influence of environmental factors such as deterrence, facilitating conditions, and social influence. To explore the social influence more thoroughly, we evaluate multiple dimensions, including subjective and descriptive norms. Using employee responses from 78 organisations, we validate and test the theoretical model. Our integrated model is valuable for understanding information security compliance in a more holistic manner.

We begin this paper with a review of the relevant literature in order to lay the theoretical foundation for developing an integrated theoretical model that can be tested empirically. Next, we discuss the instrument development process and its validation. Thereafter, we discuss in detail the methodology used for this survey-based study. Finally, we provide a discussion of our findings and conclude with the implications for theory and practice in addition to avenues for future research.

Literature review

Due to the importance of the behavioural aspects of information security, there has been an increase in research focusing on organisational information security practices as well as individual security behaviours. Some of the work in this area includes computer security behaviours (Loch *et al*., 1992; Stanton *et al*., 2005); security behaviour in the home setting (Anderson, 2005); access control and security perceptions (Zhang, 2005; Furnell *et al*., 2007; Post & Kagan, 2007); and malicious behaviours or computer abuse in organisations (Straub & Nance, 1990; Lee *et al*., 2004). There have been some empirical studies that evaluate organisational security practices and their effectiveness; however, the respondents in these studies are typically IT administrators or top-level managers (e.g., Straub & Collins, 1990; Loch *et al*., 1992; Knapp *et al*., 2005; Ma & Pearson, 2005; Dhillon & Torkzadeh, 2006) rather than representatives from the end-user community. The fact that the respondents in prior studies were largely those responsible for setting up and running technical security initiatives raises the question of whether or not their views are likely to be representative of the organisation as a whole (Finch *et al*., 2003). For example, even though an IT administrator might indicate that there is a formal security policy in place, this does not necessarily mean that end-users take any notice of it.

More recently, there has been some research on security policies and end-user policy compliance. Siponen (2000) provides a conceptual foundation for organisational information security whereas Vroom & von Solms (2004) provide components of effective security

governance, including information security policies. Both of these papers discuss the role of human factors in the success of security initiatives. In a similar vein, von Solms (2001) has argued that information security is a multidimensional discipline and that various dimensions such as the human/personnel dimension and the policy/governance dimension have interconnected roles that impact overall organisational information security. As Dhillon & Backhouse (2001) have pointed out, there is a great need for more empirical research that uses socio-organisational perspectives to develop key principles for the prevention of negative events in order to help in the management of information security.

In an empirical vein, D'Arcy & Hovav (2004) followed deterrence theory and developed a theoretical model that examines the effect of deterrent security countermeasures on the perceived certainty and severity of sanctions, which in turn, leads to IS misuse intentions whereas Straub (1990) finds that deterrence measures reduce computer abuse in organisations. Albrechtsen (2007) conducted a qualitative study of user views on information security and found that users do not perform many information security actions and that they prioritise other work tasks in front of information security. Albrechtsen (2007) argues that a main problem regarding user roles in information security work is their lack of motivation and knowledge regarding information security and related work. Post & Kagan's (2007) study also found that end-users perceived security practices to be a hindrance in their normal routine. In an evaluation of security policy compliance, Chan *et al*. (2005) studied the security climate in organisations and found that management practices and coworker socialisation have an impact on employee perceptions of the information security climate which, in addition to self-efficacy, positively impact security policy compliance behaviour. Stanton *et al*. (2003) examined the effect of organisational commitment on variety of security behaviours including security policy compliance. Pahnila *et al*. (2007) found that employee attitudes, normative beliefs, and habits all have a significant effect on employee intentions to comply with IS security policy whereas threat appraisal and facilitating conditions have a significant impact on shaping attitudes towards compliance. Despite recent attention to this issue by several researchers, the investigation of policy compliance is still embryonic and poses many opportunities for empirical research.

To influence more security conscious behaviours, researchers have suggested and evaluated many aspects; however, some of the dimensions remain untested empirically while others have been tested in different contexts than security policy compliance. For instance, although the effect of perceived certainty and severity of sanctions on IS misuse intentions has been theoretically modelled (D'Arcy & Hovav, 2004) and tested in a piracy context (Peace *et al*., 2003), to our knowledge it has not been tested in a security policy compliance context. Similarly, although threat appraisal and coping appraisal are evaluated on an aggregate level (Pahnila *et al*., 2007), the individual components of these concepts – perceived vulnerability and perceived severity (threat appraisal); and response efficacy, self-efficacy, and response cost (coping appraisal) – have not yet been examined in a security policy compliance context. Also, much research has been done to test some of these components, but an overarching integrated model is still lacking. When tested separately, all these factors may have a significant impact and when considered along with other influencing factors, they may show insignificance, or vice versa. This paper undertakes an investigation of an integrated model in an attempt to provide a comprehensive understanding and outline the relative importance of the factors considered by the model for security governance.

Theoretical background

In this paper, we propose and evaluate an empirical model in order to understand the effect of various factors on employee intentions to comply with an organisation's information security policies. In general, issues related to information security behaviours, such as how security conscious behaviours are shaped or influenced, what motivates people to undertake security measures, what motivates people to carry out actions that are prescribed by organisations, etc., can be studied through the lens of theories borrowed from disciplines including psychology, sociology, and criminology that give us insights into behaviours, motivations, values, and norms.

Why people behave the way they do and what drives behaviours has been examined across many different contexts and behaviours using the two most widely-used behavioural theories, the Theory of Reasoned Action (TRA) (Ajzen & Fishbein, 1980) and the Theory of Planned Behaviour (TPB) (Ajzen, 1991). These theories provide the basis for an examination of the relationship between attitude, intention, and behaviour. Both these theories have been used widely in the IT literature, including in the security policy compliance context (Pahnila *et al*., 2007). The TRA posits that intentions are based on attitudes and subjective norms. The TPB incorporates the perception of behavioural control held by an individual in the model and indicates that the intentions are predicted by attitudes, subjective norms, and behavioural control. Taylor & Todd (1995) introduced a DTPB to provide a more complete understanding of behaviour in the IT context. Their DTPB model draws on constructs from the innovations characteristics literature, explores multiple dimensions of subjective norms, and decomposes the perceived behavioural control dimension to evaluate self-efficacy along with technology and resource facilitating conditions. The DTPB provides guidance for consideration of relevant constructs in the IT environment.

The TPB postulates that attitude, which represents an individual's degree of like or dislike towards a specific behaviour, predicts an individual's intention to carry out

that behaviour. In the context of intention to comply with security policies, this attitude relates to the attitude towards security policies. As security policies encourage end-user behaviours that protect information assets from threats posed to them, the literature in fear appeals and Protection Motivation Theory (PMT) (Rogers, 1975, 1983; Maddux & Rogers, 1983), which provides an account of protective behaviour, offers a relevant background. In the fear appeals literature, a number of motivational models of health behaviour such as PMT, the Health Belief Model (HBM), Social Cognitive Theory (SCT), the TRA, and the TPB have been proposed and investigated. Typically these models have been designed to identify the variables that underlie decisions that account for risk and to assess their ability to predict protective behaviour.

Rooted in fear appeals, PMT (Rogers, 1975) describes coping with a threat as the result of two appraisal processes – a process of threat appraisal and a process of coping appraisal – in which the options to diminish the threat are evaluated. Over 50 years of research in fear appeals (Witte & Allen, 2000) as well as the original PMT (Rogers, 1983) identifies that the motivation to protect depends upon three factors: (1) perceived severity of a threat; (2) perceived probability of the occurrence, or vulnerability; and (3) the efficacy of the recommended preventive behaviour (the perceived response efficacy). Later, Rogers (1983) amended the theory to include perceived self-efficacy (i.e., the level of confidence in one's ability to undertake the recommended preventive behaviour) as a factor in the coping appraisal process. The intrinsic and extrinsic rewards of risky behaviour as well as the response cost of protective behaviour were also included in the model.

Protection motivation deriving from the appraisal of the two processes of threat appraisal and coping appraisal is defined as 'an intervening variable that has the typical characteristics of a motive: it arouses, sustains and directs activity' (Rogers, 1975, p. 98). With this somewhat broad definition, although it has most often used intention as a dependent variable (e.g., Stanley & Maddux, 1986; Steffen, 1990; Neuwirth *et al.*, 2000); the literature in PMT has also considered attitudes (e.g., Stanley & Maddux, 1986; Steffen, 1990), and behaviour as dependent variables (e.g., Melamed *et al.*, 1996; Palardy *et al.*, 1998). Over decades, a diverse and rich plethora of variables and relationships have been considered in the PMT literature. In addition to the four main factors of PMT, the literature has considered a variety of constructs such as fear, worry, barriers, social factors, and socio-demographic variables in reference to the context under investigation. Initially envisioned as multiplicative in nature, the constructs of PMT were later investigated as being additive in nature. Additionally, while Rogers (1983) visualised his PMT model to be parallel or an unordered sequence of appraisal processes, others contended the processes were sequential/ordered (e.g., Tanner *et al.*, 1991). Tanner *et al.* (1991) offer an ordered PMT model that indicates that a state of fear (identified as a security concern in this study) is created by the threat appraisal process. If a threat appraisal results in fear, the coping appraisal then occurs to invoke protection motivation.

PMT has been used in variety of fields (see the following meta-analytic studies for additional references: Floyd *et al.*, 2000; Milne *et al.*, 2000; Neuwirth *et al.*, 2000; Witte & Allen, 2000). Although, primarily related to threats posed to an individual, PMT also has been used to understand the individuals' actions based on their perception of threats posed to themselves and their surroundings. For example, in the case of nuclear threats, the threats are not only posed to the individuals but also to the society surrounding the individuals (Axelrod & Newton, 1991). In the context of information security, if the organisation is affected by a threat, an employee within that organisation is likely to feel some effects. Thus, the concepts explored in the PMT and fear appeal literature can be applied to and are relevant in the context of information security. In the information security literature, in addition to threats affecting individuals (Anderson, 2005; Woon *et al.*, 2005), PMT has been applied to threats posed to organisations in a security policy compliance context (Pahnila *et al.*, 2007).

Although meta-analyses of the related motivation models suggest that they provide parsimonious accounts of protective behaviour, Armitage & Conner (2000) argue that the TPB provides an improvement on HBM, SCT, and PMT, and a possibility exists that the apparent superiority of the TPB may be due to a better definition of its constructs. In a view congruent to that of the TPB, Bagozii's (1992) theory of goal pursuit examines the motivational influences on goal intentions and suggests that goal intentions are functions of desires which are derived from attitudes (toward process, success, and failure), subjective norms, and efficacy (Armitage & Conner, 2000). In line with this view, we contend that intentions to comply with security policies will be based on attitudes towards the security policies, the perceived norms, and the efficacy to carry out the actions, whereas attitudes towards security policies will be shaped by perceptions of the security threat and the coping response.

In terms of what may deter a negative behaviour such as disobedience of rules and policies, General Deterrence Theory from the discipline of criminology can be used to understand the effect of deterrent factors on security policy compliance. Deterrence has been shown to play a role in reducing negative behaviours and has also been found to be an effective mechanism in governance. Deterrence theory proposes that unwanted behaviours can be deterred through a certain, swift, and/or severe threat of punishment (Williams & Hawkins, 1986).

Security-related behaviours may be connected to an individual's motivation to protect organisational information assets due to an awareness and fear of the outside environment, as well as his/her closeness to the organisation. As such, another relevant research stream that may

shed light on positive organisational behaviours of policy compliance is employee commitment to organisational well-being. Organisational commitment has been shown to act in a way that meets organisational interests (Mowday, 1998). Social Bond theory, which posits that strong social bonds prevent a person from committing negative behaviours, can also be seen from the organisational commitment perspective.

Based on the above discussion, Table 1 provides a brief summary of the constructs and related theories considered in this study.

Hypotheses development

Based on the preceding arguments, we propose a general research model as presented in Figure 1.

The TPB and TRA posit that positive attitude, evaluated belief, or positive or negative feeling towards a stimulus object influences behavioural intention. IS-related research using TRA and TPB-based models has supported this relationship (Karahanna *et al*., 1999). As a result, we anticipate that a positive attitude regarding security measures will lead to positive intentions to comply with security policies. Thus,

H1 *Attitudes towards information security policies will positively influence security policy compliance intentions*

Protection motivation

An individual's beliefs regarding whether the security policies are essential may come from their understanding of security threats and the effectiveness of security policies as coping mechanisms. In this context, the PMT of fear appeals PMT (Rogers, 1975, 1983) provides a good background. According to Rogers (1975), fear can be aroused in response to a situation that is judged dangerous and regarding which a protective action needs to be taken. Fear appeals are multifaceted stimuli and include the severity or seriousness of the noxious event, perceived vulnerability to the threat, concern over the

Table 1 Main constructs and related theories

Construct	*Theory*	*Construct*	*Theory*
Punishment severity	GDT	Security policy compliance intention	TPB; DTPB; PMT
Detection certainty	GDT	Security policy attitude	TPB; DTPB; PMT
Perceived probability of security breach	PMT	Self-efficacy	TPB; DTPB; PMT
Perceived severity of security breach	PMT	Subjective norm	TPB; DTPB
Security breach concern level	PMT	Descriptive norm	TPB; DTPB
Response efficacy	PMT	Resource availability	DTPB
Response cost	PMT	Organisational commitment	OC

Note: General Deterrence Theory (GDT); Protection Motivation Theory (PMT); Theory of Planned Behaviour (TPB); Decomposed Theory of Planned Behaviour (DTPB); Organisational Commitment (OC).

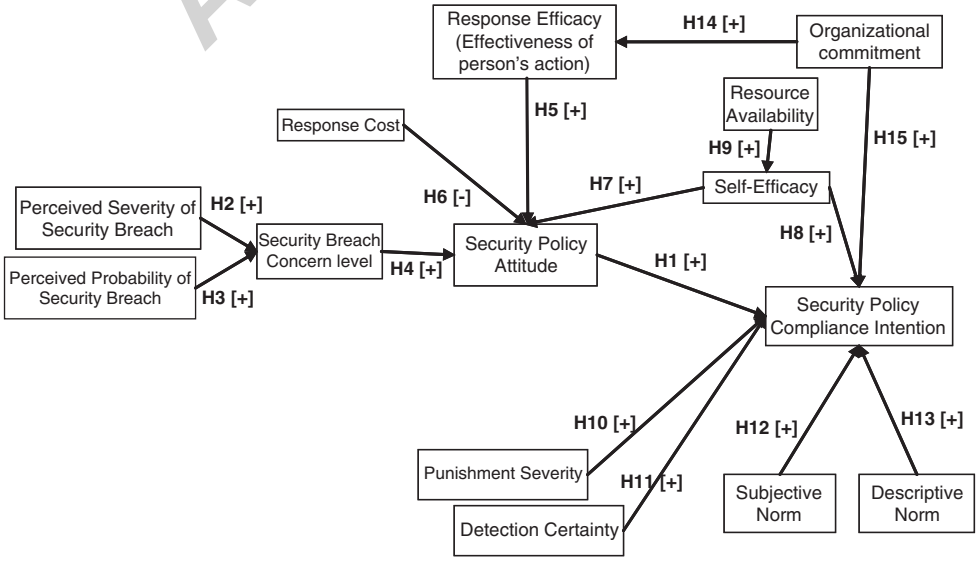

Figure 1 Integrated framework for security policy compliance intentions.

threat and coping response efficacy. Rogers (1983) contends that typically an individual is exposed to persuasive communication that depicts the noxious consequences accruing to a specified course of action in response to which a protective action may be taken. In the context of information security, an employee may gain information and have a general understanding about cyber-security threats from a variety of sources such as external media, corporate communication, and social networks.

Protection motivation arises from the cognitive appraisal of two processes: threat appraisal and coping response appraisal. Threat appraisal relates to the perceptions of how threatened an individual feels based on an evaluation of the components of fear appeal. The PMT variables that capture the threat appraisal are perceived severity (degree of harm associated with the threat), perceived vulnerability (probability of the threat occurring), and fear arousal (how much fear the threat invokes) (Tanner *et al*., 1991; Milne *et al*., 2000). In the IS security context, these can be visualised in terms of an employee's assessment of the consequences of the security threat and the probability of exposure to a substantial security threat. Fear arousal is envisioned as a security concern in this study and is defined as the level to which an employee believes that her/his organisational information assets are threatened. If employees perceive that a security threat can impose significant damages or disturbances, they are more likely to be concerned. Conversely, if employees do not believe that they are truly confronted by security threats, they are less likely to be concerned. In essence, if employees perceive the threat to be real and are concerned, they are more likely to have a more positive attitude towards protection mechanisms such as security policies. Thus, we can hypothesise:

H2 *The perceived severity of a potential security breach will positively affect the level of security breach concern.*

H3 *The perceived probability of a security breach will positively affect the level of security breach concern.*

H4 *Higher levels of security breach concern will result in more positive attitudes towards security policies.*

The second process that plays a central role in protection attitudes is the coping appraisal. The coping appraisal process evaluates response efficacy, response cost, and self-efficacy. Response efficacy relates to beliefs about whether the recommended coping response will be effective in reducing the threat. In the context of this study, it can be an employee's perception regarding the effectiveness of abiding by the organisation's computer security policies. The effectiveness of the action can be viewed as the perceived usefulness in DTPB. Culnan's (2004) and Anderson's (2005) studies on the information security behaviours of home users consider the perceived citizen effectiveness which represents an individual's belief that her/his individual actions can make a difference in securing the Internet. Anderson (2005) found that individuals have more favourable security attitudes when they have high perceptions of citizen effectiveness. Similarly, it is likely that employees who believe that their actions have a beneficial impact on their organisation will have a more positive attitude towards security policies. Thus, we hypothesise:

H5 *The perceived effectiveness of one's actions will positively affect one's attitude towards security policies.*

In PMT, response costs refer to beliefs about how costly performing the recommended response will be. In a study related to insulin use, Palardy *et al*. (1998) found that response costs negatively influenced protection motivation. In information security, the hindrance caused by security practices is noted as one of the reasons employees dislike or neglect security practices. A recent study of access controls found that employees believed higher levels of information security were counter-productive as they restricted the ability to follow flexible operation routines (Post & Kagan, 2007). Hence, we expect:

H6 *The perceived response cost will negatively influence one's attitude towards security policies.*

Facilitating conditions

Another aspect of coping appraisal is an individual's perception of self-efficacy, which is one's ability to perform a task. Although self-efficacy is presumed to be an important factor in protection motivation, it has also been an important factor in TPB. The perceived behavioural control considered in TPB is a belief about the presence of factors that may facilitate or impede a certain behaviour (Ajzen, 1991). Taylor & Todd (1995) captured this concept in two components: the availability of resources needed to engage in behaviour, and self-efficacy, which is the individual's self-confidence in his/her ability to perform the behaviour.

Individuals appear to evaluate information about their capabilities and then regulate their choices and efforts accordingly (Bandura *et al*., 1980). Self-efficacy has been shown to have a significant impact on task behaviours. Stajkovic & Luthans (1998) evaluated the role of self-efficacy in organisational behaviours through a meta-analysis of 114 studies and concluded that self-efficacy and work-related performance are highly correlated. Self-efficacy has also been shown to have a significant impact on IT usage (Compeau & Higgins, 1995). An individual confident in having the skills to undertake an activity is more likely to be inclined to take that action. With regard to security policy compliance, an individual who believes that she/he has the ability to act in accordance with the policies is likely to have more positive feelings towards

the policies and is also more likely to comply with those policies. Thus, we propose:

H7 *Self-efficacy will positively influence one's attitude towards security policies.*

H8 *Self-efficacy will positively affect intention to comply with organisational information security policies.*

Gist (1987) suggests that the implications of self-efficacy for training and organisational development are numerous. Arguing that the 'availability of assistance to individuals who need it is likely to increase their ability to perform a task' (p. 591), Igbaria & IIvari (1995) tested the effect of organisational support on self-efficacy. They found that organisational support significantly affected self-efficacy perceptions. In particular, computer training was found to significantly improve an individual's computer self-efficacy (Torkzadeh *et al*., 1999). Security literature has placed a strong emphasis on the availability of resources, including training, the online availability of policies and other mechanisms of promoting and enabling policy compliance (Thomson & von Solms, 1998; Siponen, 2000; Saks & Belcourt, 2006). Computer training has been found to significantly improve an individual's computer self-efficacy (Torkzadeh *et al*., 1999). If organisations proactively provide training to employees when they join a firm and in regular intervals thereafter, the training is likely to empower employees to take security-related action. It is also likely to remind employees of the organisational views of information security and emphasise the importance of security. The awareness mechanisms such as posters, newsletters, and notices can also act as reminders as well as facilitating mechanisms. If resources such as security policies are easily accessible and available when needed, or if help is available when needed, employees are more likely to believe that they can undertake an action. In this regard, we can expect 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. Hence, we hypothesise.

H9 *Resource availability will positively affect self-efficacy.*

Deterrence

Deterrence theory proposes that, as punishment certainty and punishment severity are increased, the level of unacceptable behaviour decreases. In essence, unwanted behaviour can be deterred through certain, swift, and/or severe threats of punishment (Williams & Hawkins, 1986; Akers, 1990). Ehrlich (1996) offers empirical evidence that punishment exerts a deterrent effect on offenders. Studies related to deterrence in organisational settings abound. In the IT context, several studies have noted the effect of deterrence on illegal computing activities in organisations; for example, Straub (1990) notes that deterrence measures are a useful primary strategy for reducing computer abuse.

Peace *et al*. (2003) found that punishment severity significantly influences piracy attitudes in organisational software piracy. Similarly, non-adherence to security policies can be deterred by imposing penalties. For instance, if an employee's actions result in an organisation facing a security breach, the organisation can investigate the cause of the security breach and punish the employee by imposing a penalty. If individuals perceive that the severity of penalties for non-compliance is high, their intention to commit undesired behaviours is likely to decrease. Therefore, we anticipate:

H10 *The severity of penalty will positively affect intention to comply with organisational information security policies.*

Not only severity but also certainty of organisational action is an important aspect of enforcement. Vroom & von Solms (2004) argue that to ensure that employees behave and act responsibly by adhering to prescribed security policies in the organisation, some form of evaluation is required that will investigate the security compliance of the individual. Although Deterrence Theory suggests that severe and certain punishments will reduce the unwanted behaviour, it assumes that potential violators are made aware of efforts to control anti-social behaviours (Straub, 1990). Peace *et al*. (2003) emphasise that simply having the rules in the books will do little to create change if the rules are not enforced. The low probability of being caught was listed as one of the most important factors in decisions to copy software illegally (Cheng *et al*., 1997).

Enforcing penalties is possible if organisations are able to detect employee misbehaviour. Organisations can deploy processes and technologies to observe appropriate behaviours. Kankanhalli *et al*. (2003) assert that 'deterrent efforts correspond to certainty of sanctions because the amount of such efforts directly affects the probability that IS abusers will be caught' (p. 141). Thus, we can expect that if the employees are aware of monitoring and detection efforts and if they perceive the chances of their non-compliance being detected to be high, they are more likely to obey the policies. Hence, we hypothesise:

H11 *The certainty of detection will positively affect the intention to comply with organisational information security policies.*

Social influence is the extent to which social networks influence members' behaviour through messages and signals that help form perceptions of an activity's value (Venkatesh & Brown, 2001). Regarding norms, a large number of IS studies have considered subjective norms (the belief as to whether or not a significant person wants

the individual to do the behaviour in question). Recently, IT literature has recognised the wider role of social influence. Venkatesh *et al*. (2003) argue that the role of social influence in technology acceptance decisions is complex and subject to a wide range of contingent influences.

Individuals are influenced both by messages about expectations and the observed behaviour of others. Sheeran & Orbell (1999) state that 'there is a long-standing distinction in the literature on social influence between the *is* (descriptive) and the *ought* (subjective) meaning of social norms because these are separate sources of motivation' (p. 2112). Sometimes people consult the behaviour of those around them to find out what to do. They see others' behaviour as a source of information to help them define social reality. These beliefs about what the majority of people do in specified environments are also referred to as descriptive norms (Cialdini *et al*., 1991). A number of studies indicate that descriptive norms do not refer to the same construct as subjective norms, and that descriptive norms enhance the TPB's capacity to predict behavioural intentions (e.g., Grube *et al*., 1986; Sheeran & Orbell, 1999).

Subjective norms are based on normative beliefs and motivation to comply. The view that individuals are more likely to comply with a relevant other's expectations is consistent with findings in technology acceptance literature. Although IS literature based on the TRA, Technology Acceptance Model (TAM, TAM2), TPB, Innovation Diffusion Theory, and other theories has used a variety of labels for subjective norm constructs, each of these constructs contains the notion that an individual's behaviour is influenced by what relevant others expect her/him to do. In considering norms in an organisational setting, studies have examined employees' perceptions of the expectations of superiors, managers, and peers in relevant IS departments (Karahanna *et al*., 1999; Venkatesh *et al*., 2003). If the employee believes that the managers, IT personnel, or peers expect information security policy compliance, she/he is more likely to intend to comply. Hence, we propose:

H12 *Subjective norms [expectations of relevant others] will positively affect intention to comply with organisational information security policies.*

In addition to subjective norms, the influence of peer behaviour encourages a person to do certain things under pressure. Descriptive norms, which are the extent to which one believes that others are performing the desired behaviour, focus on the propensity that an individual may have to replicate the believed behaviour of others (Sheeran & Orbell, 1999; Rivis & Sheeran, 2003). Information technology literature has considered the role of the subjective culture of referent groups or peer behaviours as a motivational source for performing a behaviour in question (Thompson *et al*., 1991, 1994; Venkatesh *et al*., 2003). People often perform (or believe in) certain actions or non-actions because many other people do (or believe) the same. In the context of this study, if an employee believes that her/his colleagues follow the organisational security policies, she/he is more likely to have positive intentions to follow them as well. Thus, we can expect:

H13 *Descriptive norms [behaviour of similar others] will positively influence intentions to comply with security policies.*

Organisational commitment

The study of organisational commitment has a long history that has produced a large body of literature (Mowday, 1998). Organisational behaviour literature has noted that organisational commitment influences employee outcomes in various ways. Organisational commitment, which is defined as the overall strength of an individual's identification with and involvement in an organisation, captures the relationship between employees and their work organisations (Mowday, 1998). It is viewed as an internalised normative pressure to act in a way that meets organisational goals and interests such that the stronger the commitment, the stronger the predisposition to be guided in actions (Wiener, 1982). In general, with high organisational commitment the organisation is assured of high levels of performance and task completions (Randall, 1987).

An employee's commitment to an organisation is likely to play a role in his/her engagement in security behaviours. People in an organisation are less likely to enact counterproductive computer behaviours that put the company systems at risk if their organisational commitment is high (Stanton *et al*., 2003). Also, employees with higher involvement in an organisation are likely to believe that their actions have an impact on the organisation's overall performance. In a security context, such employees tend to believe that their security-conscious behaviours are likely to have an impact on the achievement of overall organisational information security. Thus, we can expect that:

H14 *Higher levels of organisational commitment will lead to higher employee perceptions of the effectiveness of their actions.*

H15 *The level of organisational commitment will positively affect the intentions to follow security policies.*

Methodology

The overall approach taken to perform an empirical test of the relationships suggested by the research model was a field study using survey methodology for data collection. In the following sections, we discuss the details of

the instrument development and survey administration processes.

Instrument development

Using validated and tested questions improves the reliability of results (Straub, 1989). To reduce problems with the reliability and validity of questionnaire, whenever possible, we adopted the items from previous validated studies. Policy compliance intention was considered a dependent variable in this study. The items for policy compliance intention were adapted from Anderson (2005) and Chan *et al*. (2005). Each item involved a 7-point Likert scale to indicate a respondent's level of agreement with the statements regarding the likelihood of complying with the information security policies of their organisations. All questions considered in this study were measured using a 7-point Likert scale.

The effect of protection motivation was captured using four constructs: severity of security breach (*Strongly Disagree–Strongly Agree*), certainty of security breach (*Highly Unlikely–Strongly Likely*), security breach concern (*Strongly Disagree–Strongly Agree*), and effectiveness of a person's actions (*Strongly Disagree–Strongly Agree*). The questions were adapted from Ellen *et al*. (1991) and Anderson (2005). The attitude construct captured users' attitudes towards security policies, and was adapted from Peace *et al*. (2003) and Riemenschneider *et al*. (2003). Items for employees' perceptions of the effectiveness of their security behaviour were adapted from studies by Culnan (2004) and Anderson (2005). These items capture an individual's belief that her/his individual actions can make a difference in securing the organisational IS using a 7-point Likert scale (*Strongly Disagree–Strongly Agree*).

To understand the role of deterrence, two constructs were used in our study. Punishment severity and certainty of detection items were adopted from a piracy-related study by Peace *et al*. (2003) and an information security-related study by Knapp *et al*. (2005) which considered the policy enforcement dimension for managers. The questions were designed to gauge the level of agreement with statements related to the likelihood of detection and possible penalty with a set of 7-point Likert scale questions.

In order to understand the role of social influence, we used subjective norms and descriptive norms. Questions pertaining to subjective norms were taken from the study by Karahanna *et al*. (1999). Descriptive norm questions were adapted from Anderson (2005). Self-efficacy and resource availability questions were adopted from facilitating conditions questions used in Taylor & Todd (1995), whereas the organisational commitment items were adopted from Mowday, Steer, and Porter's organisational commitment questionnaire reprinted in Barge & Schlueter (1988).

Moreover, to control for an explanation of results due to extraneous factors, several control variables were added. These included demographic characteristics such as gender, age, education, and participant job role. Job affiliation, in terms of IT or non-IT jobs, was added as a control variable as the varied participant roles in their organisations may lead to different expectations and appreciation with respect to security policy compliance. A large, well-organised company and its IT department are likely to have a set of well-specified policy and practices in place. Also, an adequate annual security budget is likely to result in an IT department having more enforcement as well as more awareness mechanisms. Hence, the size of the company based on the number of computers and annual security budget in the organisation were added as an organisational control factors.

When most of the constructs are adopted from earlier studies, although the validation may be sound, additional content validation using a multi-stage iterative procedure is recommended. The instrument was pretested by field experts through interviews that sought ways to reduce ambiguity. Experts on the panel included personnel from both academia and industry. A group consisting of faculty members from MIS, Sociology, and Computer Science; three IT professionals from the banking industry; and three FBI experts working in cybersecurity were solicited to give input regarding content validity and the clarity of the wording for each item. The field experts were encouraged to give feedback about the comprehensiveness and exclusiveness of the instrument. The revised version of the questionnaire was also reviewed to remove any ambiguity. Items were added, reworded, and deleted in the pre-test. The instrument was examined several times by this panel (twice by some experts and three times by others). Once consensus was reached regarding the clarity and validity of the instrument, the online survey was prepared. Where necessary, terms were explicitly defined (e.g., IS security, security policies, security precautions) so that each respondent had a common understanding of each term.

A pilot test was carried out to ensure the initial reliability of the scales and the general mechanics of the questionnaire, particularly survey instructions, completion time, and appropriate wording. The pilot was conducted with a group of undergraduate students, graduate students, and employees of a large northeastern American university. Twenty-three students and 25 employees participated in the pilot test. A Cronbach's alpha test was conducted to do a preliminary reliability test of the scale.

Survey administrations and participants

The study was carried out in collaboration with the Cyber Task Force, Buffalo Division,FBI. Employees from several organisations were requested to participate in the web-based survey (10 employees from each organisation). Due to the nature of the study, permission to carry out the study needed to be sought from the top management in each respective organisation. High-level IS managers in approximately 690 organisations were contacted, of which approximately 120 indicated their interest in participating. After identifying the employees in each

organisation, who worked in diverse roles but used computers and the Internet as part of their daily work routine, invitations to participate were distributed through administrative assistants. Our data set shows that employees from 78 organisations in the western New York area participated in this study.

Due to the relatively sensitive nature of the information sought, many safeguards were put in place to encourage participation and solicit honest responses. Precautionary measures were adopted to ensure the anonymity of survey responses. Participants were directed to a survey website hosted on a secure university server. The raw data collected was not available to anyone other than the primary investigator. Moreover, to boost confidence, survey respondents were assured that no personal information was attached to their responses and that the data collected was for research purposes only. Code numbers were used to ensure that each respondent completed only one survey. Incentives to encourage participation were offered in the form of a draw for several gift certificates valued at $25 and $50. If participants wished to participate in the draws, they were directed to enter their information on a separate website.

The consideration of various types of organisations as well as participants working in different roles within the organisations ensures the heterogeneity of the sample and provides robustness and generalisability to the results. The 312 responses represent employees from 78 organisations. The average age of participants was 42.3 years, ranging from 18 to 70 years. The participants worked in various roles, including IT personnel, non-IT personnel, engineers, technicians, accounting managers, medical professionals, administrative assistants, etc. 46% of the respondents were female, whereas 54% of the respondents were male. The average education level reported was: 'completed a university or bachelor's degree'. Details of the sample demographics are reported in Table A1 of the appendices.

Data analysis

We used SmartPLS and SPSS for measurement validation and to test the structural model. Partial Least Square (PLS) employs a component-based approach for estimation and places minimal restrictions on sample size and residual distributions. Bootstrapping with 500 re-samples was performed to get the statistical significance of path coefficients using a t-test.

Instrument validation

Before testing the hypothesised structural model, the psychometric properties of the measures were evaluated. The subjective norm was modelled as a formative (aggregate or composite) latent construct, following Karahanna *et al*. (1999). Similarly, resource availability was also modelled as formative, as theoretically, the indicators may be seen to employ different themes and may not be interchangeable. For the formative constructs, the examination of weights in the principal component analysis is suggested rather than the evaluation of loadings in common factor analysis (Bollen & Lennox, 1991). The results (depicted in Figure 2) indicate that item weightings for three of the five subjective norm measures were found to be significant. In considering the various resources, the formative resource availability construct also revealed that three of the five items were significant. However, to retain content validity (Petter *et al*., 2007) all of the indicators were kept in the model.

Excessive multicollinearity between the construct items in formative constructs can destabilise the model. Hence, a variance inflation factor (VIF) test is suggested to determine whether the formative measures are highly correlated to ensure multicollinearity is not present. VIF statistics for all the formative measures considered in the two constructs presented were under the 3.3 threshold, which suggests that a high multicollinearity was not present (Petter *et al*., 2007). In addition, we carried out MTMM analysis as suggested by Loch *et al*. (2003). We report the inter-item and item-to-construct correlation matrix and related analysis in the Appendix (Appendix Table A4).

To assess reflective constructs in our measurement model, we examined construct reliability, convergent validity, and discriminant validity. Construct reliability measures the degree to which items are free from random error, and therefore, yields consistent results. Reliability for the constructs was assessed using composite reliability scores. The composite reliability (Table 2) for all constructs was considered acceptable because it exceeded the 0.70 threshold (Gefen *et al*., 2000).

Convergent validity assesses consistency across multiple items. Convergent validity is shown when the PLS indicators load much higher on their hypothesised factor than on other factors (i.e., own loadings are higher than cross loadings). All estimated standard loadings were significant ($P<0.001$) (Gefen & Straub, 2005) and of acceptable magnitude (above 0.70) (Chin & Marcolin, 1995), which suggests good convergent validity. The loadings, weights, and the items used in this study are presented in Appendix Table A2.

To test discriminant validity, the extent to which different constructs diverge from one another, the square root of the Average Variance Extracted (AVE) of the multi-item reflective constructs should be greater than the absolute value of the inter-construct correlations (Gefen & Straub, 2005). As shown in Table 2, the square root of the AVE of all constructs was found to be much larger than all other cross-correlations.

Cross loadings were evaluated to further test for convergent and discriminant validity. All the loadings of the measurement items on their assigned latent variables were found to be at least an order of magnitude larger than any other loading (Gefen & Straub, 2005). All AVE values were above 0.50, which suggests that the principal constructs capture a much higher construct-related variance than error variance. Correlations among all constructs were all well below the 0.90 threshold,

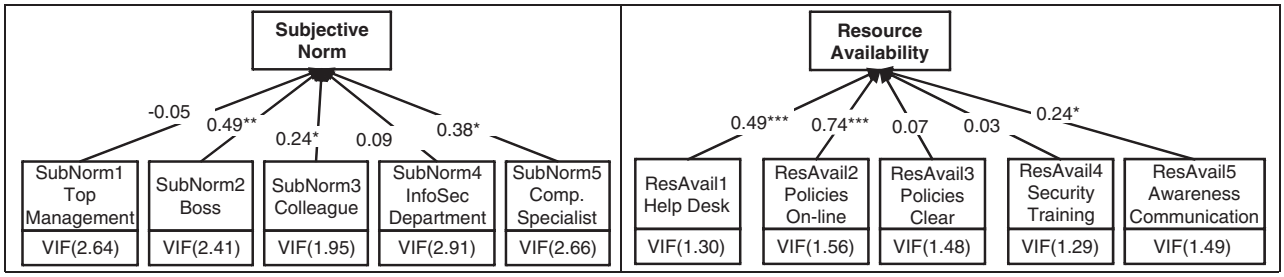

Figure 2 Formative nature of subjective norm and resource availability.
Note: * significant at $P<0.05$ level; ** significant at $P<0.01$ level; *** significant at $P<0.001$ level.

Table 2 Cross correlation matrix, average variance extracted and reliability statistics of principal reflective constructs

	AVE	*Comp. reliab.*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*
IncCert	0.82	0.93	**0.90**													
IncSev	0.83	0.93	0.62	**0.91**												
SecConcern	0.56	0.79	0.18	0.23	**0.75**											
ResAvail	0.00	0.00	−0.14	−0.09	0.21	—										
SelfEfficacy	0.87	0.95	−0.08	0.00	0.36	0.50	**0.93**									
ResEff	0.66	0.85	0.01	0.02	0.29	0.24	0.26	**0.81**								
Cost	1.00	1.00	−0.01	0.02	−0.12	−0.07	−0.02	−0.29	**1.00**							
SecPolAtt	0.87	0.95	0.05	0.05	0.55	0.28	0.37	0.50	−0.33	**0.93**						
OrgCommit	0.55	0.79	−0.07	−0.04	0.24	0.21	0.37	0.43	−0.23	0.34	**0.74**					
PunSev	0.71	0.88	−0.17	−0.10	0.07	0.42	0.25	0.13	−0.07	0.19	0.25	**0.84**				
DetCert	0.76	0.86	−0.15	−0.16	0.09	0.39	0.25	0.13	−0.10	0.17	0.20	0.63	**0.87**			
DesNorm	0.88	0.96	−0.25	−0.15	0.04	0.38	0.32	0.12	−0.10	0.13	0.25	0.54	0.45	**0.94**		
SubNorm	0.00	0.00	−0.09	0.05	0.40	0.52	0.58	0.35	−0.13	0.45	0.39	0.29	0.28	0.41	—	
CompInt	0.84	0.94	−0.04	0.04	0.31	0.39	0.51	0.38	−0.19	0.38	0.43	0.24	0.32	0.33	0.59	**0.92**

Note: The shaded bold values in diagonal represent the sqrt (AVE) values. Resource availability and subjective norm are formative constructs.

which suggests that all constructs are distinct from each other. Jointly, these tests suggest good convergent and discriminant validity.

Testing of structural model

The standardised PLS path coefficients are shown in Figure 3. Our results show that nearly 48% of the variance in the security policy attitudes and 47% of the variance in policy compliance intentions were explained by the factors considered in the integrated model.

Security policy attitude was found not to have a significant impact on policy compliance ($\beta=0.073$: H5); therefore H1 is not supported. The employee-perceived severity of a security breach was found to have a significant effect on the security concern ($\beta=0.191$ $P<0.05$), which supports H2. The perceived probability of a security breach was not found to have a significant effect on the security breach concern ($\beta=0.065$), thus H3 is not supported. Supporting H4, security breach concern was found to have a significant effect on attitudes towards security policies ($\beta=0.393$ $P<0.001$).

As anticipated, response efficacy or effectiveness of one's action, the fourth dimension of protection motivation considered in this study, was also found to have a significant effect on attitudes towards security policies ($\beta=0.288$ $P<0.001$), thus supporting H5. Response cost was found to have a significant negative impact on security policy attitudes ($\beta=-0.195$ $P<0.001$) which supports H6.

Self-efficacy was found to have a significant impact both on the attitude towards security polices ($\beta=0.148$ $P<0.05$: H7) as well as intentions of complying with security policies ($\beta=0.173$ $P<0.05$: H8), thus supporting hypotheses H5 and H6. Self-efficacy was in turn significantly associated with the resource availability ($\beta=0.505$ $P<0.001$), which supports H9.

Regarding the deterrence dimension, punishment severity was found to have a significant impact on policy compliance intention ($\beta=-0.14$ $P<0.005$ level); however, the direction of the relationship was opposite to that hypothesised. Thus, H10 was not supported. On the other hand, certainty of detection was found to have a

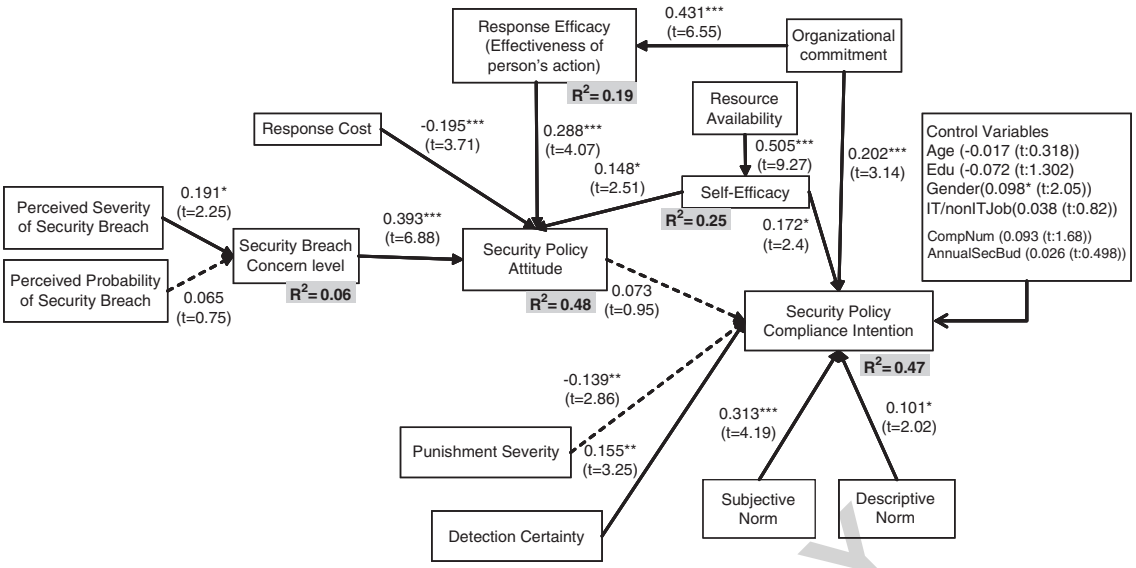

Figure 3 Results for the proposed research model.
Note: * significant at $P<0.05$ level; ** significant at $P<0.01$ level; *** significant at $P<0.001$ level.

significant effect on policy compliance intention in the hypothesised direction ($\beta=0.155$ $P<0.001$), thus supporting H11.

In support of H12, the subjective norm was found to have a significant impact on policy compliance intention ($\beta=0.313$ $P<0.001$); the descriptive norm also was found to have a significant impact on policy compliance intention ($\beta=0.101$ $P<0.05$), thus supporting H13.

The two relationships envisioned regarding organisation commitment were both found to be significant. Supporting H14, organisational commitment was found to significantly impact response efficacy ($\beta=0.431$ $P<0.001$), and it was also found to have a significant effect on policy compliance intention ($\beta=0.202$ $P<0.001$), thus supporting H15.

Discussion of key findings and implications

This study has several key findings and offers several theoretical and practical implications. Despite the recent emphasis on behavioural research in information security, this study is one of the earliest to evaluate policy compliance intentions. On the theoretical level, we evaluate the behaviours of an organisation's employees as related to security policy compliance intentions in an integrated framework that uses PMT, Deterrence Theory, Organisational Commitment, and the DTBP. From a practical standpoint, our research offers implications for security policy compliance in organisations.

Our results indicate that employees' understanding of the severity of the threat significantly affects their concern regarding security breaches. We, however, found that the certainty of security breaches does not have a significant impact on the security concern. Our data suggests that on average, employee perceived security breach certainty perceptions are low (below neutral, with mean = 3.78, SD = 1.56). Our results suggest that if employees believe that complying with policies is a hindrance to their day-to-day job activity, they are less likely to have favourable views towards security polices. However, the perceived effectiveness of employee actions was found to play a role in behaviours related to information security policy compliance. We found that if employees perceive that their compliance behaviours have a favourable impact on the organisation or benefit the organisation, they are more likely to have more positive attitudes towards the security policies. It is critical that IT management make efforts to convey to employees that information security is important to an organisation and that employee actions make a difference in achieving the overall goal of system security. More importantly, it is necessary for IT management to communicate the reality of security threats to organisational end-users.

Resource availability was found to significantly enhance employees' abilities to perform the necessary security-related actions. These abilities (self-efficacy) were found to have an effect on both security policy attitudes and intentions to comply with policies. Thus, employee self-efficacy is likely to result in favourable attitudes and more compliance intentions. As such, managers need to make security policy-related resources easily available to employees. As Gist (1987) argues, the implications of self-efficacy for training or organisational development are numerous. Security literature has emphasised that managers need to pay attention to security awareness and training initiatives.

We found the impact of attitude on policy compliance intentions to be insignificant. In line with the vast

literature that has considered the direct relationship of PMT constructs to intentions, we carried out a *post-hoc* analysis which shows that amongst the PMT constructs, response efficacy and self-efficacy have a direct and significant impact on compliance intentions, whereas response cost and security concern did not significantly contribute to predicting compliance intentions.

Our findings suggest that social influence also plays a role in employee security behaviours. Findings from our sample suggest that normative beliefs related to expectations from relevant others have a significant impact on employee behaviours. This suggests that beliefs regarding the expectations of superiors, peers, and IT personnel seem to have the most impact on employee security behaviours. Not only the expectations of others, but also the perceived behaviour of similar others, was found to be a significant contributor in employee intentions to comply with the policies. Managers can improve security compliance by enhancing the security climate in their organisation. We would like to note here that in the formative construction of the five items related to subjective norms, three weights (boss, colleague, and computer specialist) were found to be significant whereas two weights (top management and IS security department) were found to be insignificant. This may be due to the fact that not all organisations have separate security department. Also, employees may not be aware of the top management's expectations. Broadly, our items fall into two categories: expectations from individuals and expectations from the organisation. An analysis based on this view of our results suggests that employees may not have direct knowledge of organisational expectations.

In testing the effects of deterrence, the certainty of detection was found to have a positive impact on security policy compliance intentions. If employees perceive that there is high likelihood of getting caught if they violate security policies, they are more likely to follow the security policies. Surprisingly, the severity of penalty was found to have a negative impact on security behaviour intentions. In fact, sanctions have been found to have mixed results in the IS security literature (Kankanhalli *et al*., 2003; Pahnila *et al*., 2007). Our results suggest that the existence and visibility of detection mechanisms is perhaps more important than the severity of penalty imposed.

Employee organisational commitment was found to have a significant impact on both the policy compliance intentions and perceived effectiveness of employee actions. The extant literature in organisational behaviour suggests ways to increase organisational commitment and can give us insights into the managerial actions that promote employee involvement.

The limitations of this study create several opportunities for further research. The formative resource availability construct reveals that two of the five items considered did not have statistically significant weights. These two items relate to the online availability of policies and to security training. Various resources and their role in security facilitation need further investigation. The insignificant effect of attitude on policy compliance intention may be due to reasons such as context, sample, or other extraneous factors. Also one may posit that attitudes may be desensitised when deterrent efforts in the organisation, norms, efficacy, and commitment come into play, resulting in less of an impact on intention. Additional research is needed to substantiate and understand this issue. Further investigation into security policy and policy compliance attitudes can be carried out with in-depth interviews and focus group discussion. This study did not consider reward systems as a means to promote policy compliance that may exist, so this should be considered by future studies. This study focuses on user intentions to comply with the security policies. Although intentions are likely to have a significant impact on actual behaviour, many factors such as habits and time needed for task achievement are likely to play important roles and need to be considered by future studies. Moreover, the consideration of the characteristics of the individuals such as personality traits was outside the scope of this study. Personality factors such as responsibility acceptance, conscientiousness, and agreeableness that have recently been used in the security literature (Shropshire *et al*., 2006) can be further incorporated to understand their effect on the threat perceptions, protection motivations, and policy compliance. Furthermore, this study uses a data set collected in a limited geographic area of Western New York. Further investigation is warranted with wider samples, samples collected from different countries, as well as additional personal characteristics and organisational variables. Future studies with larger samples representing various sectors may allow an examination of patterns contributing to a shared sense of mission. For example, the banking industry, the health care industry, or academic organisations may show patterns that are driven by the unique needs of the sector. Also, the mandatory nature of policy compliance in organisations that is likely to arise from sector specific demands may be an issue for further investigation. This study considers the hindrance caused by policy compliance in terms of response cost; however, the rewards of continuing the maladaptive practice of ignoring the policies were not captured in this study and remain to be investigated.

Conclusion

Although organisations are actively using security technologies and practices, it is known that information security cannot be achieved through technological tools alone, and thus, organisations are forced to consider information security policies. Most organisations spend time and resources to provide, establish, and monitor computer security policies; however, if the end-users of organisational IS are not keen or willing to follow the policies, then these efforts are in vain. In this paper, we develop an Integrated Protection Motivation and Deterrence Model of security policy compliance under the

umbrella of Taylor-Todd's Decomposed Theory of Reasoned Action. We also evaluate the effect of organisational commitment on employee security compliance intentions. With the help of 312 employee responses from 78 organisations, we perform an empirical test on the proposed model. Our results suggest that (a) perceptions about the severity of breach, response efficacy and self-efficacy are likely to have a positive effect on attitudes towards security policies, whereas response cost negatively influences the favourable attitudes; (b) social influence has a significant impact on compliance intentions; (c) resource availability is a significant factor in enhancing self-efficacy, which in turn, is a significant predictor of policy compliance intentions; and (d) organisational commitment plays a dual role by impacting intentions directly as well as promoting a belief that employee actions have an effect on an organisation's overall information security.

Acknowledgements

We appreciate the support and collaboration on this project by the Cyber Task Force, Buffalo Division, FBI. This research is funded in part by NSF under grant #0402388 and MDRF grant #F0630. The research of the second author is also supported in part by NSF under grant #0809186. The usual disclaimer applies.

About the Authors

Tejaswini Herath, Ph.D., is an assistant professor in the Faculty of Business at Brock University, Canada. She graduated from Department of Management Science and Systems at State University of New York, Buffalo (UB). Previously she worked as a systems analyst and a part-time lecturer at UNBC, Canada. Her research interests are in Information Assurance and include topics such as information security and privacy, diffusion of information assurance practices, economics of information security, and risk management. Her work has been accepted or published in the *Journal of Management Information Systems*, *Decision Support Systems*, *Information Systems Management*, and *International Journal of E-Government Research*. She was the recipient of the Best Paper Award at the 30th McMaster World Congress (2009) on E-Crime Prevention, and the recipient of the UB Ph.D. Student Achievement Award (2007–2008).

H. Raghav Rao, Ph.D., graduated from Krannert Graduate School of Management at Purdue University. He has chaired sessions at international conferences and presented numerous papers. He also has co-edited four books of which one is on Information Assurance in Financial Services. He has authored or co-authored more than 150 technical papers, of which more than 75 are published in archival journals. His work has received best paper and best paper runner up awards at AMCIS and ICIS. Dr. Rao has received funding for his research from the National Science Foundation, the Department of Defense, and the Canadian Embassy and he has received the University's prestigious Teaching Fellowship. He has also received the Fulbright fellowship in 2004. He is a co-editor of a special issue of *The Annals of Operations Research*, *The Communications of ACM*; and associate editor of *Decision Support Systems*, *Information Systems Research*, and *IEEE Transactions in Systems*, *Man and Cybernetics*; and co-editor-in-chief of *Information Systems Frontiers*. Dr. Rao also has a courtesy appointment with Computer Science and Engineering as an adjunct professor. He is the recipient of the 2007 SUNY Chancellor's award for excellence.

References

AJZEN I (1991) Theory of planned behavior. *Organizational Behavior and Human Decision Processes* **50(2),** 179–211.

AJZEN I and FISHBEIN M (1980) Prediction of goal-directed behavior: attitudes, intentions, and perceived behavioral control. *Journal of Experimental Social Psychology* **22,** 453–474.

AKERS R (1990) Rational choice, deterrence, and social learning theory in criminology: the path not taken. *The Journal of Criminal Law and Criminology* **81(3),** 653–676.

ALBRECHTSEN E (2007) A qualitative study of users' view on information security. *Computers & Security* **26(4),** 276–289.

ANDERSON C (2005) Creating the conscientious cybercitizen: an examination of home computer user attitudes and intentions towards security. In *Tenth INFORMS Conference on Information Systems and Technology (CIST)* San Francisco, California, USA.

ARMITAGE C and CONNER M (2000) Social cognition models and health behaviour: a structured review. *Psychology and Health* **15(2),** 173–189.

AXELROD LJ and NEWTON JW (1991) Preventing nuclear war: beliefs and attitudes as predictors of disarmist and deterrentist behavior. *Journal of Applied Social Psychology* **21(1),** 29–40.

BAGOZII RP (1992) The self-regulation of attitudes, intentions and behavior. *Social Psychology Quarterly* **55(2),** 178–204.

BANDURA A, ADAMS NE, HARDY AB and HOWELL GN (1980) Tests of the generality of self-efficacy theory. *Cognitive Theory And Research* **4(1),** 39–66.

BARGE JK and SCHLUETER D (1988) A critical evaluation of organizational commitment and identification. *Management* **2(1),** 116–133.

BOLLEN K and LENNOX R (1991) Conventional wisdom on measurement: a structural equation perspective. *Psychological Bulletin* **110(2),** 305–314.

CERT/CC (2004) 2004 e-Crime watch survey summary of findings. Computer Emergency Response Team Coordination Center (CERT/CC). Available at http://www.cert.org/archive/pdf/2004eCrimeWatchSummary.pdf. Accessed 15 January 2007.

CHAN M, WOON I and KANKANHALLI A (2005) Perceptions of information security at the workplace: linking information security climate to compliant behavior. *Journal of Information Privacy and Security* **1(3),** 18–41.

CHENG H, SIMS R and TEEGEN H (1997) To purchase or to pirate software: an empirical study. *Journal of Management Information Systems* **13(4),** 49–60.

CHIN WW and MARCOLIN B (1995) A holistic approach to construct validation in is research: examples of the interplay between theory and measurement. In *Administrative Sciences Association of Canada – 23rd Conference* (CAMPEAU D, Ed.), Windsor, Ontario.

CIALDINI RB, KALLGREN CA and RENO RR (1991) A focus theory of normative conduct: a theoretical refinement and reevaluation of the role of norms in human behavior. In *Advances in Experimental Social Psychology* (ZANNA MP, Ed.), pp 201–234, Academic Press, San Diego, CA.

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

CULNAN M (2004) Bentley survey on consumers and internet security: summary of findings. [WWW document] http://www.bentley.edu/events/iscw2004/survey_findings.pdf (accessed on 31 January 2009).

D'ARCY J and HOVAV A (2004) The role of individual characteristics on the effectiveness of IS security countermeasures. In *Tenth Americas Conference on Information Systems* New York.

DHILLON G and BACKHOUSE J (2001) Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal* **11(2),** 127–153.

DHILLON G and TORKZADEH G (2006) Value-focused assessment of information system security in organizations. *Information Systems Journal* **16(3),** 293–314.

EHRLICH I (1996) Crime, punishment, and the market for offenses. *Journal of Economic Perspectives* **10(1),** 43–67.

ELLEN PS, WIENER JL and COBB-WALGREN C (1991) The role of perceived consumer effectiveness in motivating environmentally conscious behaviors. *Journal of Public Policy & Marketing* **10(2),** 102–117.

FINCH J, FURNELL S and DOWLAND P (2003) Assessing IT security culture: system administrator and end-user perspectives. In *Proceedings of ISOneWorld 2003 Conference and Convention* Las Vegas, Nevada, USA.

FLOYD DL, PRENTICE-DUNN S and ROGERS RW (2000) A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology* **30(2),** 407–429.

FURNELL SM, BRYANT P and PHIPPEN AD (2007) Assessing the security perceptions of personal internet users. *Computers & Security* **26(5),** 410–417.

GEFEN D and STRAUB DW (2005) A practical guide to factorial validity using PLS-graph: tutorial and annotated example. *Communications of the Association for Information Systems* **16,** 91–109.

GEFEN D, STRAUB DW and BOUDREAU M-C (2000) Structural equation modelling and regression: guidelines for research practice. *Communications of the Association for Information Systems* **4,** 1–77.

GIST M (1987) Self-efficacy: implications for organizational behavior and human resource management. *Academy of Management, The Academy of Management Review* **12(3),** 472–485.

GORDON LA, LOEB MP, LUCYSHYN W and RICHARDSON R (2006) 2006 CSI/FBI computer crime and security survey. Computer Security Institute.

GRUBE JW, MORGAN M and MCGREE ST (1986) Attitudes and normative beliefs as predictors of smoking intentions and behaviours: a test of three models. *British Journal of Social Psychology* **25,** 81–93.

IGBARIA M and IIVARI J (1995) The effects of self-efficacy on computer usage. *International Journal of Management Science* **23(6),** 587–605.

KANKANHALLI A, TEO H-H, TAN BCY and WEI K-K (2003) An integrative study of information systems security effectiveness. *International Journal of Information Management* **23(2),** 139–154.

KARAHANNA E, STRAUB DW and CHERVANY NL (1999) Information technology adoption across time: a cross-sectional comparison of pre-adoption and post-adoption beliefs. *MIS Quarterly* **23(2),** 183–213.

KNAPP KJ, MARSHALL TE, RAINER RK and FORD FN (2005) *Managerial Dimensions in Information Security: A Theoretical Model of Organizational Effectiveness* (ISC)2 Inc., Palm Harbor, Florida and Auburn University, Auburn, Alabama.

LEE SM, LEE S-G and YOO S (2004) An integrative model of computer abuse based on social control and general deterrence theories. *Information and Management* **41(6),** 707–718.

LOCH KD, CARR HH and WARKENTIN ME (1992) Threats to information systems: today's reality, yesterday's understanding. *MIS Quarterly* **16(2),** 173.

LOCH KD, CONGER S and OZ E (1998) Ownership, privacy and monitoring in the workplace: a debate on technology and ethics. *Journal of Business Ethics* **17(6),** 653–663.

LOCH KD, STRAUB DW 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),** 45–63.

MA Q and PEARSON JM (2005) ISO 17799: 'Best practices' in information security management? *Communications of the Association for Information Systems* **15,** 577–591.

MADDUX JE and ROGERS RW (1983) Protection motivation and self-efficacy: a revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology* **19(5),** 469–479.

MELAMED S, RABINOWITZ S, FEINER S, WEISBERG E and RIBAK J (1996) Usefulness of the protection motivation theory in explaining hearing protection device use among male industrial workers. *Health Psychology* **15(3),** 209–215.

MILNE S, SHEERAN P and ORBELL S (2000) Prediction and intervention in health-related behavior: a meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology* **10(1),** 106–143.

MISHRA S and DHILLON G (2006) Information systems security governance research: a behavioral perspective. In *1st Annual Symposium on Information Assurance, Academic Track of 9th Annual NYS Cyber Security Conference* pp 27–35 New York, USA.

MOWDAY R (1998) Reflections on the study and relevance of organizational commitment. *Human Resources Management Review* **8(4),** 387–401.

NEUWIRTH K, DUNWOODY S and GRIFFIN RJ (2000) Protection motivation and risk communication. *Risk Analysis* **20(5),** 721–734.

PAHNILA S, SIPONEN M and MAHMOOD A (2007) Employees' behavior towards IS security policy compliance. In *40th Hawaii International Conference on System Sciences (HICSS 07)* Hawaii, USA.

PALARDY N, GREENING L, OTT J, DOLDERBY A and ATCHISON J (1998) Adolescents' health attitudes and adherence to treatment for insulin-dependent diabetes mellitus. *Developmental and Behavioral Pediatrics* **19(1),** 31–37.

PEACE AG, GALLETTA D and THONG J (2003) Software piracy in the workplace: a model and empirical test. *Journal of Management Information Systems* **20(1),** 153–177.

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

POST GV and KAGAN A (2007) Evaluating information security tradeoffs: restricting access can interfere with user tasks. *Computers & Security* **26(3),** 229–237.

PRIVACYRIGHTS.ORG (2005) A chronology of data breaches. Available at http://www.privacyrights.org/ar/chronDataBreaches.htm, accessed 21 January 2007.

PRIVACYRIGHTS.ORG (2006) 2006 disclosures of U.S. data incidents. Available at http://www.privacyrights.org/ar/chronDataBreaches.htm, accessed 21 January 2007.

RANDALL D (1987) Commitment and the organization: the organization man revisited. *Academy of Management Review* **12(3),** 460–471.

RIEMENSCHNEIDER CK, HARRISSON D and MYKYTYN PP (2003) Understanding IT adoption decisions in small business: integrating current theories. *Information and Management* **40,** 269–285.

RIVIS A and SHEERAN P (2003) Social influences and the theory of planned behavior: evidence for a direct relationship between prototypes and young people's exercise behavior. *Psychology and Health* **18(5),** 567–583.

ROGERS RW (1975) A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology* **91,** 93–114.

ROGERS RW (1983) Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protected motivation. In *Social Psychophysiology: A Sourcebook* (CACIOPPO JT and PETTY RE, Eds), pp 153–176, The Guilford Press, New York.

SAKS A and BELCOURT M (2006) An investigation of training activities and transfer of training in organizations. *Human Resources Management* **45(4),** 629–648.

SHEERAN P and ORBELL S (1999) Augmenting the theory of planned behavior: roles for anticipated regret and descriptive norms. *Journal of Applied Social Psychology* **29(10),** 2107–2142.
SHROPSHIRE J, WARKENTIN M, JOHNSTON AC and SCHMIDT MB (2006) Personality and it security: an application of the five-factor model. In *Proceedings of the Americas Conference on Information Systems* pp 3443–3449.
SIPONEN MT (2000) A conceptual foundation for organizational information security awareness. *Information Management and Computer Security* **8(1),** 31–41.
STAJKOVIC A and LUTHANS F (1998) Self-efficacy and work-related performance: a meta analysis. *Psychological Bulletin* **124(2),** 240–261.
STANLEY MA and MADDUX JE (1986) Cognitive processes in health enhancement: investigation of a combined protection motivation and self-efficacy model. *Basic and Applied Social Psychology* **7(2),** 101–113.
STANTON JM, STAM K, GUZMAN I and CALDERA C (2003) Examining the linkages between organizational commitment and information security. In *IEEE Systems, Man, and Cybernetics Conference* Washington DC, USA.
STANTON JM, STAM KR, MASTRANGELO P and JOLTON J (2005) Analysis of end user security behaviors. *Computers & Security* **24(2),** 124–133.
STEFFEN VJ (1990) Men's motivation to perform the testicle self-exam: effects of prior knowledge and an educational brochure. *Journal of Applied Social Psychology* **20(8),** 681–702.
STRAUB DW (1989) Validating instruments in MIS research. *MIS Quarterly* **13(2),** 147–169.
STRAUB DW (1990) Effective is security: an empirical study. *Information Systems Research* **1(3),** 255–276.
STRAUB DW and COLLINS RW (1990) Key information issues facing managers: software piracy, proprietary databases, and individual rights to privacy. *MIS Quarterly* **14(2),** 143–156.
STRAUB DW and NANCE WD (1990) Discovering and disciplining computer abuse in organization. *MIS Quarterly* **14(1),** 45–60.
TANNER JF, HUNT JB and EPPRIGHT DR (1991) The protection motivation model: a normative model of fear appeals. *Journal of Marketing* **55(3),** 36–45.
TAYLOR S and TODD PA (1995) Understanding information technology usage – a test of competing models. *Information Systems Research* **6(2),** 144–176.
THOMPSON RL, HIGGINS CA and HOWELL JM (1991) Personal computing: toward a conceptual model of utilization. *MIS Quarterly* **15(1),** 124–143.
THOMPSON RL, HIGGINS CA and HOWELL JM (1994) Influence of experience on personal computer utilization. *Journal of Management Information Systems* **11(1),** 167–187.
THOMSON KL and VON SOLMS R (1998) Information security awareness: educating your users effectively. *Information Management & Computers Security* **6(4),** 167–173.
TORKZADEH R, PFLUGHOEFT K and HALL L (1999) Computer self-efficacy, training effectiveness and user attitudes: an empirical study. *Behaviour and Information Technology* **18(4),** 299–309.
VENKATESH V and BROWN S (2001) A longitudinal investigation of personal computers in homes: adoption determinants and emerging challenges. *MIS Quarterly* **25(1),** 71–102.
VENKATESH V, MORRIS MG, DAVIS GB and DAVIS FD (2003) User acceptance of information technology: toward a unified view. *MIS Quarterly* **27(3),** 425–478.
VON SOLMS B (2001) Information security – a multidimensional discipline. *Computers & Security* **20(6),** 504–508.
VON SOLMS R and VON SOLMS B (2004) From policies to culture. *Computers & Security* **23(4),** 275–279.
VROOM C and VON SOLMS R (2004) Towards information security behavioural compliance. *Computers & Security* **23(3),** 191–198.
WIENER Y (1982) Commitment in organizations: a normative view. *Academy of Management Review* **7(3),** 418.
WILLIAMS K and HAWKINS R (1986) Perceptual research on general deterrence: a critical review. *Law and Society Review* **20(4),** 545–572.
WITTE K and ALLEN M (2000) A meta-analysis of fear appeals: implications for effective public health campaigns. *Health Education & Behavior* **27(5),** 591–615.
WOON IMY, TAN GW and LOW RT (2005) A protection motivation theory approach to home wireless security. In *International Conference on Information Systems* pp 367–380 Las Vegas, USA.
ZHANG X (2005) What do consumers really know about spyware. *Communications of the ACM* **48(8),** 44–48.

Appendix

See Tables A1–A4.

Table A1 Descriptive statistics

312 employees from 78 organisations	*Count*	*%*	*Count*	*%*
Participants (Employee information)				
Gender			*Age*	
Female	168	54	Under 20	4	1.3
Male	142	46	20–29	41	13.1
			30–39	79	25.3
Education			40–49	100	32.1
Grade school or some high school	3	1.0	50–59	77	24.7
Completed high school	13	4.2	60 and above	11	3.5
Some community college or university – did not complete	43	13.8	Min (15 years); Max (70 years); Average (42 years)		
Completed technical school or a community college	61	19.6			
Completed a university or Bachelor's degree	120	38.5	*Job role*		
Completed a post-graduate degree – Master's or Ph.D.	71	22.8	IT	73	24
			Non-IT	235	76
Participants (Company information)					
Number of users			*Sector*		
1–20	9	15	1 Aerospace	2	
21–50	14	23	2 Beverage distribution – wholesale	1	
51–100	5	8	3 Chemical/chemical distribution	2	

Table A1 Continued

312 employees from 78 organisations	*Count*	*%*	*Count*		*%*
101–500	14	23	4	Computer software company	1
501–1000	3	5	5	Construction	2
1000 or more	15	25	6	Defense contracting	1
			7	Engineer/architect firm	4
Annual information security budget			8	Financial services	8
None, no separate budget	28	50	9	Government facility	1
Less than $50,000	19	34	10	Health care	11
$50,000–$99,999	4	7	11	Internet service provider	2
$100,000–$249,999	3	5	12	Manufacturing	16
$250,000–$499,999	1	2	13	Media company	3
$500,000–$999,999	1	2	14	Nonprofit	1
$1–$4.9 million	3	5	15	Oil/Gas	1
$5–$9.9 million	1	2	16	Pharmaceutical research	1
$10 million or more	0	0	17	Power/Energy	2
			18	Service_Computer Services	2
Length of time security policies were in place			19	Service_Legal Service	2
Not yet adopted	8	14	20	Service_Personnel Staffing	1
Less than 6 months	1	2	21	Telecommunications	1
6 months to 1 year	1	2	22	Transportation	2
1–3 years	10	17	23	University/College	10
3–5 years	16	27			
More than 5 years	23	39			

Note: The discrepancies in the numbers are due to data not reported.

Table A2 Instrument, item loadings and item weights

Construct	*Items*	*Item loadings (t value)*	*Item weight (t value)*	
Perceived probability of security breach	IncCert1	**0.91** (5.48)	0.39 (2.77)	How likely is it that a security violation will cause a significant outage that will result in loss of productivity?
	IncCert2	**0.89** (6.23)	0.28 (2.90)	How likely is it that a security violation will cause a significant outage to the Internet that results in financial losses to organisations?
	IncCert3	**0.91** (5.98)	0.44 (3.96)	How likely is it that organisation will lose sensitive data due to a security violation?
Perceived severity of security breach	IncSev1	**0.83** (8.67)	0.22 (1.52)	I believe that information stored on organisation computers is vulnerable to security incidents.
	IncSev2	**0.95** (21.93)	0.44 (6.08)	I believe the productivity of organisation and its employees is threatened by security incidents.
	IncSev3	**0.94** (19.45)	0.42 (7.02)	I believe the profitability of organisations is threatened by security incidents.
Security breach concern level	SecConc1	**0.78** (21.02)	0.45 (10.86)	The IS security issue affects my organisation directly.
	SecConc2	**0.63** (7.67)	0.27 (4.13)	The IS security issue is exaggerated (Reverse coded).
	SecConc3	**0.84** (27.83)	0.58 (11.95)	I think IS security is serious and needs attention.
Response efficacy	ResEff1	**0.82** (17.94)	0.37 (11.38)	Every employee can make a difference when it comes to helping to secure the organisation's IS.
	ResEff2	**0.76** (14.82)	0.35 (8.72)	There is not much that any one individual can do to help secure the organisation's IS.
	ResEff3	**0.86** (29.62)	0.49 (11.03)	If I follow the organisation IS security policies, I can make a difference in helping to secure my organisation's IS.
Cost	Cost1	**1.00** (0.00)	1.00 (0.00)	Adopting security technologies and practices poses hindrance.

Table A2 Continued

Construct	*Items*	*Item loadings (t value)*	*Item weight (t value)*	
Resource availability	ResAvail1	0.76 (9.89)	**0.49** (4.19)	Help desk help is available when needed.
	ResAvail2	0.88 (16.51)	**0.74** (7.16)	Information Security policies are made available to employees online.
	ResAvail3	0.48 (4.48)	**0.07** (0.55)	Information security policies are written in a manner that is clear and understandable.
	ResAvail4	0.38 (3.16)	**0.03** (0.20)	Users receive adequate security training before getting a network account.
	ResAvail5	0.29 (2.49)	**0.24** (2.08)	A variety of business communications (notices, posters, newsletters, etc.) are used to promote security awareness.
Self-efficacy	SEff1	**0.93** (73.79)	0.39 (24.75)	I would feel comfortable following most of the IS security policies on my own.
	SEff2	**0.94** (63.42)	0.35 (25.25)	If I wanted to, I could easily follow IS security policies on my own.
	SEff3	**0.92** (41.80)	0.33 (23.97)	I would be able to follow most of the IS security policies even if there was no one around to help me.
Security policy attitude	SecPolAtt1	**0.95** (100.41)	0.37 (28.20)	Adopting security technologies and practices is important.
	SecPolAtt2	**0.97** (131.51)	0.38 (27.09)	Adopting security technologies and practices is beneficial.
	SecPolAtt3	**0.87** (28.46)	0.33 (18.01)	Adopting security technologies and practices is helpful.
Organisational commitment	OCM1	**0.82** (19.64)	0.61 (7.53)	I am willing to put in a great deal of effort beyond that normally expected in order to help this organisation be successful.
	OCM2	**0.72** (8.32)	0.39 (6.37)	I really care about the fate of this organisation.
	OCM3	**0.68** (9.66)	0.32 (6.07)	For me, this is the best of all possible organisations for which to work.
Punishment severity	PunSev1	**0.92** (40.77)	0.53 (7.66)	The organisation disciplines employees who break information security rules.
	PunSev2	**0.80** (15.59)	0.26 (3.35)	My organisation terminates employees who repeatedly break security rules.
	PunSev3	**0.80** (15.07)	0.37 (4.95)	If I were caught violating organisation information security policies, I would be severely punished.
Detection certainty	DetCer1	**0.88** (31.10)	0.59 (11.72)	Employee computer practices are properly monitored for policy violations.
	DetCer2	**0.86** (26.26)	0.56 (10.99)	If I violate organisation security policies, I would probably be caught.
Subjective norm	SubNorm1	0.74 (8.50)	−**0.05** (0.32)	Top management thinks I should follow organisational IS security policies.
	SubNorm2	0.92 (18.93)	**0.49** (2.46)	My boss thinks that I should follow organisational IS security policies.
	SubNorm3	0.80 (14.46)	**0.24** (1.77)	My colleagues think that I should follow organisational IS security policies.
	SubNorm4	0.81 (11.14)	**0.09** (0.47)	The information security department in my organisation thinks that I should follow organisational IS security policies.
	SubNorm5	0.88 (14.11)	**0.38** (2.29)	Other computer technical specialists in the organisation think that I should follow organisational security policies.
Descriptive norm	DesNorm1	**0.95** (94.39)	0.31 (15.33)	I believe other employees comply with the organisation IS security policies.
	DesNorm2	**0.94** (88.33)	0.34 (13.80)	I am convinced other employees comply with the organisation IS security policies.
	DesNorm3	**0.93** (74.25)	0.42 (15.77)	It is likely that the majority of other employees comply with the organisation IS security policies to help protect organisation's IS.
Security policy compliance intention	CompInt1	**0.93** (47.18)	0.39 (15.09)	I am likely to follow organisational security policies.
	CompInt2	**0.87** (14.66)	0.31 (10.64)	It is possible that I will comply with organisational IS security policies to protect the organisation's IS.
	CompInt3	**0.95** (78.77)	0.39 (16.23)	I am certain that I will follow organisational security policies.

Table A3 Cross loadings

	IncCert	*IncSev*	*SecConcern*	*ResEff*	*Cost*	*ResAvail*	*SelfEfficacy*	*SecPolAtt*	*OrgCommit*	*PunSev*	*DetCert*	*SubNorm*	*DesNorm*	*CompInt*
IncCert1	**0.91**	0.62	0.17	0.01	0.03	−0.10	−0.02	0.05	−0.02	−0.14	−0.13	−0.03	−0.19	−0.01
IncCert2	**0.89**	0.54	0.12	−0.02	0.00	−0.07	−0.08	0.03	−0.05	−0.05	−0.08	−0.08	−0.15	−0.05
IncCert3	**0.91**	0.53	0.19	0.04	−0.04	−0.19	−0.12	0.07	−0.10	−0.23	−0.19	−0.12	−0.30	−0.06
IncSev1	0.63	**0.83**	0.12	−0.01	0.02	−0.13	−0.06	0.02	−0.08	−0.09	−0.19	−0.01	−0.20	0.02
IncSev2	0.59	**0.95**	0.24	0.01	0.03	−0.06	0.05	0.03	−0.02	−0.11	−0.14	0.08	−0.13	0.06
IncSev3	0.53	**0.94**	0.23	0.04	0.01	−0.08	−0.01	0.07	−0.03	−0.09	−0.13	0.03	−0.12	0.02
SecConc1	0.17	0.21	**0.78**	0.22	0.00	0.15	0.31	0.39	0.18	0.09	0.11	0.30	0.02	0.22
SecConc2	−0.02	0.08	**0.63**	0.24	−0.26	0.18	0.23	0.28	0.20	0.11	0.14	0.31	0.11	0.23
SecConc3	0.19	0.20	**0.84**	0.22	−0.09	0.15	0.27	0.53	0.19	0.00	0.01	0.31	0.00	0.26
ResEff1	0.03	0.06	0.22	**0.82**	−0.19	0.25	0.21	0.37	0.31	0.07	0.04	0.28	0.05	0.29
ResEff2	−0.03	−0.06	0.22	**0.76**	−0.31	0.12	0.14	0.31	0.34	0.06	0.10	0.20	0.06	0.29
ResEff3	0.02	0.03	0.26	**0.86**	−0.22	0.21	0.26	0.50	0.40	0.16	0.16	0.35	0.15	0.35
Cost1	−0.01	0.02	−0.12	−0.29	**1.00**	−0.07	−0.02	−0.33	−0.23	−0.07	−0.10	−0.13	−0.10	−0.19
ResAvail1	−0.16	−0.06	0.12	0.13	−0.03	**0.76**	0.39	0.15	0.16	0.30	0.29	0.41	0.30	0.36
ResAvail2	−0.13	−0.07	0.20	0.25	−0.08	**0.88**	0.45	0.29	0.20	0.47	0.38	0.46	0.37	0.31
ResAvail3	−0.29	−0.14	0.05	0.13	−0.12	**0.48**	0.24	0.12	0.14	0.52	0.41	0.35	0.53	0.17
ResAvail4	−0.13	−0.04	0.17	0.14	−0.12	**0.38**	0.19	0.12	0.12	0.27	0.16	0.26	0.23	0.12
ResAvail5	−0.22	−0.02	0.03	0.11	−0.05	**0.29**	0.15	0.08	0.11	0.47	0.27	0.20	0.36	0.11
SEff1	−0.07	0.01	0.34	0.26	−0.05	0.48	**0.93**	0.39	0.40	0.25	0.28	0.60	0.37	0.53
SEff2	−0.11	−0.02	0.32	0.25	−0.01	0.50	**0.94**	0.31	0.31	0.22	0.23	0.53	0.26	0.45
SEff3	−0.05	0.03	0.34	0.21	0.01	0.43	**0.92**	0.32	0.32	0.22	0.18	0.48	0.24	0.43
SecPolAtt1	0.05	0.05	0.55	0.46	−0.26	0.28	0.36	**0.95**	0.29	0.19	0.15	0.43	0.11	0.37
SecPolAtt2	0.05	0.05	0.54	0.47	−0.30	0.27	0.41	**0.97**	0.34	0.20	0.15	0.46	0.15	0.39
SecPolAtt3	0.05	0.03	0.45	0.45	−0.37	0.23	0.25	**0.87**	0.32	0.13	0.17	0.35	0.10	0.29
OCM1	0.00	0.03	0.31	0.46	−0.22	0.23	0.37	0.37	**0.82**	0.23	0.18	0.34	0.23	0.38
OCM2	−0.07	−0.06	0.10	0.21	−0.13	0.06	0.20	0.20	**0.72**	0.11	0.10	0.25	0.12	0.33
OCM3	−0.13	−0.09	0.05	0.21	−0.16	0.13	0.20	0.10	**0.68**	0.19	0.17	0.25	0.18	0.23
PunSev1	−0.13	−0.08	0.05	0.16	−0.12	0.37	0.24	0.18	0.29	**0.92**	0.57	0.28	0.52	0.26
PunSev2	−0.08	−0.03	0.12	0.03	−0.04	0.25	0.12	0.14	0.12	**0.80**	0.47	0.18	0.37	0.13
PunSev3	−0.20	−0.15	0.03	0.09	0.00	0.42	0.23	0.14	0.17	**0.80**	0.53	0.23	0.45	0.18
DetCer1	−0.14	−0.15	0.12	0.13	−0.07	0.30	0.24	0.17	0.18	0.52	**0.88**	0.25	0.34	0.28
DetCer2	−0.13	−0.13	0.04	0.10	−0.10	0.39	0.20	0.12	0.18	0.58	**0.86**	0.24	0.45	0.27
SubNorm1	−0.12	−0.02	0.32	0.30	−0.18	0.46	0.47	0.36	0.32	0.37	0.31	**0.74**	0.48	0.43
SubNorm2	−0.10	0.05	0.37	0.33	−0.14	0.47	0.54	0.43	0.36	0.25	0.22	**0.92**	0.36	0.54
SubNorm3	−0.10	−0.01	0.30	0.25	−0.09	0.48	0.45	0.34	0.29	0.35	0.30	**0.80**	0.45	0.47
SubNorm4	−0.08	0.02	0.33	0.29	−0.10	0.46	0.45	0.33	0.33	0.23	0.23	**0.81**	0.36	0.47
SubNorm5	−0.04	0.06	0.35	0.32	−0.10	0.44	0.52	0.39	0.35	0.22	0.26	**0.88**	0.32	0.52
DesNorm1	−0.24	−0.15	0.01	0.07	−0.10	0.35	0.28	0.10	0.20	0.48	0.41	0.37	**0.95**	0.27
DesNorm2	−0.21	−0.15	0.03	0.11	−0.05	0.33	0.27	0.11	0.23	0.49	0.40	0.36	**0.94**	0.29
DesNorm3	−0.24	−0.12	0.07	0.13	−0.13	0.37	0.33	0.16	0.26	0.54	0.45	0.41	**0.93**	0.36
CompInt1	−0.06	0.04	0.33	0.35	−0.18	0.40	0.51	0.35	0.43	0.23	0.32	0.57	0.32	**0.93**
CompInt2	0.02	0.05	0.22	0.32	−0.14	0.29	0.39	0.33	0.34	0.17	0.19	0.47	0.26	**0.87**
CompInt3	−0.06	0.02	0.29	0.38	−0.21	0.38	0.49	0.36	0.42	0.24	0.34	0.57	0.33	**0.95**

Note: ResAvail and SubNorm were modeled as formative in the model.
The bold values indicates the factor loading for the items (represented in rows) relate to the respective constructs represented in the columns.

Table A4 Inter-item and item-to-construct correlation matrix for formative constructs

	NBMgt1	*NBMgt2*	*NBMgt3*	*NBMgt4*	*NBMgt5*	*Cal_SubNorm*	*ResAvail1*	*ResAvail2*	*ResAvail3*	*ResAvail4*	*ResAvail5*	*Cal_ResAvail*
NBMgt1	—											
NBMgt2	0.80**	—										
NBMgt3	0.61**	0.69**	—									
NBMgt4	0.71**	0.76**	0.60**	—								
NBMgt5	0.57**	0.66**	0.54**	0.71**	—							
Cal_SubNorm	0.75**	0.92**	0.81**	0.83**	0.86**	—						
ResAvail1	0.39**	0.42**	0.42**	0.48**	0.39**	0.47**	—					
ResAvail2	0.42**	0.40**	0.38**	0.33**	0.31**	0.41**	0.40**	—				
ResAvail3	0.31**	0.28**	0.31**	0.28**	0.24**	0.31**	0.35**	0.45**	—			
ResAvail4	0.22**	0.24**	0.17*	0.23**	0.19**	0.24**	0.25**	0.40**	0.30**	—		
ResAvail5	0.26**	0.21**	0.19**	0.17*	0.13**	0.20**	0.30**	0.43**	0.45**	0.39**	—	
Cal_ResAvail	0.48**	0.47**	0.46**	0.45**	0.39**	0.50**	0.74**	0.88**	0.57**	0.46**	0.64**	—

Note: All ** values are significant at $P<0.001$; except * significant at $P<0.01$.

Upon suggestion from an anonymous reviewer, we carried out an MTMM analysis to evaluate the convergent and discriminant validity of the formative measures. We followed Loch *et al*. (2003) in creating and evaluating the inter-item and item-to-construct correlation matrix presented above.

We did not have multiple methods for measuring the constructs; however, we were able to compare the traits (scale items) and the constructs due to the properties of formative constructs and PLS statistics available to us. In PLS, loadings represent the influence of individual scale items on reflective constructs; PLS weights represent a comparable influence for formative constructs.

We had measured all the items on the 7-point scale. We multiplied item scores by their individual PLS weights creating a weighted score for each measure. We added these weighted scores to get the composite score for each formative construct (Cal_SubNorm and Cal_ResAvail). Using these values, we ran inter-item correlations as well as item-to-construct correlations and created a matrix of these values, as shown above.

To evaluate convergent validity, measures thought to be part of the same construct should correlate at a significant level with each other and the composite construct value (Loch *et al.*, 2003). As can be seen in the matrix, the weighted and transformed formative measures all qualify by this standard. The inter-item correlations and the item-to-construct correlations for SubNorm and ResAvail are all significant.

For evaluation of the discriminant validity the inter-item and item-to-construct correlations should correlate more highly with each other than with the measures of other constructs, and with the composite constructs themselves (Loch *et al.*, 2003). By comparing values in the SubNorm and ResAvail rectangles with values in their own rows and columns, we can see that there are only a few violations of this basic principle (related only to ResAvail2 correlation with ResAvail1). Loch *et al*. (2003) also notice such violations and suggest that such exceptions are not necessarily meaningful and one should use judgment in determining whether the number of violations is low enough to conclude that the instrument items discriminate well.