Computers in Human Behavior 24 (2008) 2799–2816

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

Security lapses and the omission of information security measures: A threat control model and empirical test

Michael Workman [a,*], William H. Bommer [b], Detmar Straub [c]

[a] Florida Institute of Technology, College of Business, 150 W University Blvd, Melbourne, FL 32901, United States
[b] California State University at Fresno, Craig School of Business, 5245 North Backer, Fresno, CA 93740, United States
[c] Georgia State University, J. Mack Robinson College of Business, 35 Broad Street N.W., Atlanta, GA 30303, United States

ARTICLE INFO

Article history:
Available online 22 May 2008

Keywords:
Information security
Omissive behaviors
Threat control model
Social cognitive theory
Protection motivation theory

ABSTRACT

Organizations and individuals are increasingly impacted by misuses of information that result from security lapses. Most of the cumulative research on information security has investigated the technical side of this critical issue, but securing organizational systems has its grounding in personal behavior. The fact remains that even with implementing mandatory controls, the application of computing defenses has not kept pace with abusers' attempts to undermine them. Studies of information security contravention behaviors have focused on some aspects of security lapses and have provided some behavioral recommendations such as punishment of offenders or ethics training. While this research has provided some insight on information security contravention, they leave incomplete our understanding of the omission of information security measures among people who know how to protect their systems but fail to do so. Yet carelessness with information and failure to take available precautions contributes to significant civil losses and even to crimes. Explanatory theory to guide research that might help to answer important questions about how to treat this omission problem lacks empirical testing. This empirical study uses protection motivation theory to articulate and test a *threat control model* to validate assumptions and better understand the "knowing-doing" gap, so that more effective interventions can be developed.

* Corresponding author. Tel.: +1 321 253 4491.
E-mail addresses: workmanfit@yahoo.com (M. Workman), wbommer@csufresno.edu (W.H. Bommer), dstraub@gsu.edu (D. Straub).

0747-5632/$ - see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.chb.2008.04.005

1. Introduction

There are many threats to the integrity, confidentiality, and availability of information maintained by organizational systems, as well as many countermeasures such as virus scanners, firewalls, security patches, and password change control systems and a range of other technologies and techniques that are available to improve information systems (IS) security. Even though many of these security mechanisms can be automated, and even though the general public has become increasingly aware of the pervasive IS security threats, they frequently do not utilize these technologies even when they are readily, and often freely, available (Workman, 2007). An important question then is why do people who are aware of IS security threats and countermeasures neglect to implement them? As one example, a letter was recently circulated by the Administaff Corporation that read in part: "On October 3, 2007, an Administaff laptop computer containing personal information including social security numbers, names and addresses of current and former Administaff worksite employees was reported missing... The laptop computer is password protected; however, the personal information was not saved in an encrypted location, which is a clear violation of company policies..."

Some theoretical development and testing has been done to help explain various aspects of this "knowing-doing gap" such as factors associated with security policy adherence (Siponen & Iivari, 2006; Siponen, Pahnila, & Mahmood, 2006); however, most of these studies have suffered from a variety of methodological weaknesses including non-randomization, low response rates, localization, confusing formative with reflective analyses, and a reliance on purely self-reported data (e.g., Pahnila, Siponen, & Mahmood, 2007). Meanwhile, the problem is not well understood and the security problem continues to grow worse because it is unclear to managers and organizational developers what interventions to apply, why, and when (Shreve, 2004; Workman & Gathegi, 2007).

Recommended behavioral interventions to address the knowing-doing gap problem in security breaches include punishment (Straub & Welke, 1998), instruction on situational ethics (Harrington, 1996; Hsu & Kuo, 2003; Kurland, 1995), and raising security awareness (Calluzzo & Cante, 2004; Straub & Nance, 1990). There has also been suggestions from the IS security literature that include augmenting security procedures as a solution (Debar & Viinikka, 2006), addressing situational factors such as reducing workload so that security professionals have time to implement the recommend procedures (Albrechtsen, 2006;), improving the quality of policies (von Solms & von Solms, 2004), improving the alignment between an organization's security goals and its practices (Leach, 2003), and gaining improvements from software developers regarding the security implementations during the software development cycle (Jones & Rastogi, 2004).

Yet in spite of all these important recommendations, people often fail to take basic security precautions that result in billions of dollars annually in individual and corporate losses (Calluzzo & Cante, 2004; Shreve, 2004). It has even been found that when people lack the skills necessary to utilize security technology and say they are willing to pay a fee to have their information protected, in practice they often do not take advantage of this opportunity to improve their system security (Acquisti & Grossklags, 2005, 2007; Leyden, 2004). Thus while our understanding of security behaviors has improved in recent years, "knowing better, but not doing better" remains one of the key scholarly and practical issues that have not been fully addressed.

1.1. Why automation alone is insufficient

The IS community has proposed to circumvent the "weakest link" and thereby avoiding the knowing-doing gap by using automated and mandatory security measures, such as, automatically requiring users to periodically change their passwords, and restricting acceptable passwords to a designated range of characters and numeric values including case alterations and special ASCII characters such as asterisks. However, in practice, we have seen that these kinds of controls alone are not sufficient. Reasons that automated solutions are not universally utilized fall into four categories: (1) financial, (2) situational, (3) cultural, and (4) technological.

First, many companies do not implement mandatory automated controls because they believe that the threat level does not warrant such financial investments or the inevitable loss of efficiency and

productivity (Ong, Tan, Tan, & Ting, 1999). Security technologies such as firewall processing of communications and encryption have a decided impact on productivity (Ruighaver, Maynard, & Chang, 2007). In other cases, people find ways to circumvent them (Workman, 2007). In fact, many of the organizational members who participated in our study stated that they cancelled the automatic virus scanning because it "slowed down their computer." This is the standard trade-off of security versus productivity that makes it difficult to dictate an all-or-nothing policy when time is money. This is not a trivial concern since as an overhead cost of doing business, security technology and process infrastructure have doubled since 2001, growing to more than 8% of an average company's budget (Bartels, 2006).

Second, while there are innumerable situational factors that could be recounted, among these is the evidence that a large number of firms do not have the infrastructure and/or expertise to implement automatic techniques and so must substantially rely on discretionary controls (Post & Kagan, 2007). In other cases, it is simply impossible because of technological and standards incompatibilities. For business road warriors, it is sometimes necessary to reconfigure laptops in the field to allow them to secure access to WiFi networks. It is not possible to create a monolithic automated solution for all possible networks that employees might encounter. The participating organization in our study did not implement many available security measures, and some of the stated reasons given by participants involved the disparate and even incompatible technologies and approaches across their distributed organizational boundaries.

Third, in some rare cases, a mechanistic system that enforces security compliance is antithetical to some organizational cultures and are not seen by managers as a viable approach. Automated solutions imply a certain degree of centralization. If the organizational culture is highly decentralized, single points of control may not be welcome. In cultures where intrapreneurialism is valued, security measures may be seen as individual responsibilities that should not be abrogated (Ruighaver et al., 2007).

Fourth and finally, there are circumstances in which there are some good reasons to preclude full-scale automation. In some organizations, network engineers configure firewalls to prevent promiscuous connections. In some such cases, automatic security updates are prevented and individuals must take on the personal responsibility of protecting their own systems (Sherif, Ayers, & Dearmond, 2003). Furthermore, some software requires the use of ActiveX controls or other inter-process communications that force security administrators to lower the centralized defensive posture, and while antivirus software might be activated before a server uploads attachments or emails, there are many security situations where parameters have to be individualized (Debar & Viinikka, 2006; Ong et al., 1999). Thus, in summary, complete automation of security will likely never be possible and varying levels of human action and decision-making will continue to be necessary (Ruighaver et al., 2007). User choice and behavior will most likely always play a key role in whether or not IS security is fully implemented.

1.2. Need for objective-empirically tested theory

There are many published research manuscripts related to security behaviors such as insider contravention, intentional misuse of information, and other facets of security behaviors (c.f. Eloff & von Solms, 2000; Workman & Gathegi, 2007). Relative specifically to the knowing-doing gap however, while various theoretical frameworks have been created (c.f. Dhillon & Backhouse, 2001 – just to name one), most have not been empirically tested (e.g., Ruighaver et al., 2007; Theoharidou, Kokolakis, Karyda, & Kiountouzis, 2005: see: Stanton, Stam, Mastrangelo, & Jolton, 2005, for a review). In one knowing-doing gap context, Pahnila et al. (2007) set out to explain why one would or would not follow a well-specified, well-publicized organizational security policy. They tested different theoretical models using self-report. But since there is a characteristic discrepancy between self-report and actual behaviors, we cannot be sure how well the respondents' perceptions matched their actual security behaviors, and this may have contributed to some incommensurable findings in the literature. For example, Pahnila et al. (2007) found no relationship between rewards and security policy compliance whereas Stanton et al. (2005) did. A consolidation in the literature is required, and to enable this, objective study is needed to get beyond the realm of speculation.

Our over-riding research question was, why do people who are aware of IS security threats and countermeasures neglect to implement them? For the grounding of our study, we examined taxonomical literature (e.g., Stanton et al., 2005) and theoretical frameworks (e.g., Siponen & Iivari, 2006). Synthesizing a *threat control model* (TCM) from *protection motivation theory* (Rogers, 1975, 1983), which has been extensively used to ground health-related threat control research and has been incorporated into theoretical frameworks in non-empirically tested IS security studies (Pahnila et al., 2007; Woon, Tan, & Low, 2005), we conducted a field study by triangulating self-perceptions with samples of observed security behaviors. Even though social scientists prefer to observe behaviors because self-reports are often poor predictors of actual behaviors (Ettredge & Richardson, 2003; Post & Kagan, 2007), since we cannot observe all possible behaviors in a category (e.g., security behavior), observation alone is incomplete (the so-called nomothetic–ideographic paradox). Combining self-report with observational sampling in triangulation, we are able to assess how congruent these are in a given study.

2. Threat control and hypothesized relationships

In the context of the knowing-doing gap in IS security, people primarily consider whether a threat is preventable in the first place (Boer & Seydel, 1996; Wu, Stanton, Li, Galbraith, & Cole, 2005). Protection motivation theory (Rogers, 1975, 1983) incorporates controllability factors (locus of control and self-efficacy) from social cognitive theory (Bandura, 1977) in this cognitive assessment. Studies (Harrington, 1996; Kuo & Hsu, 2001; Lin & Ding, 2003) have found that computer self-efficacy and locus of control play an important role in people's perceptions of threat prevention, and offers a useful framework to help understand why people may or may not take security precautions (Workman & Gathegi, 2005).

A person's locus of control (Rotter, 1966) impacts the extent to which an individual's behavior is proactive or reactive (Milgram & Naaman, 1996; O'Donoghue & Rabin, 2000). *Internal locus of control* is the belief that people control their own destinies and therefore "internals" tend to claim responsibility for their own actions. "Externals," on the other hand, believe that outcomes are controlled by fate or powerful others and psychologically speaking, they tend to transfer responsibility for actions to these others (Rotter, 1966). Thus, locus of control can be used to predict why people assume responsibility for taking IS security precautions or forego them leaving that responsibility to others, such as the "company" (Harrington, 1996), and may not only help to account for whether people might contravene IS security, but also explain why they have a propensity to ignore security measures (Harrington, 1996; Kuo & Hsu, 2001; Lin & Ding, 2003). Where locus of control is concerned with whether an event is controllable, self-efficacy (Bandura, 1991; Bandura & Walters, 1963) involves the perceptions of oneself being capable of preventing a threatened event by means of one's skills and abilities in performing a particular preventative behavior.

In the theory of planned behavior, Ajzen (2002) combined locus of control and self-efficacy into a single concept, called perceived behavioral control, although locus of control and self-efficacy are decidedly different constructs (Bandura, 2001). The blending of these constructs is problematic because the type of interventions that organizational developers target is different based on whether the controllability is belief-based (locus of control) or skills-based (self-efficacy). Blending them together confuses practitioners about what and how to address the problem.

Beyond the controllability aspects over a threatened event, the psychological research into motivations for taking precautions against these various threats (cf., Wu et al., 2005) is particularly relevant. This research on precautionary behavior describes adaptive and maladaptive coping strategies to diminish threats. These strategies derive from two cognitive appraisal processes: a process of threat assessment and a process of coping assessment (Boer & Seydel, 1996). According to protection motivation theory, or PMT (Rogers, 1975, 1983), threat appraisal and coping behavior is a product of: (1) the intrinsic rewards for maladaptive behavior, (2) the perceived severity of a threatened event, (3) the perceived probability of a threat or vulnerability to a threat, (4) the efficacy of a recommended preventive behavior (perceived response efficacy), and (5) the perceived self-efficacy or confidence in one's ability to undertake a recommended preventative behavior, and the (6) the cost of coping with

the threat. Extending PMT into the IS security realm, we propose a "threat control model" (TCM) as an explanation for the know-doing gap in IS security.

The TCM can be divided into two components: threat assessment and coping assessment factors and processes. *Threat assessment* involves perennial antecedents to arousal as well as motivations for taking coping actions. *Coping assessment* involves perceptions of intrinsic and extrinsic factors available to prevent a threat; it also includes perceptions of whether the threat is preventable. For instance, people generally take actions to prevent a threat they perceive to be severe and imminent so long as they believe they have the ability and tools to stop it (Boer & Seydel, 1996; Wu et al., 2005).

2.1. Threat assessment

The perception of threat is defined as the anticipation of a psychological (e.g., assault), physical (e.g., battery), or sociological (e.g., theft) violation or harm to oneself or others, which may be induced vicariously (Lazarus, 1991). Threats to IS security include unauthorized interception of information; unauthorized modification of information; exposure of information to unauthorized individuals; and the destruction of hardware, software and/or information for which security measures exist to help protect the confidentiality, integrity, and availability of these information resources (SANS, 2005). In an organizational context, protecting the firm's information security is important, not only because of the organizational losses, but also because security breaches can lead to individuals losing their jobs.

When a threat is perceived, people adjust their behavior according to the amount of risk from the threat that they are willing to accept (sometimes known as risk homeostasis). This adjustment is based on the degree or severity and costs of damage they perceive to be associated with the threat (Grothmann & Reusswig, 2006). Thus, people tend to adjust their behavior in response to the extent of the damage the threat may cause (Pyszczynski, Greenberg, & Solomon, 1997). Perceived severity of threat will lead people to behave in a more cautious manner if their perceptions of the damage or danger increases. The reverse of this, however, is also true: when people perceive that a risk has diminished, they will behave in a less cautious manner. This reverse effect, which has been widely documented, has proven to be a complicating factor in a number of safety-related areas. More specifically, there is compelling evidence from traffic studies and the use of safety features such as car seat belts, antilock braking systems, and bicycle helmets that demonstrate these effects. That is, people use seatbelts less when they are driving close to home (lower perceived danger) or at slower speeds (lower perceived damage) (Dorn & Brown, 2003). Extending from this line of reasoning, the theory of terror management (Pyszczynski et al., 1997) suggests that coping mechanisms are chosen depending on the controllability and severity of the threat. In particular, people exhibit greater exogenous coping behavior toward severe threats over which they perceive they have more control (greater self-efficacy). On the other hand, people retreat into endogenous coping mechanisms and form more fatalistic attitudes about severe threats over which they feel little control (external locus of control). Examples of these endogenous mechanisms include clinging to patriotism when the threat involves their own mortality or dismissal of the threat as unimportant when it is not perceived as severe.

To summarize, in the threat assessment literature the perceived severity of threat and the associated acceptance of risk behavior are based on the premises that: (1) people place a certain intangible value on "life," "liberty," and "property"; (2) they have a threshold level of risk they will accept, tolerate, prefer, desire, or choose; (3) the "target level" of risk they will accept before putting up a defense depends on the perceived advantages or benefits versus the disadvantages or costs of safe and unsafe behavioral alternatives; and, finally, (4) this assessment determines the degree to which people will expose themselves to a threat or hazard before taking coping behaviors to mitigate the threat (Wilde, 2001). Thus, our first hypothesis is[1]:

H_{1a-b}: People who perceive a higher severity of an IS security threat will be less likely to omit security precautions than people who perceive a lower severity of an IS security threat.

[1] We show all numbered hypotheses as versions a&b to reflect the two forms of the dependent variables, that is, subjective measures and objective measures.

People operate day-to-day on the basis of assumptions and personal beliefs that allow them to set goals, plan activities, and order their behavior. This conceptual system is developed over time and provides them with expectations regarding their environment. While they operate on the basis of this conceptual system, they tend not to be aware of its central postulates. Among these generally shared postulates is the belief in personal invulnerability (Dorn & Brown, 2003; Hochhauser, 2004). For instance, people may recognize that crimes are common, but they believe at the same time that "it can't happen to them" (Roe-Berning & Straker, 1997). As an example, Lejeune and Alex (1973) found that mugging victims first defined the event with disbelief and in a non-threatening way, such as a practical joke. Hence, people operate on the basis of an "illusion of invulnerability" to support their need to view the world as orderly, stable, and meaningful, thus underestimating the probability of their own misfortunes and overestimating the probability of misfortunes to others (Hochhauser, 2004; Roe-Berning & Straker, 1997). Events such as, criminal acts, accidents, disasters, and disease force people to recognize and make objective their basic assumptions about their environment and the world (Janoff-Bulman & Frieze, 1983). Those who have been subjected to a burglary, for example, tend to assess their chances of falling victim to future burglaries to be higher than those who have never been a victim (Lejeune & Alex., 1973). In general, the illusion of invulnerability is an immunizing stratagem from the fear, stress, and anxiety associated with the perceived threat of misfortune. Once victimized, however, it becomes easier to see oneself again in the role of victim (Janoff-Bulman & Frieze, 1983; Roe-Berning & Straker, 1997).

Applying this line of thought to IS security, we hypothesize that when people operate with the assumption of invulnerability, they are less likely to take security precautions such as updating or protecting their passwords, keeping their security software up to date, using firewalls, backing up their systems, using surge protectors and paper shredders, maintaining systems access controls, implementing redundant systems, or using system activity and intrusion detection monitors (Ryan, 2004; Sasse, Brostoff, & Weirich, 2004). However, when they perceive they are vulnerable to a security breach, they are more likely to take these security precautions (Dorn & Brown, 2003; Ettredge & Richardson, 2003; Ryan, 2004; Sasse et al., 2004). Therefore,

H_{2a-b}: People who perceive a higher vulnerability to an IS security threat will be less likely to omit security precautions than people who perceive a lower vulnerability to an IS security threat.

2.2. Coping assessment

Social cognitive theory maintains that when people perceive they have the capabilities to perform an act that benefits them, they will expend substantial effort to accomplish that act (Bandura, 1977). In SCT, having such capabilities relies principally on two elements: locus of control (Rotter, 1966) and self-efficacy (Bandura, 1977). *Locus of control* is a generalized expectancy that predicts individuals' behavior across situations, depending on whether they view an outcome as controllable (internal) or controlled (external) in the first place (Rotter, 1966). There is variability among people along the internal–external continuum because experience provides a sense of control based on the reinforcement individuals receive under certain conditions (Marsh & Richards, 1986). Therefore, whereas self-efficacy attends more to whether or not people feel they have requisite skills and abilities to accomplish a goal, locus of control is a more interactive expression of the relationship between a person and his or her environment.

Locus of control affects the extent to which people assume responsibility for their actions (Milgram & Naaman, 1996; O'Donoghue & Rabin, 2000). When individuals perceive that they have control over outcomes, they tend to believe that they control their own destinies, will accept responsibility and subsequently will take action. Conversely, when they feel that outcomes are controlled by fate or powerful others, and they tend to shift responsibility for their actions to others (Rotter, 1966).

Whether one takes defensive countermeasures against potential aggression or shifts that responsibility to a powerful other (such as a custodian or caretaker, or even a corporation or government agency) determines an individual's perceived locus of control (Blankenship & Whitley, 2000). "People's tendency to ascribe responsibility to oneself or to diffuse it to depersonalized others is related

to rationalizing the consequences of one's behavior" (Harrington, 1996, p. 262). Denial or acceptance of responsibility is thus a product of rationalizations, based in part on one's perceptions of control.

With respect to taking security precautions, people who have high perceptions of control tend to be more proactive in taking precautionary measures against possible security breaches (Tang, Pun, & Cheung, 2002). In addition, they tend to accept responsibility for upholding the welfare of others, live up to commitments, and follow personal or societal rules. This is less the case for people who have low perceptions of control (Harrington, 1996; Tang et al., 2002). This perspective has been associated with undertaking higher security precautions, including updating and protecting passwords, keeping security and virus software up to date, using firewalls, backing up systems, and using surge protectors and paper shredders (Proctor, Kim, Vu Schultz, & Salvendy, 2002; Ryan, 2004; Sasse et al., 2004). Therefore,

H_{3a-b}: People who have an internal locus of control are less likely to omit security precautions than people who have an external locus of control.

There are other coping mechanisms in addition to locus of control. *Self-efficacy* is defined as the beliefs people have about their capabilities to produce designated levels of performance and exercise influence over the events that affect their lives (Bandura, 1977). Self-efficacy beliefs determine how people feel, think, and motivate themselves to behave in a certain way based on cognitive, motivational, affective, social influence, and selection processes. Such beliefs lead people to think pessimistically or optimistically, and to think in ways that are self-enhancing or self-hindering (Stajkovic & Luthans, 1998). "It is partly on the basis of efficacy beliefs that people choose what challenges to undertake, how much effort to expend in the endeavor, how long to persevere in the face of obstacles and failures, and whether failures are motivating or demoralizing... [and a] strong sense of coping efficacy reduces vulnerability to stress and depression in taxing situations and strengthens resiliency to adversity" (Bandura, 1977, p. 10).

The prediction that low self-efficacy leads to omission of security measures is consistent with both SCT and PMT, and related research into omissive security behaviors finds support for these predictions (Pahnila et al., 2007, Woon et al., 2005). Moreover, research in related areas finds support for similar predictions, for instance, people who have higher self-efficacy are more effective in learning how to implement IS security measures than those who have lower self-efficacy (Workman & Gathegi, 2005). Additionally, people who have a higher self-efficacy concerning the use of technology tend to use the technology more than those with a lower self-efficacy (Compeau & Higgins, 1995). Also, in conducting online transactions, people may be well aware of IS security threats and have knowledge about preventative countermeasures; but if they believe that they do not have the ability to undertake available countermeasures effectively enough to preclude a threat, they are less likely to undertake such security measures than when they believe they have this ability (Jutla & Bodorik, 2005). Therefore:

H_{4a-b}: People who have a higher perceived self-efficacy to cope with an IS security threat will be less likely to omit security precautions than people who have a lower perceived self-efficacy to cope with an IS security threat.

Concomitant with perceptions about whether people have the requisite skills and abilities to undertake sufficient security measures and whether IS security outcomes are controllable, it is clear that individuals have at least one other coping mechanism and that this derives from the fact that they hold different views about the effectiveness of available countermeasures. For example, many consumers perceive that, in online transactions, "unsatisfactory security on the Internet continues to exist even when vendors undertake security enforcement mechanisms" (Challappa & Pavlou, 2002, p. 17). Indeed, there are a number of studies (e.g., Bresz, 2004; Sasse et al., 2004) indicating that the numbers of security breaches are on the increase, which has fueled perceptions that IS security measures are inadequate (Kim & Kim, 2005). On the other hand, there are studies indicating that available security measures are improving (Kankanhalli, Teo, Tan, & Wei, 2003). Whether people perceive the available coping mechanisms as adequate or not is likely to affect their omissive behavior. Thus,

H_{5a-b}: People who perceive a higher efficacy of a recommended security measure response are less likely to omit security precautions than people who perceive a lower efficacy of a recommended security measure response.

A final area of the threat control framework is the cost assessment of the measure. Rogers (1983) separated the rewards (or benefits) from the costs constructs in health-related research applications, where a reward for a given behavior was classified into a maladaptive response, and cost was classified into an adaptive response. Others have criticized this and therefore incorporated these concepts into a cost/benefit assessment (e.g., Milne & Orbell, 2000). Cost-benefit assessment may be thought of as the favorable or unfavorable affective and cognitive evaluation of a target acquired through experience that generally influences behavior (Ajzen, 2002).[2] Using this latter conceptualization in order to best suit omissive behavior, an individual's intentions to implement information security protections may be influenced by whether that which is to be protected is perceived as worth the effort to try to protect it. In other words, the perceived effort is compared to the perceived value (Pechmann, Zhao, Goldberg, & Reibling, 2003).

From this frame of reference, it is important to note that people maintain different cost/benefit attitudes about information security measures that are independent of the perceived business value or sensitivity of the informational assets (i.e., severity of threat), particularly in relation to their own self-interests (International Federation of Accountants, 2006). One aspect of this is seen in studies (e.g., Adams, Nelson, & Todd, 1992, Gregor & Benbasat, 1999) that show how technology acceptance and ease-of-use (Davis, Bagozzi, & Warshaw, 1989) impacts assessments about whether or not to use a given technology. This factor likely carries over to cost/benefit assessment of information security measures and whether people are willing to expend the effort to take precautions such as performing backups or keeping virus scanning software up-to-date.

In the context of omissive IS security, then, response cost is primarily seen in reference to the cost of implementing a security measure versus its potential benefits, even if only limited in efficacy. As an example, if the effort to implement an IS security measure hinders the production of time-sensitive results needed for positive job performance, then the perceived benefits of working without security precautions may be perceived as outweighing the benefits from implementing preventative measures (Thomas, 2004). On the other hand, if the cost of implementing a measure is small, even if it delivers only a small incremental degree of benefit, it may be adopted (Pechmann et al., 2003). Hence, when people perceive that benefits of implementing protections of information and information assets outweigh the cost of protecting them, they are more likely to enact security practices, and vice-versa (Hsu & Kuo, 2003):

H_{6a-b}: People who have higher response cost perceptions of a recommended security response are less likely to omit security precautions than people who have lower response cost perceptions of recommended response.

3. Method

3.1. Sample

To study the TCM, we chose a field study with two data-gathering techniques, as described below. Field studies are thought to be a good choice when the theory is highly relevant to real-world events and the researchers wish to be able to generalize to the world of practice. Although IS security is of general concern to the population at-large, we were particularly interested in understanding the behavior of people who were already familiar with IS security policies. In this way, we felt that a stronger practical case could be made for our findings than if a less experienced population were to be selected. As a result, we chose a random sample of 588 people from a large technology-oriented services corporation (pseudonym: Ingenious Company). The company performs computer hardware and software installations and maintenance for many *Fortune* 500 corporations in finance, government, health care, and other lines of business, many of which have sensitive information that they must protect. Participants were located in nine cities across the United States. Eight hundred fifty participants were

[2] Unless one is ambivalent (Ajzen, 2002).

selected randomly from the employee lists and 612 responded; however, of those 612, 24 were incomplete and were discarded, yielding a 69% response rate and a ±3.5% sampling confidence with a standard error of estimate of 0.05. This indicates a high level of sampling validity (Salant & Dillman, 1994).

3.2. Data collection

Data were collected with two techniques: (1) an online questionnaire and (2) direct observations of behavior such as via computer logs. Where subjective measures assess perceptions of overall general security behaviors (they are nomothetic), objective measures sample those perceptions in practice (they are ideographic). In the survey, the instrument used the threat control factors of locus of control, self-efficacy, perceived threat probability, perceived threat severity, perceived efficacy, and cost-benefit evaluation of the recommended preventative measures. We also gathered self-report items for the dependent variables to correlate them with objective observations of participant behaviors. The sources of the items associated with each scale are noted in Table 1.

The observed dependent variables in this study tapped into security behaviors described by Sasse et al. (2004), Proctor et al. (2002), and Ryan (2004), which were: (a) whether passwords were updated and protected, (b) whether security and virus software were kept up to date, and (c) whether systems were backed up, according to instructions given participants and as stated in the company security policy. It is important to note that the organization under study chose not to automate these features because of a variety of political and practical reasons, and hence these samples were amenable as triangulation with self-reported general perceptions of security behaviors.

3.3. Procedures

The President and the COO of Ingenious Company facilitated access into the firm once the researchers had signed a non-disclosure agreement (NDA) and a confidentiality agreement. Using the company employee directory of employees' locations and e-mail addresses, the President/COO sent each employee a message (with an acknowledgement flag set) informing them about the purpose of the study and about the researchers conducting it. It asked for their cooperation after assuring them about the confidentiality of their responses. The organization in which we conducted the field study was a government-regulated entity that had had serious security breaches in the past. In the public interest, they encouraged us to study the problem and acceded to our requirement that participation would be anonymous and the data gathered held in strict confidence. Prior to engaging in the study, we received approvals from two institutional human-subjects review boards.

The company monitors data and communication as a standard practice and requires employees to sign an employment agreement that includes their consent to monitoring when they are hired. Laws in the US and the EU generally support the right of corporations to inspect and monitor work and workers, which arises from needs related to business emergencies and a corporation's rights to protect its interests (Borrull & Oppenheim, 2004; Harvey, 2007; Keck, 2005; Losey, 1998). In many cases, companies can monitor employees, and while advisable to take overt action to notify its employees of the practice, it is generally not required by law (Scholz, 1997).

Contacting the employees via e-mail with a cover letter and attachment, the researchers explained once again to the participants that the study would inquire about attitudes regarding IS security and assured participants of their anonymity and data confidentiality. The URL to data collection instrument accompanied this e-mail. Each participant received an authentication password to access the Website. When the participants completed the survey, the authentication password was used to produce a unique identifier to keep track of those who had completed the survey and to ensure that the survey was taken only once by each participant. Responses were de-individualized at the beginning of the data collection.

3.4. Measures

Subjective measures were collected as self-report items via the online questionnaire. As suggested by Straub, Carlson, and Jones (1993), pre-existing scales were used in all cases, both for their validation characteristics and for efficiency. Sources for the scales, along with the validation statistics, are

Table 1
Scales, loadings, weights, *T*-values, and reliabilities

Item code	Perceived severity ($\mu = 4.34$, SD = 1.38)	Loading	*t*-stat	Composite reliability
SEV11	I believe that protecting my confidential information is: Unimportant . . . important	0.9066	46.3399	0.947
SEV17	Threats to the security of my confidential information are: Harmless . . . severe	0.8774	36.2518	
SEV42	Having my confidential information accessed by someone without my consent or knowledge is: Harmless . . . severe	0.9249	58.1726	
SEV46	Having someone successfully attack and damage my system is: Harmless . . . severe	0.9129	40.1054	
SEV50	In terms of information security violations, [attacks on my information systems and equipment] are: Harmless . . . severe	0.9175	0.9175	
Adapted from Rippetoe and Rogers (1987) and modified according to Milne et al.'s (2000) recommendations				
	Vulnerability ($\mu = 3.74$, SD = 0.99)	Loading	*t*-stat	Composite reliability
VUL18	The vulnerability of my confidential information to security violations is: Invulnerable . . . vulnerable	0.8320	19.6888	0.854
VUL10	I believe that trying to protect my confidential information will reduce illegal access to it: Unlikely . . . likely	0.7709	17.7709	
VUL43	The likelihood of someone getting my confidential information without my consent or knowledge is: Unlikely . . . likely	0.8097	10.7219	
VUL49	The likelihood of someone damaging my system is: Unlikely . . . likely	0.7480	27.0088	
VUL53	The likelihood of an information security violation occurring to me is: Unlikely . . . likely	0.7742	10.5591	
Adapted from Rippetoe and Rogers (1987) and modified according to Milne et al.'s (2000) recommendations				
	Locus of control ($\mu = 3.96$, SD = 1.19)	Loading	*t*-stat	Composite reliability
LOC8	Keeping my confidential information safe is: beyond my control . . . within my control	0.9188	51.6414	0.881
LOC15	I believe that it is within my control to protect myself from information security violations: Disagree . . . agree	0.9128	45.9451	
LOC56	The primary responsibility for protecting my confidential information belongs to: My employer . . . myself	0.8629	21.3818	
Adapted from Rotter (1971) modified for the target population according to Harrington's (1996) guidelines				
	Self-efficacy ($\mu = 3.94$, SD = 1.23)	Loading	*t*-stat	Composite reliability
SELF9	For me, taking information security precautions is: Hard . . . easy	0.8599	23.5612	0.929
SELF16	I have the necessary skills to protect myself from information security violations: Disagree . . . agree	0.8957	39.3257	
SELF45	I have the skills to implement the available preventative measures to stop people from getting my confidential information: Disagree . . . agree	0.9081	35.7983	
SELF47	I have the skills to implement the available preventative measures to stop people from damaging my system: Disagree . . . agree	0.8708	34.3423	
SELF52	My skills required to stop information security violations are: Inadequate . . . adequate	0.8741	33.0778	
Adapted from Bandura (1977) modified for the target population according to Compeau and Higgins (1995) guidelines				
	Response efficacy ($\mu = 3.80$, SD = 0.92)	Loading	*t*-stat	Composite reliability
RESP6	Efforts to keep my confidential information safe are: Ineffective . . . effective	0.7981	16.3923	0.913
RESP19	The effectiveness of available measures to protect my confidential information from security violations are: Ineffective . . . effective	0.8884	30.1929	
RESP44	The preventative measures available to me to stop people from getting my confidential information are: Inadequate . . . adequate	0.8804	30.1137	
RESP48	The preventative measures available to me to stop people from damaging my system is: Inadequate . . . adequate	0.8628	27.0419	
RESP51	The preventative measures available to keep people from violating information security are: Inadequate . . . adequate	0.8728	26.5713	
Adapted from Rippetoe and Rogers (1987) and modified according to Milne et al.'s (2000) recommendations				

Table 1 (*continued*)

	Response cost (μ = 3.91, SD = 1.05)	Loading	*t*-stat	Composite reliability
COST24	The inconvenience to implement recommended security measures: exceeds benefits ... outweighed by benefits	0.9114	34.4425	.793
COST25	The cost to implement recommended security measures: exceeds benefits ... outweighed by benefits	0.8735	23.2634	
COST26	The impact to my work from recommended security measures: exceeds benefits ... outweighed by benefits	0.7315	8.0854	
Adapted from Rippetoe and Rogers (1987) and modified according to Milne, et al.'s (2000) recommendations				
	Subjective omission of security (μ = 4.19, SD = 1.25)	Loading	*t*-stat	Composite reliability
OMIT7	I take measures to protect my information from security violations: Never ... always	0.9383	53.2516	.959
OMIT13	I take precautions against information security violations: Never ... always	0.9514	70.2334	
OMIT57	I use information security protections: Never ... always	0.9357	50.1780	
Developed according to Ajzen's (2002) recommendations for measuring intentions				
	Observed samples of omission of security		Weight	*t*-stat
PWDOMIT	Computer logs of password changes		0.6051	18.2871
UPOMIT	Computer logs of security patch updates		0.5162	15.8049
BACKOMIT	Computer logs of backups		−0.1002	4.7784

shown in Table 1. With respect to the objective security behavioral measures, these were collected using a "time sheet and project tracking" compliance software application (the "Application") and computer logs that the firm had been using for some time. In accordance with this organization's common practice, participants were provided with a security policy on the use of the Application, and were asked to sign a form that stated they had read and understood the policy. This policy requested password changes weekly, cryptic passwords, and cautioned not to share passwords. Participants were told to download security patches to the Application weekly, and to backup their timekeeping files. They were instructed about the handling of confidential information such as employee lists and proprietary documents, along with instructions regarding other security behaviors that were the subject of our investigation.

To ensure that employees were aware of the importance of the security measures, Ingenious Company already had in place an IS security policy entitled, *Policy against Fraudulent, Unethical, and Other Dishonest Acts.* Ingenious Company used Measurement-By-Objectives (MBO) for their performance evaluations, and so security conscientiousness was part of every employee's MBO. In this policy, among sundry employee responsibilities, individuals were to "insure that assets are physically secured, computer passwords are protected and not shared, and confidential and sensitive information is protected from unauthorized access." The policy detailed other specific behaviors that we sought to investigate, such as maintaining the most current version of virus scanning software. Violations of this policy were stipulated: "Criminal, civil and/or other administrative actions may be taken against employees who are found to have participated in unlawful acts. Violations of the IS security policy may result in other disciplinary actions...[including that employees may be] required to attend an IS security training course that carries with it an out of pocket fee to the employee." To account for behavioral lapses, behaviors were observed over a period of six months, in accordance with the Burke (2001) and Marx (1982) relapse models. In this way, we were able to observe how well participants conformed to the security policy. The Application automatically tracked password change frequencies (whether they were made, not what they were), downloads of security patches, and dates of backups. We also assessed whether virus scanners were run to completion (as seen in the log files).

4. Results

Each of the hypotheses was tested using both self-reported and objective omissive behavior measures as latent dependent variables. This allowed for a more robust test of the hypotheses rather than

relying on either subjective or objective sets of measures. The objective measures of omissive behavior are formative while the subjective measures are reflective. Combining them served no good purpose in that the entire construct would thereby become formative. By keeping them separate, we were able to check the measurement properties of the subjective measures using traditional validation methods. As a result, we kept the objective and subjective measures separate and tested the hypotheses against each set of criterion variables.

4.1. Test of second order model

To examine the second order modeling of our threat control model, we ran a Varimax Principal Components Analysis on the relevant items. If threat assessment and coping assessment were appropriate grouping variables for the six IVs as predicted, then the items for these constructs will load highly on the posited two factors and not cross-load. As can be seen from Table 2, the loadings do indeed cleanly discriminate between these factors.

4.2. Measurement and structural models

A partial least squares (PLS) analysis allowed us to test the measurement properties of the instrument at the same time as the path coefficients, and, thus the hypotheses. Tests for convergent and discriminant validity are best viewed through a matrix showing on the diagonal the average variance explained (AVE) for each of the IVs, and comparing these with the inter-correlations between constructs (cf., Fornell & Larcker, 1981). Convergent validity is assured when the AVEs exceed .50, seen in Table 3. Discriminant validity is established when the square root of each AVE is higher than its correlation with any other construct in its row or column. Table 3 shows that this is the case and thus the instrument demonstrates acceptable psychometric properties.

Table 2
Factor analysis of second order model

Item	Factor 1	Factor 2
45SELF	.822	.062
16SELF	.793	.144
47SELF	.785	−.003
51RESP	.772	.140
52SELF	.769	.140
48RESP	.752	.161
44RESP	.735	.232
9SELF	.727	.176
19RESP	.695	.249
8LOC	.625	.278
6RESP	.617	.152
15LOC	.607	.224
56LOC	.583	.272
24COST	.311	.911
25COST	.192	.874
43VUL	.003	.766
17SEV	.303	.742
42SEV	.396	.732
26COST	.195	.731
18VUL	.072	.724
53VUL	−.109	.722
50SEV	.377	.716
11SEV	.397	.704
46SEV	.377	.700
49VUL	−.038	.659
10VUL	.390	.559

Extraction method: principal component analysis. Rotation method: varimax.

Table 3
Latent variable AVEs (square roots of AVEs) and correlations

	Locus	Response effect	Self-efficacy	Severity	Vulnerability	Response cost
Locus	0.807 (.898)					
Response effect	0.526	0.742 (.861)				
Self-efficacy	0.543	0.597	0.778 (.882)			
Severity	0.431	0.484	0.435	0.825 (.908)		
Vulnerability	0.373	0.321	0.270	0.556	0.621 (.788)	
Response cost	0.454	0.470	0.459	0.480	0.372	0.709 (.842)

A final test of construct validity indicated that the reflective items all loaded at significant levels ($p < .05$) on the latent constructs. The composite reliabilities are also at very respectable levels (Nunnally, 1978). The objective measures of omissive behavior were formative, and, as such the weightings need to be examined rather than the loadings. Whereas one of the three items was not significant, it was retained for a holistic test of the model, as suggested by Diamantopoulos and Winklhofer (2001). Internal consistency measures are not relevant for formative constructs (Diamantopoulos & Winklhofer, 2001).

The structural test of the model was conducted by creating paths from the IVs directly to the two sets of dependent variables (i.e., the subjective and objective omissive behavior constructs). The PLS model with the path coefficients (in parentheses) are shown in Fig. 1. The first aspect to note about this test is that all coefficients are in the correct, negative direction. It is also useful to observe that in all cases the independent variables were significantly related to either the subjective or objective measures of omissive behavior. Of the twelve paths examined, there was an insignificant result at the .05 alpha protection level (although significant at the .10 level). On the paths leading to objective

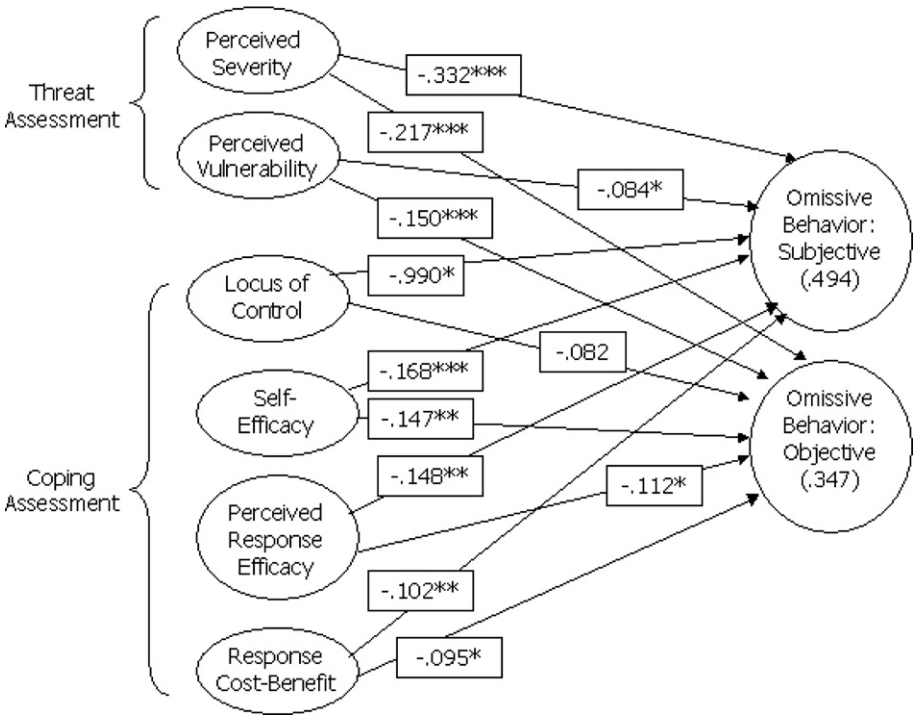

Fig. 1. Results of structural test of the threat control model. *Note*: $^{*}p$-value < .05, $^{**}p < .01$, $^{***}p < .001$. R^{2adj} in parentheses.

omissive behavior, this was locus of control. The explained variances for subjective and objective omissive behaviors are quite respectable at 49.4% and 34.7%, respectively. From a holistic perspective, the IVS are clearly related to lapses in user security as captured by either subjective or objective measures and the TCM was reasonably good at predicting omissive security behaviors.

5. Discussion and limitations

From an overall perspective, our findings suggest that the extent to which people perceive the severity of a threat dictates how motivated they are to prevent it from happening. People implement security measures with greater consistency when the threat is perceived as more severe than when a threat is seen as innocuous, especially when a severe threat is also perceived as imminent. Combining these factors is what is called in the literature as threat assessment. From a practical perspective, however, at a certain level, fear appeals can be counter-productive. When there are excessive false-positive alarms, people will tend to discount fear appeals. And when the level of fear is chronic and extreme, people will adopt a fatalistic attitude about the outcome and fail to take any action. Managers, human resources personnel, and organizational developers should keep in mind this tenuous balance when orchestrating security policies, procedures, and interventions.

From a more macro-perspective, research shedding light on the effects of ethics training and punishment on preventing contravention has emerged in recent years. However, most of the research on IS security defenses has looked either at available security technologies or the management of security infrastructure, such as conducting risk analyses for the application of technological defenses. But, as with contravention, the security defense problem is more appropriately grounded in behavior and in individuals' failure to take precautions against IS security threats. This research has been largely ignored, especially in studies of people who know how to implement security measures but ultimately fail to do so (the knowing-doing gap).

Failing to implement IS security precautions continues to be a significant problem. Carelessness with information and failure to use available security precautions contributes to the loss of information and even to crimes. One prominent example of this is the rampant growth of corporate espionage and identity theft. The US Department of Justice (2004) estimates that one person in three will become victims of computer-based crime at some point in their lifetime. One serious drawback to understanding this phenomenon has been the nearly total lack of testing explanatory theory. To begin laying groundwork in this regard, we adapted protection motivation theory originally employed in the explanation of health-related threats. Our contribution to a better understanding of this phenomenon is a *threat control model* (TCM) that attempts to explain the knowing-doing gap in IS security. An important challenge, however, is how to take these relatively micro-level findings and implement them as a matter of organizational or even national policy.

To highlight this, as a matter of socio-political policy, governments have used terror-management theory (Cohen, Ogilvie, Solomon, Greenberg, & Pyszczynski, 2005) for making fear appeals to the public in attempts to elicit vigilance against terrorist threats, for example. The media and other social influences also serve to propagate and exacerbate the perceptions of threat severity, or they may propose coping behaviors. In terms of IS security, the effectiveness of defensive countermeasures depends on individuals implementing available preventive measures. Hence, our threat control model is concerned with how individuals respond to fear appeals and social influences concerning IS security.

For people to take IS security precautions they must positively assess their ability to cope with the perceived threat. The results of our study indicate an interesting relationship between people's perceptions of their behaviors and their actual behaviors in a couple of respects. First, coping depends on whether people feel that their ability to take security actions have been reasonable (self-efficacy), providing that they perceived that the threat is preventable in the first place (locus of control). However, the objective behavior link between locus of control and actual behavior was not significant. We see in this case, the importance of the triangulation between perceived and actual security behaviors. The disparity may indicate that locus of control might be acting as an antecedent to self-efficacy in the case of such IS security threats, or it may highlight that this factor is subject to "social desirability

effects." This finding presents an interesting opportunity for further investigation into coping versus actual and perceived behavioral outcomes.

Also, it seems intuitive, and it is certainly suggested by current theory, that when people perceive a threat as severe and likely, they only undertake those measures that they think are effective in preventing the IS security threat. This, of course, is the influence of perceived response efficacy on omissive behavior. However, in spite of the fact people may claim to attempt to prevent a threat, the perceived inevitability of the threatened event may nullify their behavior. Future research may investigate the interactions of perceived response efficacy and locus of control under different threat conditions.

This leads us to some study points worth noting. First, as we have indicated there is always some discrepancy between what people report about their behaviors and what they actually do. Therefore, we used objective, observational measures not only to address this limitation but also to explore where there might be discrepancies. However, observational measures cannot exhaust the range of possible IS security behaviors. In other words, because it is ideographic in nature, one cannot practically observe every possible IS security behavior. By combining self-reported security behaviors with the observed security behaviors we exploited an advantage in that we were able to gather a nomothetic or general classification of IS security behavior ("I take security precautions to protect my information"). This triangulation strengthens the TCM by suggesting how self-report measures can tap into a general classification of IS security behavior.

While people generally state that they are concerned about IS security and privacy, and may even claim that they are willing to pay a fee to protect their personal information, in many cases they are willing to trade-off privacy for convenience, or even bargain for the release of very personal information in exchange of relatively small rewards (Acquisti & Grossklags, 2007). While this was not the focus of our study, it presents some interesting considerations for future research into the effects of cost, convenience, and benefits of IS security technologies on omissive security behavior.

6. Conclusion and suggestions for future research

It is well known that workers are not very security-conscious. A variety of security countermeasures are available to employees, but they often fail to employ these options. The result is that the deployment of IS security precautions is generally lax in many organizations. It is also the case that large, and in some cases huge, expenditures in security software and hardware prove to be worthless against even modest and uninspired security attacks. What thus can be done to secure organizational systems worldwide? The present study is hopefully part of what will be many follow-up studies that will attack this very real problem. Omissive security behavior threatens the integrity of mission-critical systems and needs to be seriously addressed.

There are several implications for managers, organizational developers, and human resources personnel to consider. Our research helps to address the "what to educate" question. Training has tended to focus on the use or implementation of security technology and has not addressed underlying behavioral dimensions that may motivate use once the skills are acquired (Calluzzo & Cante, 2004). The perceived severity and the extent to which people feel vulnerable appear to be important components in this underlying motivation. A technique known as *benign hacking* or *white-hat penetration* or *controlled exploitation*, has been used to find technological vulnerabilities in security infrastructure, but it may serve another purpose and could be incorporated into interventions. Chief Security Officers and other security officials could and should communicate actual threat levels to employees so that their perceptions of the extent of the threat are not underestimated. A correct threat assessment will lead, in many cases, to fewer lapses, which is the goal of security training.

When people have been victimized in the past, it becomes easier to see themselves as victims once again, thus controlling for victimization (as we did in our study) is important. Since not everyone in an organization is likely to have succumb to a security violation, holes found in the security of people's systems could be incorporated into an experiential training intervention that elevates people's perceptions of vulnerability and severity of IS security threats. This technique could also apply to coping responses. By showing employees the effectiveness of subsequent corrective measures for preventing

exploitations, perceptions of control and efficacy should increase and this will decrease security lapses. The use of behavioral modification simulation software has tremendous potential in this regard because of its ability to modify habituated behaviors and behavioral relapses.

In addition to the training interventions, our research points to the importance of choosing "the right" security technology. Since there is a perceived trade-off between threat assessments and coping responses, security technology should be user-centered. Research has shown that two elements are particularly germane, namely, technology ease-of-use and usefulness. Ease-of-use is related to *self*-efficacy whereas usefulness is related to *response* efficacy, and chosen technologies should not possess characteristics of one to the exclusion of the other if people are to use them. Comments from one participant illustrates this: "[My virus scanning software] is very effective but I have quit using it because it kept corrupting my registry [in Microsoft Windows] when I upgraded it." In light of our findings concerning perceived response efficacy, future research might benefit by incorporating perceptions of ease-of-use and usefulness concepts from the Technology Acceptance Model (Davis, 1989; Davis et al., 1989). Because IS security behavior is so fundamental to the implementation of security measures, managers and security personnel cannot afford to ignore the knowing-doing gap.

References

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security and Privacy, 3*, 26–33.

Acquisti, J., & Grossklags, A. (2007). When 25 cents is too much: An experiment on willingness-to-sell and willingness-to-protect personal information, Sixth Workshop on the Economics of Information Security (WEIS 2007), June 6, Pittsburgh, PA (pp. 7–18).

Adams, D. A., Nelson, R. R., & Todd, P. A. (1992). Perceived usefulness, ease of use, and usage of information technology: A replication. *MIS Quarterly, 16*, 227–247.

Ajzen, I. (2002). Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. *Journal of Applied Social Psychology, 32*, 665–683.

Albrechtsen, E. (2006). A qualitative study of users' view on information security. *Computers and Security, 25*, 445–451.

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

Bandura, A. (1991). Social cognitive theory of self-regulation. *Organizational Behavior and Human Decision Processes, 50*, 248–287.

Bandura, A. (2001). Social cognitive theory: An agentive perspective. *Annual Review of Psychology*(52), 1–26.

Bandura, A., & Walters, R. H. (1963). *Social learning and personality development*. New York: Holt, Rinehart and Winston.

Bartels, A. (2006). Global IT spending and investment forecast, 2006 To 2007. *Forrester Research, 12*, 4–31.

Blankenship, K. L., & Whitley, B. E. (2000). Relation of general deviance to academic dishonesty. *Ethics and Behavior, 10*(1), 1–12.

Boer, H., & Seydel, E. (1996). Protection motivation theory. In M. Conner & P. Norman (Eds.), *Predicting health behavior: Research and practice with social cognition models* (pp. 95–120). Buckingham, UK: Open University Press.

Borrull, A. L., & Oppenheim, C. (2004). Legal aspects of the Web. In Blaise Cronin (Ed.). *Annual Review of Information Science and Technology* (Vol. 38, pp. 483–548). Medford, NJ: Information Today.

Bresz, F. P. (2004). People – Often the weakest link in security, but one of the best places to start. *Journal of Health Care Compliance*, 57–60.

Burke, P. B. (2001). Collaboration for successful prisoner reentry: The role of parole and the courts. *Corrections Management Quarterly, 5*, 11–22.

Calluzzo, V. J., & Cante, C. J. (2004). Ethics in information technology and software use. *Journal of Business Ethics, 51*(3), 301–312.

Challappa, R. K., & Pavlou, P. (2002). Perceived information security, financial liability, and consumer trust in electronic commerce transactions. *Journal of Logistics Information Management*(15), 358–368.

Cohen, F., Ogilvie, D. M., Solomon, S., Greenberg, J., & Pyszczynski, T. (2005). American roulette: The effect of reminders of death on support for George W. Bush in the 2004 Presidential Election. *Analyses of Social Issues and Public Policy, 5*, 177–187.

Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly, 19*, 189–211.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*, 319–340.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science, 35*, 982–1003.

Debar, H., & Viinikka, J. (2006). Security information management as an outsourced service. *Information Management and Computer Security, 14*, 417–435.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: Towards socio-organizational perspectives. *Information Systems Journal, 11*, 127–153.

Diamantopoulos, A., & Winklhofer, H. M. (2001). Index construction with formative indicators: An alternative to scale development. *Journal of Marketing Research, 38*, 269–277.

Dorn, L., & Brown, B. (2003). Making sense of invulnerability at work – A qualitative study of police drivers. *Safety Science, 41*, 837–859.

Eloff, M. M., & von Solms, S. H. (2000). Information security management: A hierarchical framework for various approaches. *Computers and Security, 19*, 243–256.

Ettredge, M. L., & Richardson, V. J. (2003). Information transfer among internet firms: The case of Hacker attacks. *Journal of Information Systems, 17*(2), 71–82.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*, 39–50.
Gregor, S., & Benbasat, I. (1999). Explanations from intelligent systems: Theoretical foundations and implications for practice. *MIS Quarterly, 23*, 497–527.
Grothmann, T., & Reusswig, F. (2006). People at risk of flooding: Why some residents take precautionary action while others do not. *Natural Hazards, 38*, 101–120.
Harrington, S. J. (1996). The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly, 20*, 257–258.
Harvey, C. (2007). The boss has new technology to spy on you. *Datamation*, April (pp. 1–5).
Hochhauser, M. (2004). Smart executives, dumb decisions. *Journal of Risk Management, 51*, 64–73.
Hsu, M-H., & Kuo, F-Y. (2003). An investigation of volitional control in information ethics. *Behavior and Information Technology, 22*, 53–62.
International Federation of Accountants (2006). Intellectual assets and value creation: Implications for corporate reporting. Paris France. <http://www.oecd.org/dataoecd/2/40/37811196.pdf> Retrieved 11.4.07.
Janoff-Bulman, R., & Frieze, I. H. (1983). A theoretical perspective for understanding reactions to victimization. *Journal of Social Issues, 39*, 1–17.
Jones, R. L., & Rastogi, A. (2004). Secure coding: Building security into the software development life cycle. *Information Systems Security, 13*, 29–39.
Jutla, D. N., & Bodorik, P. (2005). Sociotechnical architecture for online privacy. *IEEE, Security and Privacy, 3*, 29–39.
Kankanhalli, A., Teo, H.-H., Tan, B. C. Y., & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management, 23*, 139–154.
Keck, R. (2005). Disruptive technologies and the evolution of the law. *Legal Briefs, 23*, 22–49.
Kim, Y., & Kim, D. J. (2005). A study of online transaction self-efficacy, consumer trust, and uncertainty reduction in electronic commerce transaction. In *Proceedings of the 38th annual Hawaii international conference on system sciences (HICSS), June* (pp. 170–183).
Kuo, F.-Y., & Hsu, M.-H. (2001). Development and validation of ethical computer self-efficacy measure: The case of shoplifting. *Journal of Business Ethics, 32*, 299–315.
Kurland, N. B. (1995). Ethical intentions and the theories of reasoned action and planned behavior. *Journal of Applied Social Psychology, 25*, 297–313.
Lazarus, R. S. (1991). *Emotion and adaptation*. New York: Oxford University Press.
Leach, J. (2003). Improving user security behaviour. *Computers and Security, 22*, 685–691.
Lejeune, R., & Alex, N. (1973). On being mugged: The event and its aftermath. *Urban Life and Culture, 2*, 259–287.
Leyden, J. (2004). Clueless office workers help spread computer viruses, *The Register*, February 6 (pp. 17–21).
Lin, C-P., & Ding, C. G. (2003). Modeling information ethics: The joint moderating role of locus of control and job insecurity. *Journal of Business Ethics, 48*, 335–347.
Losey, R. C. (1998). The electronic communications privacy act: United States Code. Orlando, FL. <http://floridalawfirm.com/privacy.html> Retrieved 10.12.07.
Marsh, H. W., & Richards, G. E. (1986). The rotter locus of control scale: The comparison of alternative response formats and implications for reliability, validity and dimensionality. *Journal of Research in Personality, 20*, 509–558.
Marx, R. D. (1982). Relapse prevention in managerial training: A model for maintenance of behavior change. *Academy of Management Review, 7*(1), 433–441.
Milgram, N. N., & Naaman, N. (1996). Typology in procrastination. *Personality and Individual Differences, 20*, 679–683.
Milne, S. S. P., & Orbell, S. (2000). Prediction and intervention in health-related behaviour: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology, 30*, 106–143.
Nunnally, J. C. (1978). *Psychometric theory*. New York: McGraw-Hill.
O'Donoghue, T., & Rabin, M. (2000). The economics of immediate gratification. *Journal of Behavioral Decision Making, 13*, 233–250.
Ong, T. H., Tan, C. P., Tan, Y. T., & Ting, C. (1999). SNMS – Shadow network management system. In *Symposium on network computing and management*. Singapore. May 21 (pp. 1–9).
Pahnila, S., Siponen, M. T., & Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. In *Proceedings of the 40th Hawaii International Conference on System Sciences, HICSS* (pp. 156–165).
Pechmann, C., Zhao, G., Goldberg, M., & Reibling, E. T. (2003). What to convey in antismoking advertisements of adolescents: The use of protection motivation theory to identify effective message themes. *Journal of Marketing, 67*, 1–18.
Post, G. V., & Kagan, A. (2007). Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computers and Security, 26*, 229–237.
Proctor, R. W., Kim, P. L., Vu Schultz, E., & Salvendy, G. (2002). Improving computer security for authentication of users: Influence of proactive password restrictions. *Behavior Research Methods, Instruments, and Computer, 34*, 163–169.
Pyszczynski, T., Greenberg, J., & Solomon, S. (1997). Why do we need what we need? A terror management perspective on the roots of human social motivation. *Psychological Inquiry, 8*, 1–20.
Rippetoe, P. A., & Rogers, R. W. (1987). Effects of components of protection–motivation theory on adaptive and maladaptive coping with a health threat. *Journal of Personnel Social Psychology, 52*, 596–604.
Roe-Berning, S., & Straker, G. (1997). The association between illusions of invulnerability and exposure to trauma. *Journal of Traumatic Stress, 10*, 319–327.
Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology, 91*, 93–114.
Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. Cacioppo & R. Petty (Eds.), *Social Psychophysiology* (pp. 153–176). New York: Guilford Press.
Rotter, J. (1966). Generalized expectancies for internal versus external control of reinforcement. *Psychological Monographs, 1*, 1–28.
Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers and Security, 26*, 56–62.

Ryan, J. (2004). Information security tools and practices: What works? *IEEE Transactions on Computers, 53*, 1060–1064.
Salant, P., & Dillman, D. A. (1994). *How to conduct your survey*. New York: John Wiley and Sons.
SANS. (2005). The SANS security policy project. Bethesda, MD.
Sasse, M. A., Brostoff, S., & Weirich, D. (2004). Transforming the weakest link – A human/computer interaction approach to usable and effective security. *BT Technology Journal, 19*, 122–131.
Scholz, J. T. (1997). Enforcement policy and corporate misconduct: The changing perspective of deterrence theory. *Law and Contemporary Problems, 60*, 153–268.
Sherif, J. S., Ayers, R., & Dearmond, T. G. (2003). Intrusion detection: The art and the practice. *Information Management and Computer Security, 11*, 175–186.
Shreve, M. (2004). The office now a major place for identity theft. *Crains*. September, (pp. 1–4).
Siponen, M. T., Pahnila, S., Mahmood, A. (2006). Factors influencing protection motivation and IS security policy compliance, *Innovations in Information Technology*, November, 1–5.
Siponen, M. T., & Iivari, J. (2006). IS security design theory framework and six approaches to the application of IS security policies and guidelines. *Journal of the Association for Information Systems, 7*(7), 445–472.
Stajkovic, A. D., & Luthans, F. (1998). Self-efficacy and work-related performance: A meta-analysis. *Psychological Bulletin, 124*, 240–261.
Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Journal of Computers and Security, 24*, 124–133.
Straub, D. W., Carlson, P. J., & Jones, E. H. (1993). Deterring cheating by student programmers: A field experiment in computer security. *Journal of Management Systems, 5*, 33–48.
Straub, D. W., & Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: A field study. *MIS Quarterly, 14*, 45–62.
Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22*, 441–469.
Tang, C. S.-K., Pun, S. H., & Cheung, F. M. (2002). Responsibility attribution for violence against women: A study of Chinese public service professionals. *Psychology of Women Quarterly, 26*, 175–185.
Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of IS017799. *Computers and Security, 24*, 472–484.
Thomas, T. M. (2004). *Network security first-step*. Indianapolis, IN: Cisco Press.
von Solms, B., & von Solms, R. (2004). The 10 deadly sins of information security management. *Computers and Security, 23*, 371–376.
Wilde, G. J. S. (2001). *Target risk*. Toronto: PDE Publications.
Woon, I. M. Y., Tan, G. W., & Low, R. T. (2005). A protection motivation theory approach to home wireless security. International Conference on Information Systems, Las Vegas (Vol. 26, pp. 367–380).
Workman, M. (2007). Gaining access with social engineering: An empirical study of the threat. *Information Systems Security Journal, 16*, 315–331.
Workman, M., & Gathegi, J. (2005). Observance and contravention of information security measures. In *Proceedings of the world conference on security management and applied computing*, Las Vegas, NV (pp. 241–247).
Workman, M., & Gathegi, J. (2007). Punishment and ethics deterrents: A study of insider security contravention. *Journal of the American Society for Information Science and Technology, 58*, 210–222.
Wu, Y., Stanton, B. F., Li, X., Galbraith, J., & Cole, M. L. (2005). Protection motivation theory and adolescent drug trafficking: Relationship between health motivation and longitudinal risk involvement. *Journal of Pediatric Psychology, 30*, 122–137.