MeRC

McMaster eBusiness Research Centre

Understanding Employee Security Misbehavior in Using Organizational Information Systems

by
Ken H. Guo
And
Yufei Yuan

McMaster eBusiness Research Centre (MeRC)

WORKING PAPER No. 31
January 2010

McMaster University

UNDERSTANDING EMPLOYEE SECURITY MISBEHAVIOR IN USING ORGANIZATIONAL INFORMATION SYSTEMS

By

Ken H. Guo and Yufei Yuan

MeRC Working Paper #31

January 2010

McMaster eBusiness Research Centre (MeRC) ©

DeGroote School of Business

McMaster University

Hamilton, Ontario, L8S 4M4

Canada

guoh4@mcmaster.ca

yuanyuf@mcmaster.ca

ABSTRACT

This study aims to investigate why users engage in "security misbehavior" (SMB) when using organizational information systems (IS). It is posited that user intention to engage in SMB is influenced by attitude toward SMB, workgroup norm, and perceived professional identity mismatch. Attitude toward SMB in turn is predicted by attitude toward targets (IS department and security policy), expectations of utilitarian outcome (perceived security risk, perceived accountability, and job performance expectation), workgroup norm, and perceived professional identity mismatch. The model was tested with partial least square (PLS) technique on data collected from a survey (N=104). The results suggested that both attitude toward SMB and workgroup norm have significant influence on SMB intention. User attitude toward SMB is influenced by workgroup norm and perceived identity mismatch. Workgroup norm appear to be a key determinant of user SMB intention.

Keywords: security misbehavior, information security

INTRODUCTION

One of the often-recommended measures for managing organizational information systems (IS) security is security policy (e.g. Baskerville and Siponen 2002). The implementation and enforcement of security policy can help organizations make sure proper measures are in place to protect their information systems and reduce undesirable uses that may cause security problems. The importance of security policy is widely recognized in various standards such as ISO/IEC 27002, which requires management "set a clear policy direction in line with business objectives and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization" (ISO/IEC 2005).

Having a policy in place, however, does not necessarily guarantee security. Because users interact with information systems on a regular basis in their business activities, how they use the systems and whether they follow established measures will ultimately influence the overall security of an organization's information systems. Fundamentally, IS security has a "behavioral root" (Workman and Gathegi 2006) and it is a subject of psychological and sociological behavior of people (Parker 1981). Even if an organization has the most advanced technology and a good security policy in place, security could still be compromised if users do not follow the policy. One should not expect humans to always act as prescribed (Besnard and Arief 2004). In fact, practitioners see the enforcement of policy, i.e. making sure the policy is properly followed by users, as a critical issue in security management. It is not surprising that people are viewed as the "weakest link" in the security chain (Schneier 2000). A recent industry survey of remote workers has found that even if users are aware of potential security problems related to their actions, many of them do not follow security best practices and yet continue to engage in behavior that can open their organizations to serious security risks (Cisco 2006). For example, the survey found that many workers allowed others to use their work computing devices despite their awareness of the possible security implications. It was also reported that many users don't follow policies and some of them knowingly violate policies without worry of repercussions (Dubie 2007). In the IS security literature, there is also a lack of empirical evidence to prove the effectiveness of IS security policies. A recent study showed no statistically significant relationships between the adoption of security policies and the incidence or severity of security breaches (Doherty and Fulford 2005). Standards such as ISO/IEC 27002 recommend that a security policy should state the consequences of violations. However, recent research found that the existence of punishment does not have effect on user intention to misuse information systems (D'Arcy et al. 2009). This phenomenon raises an important question: what motivate workers to engage in such behaviors?

This research aims to study this type of insecure behavior of employees in using an organization's information systems. More specifically, this paper tries to answer the following research question: why do users intend to engage in insecure use of IS although such uses violate the organization's security policy? To achieve this end, this paper proposes and tests a theoretical model to explain the antecedents of users' insecure behaviors.

LITERATURE REVIEW

Conceptualization of Security Misbehavior

In the present study, security misbehavior (SMB) is defined as those behaviors engaged by employees who violate or bypass the organizational IS security policies with the intention to benefit themselves from their own job perspective. Organizational security policy in this study refers to the set of rules and regulations that govern employee actions in dealing with security issues when using IS for routine business tasks. In general, an IS security policy defines what users are allowed to do or what they are not allowed to do. Policy is the basis for the dissemination and enforcement of sound security practices within the organizational context (Baskerville and Siponen 2002). SMBs have a number of characteristics: 1) Intentional - SMBs are intentional employee behaviors. Thus, such behaviors should be differentiated from accidental events that may lead to the breach of information systems rules and policies. Examples of accidental events include human errors and power outages that may damage the operation of IS. The term "intentional" in this context implies the actor makes some "conscious decisions" to follow a course of action. 2) Self-benefiting - Employees who engage in SMBs may try to benefit themselves by, for example, saving time and effort that may be required in order to follow specific rules and policies. It should be noted, however, that employees who engage in SMBs do not necessarily have the malicious intent to harm the security or general business operation of the organization. 3) Rule-breaking - When employees engage in security misbehavior, they actually break the organization's policies to various degrees. 4) Possibly causing damage or security risk - In addition to rule-breaking, it is "misbehavior" in the sense that such behaviors are undesirable from IS security perspective and may cause damages to the organizations' information systems or put the system at risk, although the employee in question may not have such malicious intent. As such, the term security misbehavior in this context is not the same as behaviors with malicious intentions defined in the literature (Stanton et al. 2005).

Prior Research on User Security Behaviors

In the IS security research literature, the general deterrence theory (GDT) has been applied to investigate the effect of organizational deterrent measures on computer abuses by employees. For example, the security impact model (Straub 1990) suggests that deterrent measures can reduce computer abuses by potential offenders if the risk of punishment is high (deterrent certainty) and penalties for violations are severe (deterrent severity). In this model, deterrent measures include IS security efforts, dissemination of information about penalties, guidelines for acceptable system use, policies for system use, among others. Computer abuse is measured by number of incidents, actual dollar loss caused by security incidents, as well as opportunity dollar loss. The study suggests that deterrent severity has greater explanatory power than deterrent certainty.

There have been mixed findings, however, about the effectiveness of deterrence measures in the literature. In one study, deterrent efforts and preventive efforts were found to positively impact the effectiveness of IS security (Kankanhalli et al. 2003). Deterrent severity, on the other hand, did not have significant impact. In another study, physical security systems (e.g. physical entry control and secured computer rooms) influence computer users' self-defense intention, which is defined as the intention to install access control software and intrusion detection software (Lee et al. 2004). Two other factors - security policy and security awareness – did not have significant

impact, opposite to what was expected according to GDT. In a most recent study, an extended GDT model (D'Arcy et al. 2009) was proposed to capture the antecedents of IS misuse intention. It was found that perceived severity of sanctions reduces IS misuse intention; on the other hand, however, the influence of perceived certainty of sanctions is not significant, contrary to what is expected based on GDT. An interesting finding of the study is that awareness of security policy reduces perceived certainty of sanction, contrary to the positive relationship that is predicted by the model. While this unexpected negative relationship may be attributed to reasons such as research design and user knowledge about the difficulties in detecting misuse incidents (D'Arcy et al. 2009), it may very well be that user attitude toward the policies influenced the relationship. Users may think the policies are just on paper and will not be enforced, although the punishments of violation may be severe. The factor of user attitude, however, has not been fully investigated in the literature.

Some other studies investigated the user security behaviors from an ethics perspective (Banerjee et al. 1998; Harrington 1996; Leonard and Cronan 2001). IS ethics, which refer to the ethical content of informal norms and behaviors, may help deal with those situations where there are no formal rules or policies (Dhillon and Backhouse 2000). One common limitation of ethical research is that the classification of ethical and unethical behaviors is not always straightforward and there are no clear-cuts. In fact, prior research found that some undesirable behaviors related to use of organizational IT property were view as neutral, i.e. neither ethical nor unethical by survey participants (Calluzzo and Cante 2004). One example of such behaviors is the downloading files on job or at school from the Internet for personal use.

Still other studies focused on user compliance to security policies. In one study, an IS security policy compliance model (Pahnila et al. 2007) suggests that user intention to comply with security policy is influenced by user attitude toward complying. Both attitude and intention are also influenced by a number of negative reinforcements (including sanctions, threat appraisal, coping appraisal, and normative beliefs) and positive reinforcements (including information quality of the policies, facilitation conditions, and habits). A survey of employees in a Finish company indicated that attitude, normative beliefs, and habits have significant effect on user intention to comply with security policies; threat appraisal and facilitation conditions have significant influence on attitude toward complying. It is notable that, contrary to what is expected, coping appraisal did not have significant impact on user attitude toward complying. Sanctions did not have significant effect on user intention to comply, contrary to the prediction of the general deterrence theory (GDT). In a different study, an employee compliant behavior model (Chan et al. 2005) was proposed. It found that user compliant behavioral intention is influenced by the information security climate perceived by users and users' self-efficacy (of breaching security). User perception of security climate is determined by individuals' observation of upper management practices, direct supervisory practices, and coworker socialization.

Workman et al (2008) proposed a "threat control model" to explain why people who are aware of IS security threats and countermeasures fail to implement those measures ("omissive behavior"). It was contended that users' omissive behavior depends on their "threat assessment" and "coping assessment", based on the assumption that when a threat is perceived, people adjust their behavior according to the acceptable level of risk. Threat assessment includes users' perceptions of threat severity and vulnerability (whether they perceive they are vulnerable to security breach). Coping assessment involves users' evaluation of their capability to deal with certain

situations. It includes the assessment of locus of control, self-efficacy (of dealing security issues), perceived response efficacy (whether security measures are effective), and response cost-benefit. As previously discussed, similar concepts of threat appraisal and coping appraisal have been studied in the security policy compliance model (Pahnila et al. 2007). The conclusions of the two studies, however, are inconsistent. In the study by Pahnila et al, it was found that coping appraisal had insignificant effect on user attitude toward complying (which in turn is hypothesized to influence compliance intention and actual compliance).

Siponen and Vance (2009) proposed a neutralization model to investigate the problem of employee IS security policy violations. Based on the neutralization theory in criminology literature, the model suggests that employees rationalize their violations of security policies by a number of neutralization techniques: 1) defense of necessity; 2) appeal to higher loyalties (justifying by appealing to organizational values or hierarchies); 3) condemn the condemners (justifying by blaming the target of action, e.g. IS security policy); 4) metaphor of the ledger (justifying bad behaviors with prior good behaviors); 5) denial of injury (justifying by minimizing harms); and 6) denial of responsibility (justifying by beyond-control excuse). The study found that neutralization had significant effects on employee intention to violate IS security policies. The effects of formal sanctions and informal sanctions, on the other hand, were not significant.

Although these prior studies have provided some valuable insights on conceptualization of user security behaviors and the antecedents of such behaviors, there are some limitations and gaps that may warrant further investigation. First of all, in the context of security misbehavior (SMB), those ethical/unethical behavioral models may not be directly applicable. First, security misbehavior may not be "unethical" per se as discussed in previous section. Thus code of ethics may not have significant impact on users' intention to engaging in SMB, nor do those factors affecting ethical behaviors. Furthermore, although SMB may trigger disciplinary actions that are often prescribed in security policies, such disciplinary actions, i.e. deterrence, may be deemed as unfair because the actor may intend to improve job performance by engaging in SMB.

Secondly, security compliance models do not explain while users break rules. In general, compliance behavior and security misbehavior may appear to be the two sides of the same coin. They may share some common antecedents such as threat appraisal. For example, someone who perceived high security threat may tend to comply with security policy while others who perceive low threat may actually engage in security misbehavior (or non-compliance). Despite this commonality, however, the antecedents of the two types of behaviors may be quite different. Following rules or policies could be human's common sense and may not require any salient cues. To break rules, on the other hand, the actors may think about the rule breaking and look for salient cues or some sorts of purposes and excuses for themselves. Practically, it may be more worthwhile to investigate why users misbehave rather than why they comply with policies so that proper measures could be put in place to discourage them from breaking rules. Theoretically, when deviant behaviors, which refer to those behaviors that are not typical ones that similar others would make in similar situations, are observed, it means that something surprising occurred and requires an explanation (Blanton and Christie 2003; Hilton and Slugoski 1986). In other words, deviant behaviors are more "informative" (Blanton and Christie 2003). From this perspective, studying security misbehavior, which can be seen as at type of deviant behavior, may enable us to have some insightful understanding of employees' actions in using organizational information systems.

Third, similar to those compliance models, deterrence models may help explain why users comply with computer use or security rules (by not engaging in SMB), but not why they break those rules or engage in SMB. Furthermore, as discussed previously, the effect of deterrence is not conclusive. Further study needs to be done to understand the reasons why security policies do not work even when punishment is certain.

Fourth, omissive security behavior (Workman et al. 2008) is similar to SMB in that they are both undesirable for security management. However, they are different in that the former assumes that users "do not do what they are supposed to do" while the latter assumes that users "do what they are not supposed to do". Furthermore, in their study, Workman et al (2008) considered the factor of threat only, i.e. how users evaluate and cope with threats. The model may not provide sufficient explanation about user behavior because security and the dealing of threats are perceived not to be users' tasks or responsibilities (Besnard and Arief 2004).

Fifth, although violation of IS security policy conceptualized in the neutralization model (Siponen and Vance 2009) may be manifested in behaviors similar to SMB, the former does not clearly emphasize the "knowing-doing" aspect of behavioral intention. For example, in their study, the "denial-of-responsibility" neutralization technique focuses on whether employees are aware of and understand the IS security policies in question. Furthermore, violations of IS security policy are not crime, although the two types of behaviors share some commonalities such as rule-breaking. Crimes are extremely bad behaviors that are condemned and prohibited by the society in general. Violations of IS security policies are issues within an organizational scope and are not as severe as crimes. In fact, researchers have argued that rules should be built in security policies to allow some violations under exceptional circumstances (Siponen and Iivari 2006). Thus applying criminological theories on IS security policies may not be straightforward.

Lastly, some studies investigated security behaviors of IT professionals (e.g. Banerjee et al. 1998; Harrington 1996) while others used student samples (e.g. Leonard and Cronan 2001). Arguable, the perspectives of IT professionals and students are much different from that of end-users in organizational settings. Thus, the results of these studies may not be directly applicable to the latter population.

In summary, despite the growing interest and research in user security behavior in the literature, some critical questions remain unanswered, particularly the question of why users engage in security misbehavior that violate organizational security policies and rules and may result in punishments or disciplinary actions. It is the very objective of this study to answer this question.

THEORETICAL BACKGROUND AND HYPOTHESES DEVELOPMENT

We propose an SMB model by applying the composite behavior model (CBM) (Eagly and Chaiken 1993). CBM is an extension to the theory of planned behavior (TPB) (Ajzen 1991). According to the CBM, a person's attitude toward a behavior impacts whether or not the person will engage in that behavior. Such impact is mediated by the person's intention. The person's attitude toward the behavior is in turn determined by a number of antecedents: habit, attitude toward target, utilitarian outcomes, normative outcomes, and self-identity outcomes. According to this model, a person's habit will have a direct impact on attitude toward target, attitude toward behavior, and actual behavior. The term "target" refers to the particular target that is the object of a behavior. In other words, a target is the entity (e.g. thing, person) toward which the behavior in question is directed. Attitude toward behavior is determined by habit, attitude toward target, and

expected outcomes. Outcomes are the anticipated consequences of a behavior. There are three types of outcome: utilitarian outcome, normative outcome, and self-identity outcome. Utilitarian outcome refers to either rewards or punishments that expected from engaging in the behavior in question. Normative outcome refers to the approval or disapproval by significant others regarding the behavior. In Eagly and Chaiken's term, it also refers to self-administrated rewards (pride) and punishments (guilt) that follow from the actor's internalized moral rules. Self-identity outcome refers to either affirmations or repudiations of the self-concept that are expected to follow from engaging the behavior. In addition, normative outcomes and self-identity outcomes also influence behavior through their direct impact on intention.

The most noticeable difference between CBM and TPB is that the former includes a habit factor and that it splits the attitude factor into attitude toward targets and attitude toward behavior. We contend that attitude toward targets, which is considered as external to the TPB model, is important in the IS context because user because user security behavior is not an isolated act. It involves the interaction with the IS department in an organization and users have to deal with security policies and measures. Their attitudes toward these targets may be an important antecedent of their security behaviors.

Based on Eagly and Chaiken's composite behavior model and other theoretical considerations as discussed below, we propose a security misbehavior model as shown in Figure 1. Instead of studying actual behavior as in the CBM, this research focuses on intention (i.e. SMB intention is the dependent variable). This is because that the influence of intention on behavior has been rigorously tested and well established in the literature. This approach is not uncommon in the IS literature. Examples of studying behavioral intention as dependent variable include knowledge sharing intention (Bock et al. 2005), IS misuse intention (D'Arcy et al. 2009), IT usage intention (Bhattacherjee and Sanford 2006), among others.

One notable difference from CBM is that habit is not included in the proposed SMB model. One main reason is that habits (if defined as previous behavior) have a tautological relationship with current or future behavior (Thompson et al. 1991). Using prior behavior to predict future but the same behavior does not add much theoretical value (Ajzen 1991). In the context of information system security, there are also some other reasons. First, habit implies a behavior is automatic and it has become routinized through repetition that the person does not make any conscious decision to act yet still engage in the behavior in an automatic way; and as such a behavior should be less affected by intentions to the extent that the behavior is habitual (Eagly and Chaiken 1993). Because the proposed SMB model focuses on intention instead of actual behavior, inclusion of habitual factor will less likely improve the explanatory power of the model. Secondly, SMB implies rule-breaking. The actor involved in SMB is more likely conscious in making such behavioral decision. An analogy is driving. Driving below speed limit, e.g. 50 kilometers per hour on the street, is what everyone usually does, presumably. People may just drive at that speed without any salient intention per se. However, for people to break the rule, i.e. driving over the speed limit, some salient cues or objectives are often required (although there is a possibility that people drive over the limit without realizing their speed). In other words, they are making conscious decision and self-instructed, unlike in habitual situations that lack of self-instruction.

Another difference is that the SMB model does not include the interrelationships among those antecedents of attitude toward behavior. This is because the aim of this study is to predict attitude and behavioral intention. As such, only direct effects will be modeled and analyzed. This

approach is basically consistent with that taken by Venkatesh et al (2003). It should be noted that the variance (R square) explained by the model is not affected by indirect paths (Venkatesh et al. 2003).

Attitude toward SMB

According to CBM, attitude toward behavior positively influence behavioral intention. Similarly, in the context of IS in organizations, this relationship should also apply to users' security behavior. Those users who hold a more positive attitude toward security misbehavior will be more intended to engage in such misbehavior. Hence it is hypothesized that:

H1: The more favorable the attitude toward SMB, the greater intention to engage in SMB.

Attitude toward Targets

In organizational settings, it is not uncommon that information technologies are managed by a single organizational unit, which is often referred as IT department. This is partly due to some pressures (e.g. staff professionalism) toward centralized IT management as a long-term information architecture (Applegate et al. 1996). This organizational structure, however, creates an "obvious point of friction" between IT and users because IT department manages information systems while users are responsible for the business activities that the systems are supposed to support (Applegate et al. 1996). Such intergroup conflict is inevitable in organizations for various reasons such as differences in the perception of reality (Gibson et al. 1988), competing goals, competition for resources, and cultural differences (Cox 2003). It is also seen as a consequence of the organizational decision-making context, which consists of the organization as a social system, the way the organization is structured, among others (Barclay 1991). The tension and conflict between users and IT department is a challenging organizational issue in corporate information technology management (Applegate et al. 1996; McKeen and Smith 1996). As such, it is not surprising that users may resist the information systems that IT department tries to implement (c.f. Bhattacherjee and Hikmet 2007; Lapointe and Rivard 2005).

One characteristic of users' resistance is the change of object over the time period of implementation (Lapointe and Rivard 2005). In their study, Lapointe and Rivard observed three object types: the system itself, its significance, and its advocates. Accordingly, based on the attitude-intention-behavior literature, users' resistance (as behavior) to these objects reflects their attitudes toward these objects. One of the reasons why users resist is that they "perceive threat" from the interaction with these objects. In other words, they may have negative attitudes toward these objects (or "target").

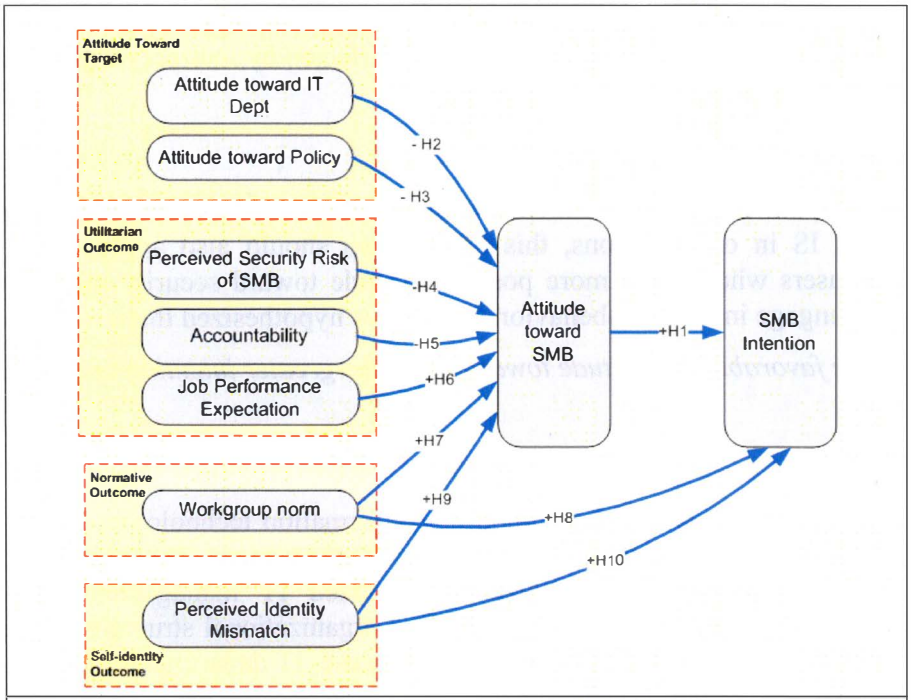

Figure 1 - Security Misbehavior Model

Similarly in the context of organizational IS security, users may as well resist the implementation and enforcement of security measures. It is often that IT department designs and enforces security policies, which define what users are allowed to do or prohibited from doing and what actions will be taken if users violate those policies. Security policies may also regulate what security measures, such as anti-virus software, should be in place. Understandably, users' attitudes toward IT department and security policies will affect their willingness to follow or their intention to ignore those policies and measures.

Attitude toward IT Department

Based on Eagly and Chaiken's definition of the general term of attitude, attitude toward IT department is defined as users' evaluation of IT department in terms of degree of favor or disfavor. In the IS security context, users may think that IT department tries to control everything about information by enforcing security policies. Users may also develop stereotypes about IT people in terms of their business knowledge and skills (Indeed, prior research found that IT professionals' business competence does influence the IT-business partnership (Bassellier and Benbasat 2004)). Based on this reasoning, it makes sense that the more negative users' attitude toward ID department, the more likely users may ignore security policies. Therefore, it is hypothesized that:

H2: User attitude toward IT department will negatively impact on attitude toward SMB. In other words, the more unfavorable attitude toward IT department, the more favorable attitude toward SMB

Attitude toward Security Policy

Attitude toward security policy refers to the degree of favor or disfavor expressed by users about organizational IS security policy. Users may have a negative attitude toward security policies because such policies may be seen as a tool used by IT department to control information or how users do their information related work. Security measures may be seen as a "barrier" or "obstacle" that creates troubles for them rather than a protective mechanism (Adams and Blandford 2005; Dourish et al. 2004). They may also perceive security as "futility" (Dourish et al. 2004). As a result, these negative attitudes may lead them to think that violating policies and bypassing security measures, i.e. security misbehavior, are justified. It is therefore hypothesized:

H3: User attitude toward security policy will negatively impact on attitude toward SMB. In other words, the more favorable attitude toward security policies, the more unfavorable attitude toward SMB

Utilitarian Outcomes

According to goal-directed behavioral theories, people distinguish between positive and negative outcomes when engaging certain behaviors (Klinger 1977; Winell 1987). Positive outcomes represent pleasant results to be attained and negative goals represent unpleasant results to be avoided. Negative outcomes can also be viewed as detrimental side effects that might occur when one pursues desired outcome (Heckhausen and Kuhl 1985). One may refrain from any intention to engage in action directed toward positive outcome if such positive outcome is outweighed by undesirable side effects. Such behavior is well documented in the human motivation literature. For example, people tend to approach or pursue desirable end-states ("goal") and avoid undesirable end-states ("anti-goal") in a self-regulatory system (Carver 2006; Carver and Scheier 1998). Stated differently, people direct behavior toward ("approach") positive stimuli such as object, events, and possibilities and away ("avoidance") from negative stimuli (Elliot 2006). In the context of IS security, we propose that three types of utilitarian outcome are salient to users when they are involved in SMB: perceived security risk, perceived accountability, and job performance expectation. The first two are negative outcome or side effects that users want to avoid while the third one is positive outcome that they pursue.

Perceived Security Risk of SMB

The first anticipated outcome is perceived security risk of SMB, which refers to the security risk perceived by users if they violate policies and rules. In this context, risk refers to likelihood of unfavorable or negative outcomes such as security breaches and data loss. Prior research indicates that perception of risk has an impact on human's behavior. For example, in the management literature, it is suggested that risk perception is negatively related to business managers' risky decision making behavior (Sitkin and Weingart 1995). In the consumer behavior literature, perceived risk can explain consumers' behavior since they are more often motivated to avoid mistakes (Mitchell 1999). Consumers often increase the use of risk-reduction activities when they perceive higher level of risks (Dowling and Staelin 1994). In the IS literature, perceived risk was found to reduce intended use of P2P (peer-to-peer) sharing software (Xu et al. 2005) and affect consumer attitude toward shopping online and consequently the willingness/intention to buy (Grazioli and Jarvenpaa 2000; Jarvenpaa et al. 2000; Malhotra et al. 2004; Pavlou 2003; Pavlou and Gefen 2004).

In the context of IS security, user perceived risk may play a similar role. Organizational security policies are put in place to secure information systems. Any actions that violate the policies have the possibility of causing damage to the overall IS security. If users perceive security risk of the organizational IS to be lower, they will be more likely to form a positive attitude toward SMB (i.e. be approval of SMB) and hence more likely to engage in SMB; other the other hand, if users perceive the risk to be higher, they will be more likely to form a negative attitude toward SMB (i.e. be disapproval of SMB). As such, it is hypothesized that:

H4: Perceived security of SMB will negatively influence user attitude toward SMB. In other words, the less perceived security risk of SMB by users, the more favorable their attitude toward SMB.

Perceived Accountability

The second anticipated outcome is perceived accountability, which refers to the extent to which users believe they are accountable for security issues. In organizational setting, accountability is often used as an element of management control (Dose and Klimoski 1995). Accountability refers to being answerable to audiences for performing up to certain prescribed standards (Schlenker et al. 1994). The actor in question is subject to observation and evaluation by the audience (Frink and Klimoski 2004). Such accountability evaluation is based on a responsibility triangle (Schlenker et al. 1994), which has three interlinked elements: prescription (rules for conduct), event (actions and consequences), and identity image (the actor's role). Based on this triangle model, people are held responsible to the extent that there is a set of defined rules applicable to the event, the actors are bounded by the rules by virtue of their roles, and the actors have personal control over the event. The essence of these three elements is similar to that of three different aspects of responsibility (Corlett 2009): blame responsibility (blameworthy for what they do, e.g. not following the rules), causal responsibility (the consequences are the result of the actors' actions), and duty responsibility (the actors' obligations and duties by virtue of their roles). The overall effect of accountability is that, the more people feel accountable, the more likelihood they act in a considered and motivated manner (Dose and Klimoski 1995).

The above accountability/responsibility concept can be applied in the IS security as well. As discussed previously, SMBs may cause damage to the overall IS security. When that happens, the actors may be hold accountable for their undesirable rule-breaking behaviors. They may be disciplined for their actions, depending on how the organization's policies treat violations. However, users may believe they are not accountable for a number of reasons. First, security is often not seen as users' task (Besnard and Arief 2004). It is more likely the "duty responsibility" of IT department. Secondly, users' actions may not be viewed as "the causal" factor of security incidents. Rather, it may well be argued that it is IT people that have not done a good job on managing IS security. Thus, users may not feel the "causal responsibility". Third, although their behaviors may seem to violate security rules, users may still have legitimate business reasons. As such, they may deny any "blame responsibility".

In sum, it is argued that perceived accountability plays an important role in influencing user's attitude and behavior. If perceived accountability is low (i.e. when users believe they are not accountable), users will be more likely to form a positive attitude toward SMB; on the other hand, if perceived accountability is high, they will be more likely to form negative attitude toward SMB. Prior research indicated that end-users don't see themselves but IT people as primarily responsible for security problems (Gross and Rosson 2007). Many users misbehaved

even they are aware that their behaviors do not fully comply with security policies because they do not expect to be made accountable (Sasse et al. 2001). It is therefore hypothesized that:

H5: Perceived accountability will negatively influence user attitude toward SMB. In other words, the less perceived accountability of users, the more favorable user attitude toward SMB

Job Performance Expectation

The third anticipated outcome is job performance expectation. As discussed previously, security is often not seen as users' task (Besnard and Arief 2004). From their perspective, users are evaluated by how well they perform their job, not how secure the information system is. A recent survey found that users often look to their managers, rather than IT people, for guidance on IS security-related issues (Cisco 2006). This may be an indication that job performance is more important for users. Many of the problems users have with security measures can be explained in terms of the mismatch between the measures and users' goals and tasks (Sasse et al. 2001). Users often talk of IS security in terms of costs and benefits and frame security measures as ones that can interfere with their job responsibilities and the practical accomplishment of their work (Dourish et al. 2004; Post and Kagan 2007). In essence, users care more about job performance than IS security. They will likely ignore those policies and bypass those security measures if doing so can help do their work and improve their job performance. Hence it is hypothesized that:

H6: Job performance expectation as a result of SMB will positively influence user attitude toward SMB.The higher job performance expectation, the more favorable attitude toward SMB.

Normative Outcomes

Workgroup Norm

Normative outcome refers to the approval or disapproval that the actor's significant others are expected to express in relation to the behavior in question (Eagly and Chaiken 1993). Arguably, people in the same workgroup, including supervisor and peers, have more influences on employee behaviors than others in the organization. This is because an employee interacts with her supervisor and peers on a daily basis. Thus she has more opportunities to observe their behavior and make sense of their attitudes than she would with other groups in the organization.

Prior studies in IT use in organizations suggest that top management, supervisors, peers, and IT department are the salient referents for users to make decisions (Karahanna et al. 1999). In IS security context, some studies have also investigated the impact of top management's support. Evidences have shown that top management support is a significant predictor of an organization's security culture and level of policy enforcement (Knapp et al. 2006). In the currently study, however, it is argued that top management may not have significant influence on employees' day-to-day IS security behaviors. Most employees do not have direct interactions with top management and do not have the opportunities to observe their behaviors and make sense of their attitudes. This is similar to the multi-level issues studied in the personnel selection literature (e.g. Yammarino and Dansereau 2002). Behaviors in organizations are inherently hierarchical (Ployhart and Schneider 2002). A minimum of three levels may be considered: individual, group (e.g. department, work group, etc), and organizational. Adjacent levels (e.g.

individual and group) are more highly interrelated that levels farther apart (e.g. individual and organization) (Ployhart and Schneider 2002). Accordingly, the effect of a group on individuals will be stronger than that of the organization (Ployhart and Schneider 2005). Top management's support can be viewed as an organizational level, while one's supervisor and coworkers are at group level. Prior research also indicates that workgroup-based social influence is a stronger predictor of individual attitudes and behaviors than the influence from people in other social networks within the same organization (Fulk 1993). So in the present study, the effect of latter will be considered. The influence of IT department has been captured in user attitude (see discussion in preceding sections). Thus it is not considered here.

Workgroup norms should be differentiated from organizational norms, which refer to formal or informal organizational policies, rules, and procedures (security policies in this study can be seen as a type of organizational norm). By definition, the two types of norm have different scopes: organizational norms may apply to organization-wide matters while workgroup norms are local to the workgroup in question. Local workgroups norms may espouse and support employee actions that violate organizational norms (Bennett and Robinson 2003). Employees, as members of workgroups, will likely use other members as role models for analyzing the appropriateness of particular beliefs, attitudes and behaviors (Robinson and O'Leary-Kelly 1998).

Based on the above reasoning, if breaking security rules, i.e. SMB, is not believed to be a good idea by supervisor and peers, users are more likely to form a negative attitude toward SMB; on the other hand, if supervisor and peers express approval or they also engage in SMB, users are more likely to form a positive attitude toward SMB, and hence more intended to engage in SMB. It is therefore hypothesized that:

H7: Workgroup norm (framed as in favor of SMB) will positively influence user attitude toward SMB.

According to the composite behavioral model (CBM), normative outcome expectation also has a direct effect on behavioral intention. Thus it is also hypothesized that:

H8: Workgroup norm (framed as in favor of SMB) will positively influence user SMB intention.

Self-identity Outcomes

Perceived Identity Mismatch

In organizations, IS security is often seen as the responsibility of IT people. For ordinary users, who are business people, IS security may not really matter in the sense that it is not in their job descriptions. To certain degree, whether they care about IS security or not does not affirm or repudiate their identity as business professionals – their "professional image" (Roberts 2005) – vis-à-vis IT people. We define this perception of non-affirmation and non-repudiation as perceived identity mismatch. For example, salespersons' professional status is more likely to be judged on their knowledge and experience in sales and their job performance rather how good they are at following security rules or performing IS-security related actions. In Blanton and Christie's terms (2003), security-related behavior does not "stick" to the identity of business professional. If employees believe that strictly following organizational security policies does not help improve their identities as a business professional, or doing otherwise (i.e. SMB) does not necessarily hurt their identities as business professional, they are more likely to form a positive attitude toward SMB and then ignore those policies.

This argument is essentially in line with the results of prior research of computer use. A significant negative relationship was found between "personal outcome expectation" and "computer use" (Compeau et al. 1999). It is not surprising because "personal outcome expectation" is measured by items such as "my coworkers will perceive me as competent". Although it may be true that using computer may improve users' "IT competence" as perceived by others, it will less likely improve the users' image as "business professional". In other words, users may very well form negative attitude toward using computer (and hence use computer less) because using computer does not help improve their image or identity of business professional, although it may help build a positive image of IT competence. Evidences were also found in other research in the IS literature. In a study of the implementation of nursing information systems, Doolin and McLeod (2007) found that the new systems challenged a strong professional nursing culture and a distinctive collective identity hold by nurses. As a result, the new systems were not welcomed. In a similar healthcare setting, physicians were found to resist the implementation of information systems at different levels (Lapointe and Rivard 2005). One reason of the resistance is that the new system was perceived by physicians as a threat to their "professional status".

Based on the above reasoning, it is therefore hypothesized that:

H9: Perceived mismatch between the identity as a business professional and following security rules and policies will positively influence user attitude toward SMB.

According to the CBM, identity outcome expectation also has a direct effect on behavioral intention. Thus it is also hypothesized that:

H10: Perceived identity mismatch will positively influence user SMB intention.

RESEARCH METHODS

A survey of office workers will be conducted to test the proposed SMB model. Office workers are most likely the group of people who use computers and organizational information systems on a regular basis.

Because IS security is often seen as a sensitive matter, prior research in this field has reported issues such as low response rate (Kotulic and Clark 2004). For overcoming these difficulties, the survey will use hypothetical scenarios ("vignettes") to solicit participants' opinion and ask them what they would do and what they believe their coworkers would do in each scenario. Vignettes are "short stories about hypothetical characters in specified circumstances, to whose situation the [subject] is invited to respond" (Finch 1987). The hypothetical scenarios will include some typical security misbehaviors. The use of vignettes has been recommended as one way to ask sensitive questions on surveys (Lee 1993). Indeed, the use of vignettes in management and IS literature is not uncommon (e.g. Banerjee et al. 1998; D'Arcy et al. 2009; Harrington 1996; James et al. 2008; Siponen and Iivari 2006; Webster and Trevino 1995).

Scenarios are developed according to the guidelines suggested in the literature (Wason et al. 2002). The following process was carried out for the development of scenarios: 1) literature review (including academic journals and trade publications); 2) interview with IT practitioners (including IT professionals at the local university and a large consumer electronics retailer in North America); and 3) interviews with academic experts. As a result this process, four initial scenarios are developed, each of which reflects security issues related to user authentication and

access control, hardware, software, and network, respectively: 1) password write-down; 2) Unauthorized mobile devices for storing organizational data; 3) Installation and use of unauthorized software; and 4) Insecure wireless connection. Survey participants are to respond one of the four scenarios. The main reason for this approach is the length of the survey. Repeated questions to similar scenarios may cause the boredom of participants and low quality of responses.

The measurement scale was developed in three steps: item creation, sorting, and item rating. In the first step, some instrument items are adapted from the literature while others are developed from scratch. In the second step, a sorting procedure similar to the one recommended by Moore and Benbasat (1991) was conducted to select candidate items. The last step of scale development is item rating. The items were given to eight persons (PhD students in MIS and Human Resources areas) for evaluation. Each of them was then asked to evaluate the items individually and to rate each item the extent to which the item measures the construct it is suppose to measure. Their responses were then used to calculate content validity ratios (CVR) (Lawshe 1975; Lewis et al. 2005). Items with a CVR below the threshold (.75, N = 8, p = .05) suggested by Lawshe were subsequently dropped from the pool, except for the "projective" measurement items of SMB intention. These items assume that the respondents are observers and measure how likely the respondents' coworkers would engage the behavior in question. For example, one item states "my coworkers would likely do the behavior if they were the person". The inclusion of the projective items is to test whether the bias of social desirability is present (Hui et al. 2004). As a result of the above development procedures, two groups of measurement items are adopted: general items and scenario-specific items. The difference between these two groups is that the latter is to be responded by survey participants based on their opinion about specific scenarios. Except for attitude toward SMB, which is measured on a semantic differential scale (1~7) using pairs of adjective words such as bad-good, all other major constructs are measured on a Likert-type scale (1 – Strongly Disagree, 7 – Strongly Agree).

A paper-based survey was conducted to collect data. Survey participants are full-time MBA students and office workers at a university. The sampled MBA students also have some years of business experience and use computers intensively for their study. Thus they are reasonably good candidates for completing the survey. Those office workers at the local university are from various administrative departments, including business management services, continuing education center, and student records. Each participant was given a $10-value coffee card as an incentive.

DATA ANALYSIS AND RESULTS

In total, 118 survey packages were distributed, 109 of them were returned (response rate: 92%). Because the characteristics of targeted sampling population are unknown, non-response bias was not assessed. A small number of cases with missing values were dropped. This resulted in 104 usable cases. In total, 79% of the participants are female and 20% are male (1% or one participant did not answer the question about gender); 89% of them have college or above education; and on average, participants spend 6.4 hours in front of computer at work and 2.1 hours at home per day.

Psychometric Properties of Measures

Reliability is first tested with coefficients of internal consistency – Cronbach Alphas (Cronbach 1951). Items with low item-item and item-total correlation (which would raise Alpha if deleted) are to be dropped. The aim is to achieve a minimum Cronbach alpha level of 0.7 (Straub et al. 2004). This step is carried out along with exploratory factor analysis (EFA) in an iterative manner. Construct validity (discriminant validity and convergent validity) is tested with exploratory factor analysis (EFA) technique. EFA tests were carried out for each stage of the proposed causal model (Straub et al. 2004). Each EFA test was run with principal component analysis (PCA) and Varimax rotation. Factors were extracted with eigenvalue > 1. For satisfactory levels convergent validity and discriminant validity, loadings of items should be at least .40 and there should be no cross-loading of items above .40. During each round of EFA test, if an item was dropped, the internal consistency reliability test was rerun to ensure the Cronbach alpha value meets the minimum requirement. After this round of test, Cronbach alpha of all constructs are above .707; the majority of item loadings on corresponding factors are above .70.

Two procedures are implemented in this study to check common-method bias. First, a Harman's single-factor test (Podasakoff et al. 2003; Podasakoff and Organ 1986) was conducted. In this test, all the measurement items were included in a single exploratory factor analysis (EFA). This result suggests that there was no substantial common method variance (CMV). Secondly, the statistical approach developed by Liang et al (2007) was adopted to further assess possible presence of CMV. The results indicated that common method bias was not a serious problem. On the one hand, the average of the variances explained by those theoretical constructs is .751, while the average of the variances explained by the method factor is .013. The ratio of these two types of variance is 56:1, which suggests that the common method variance is minimal. On the other hand, all path coefficients of the theoretical constructs are significant ($p<.000$) while most loadings of the method factor are insignificant.

PLS Measurement Model

The theoretical SMB model was tested using partial least square (PLS) approach (Chin 1998). Ideally, a new data set should be collected and used for this confirmatory hypothesis testing purpose. However, given the exploratory nature of the early stage of this study, the same data set used previously in the scale validation procedures is deemed as sufficient (this is further discussed in the limitation section).

The measurement model (or "outer model") how each block of items relates to its construct or latent variable (Chin 1998). It provides indices for assessing convergent validity and discriminant validity of the scale. The convergent validity is generally achieved if three criteria are met (Fornell and Larcker 1981): 1) all item factor loadings should be significant and greater than .70; 2) average variance extracted (AVE, the amount of variance captured by a latent variable relative to the amount caused by measurement error) should be greater than .50 (or square root of AVE > .707); and 3) composite reliability index for each construct should be greater than .80. Based on these criteria, the PLS results indicate that satisfactory level of convergent validity was achieved. All item loadings except for one are greater than .70. The loading of the exceptional one (.59) is still considered acceptable given the high loadings of other items for the same construct (Chin 1998). In addition, all item loadings are significant (two at .01

and .05 levels; others at .001 level). Furthermore, the square root of AVE is greater than .707 for each construct. The composite reliabilities of all constructs also meet the criterion of .80 (Table 1).

Discrimant validity is verified by the difference between the AVE of a construct and its correlations with other constructs. To achieve sufficient discriminant validity, the square root of AVE of a construct should be greater than its correlations with all other constructs (Fornell and Larcker 1981). As shown in Table 1, the highest construct correlation is .68 (between Risk and Attitude toward Policy) and the lowest square root of AVE is .77 (that of Attitude toward IT Department). Thus, the criterion for discriminant validity was also met in this study.

Table 1: PLS Measurement Model – Construct Correlations

Construct	CR	1	2	3	4	5	6	7	8	9
1 - Attitude: SMB	0.98	0.95								
2 - Attitude: IT	0.80	-0.15	0.77							
3 - Attitude: Policy	0.88	-0.33	0.25	0.80						
4 - Identity Mismatch	0.89	0.29	-0.05	-0.20	0.86					
5 - Intention	0.90	0.66	-0.16	-0.41	0.22	0.84				
6 - Job Performance	0.98	0.11	-0.12	-0.21	0.01	0.33	0.98			
7 - Accountability	0.86	-0.21	0.11	0.20	-0.11	-0.10	-0.06	0.82		
8 - Risk	0.91	-0.31	0.19	0.68	-0.09	-0.50	-0.29	0.16	0.85	
9 - Workgroup Norm	0.92	0.53	-0.18	-0.36	0.14	0.68	0.26	-0.13	-0.53	0.87

Note: CR = Composite Reliability; Off diagonal numbers are inter-construct correlations; Diagonal numbers are the square roots of AVE (average variance extracted).

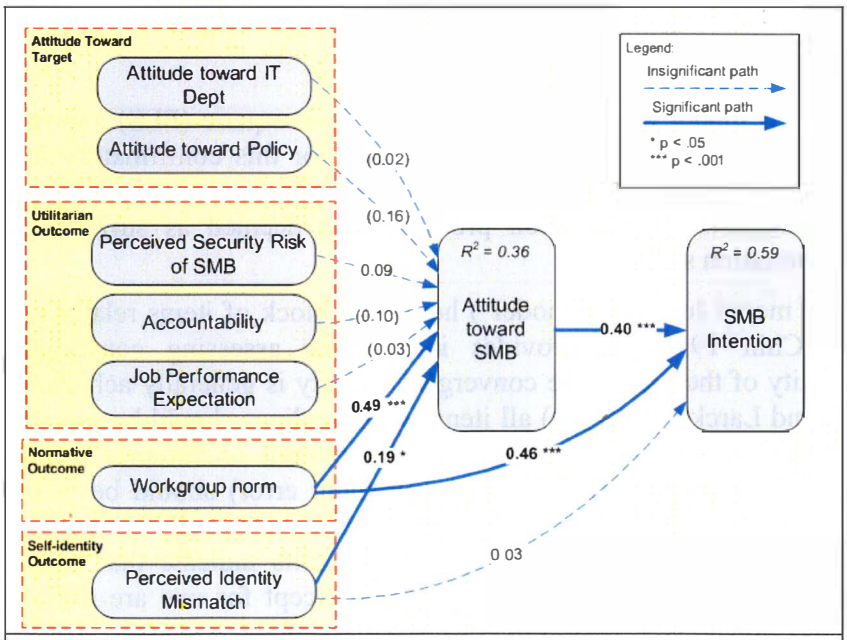

Figure 2: PLS Analysis Results

PLS Structural Model

The hypotheses were assessed by examining the parameters provided by the PLS structural model. More specifically, R-square values of dependent variables represent the predictiveness of the theoretical model and standardized path coefficients indicate the strength of the relationship between independent and dependent variables (Chin 1998). In this study, a bootstrapping resampling procedure (with 500 samples) was carried out to estimate the significance of paths in the structural model.

As shown Figure 2, the R-square value .59 indicates that the theoretical model explained a substantial amount of variance of user SMB intention. In addition, 36 percent of the variance for attitude toward SMB is accounted for by the model. Given the 10-percent criterion (Falk and Miller 1992), the theoretical model demonstrates substantive explanatory power. Both attitude toward SMB and workgroup norm had strong direct effects on SMB intention, as demonstrated by the significant path coefficients (attitude toward SMB: beta = .40, $p < .001$; workgroup norm: beta = .46, $p < .001$). Thus, H1 and H8 are supported. H7 and H9 are also supported, suggesting that workgroup norm (beta = .49, $p < .001$) and perceived identity mismatch (beta = .19, $p < .05$) are significant predictors of attitude toward SMB. Contrary to what is expected by the theoretical model, none of the constructs in the attitude toward target and utilitarian outcome blocks has significant effect on attitude toward SMB. Furthermore, perceived identity mismatch does not have expected significant effect on SMB intention.

DISCUSSION AND CONCLUSIONS

Key Findings and Theoretical Implications

Overall, the theoretical model was successful in capturing the main antecedents of user SMB intention. The explanatory power of the model was satisfactory. Consistent with the predictions of CBM, both attitude toward SMB and workgroup norm have significant influences on SMB intention. Contrary to the predictions of CBM, however, user attitude toward target (IT department and security policy) and utilitarian outcome expectations (perceived security risk, perceived accountability, and job performance expectation) did not have significant influences on user attitude toward SMB.

Perhaps the most interesting findings of this study about the antecedents of attitude toward SMB is the strong and significant effect of workgroup norm in comparison to the little impact of utilitarian outcome expectations and attitude toward targets (IT department and security policies) . Although it seems to be surprising at first glance, the different effects are not totally inconsistent with other research in the IS literature. This may be explained by the impact of job relevance and user expertise. The literature suggested that these two factors moderate the way in which users evaluate the use of information technology (Bhattacherjee and Sanford 2006). The less relevant the job and the less expertise users have, the more likelihood they turn to external sources. In other words, they make their decisions or form their opinions by consulting with other relevant people, rather than evaluating the system in question (or the use of such system) by themselves. This is arguably applicable in the information security context. End users often lack of security knowledge and skills. As such, security may also been viewed as irrelevant to their jobs. Thus it is not surprising that they turn to their supervisors and coworkers for guidance and advice rather than depend on their own evaluation of the situation on hand. In fact, it was

suggested that users may be more intended to follow practices and advices of their co-workers (Dourish et al. 2004; Wood 2000). Particularly, users tend to "delegate" security issues to other individuals who they know (Dourish et al. 2004).

Another important finding is the influential effects of workgroup norm. The results suggest that workgroup norm is a key determinant of user SMB intention, given the strong direct and indirect effects (total effect = .66). This appears to echo relevant research in the organizational behavior literature. For example, workgroups in organizational settings have the ability to influence individual members' antisocial actions (Robinson and O'Leary-Kelly 1998).

The current study has several important contributions and theoretical implications. First, it provides a clear conceptualization of security misbehavior, which refers to those actions engaged by employees who violate or bypass the organization's rules and policies that govern the security of information systems (IS) with the intention to benefit themselves. This helps clarify some confusions and undefined uses of general terms such as IS misuse, computer abuse, among others. Second, this study is the first known attempt to apply the composite behavioral model – CBM (Eagly and Chaiken 1993) to IS security issues. Based on the framework of CBM, this study proposed a number of constructs for predicting and explaining user security misbehaviors in organizations. It also developed and validated new measurement scales for several constructs. Satisfactory levels of psychometric properties have been achieved. These validated scales can provide some valuable input for future research in user behaviors related to information systems security. Third, this study contributes to the IS security literature by gaining a better understanding of the factors that predict and explain security misbehavior. The proposed model explains a satisfactory level of variance in user SMB intention (59%). Furthermore, the model also explains a substantial amount of variance in user attitude toward SMB (36%). Fourth, this study provides some preliminary evidence of the importance of workgroup influence in organizational settings. As the survey results revealed, workgroup norm not only form user attitude but also directly influence user intention to engage in security misbehaviors. It suggests that SMB is not just an individual-level phenomenon but more importantly a group-level consensus. Thus group-level studies may provide a better understanding of the reason why users engage in SMBs.

Limitations and Future Research

The research methods employed in this study have some limitations. First of all, as other survey-based cross-sectional studies, the causal relationships implied in the proposed model are inferred from underlying theories, not established by the design of the study. Second, self-report by survey participants is the single source of measurement. There is still a possibility that common method bias may be present, although two statistical tests did rule out any significant influence of such bias. A longitudinal research with multiple sources of measurement may help alleviate this problem and further validate the causal relationships. Third, the sampling process was not completely randomized. The participants were office workers from a single large organization, although they work in different departments. Thus generalization beyond the specific settings and conditions of this study may be limited. It is desirable to collect more data from a variety of organizations. Finally, this study used four specific security scenarios to solicit participants' responses. Although this scenario-based method is commonly accepted in the literature (e.g. IS, organizational, and marketing), the scenarios do not include every type of security misbehaviors. Future research should include more types of SMBs to further test the proposed model.

The proposed theoretical model has some limitations that warrant further research. First of all, the model focuses on SMB intention as the ultimate independent variable. Although this practice is not uncommon in IS literature and the prediction from intention to actual behavior is well documented, future research should try to measure actual security misbehaviors in a field setting. Second, as discussed earlier, some elements of the composite behavioral model were not included in the proposed SMB model purposefully. For example, the relationships between those antecedents are omitted from the proposed model. Future research may be conducted to include these relationships in order to get a complete picture of the forming mechanism of security misbehaviors. Finally, this is the first newly developed model based on CBM. The same data set has been used to validate the scale and to test the model. This may limit the model's external validity. To address this limitation, it is our very intention to replicate the study and collect data from a different sample to further test and refine the model.

Conclusions

The current study aimed to answer the following research question: why do users intend to engage in insecure use of IS although such uses may violate the organization's security policy? To achieve this objective, this study developed and tested an initial theoretical model to explain the antecedents of workers' security misbehavior (SMB) based on the composite behavior model – CBM (Eagly and Chaiken 1993). Overall, the theoretical model was successful in capturing the main antecedents of user SMB intention. Consistent with the predictions of CBM, both attitude toward SMB and workgroup norm have significant influence on SMB intention. In turn, user attitude toward SMB is influenced by two significant factors: workgroup norm and perceived identity mismatch. Contrary to the predictions of CBM, however, user attitude toward target (IT department and security policy) and utilitarian outcome expectations (perceived security risk, perceived accountability, and job performance expectation) did not have significant influences on user attitude. In sum, the results suggest that workgroup norm is a key determinant of user SMB intention, given the strong direct and indirect effects.

REFERENCES

Adams, A., and Blandford, A. 2005. "Bridging the Gap between Organizational and User Perspectives of Security in the Clinical Domain," *International Journal of Human-Computer Studies* (63), pp 175-202.

Ajzen, I. 1991. "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes* (50), pp 179-211.

Applegate, L.M., McFarlan, F.W., and McKenney, J.L. 1996. *Corporate Information Systems Management: The Issues Facing Senior Executives.* Chicago: Irwin.

Banerjee, D., Cronan, T.P., and Jones, T.W. 1998. "Modeling It Ethics: A Study in Situational Ethics," *MIS Quarterly* (22:1), pp 31-60.

Barclay, D.W. 1991. "Interdepartmental Conflict in Organizational Buying: The Impact of the Organizational Context," *Journal of Marketing Research* (28:2), pp 145-159.

Baskerville, R.L., and Siponen, M.T. 2002. "An Information Security Meta-Policy for Emergent Organizations," *Logistics Information Management* (15), pp 337-346.

Bassellier, G., and Benbasat, I. 2004. "Business Competence of Information Technology Professionals: Conceptual Development and Influence on It-Business Partnerships," *MIS Quarterly* (28:4), Dec2004, pp 673-694.

Bennett, R.J., and Robinson, S.L. 2003. "The Past, Present, and Future of Workplace Deviance Research," in: *Organizational Behavior: The State of the Science,* J. Greenberg (ed.). Mahwah, NJ. USA: Lawrence Erlbaum, pp. 247-281.

Besnard, D., and Arief, B. 2004. "Computer Security Impaired by Legitimate Users," *Computer & Security* (23), pp 253-264.

Bhattacherjee, A., and Hikmet, N. 2007. "Physicians' Resistance toward Healthcare Information Technology: A Theoretical Model and Empirical Test," *European Journal of Information Systems* (16), pp 725-737.

Bhattacherjee, A., and Sanford, C. 2006. "Influence Processes for Information Technology Acceptance: An Elaboration Likelihood Model," *MIS Quarterly* (30:4), pp 805-825.

Blanton, H., and Christie, C. 2003. "Deviance Regulation: A Theory of Action and Identity," *Review of General Psychology* (7:2), Jun, pp 115-149.

Bock, G.-W., Zmud, R.W., Kim, Y.-G., and Lee, J.-N. 2005. "Behavioral Intention Formation in Knowledge Sharing: Examining the Roles of Extrinsic Motivators, Social-Psychological Forces, and Organizational Climate1," *MIS Quarterly* (29:1), Mar, pp 87-111.

Calluzzo, V.J., and Cante, C.J. 2004. "Ethics in Information Technology and Software Use," *Journal of Business Ethics* (51), pp 301-312.

Carver, C.S. 2006. "Approach, Avoidance, and the Self-Regulation of Affect and Action," *Motivation and Emotion* (30:2), pp 105-110.

Carver, C.S., and Scheier, M.F. 1998. *On the Self-Regulation of Behavior.* New York: Cambridge University Press.

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), pp 18-41.

Chin, W.W. 1998. "The Partial Least Squares Approach to Structural Equation Modeling," in: *Modern Methods for Business Research,* G.A. Marcoulides (ed.). Mahwah, NJ, USA: Lawrence Erlbaum Associates, pp. 295-336.

Cisco. 2006. "Perceptions and Behaviors of Remote Workers: Keys to Building a Secure Company." Cisco Systems, Inc.

Compeau, D.R., Higgins, C.A., and Huff, S. 1999. "Social Cognitive Theory and Individual Reactions to Computing Technology: A Longitudinal Study," *MIS Quarterly* (23:2), pp 145-158.

Corlett, J.A. 2009. *Responsibility and Punishment.* Dordrecht, The Netherlands: Springer.

Cox, T., Jr. 2003. "Cultural Diversity in Organizations: Intergroup Conflict," in: *Classic Readings in Organizational Behavior,* J.S. Ott, S.J. Parkes and R.B. Simpson (eds.). Thomson Learning, pp. 263-273.

Cronbach, L.J. 1951. "Coefficient Alpha and the Internal Structure of Tests," *Psychometrika* (16:3), pp 297-334.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1).

Dhillon, G., and Backhouse, J. 2000. "Information Systems Security Management in the New Millennium," *Communications of the ACM* (43:7), pp 125-128.

Doherty, N.F., and Fulford, H. 2005. "Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis," *Information Resources Management Journal* (18:4), pp 21-39.

Doolin, B., and McLeod, L. 2007. "Information Technology at Work: The Implications for Dignity at Work," in: *Dimensions of Dignity at Work,* S.C. Bolton (ed.). Oxford, UK: Butterworth-Heinemann, pp. 154-175.

Dose, J.J., and Klimoski, R.J. 1995. "Doing the Right Thing in the Workplace: Responsibility in the Face of Accountability," *Employee Responsibilities and Rights Journal* (8:1), pp 35-56.

Dourish, P., Grinter, R.E., de la Flor, R.D., and Joseph, M. 2004. "Security in the Wild: User Strategies for Managing Security as an Everyday, Practical Problem," *Personal and Ubiquitous Computing* (8:6), pp 391-401.

Dowling, G.R., and Staelin, R. 1994. "A Model of Perceived Risk and Intended Risk-Handling Activity," *Journal of Consumer Research* (21:1), pp 119-134.

Dubie, D. 2007. "End Users Behaving Badly." *Network World*, from http://www.networkworld.com/slideshows/2007/120707-end-users-behaving-badly.html

Eagly, A.H., and Chaiken, S. 1993. *The Psychology of Attitudes.* Fort Worth, TX: Harcourt Brace Jovanovich.

Elliot, A.J. 2006. "The Hierarchical Model of Approach-Avoidance Motivation," *Motivation and Emotion* (30:2), pp 111-116.

Falk, R.F., and Miller, N.B. 1992. *A Primer for Soft Modeling*, (1st ed.). Akron, OH, USA: The University of Akron.

Finch, J. 1987. "The Vignette Technique in Survey Research," *Sociology* (21:1), pp 105-114.

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

Frink, D.D., and Klimoski, R.J. 2004. "Advancing Accountability Theory and Practice: Introduction to the Human Resource Management Review Special Edition," *Human Resources Management Review* (14:1), pp 1-17.

Fulk, J. 1993. "Social Construction of Communication Technology," *Academy of Management Journal* (36:5), Oct, pp 921-950.

Gibson, J.L., Ivancevich, J.M., and Donnelly, J.H., Jr. 1988. *Organizations: Behaviors, Structure, Processes*, (6th ed.). Plano, Texas: Business Publications, Inc.

Grazioli, S., and Jarvenpaa, S.L. 2000. "Perils of Internet Fraud: An Empirical Investigation of Deception and Trust with Experienced Internet Consumers," *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Human* (30:4), pp 395-410.

Gross, J.B., and Rosson, M.B. 2007. "Looking for Trouble: Understanding End-User Security Management," in: *The Symposium on Computer Human Interaction for the Management of Information Technology (CHIMT'07)*. Cambridge, MA, USA: ACM.

Harrington, S.J. 1996. "The Effects of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions," *MIS Quarterly* (20:3), pp 257-278.

Heckhausen, H., and Kuhl, J. 1985. "From Wishes to Action: The Dead Ends and Short Cuts on the Long Way to Action," in: *Goal Directed Behavior: The Concept of Action in Psychology,* M. Frese and J. Sabini (eds.). Hillsdale, NJ: Lawrence Erlbaum Associates, pp. 134-159.

Hilton, D.J., and Slugoski, B.R. 1986. "Knowledge-Based Causal Attribution - the Abnormal Conditions Focus Model," *Psychological Review* (93:1), Jan, pp 75-88.

Hui, M.K., Au, K., and Fock, H. 2004. "Reactions of Service Employees to Organization-Customer Conflict: A Cross-Cultural Comparison," *International Journal of Research in Marketing* (21), pp 107-121.

ISO/IEC. 2005. "Information Technology - Security Techniques - Code of Practice for Information Security Management (Iso/Iec 27002)." Geneva, Switzerland: International Organization for Standardization.

James, T., Pirim, T., Boswell, K., Reithel, B., and Barkhi, R. 2008. "An Extension of the Technology Acceptance Model to Determine the Intention to Use Biometric Devices," in: *End User Computing Challenges and Technologies: Emerging Tools and Applications,* S. Clarke (ed.). Hershey, PA, USA: IGI Global, pp. 57-78.

Jarvenpaa, S.L., Tractinsky, N., and Vitale, M. 2000. "Consumer Trust in an Internet Store," *Information Technology and Management* (1), pp 45-71.

Kankanhalli, A., Teo, H.H., Tan, B.C.Y., and Wei, K.K. 2003. "An Integrative Study of Information Systems Security Effectiveness," *International Journal of Information Management* (23), pp 139-154.

Karahanna, E., Straub, D.W., and Chervany, N.L. 1999. "Information Technology Adoption across Time: A Cross-Sectional Comparison of Pre-Adoption and Post-Adoption Beliefs," *MIS Quarterly* (23:2), Jun, pp 183-213.

Klinger, E. 1977. *Meaning & Void: Inner Experience and the Incentives in People's Lives*. Minneapolis: University of Minnesota Press.

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

Kotulic, A.G., and Clark, J.G. 2004. "Why There Aren't More Information Security Research Studies," *Information & Management* (41:597-607).

Lapointe, L., and Rivard, S. 2005. "A Multilevel Model of Resistance to Information Technology Implementation," *MIS Quarterly* (29:3), pp 461-491.

Lawshe, C.H. 1975. "Quantitative Approach to Content Validity," *Personnel Psychology* (28:4), pp 563-575.

Lee, R.M. 1993. *Doing Research on Sensitive Topics*. London; Newbury Park, Calif.: Sage Publications.

Lee, S.M., Lee, S.G., and Yoo, S. 2004. "An Integrative Model of Computer Abuse Based on Social Control and General Deterrence Theories," *Information & Management* (41), pp 707-718.

Leonard, L.N.K., and Cronan, T.P. 2001. "Illegal, Inappropriate, and Unethical Behavior in an Information Technology Context: A Study to Explain Influences," *Journal of the Association of Information Systems* (1).

Lewis, B.R., Templeton, G.F., and Byrd, T.A. 2005. "A Methodology for Construct Development in MIS Research," *European Journal of Information Systems* (14:4), pp 388-400.

Liang, H., Saraf, N., Hu, Q., and Xue, Y. 2007. "Assimilation of Enterprise Systems: The Effect of Institutional Pressures and the Mediating Role of Top Management," *MIS Quarterly* (31:1), pp 59-87.

Malhotra, N.K., Kim, S.S., and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns (Iuipc): The Construct, the Scale, and a Causal Model," *Information Systems Research* (15:4), pp 336-355.

McKeen, J.D., and Smith, H. 1996. *Management Challenges in Is: Successful Strategies and Appropriate Action*. Chicester; New York: Wiley.

Mitchell, V.-W. 1999. "Consumer Perceived Risk: Conceptualisations and Models," *European Journal of Marketing* (33:1/2), pp 163-195.

Moore, G.C., and Benbasat, I. 1991. "Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation," *Information Systems Research* (2:3), pp 192-222.

Pahnila, S., Siponen, M.T., and Mahmood, A. 2007. "Employees' Behavior Towards Is Security Policy Compliance," *40th Annual Hawaii International Conference on System Sciences*, Hawaii: IEEE.

Parker, D.B. 1981. *Computer Security Management*. Reston, VA: Reston Publishers.

Pavlou, P.A. 2003. "Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model," *International Journal of Electronic Commerce* (7:3), pp 69-103.

Pavlou, P.A., and Gefen, D. 2004. "Building Effective Online Marketplaces with Institution-Based Trust," *Information Systems Research* (15:1), pp 37-59.

Ployhart, R.E., and Schneider, B. 2002. "A Multi-Level Perspective on Personal Selection Research and Practice: Implications for Selection System Design, Assessment, and Construct Validation," in: *The Many Faces of Multi-Level Issues,* F.J. Yammarino and F. Dansereau (eds.). Oxford, UK: Elsevier Science, pp. 95-140.

Ployhart, R.E., and Schneider, B. 2005. "Multilevel Selection and Prediction: Theories, Methods, and Models," in: *The Blackwell Handbook of Personnel Selection,* A. Evers, O. Omit-Voskuyl and N. Anderson (eds.). Malden, MA, USA: Blackwell Publishing, pp. 495-516.

Podasakoff, P.M., MacKenzie, S.B., Lee, J.-Y., and Podsakoff, N.P. 2003. "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies," *Journal of Applied Psychology* (88:5), Oct, pp 879-903.

Podasakoff, P.M., and Organ, D.W. 1986. "Self-Reports in Organizational Research: Problems and Prospects," *Journal of Management* (12:4), pp 531-544.

Post, G.V., and Kagan, A. 2007. "Evaluating Information Security Tradeoff: Restricting Access Can Interfere with User Tasks," *Computer & Security* (26), pp 229-237.
Roberts, L.M. 2005. "Changing Faces: Professional Image Construction in Diverse Organizational Settings," *Academy of Management Review* (30:4), Oct, pp 685-711.
Robinson, S.L., and O'Leary-Kelly, A.M. 1998. "Monkey See, Monkey Do: The Influence of Work Groups on the Antisocial Behavior of Employees," *Academy of Management Journal* (41:6), Dec, pp 658-672.
Sasse, M.A., Brostoff, S., and Weirich, D. 2001. "Transforming The "Weakest Link" - a Human/Computer Interaction Approach to Usable and Effective Security," *BT Technology Journal* (19:2), pp 122-131.
Schlenker, B.R., Britt, T.W., Pennington, J., Murphy, R., and Doherty, K. 1994. "The Triangle Model of Responsibility," *Psychological Review* (101:4), pp 632-652.
Schneier, B. 2000. *Secrets and Lies*. John Wiley and Sons.
Siponen, M., and Vance, A. 2009. "Neutralization: New Insight into the Problem of Employee Information Systems Security Policy Violation," *MIS Quarterly* (forthcoming).
Siponen, M.T., and Iivari, J. 2006. "Six Design Theories for Is Security Policies and Guidelines," *Journal of the Association of Information Systems* (7:7), pp 445-472.
Sitkin, S.B., and Weingart, L.R. 1995. "Determinants of Risky Decision-Making Behavior: A Test of the Mediating Role of Risk Perception and Propensity," *Academy of Management Journal* (38:6), pp 1573-1592.
Stanton, J.M., Stam, K.R., Mastrangelo, P., and Jolton, J. 2005. "Analysis of End User Security Behaviors," *Computer & Security* (24:2), pp 124-133.
Straub, D.W. 1990. "Effective Is Security: An Empirical Study," *Information Systems Research* (1:3), pp 255-276.
Straub, D.W., Boudreau, M., and Gefen, D. 2004. "Validation Guidelines for Is Positivist Research," *Communications of the Associations of Information Systems* (13), pp 380-427.
Thompson, R.L., Higgins, C.A., and Howell, J.M. 1991. "Personal Computing: Toward a Conceptual Model of Utilization," *MIS Quarterly* (15:1), pp 125-143.
Venkatesh, V., Morris, M.G., Davis, G.B., and Davis, F.D. 2003. "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly* (27:3), pp 425-478.
Wason, K.D., Polonsky, M.J., and Hyman, M.R. 2002. "Designing Vignette Studies in Marketing," *Australasian Marketing Journal* (10:3), pp 41-58.
Webster, J., and Trevino, L.K. 1995. "Rational and Social Theories as Complementary Explanations of Communication Media Choices: Two Policy-Capturing Studies," *Academy of Management Journal* (38:6), Dec, p 1544.
Winell, M. 1987. "Personal Goals: The Key to Self-Direction in Adulthood," in: *Humans as Self-Constructing Living Systems: Putting the Framework to Work,* M.E. Ford and D.H. Fort (eds.). Hillsdale, NJ, USA: Lawrence Erlbaum, pp. 261-287.
Wood, C.C. 2000. "An Unappreciated Reason Why Information Security Policies Fail," *Computer Fraud & Security*: 10), pp 13-14.
Workman, M., Bommer, W.H., and Straub, D.W. 2008. "Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test," *Computers in Human Behavior* (24:6), pp 2799-2816.
Workman, M., and Gathegi, J. 2006. "Punishment and Ethics Deterrents: A Study of Insider Security Contravention," *Journal of the American Society for Information Science and Technology* (58:2), pp 212-222.

Xu, H., Wang, H., and Teo, H.-H. 2005. "Predicting the Usage of P2p Sharing Software: The Role of Trust and Perceived Risk," *The 38th Hawaii International Conference on System Sciences*, Hawaii: IEEE.

Yammarino, F.J., and Dansereau, F. (eds.). 2002. *The Many Faces of Multi-Level Issues*. Oxford, UK: Elsevier Science.

McMaster University
1280 Main St. W. DSB A201
Hamilton, ON
L8S 4M4

Tel: 905-525-9140 ext. 23956
Fax: 905-528-0556
Email: ebusiness@mcmaster.ca
Web: http://merc.mcmaster.ca