INFORMATION SYSTEMS SECURITY MISBEHAVIOR

INFORMATION SYSTEMS SECURITY MISBEHAVIOR IN THE WORKPLACE: THE EFFECTS OF JOB PERFORMANCE EXPECTATION AND WORKGROUP NORM

By

KEN HUIJIN GUO, B.A., M.SC.B.

A Thesis

Submitted to the School of Graduate Studies

In Partial Fulfillment of the Requirements

for the Degree

Doctor of Philosophy

McMaster University

DOCTOR OF PHILOSOPHY (2010) McMaster University

(Business Administration) Hamilton, Ontario

TITLE: Information Systems Security Misbehavior in the Workplace: The Effects of Job Performance Expectation and Workgroup Norm

AUTHOR: Ken Huijin Guo, B.A., M.Sc.B.

SUPERVISOR: Professor Yufei Yuan

NUMBER OF PAGES: x, 167

Abstract

Information systems (IS) security has become a major current issue for organizations. It is generally understood that not only technology but also human factors and control processes have a significant impact on organizational IS security. One of the major human factors issues is end user behavior towards IS security. End users may ignore security measures and by doing so they inadvertently put the organization's information at risk. This study investigated why end users engage in such *"security misbehavior" (SMB).* Based on Eagly and Chaiken's composite behavioral model, an SMB model was proposed and tested empirically with data collected from a survey of computer end users in the workplace (N=306). Overall, the theoretical model was successful in capturing the main antecedents of end user *SMB intention*. Both *attitude towards SMB* and *workgroup norm* were found to have significant positive influences on SMB intention. In turn, *attitude towards SMB* is positively influenced by *workgroup norm* and *job performance expectation*. Contrary to the hypotheses of the model, however, user attitude towards the target (*attitude towards security policy*) and several utilitarian outcome expectations (*perceived security risk*, *perceived accountability*, and *sanction certainty*) did not have significant influences on end user attitudes towards SMB. However, asymmetric effects were discovered among these variables. Furthermore, the influences of self-identity outcome expectation (*perceived identity match*) on both attitude towards SMB and behavioral intention were not significant. The results also indicated that end user SMB intentions are to some extent dependent on the context. In

sum, the findings suggest that job performance expectation and workgroup norm are key determinants and have strong direct and indirect effects on user SMB intention.

Acknowledgements

This thesis would not have been possible without the support I received from many people around me. I am deeply grateful to Dr. Yufei Yuan, my PhD supervisor, for his unreserved support, guidance, and advice during the last four years. My special thanks also go to my PhD Committee: Dr. Norm Archer, Dr. Catherine Connelly, and Dr. Khaled Hassanein, for their advice and help. I thank Dr. John D'Arcy, my external reviewer, for his insightful comments and suggestions.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

"The problem with security for computer system is quite simple. It is a people problem. The solution is also quite simple. It is people controlling people in a computerized environment." - William E. Perry (1985)

Information systems (IS) security has become a major challenge for organizations thanks to the increasing corporate use of the Internet and, more recently, wireless networks. When connected to the Internet, organizational networks may be attacked by hackers or infected by viruses. In the 2008 CSI computer crime and security survey of computer security practitioners in U.S. organizations, 43% of the respondents reported security incidents (Richardson, 2008). In the United Kingdom, a similar survey found that 45% of the participating companies had security incidents in 2008 (BERR, 2008). Many high-profile security breaches have been reported in the past few years. For example, the TJX corporate network was compromised and customer records such as payment card information were believed to have been stolen in 2005 and 2006 (TJX, 2007a, 2007b). According to the two published reports, TJX has accrued costs of more than 25 million US dollars due to those security breaches and expected to continue to incur such costs. On average, it was found that a disclosed security breach incident would cost a publicly-listed company more than 17 million US dollars (Garg, Curtis, & Halper, 2003).

Arguably, technology use is one thing to blame for the seemingly endless number of security breaches. After all, IS security is often seen as technically oriented and a recent review found that research in this area has focused on "technical context" (Siponen & Oinas-Kukkonen, 2007). Better technology is expected to build stronger defenses against hacker attacks, to stop the spreading of viruses, and to prevent other security breaches.

Technology, however, is not the only factor in security. Whether or not technology is advanced enough is just one consideration; how organizations use and manage the technology is another. For example, anecdotal evidence indicates that many security breaches happen because sensitive data are not encrypted, although encryption technologies are available. At the organizational level, security is more of a management issue (Dutta & McCrohan, 2002). A frequently recommended organizational measure is security policy (e.g. Baskerville & Siponen, 2002). For example, a security policy may specify what end users[1] should (or should not) do with organizational IS assets, and it may also spell out the consequences of policy violations. The implementation and enforcement of organizational security policy can arguably help organizations to ensure that 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 by international standards such as *ISO/IEC 27002*, which requires management to "set a clear policy direction in line with business objectives and

[1] In this study, the terms "users" and "end users" are used interchangeably.

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 end users interact with information systems on a regular basis, 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 & Gathegi, 2006) and it is subject to the 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 end users do not follow the policy. Although telling end users what to do about security is one option, one should not expect them to always act as prescribed (Besnard & Arief, 2004). In fact, practitioners see the enforcement of security policies, i.e. making sure policies are properly followed by end users, as a critical issue in security management. It is not surprising that end users are viewed as the "weakest link" in the IS security chain (Schneier, 2000). A practitioner survey found that, even if users were aware of potential security problems related to their actions, many of them did not follow security best practices and yet continued to engage in behaviors that could open their organizations' information systems to serious security risks (Cisco, 2006). For example, the survey found that many workers allowed others to use their computing devices at work despite their awareness of possible security implications. It was also reported that many end users do not 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 and severity of security breaches (Doherty & Fulford, 2005). Recent research found that possible punishments specified in security policies do not have an significant effect on user intention to misuse information systems (D'Arcy, Hovav, & Galletta, 2009). This phenomenon raises an important question: what factors motivate end users to engage in such behaviors? The role of motivation, however, has not been considered seriously enough in the literature (Siponen, 2000).

The focus of this thesis is on the study of end user attitudes and behavior towards organizational IS security. More specifically, the study tries to answer the following question: why do end users engage in insecure use of information systems although such actions violate the organization's security policies? To answer the above research question, this study aims to achieve the following specific objectives:

1) To review relevant concepts of security-related end user behaviors and provide a conceptualization of security misbehavior;
2) To identify antecedents of security misbehavior and propose a theoretical model that explain such misbehaviors;
3) To develop and validate a measurement scale;
4) To develop security misbehavior scenarios;
5) To collect data by surveying computer end users in workplace; and
6) To test the proposed theoretical model.

The rest of this thesis is organized as follows:

Chapter 2 gives a review of the IS security literature. More specifically, it clarifies some key terms related to IS security, including security, threats to IS security, security management, and security policy. It then provides a conceptualization of security misbehavior (which is the focus of this study) and compares this type of behavior with other concepts defined in the literature. Lastly, the chapter gives a review of prior research models on end user security-related behaviors and identifies gaps in prior research.

Chapter 3 offers a review of the composite behavioral model (Eagly & Chaiken, 1993) - the theoretical background of this study - and discusses why this theory is chosen over other relevant theories for this study. The chapter then presents a research model to explain end users' intention to engage in security misbehaviors.

Chapter 4 discusses the research design for this study. More specifically, it explains the procedures for developing security scenarios and the procedures for developing and validating measurement scale. It also discusses the result of a pilot study that has been conducted for scale validation.

Chapter 5 presents data collection procedures and the result of data analysis. It first discusses data screening procedures, preliminary reliability check, and common method bias check. The chapter then presents the result of hypothesis testing with the partial least squares technique.

Finally, Chapter 6 offers a discussion about the key findings of this study. It examines the major contributions of this study to the IS security literature and management practice. It concludes this thesis by identifying the limitations of the present study and future research directions.

Chapter 2

Literature Review

2.1 IS Security - Definition and Scope

In the IS literature, there are many seemingly similar yet much different terms used for security. Thus it is necessary to review and clarify these terms to avoid any possible confusion and misunderstanding.

Information Security

A commonly accepted viewpoint is that security encompasses confidentiality, availability, and integrity (see for example Bertino & Sandhu, 2005; Lindqvist & Jonsson, 1997). This type of security often refers to "information security" (ISO/IEC, 2000) and "database security" (Bertino & Sandhu, 2005). More specifically, confidentiality refers to the protection of data against unauthorized disclosure; integrity refers to the prevention of unauthorized and improper data modification; and availability refers to the prevention and recovery from errors and system failures (Bertino & Sandhu, 2005).

Information Systems Security

Information system security (hereinafter "IS security") differs from information security in that the former concept encompasses not only data or information itself but also those systems that process and store such data and information. In other words, IS security refers to the protection of all elements constituting an IS, including hardware, software, information, people and processes (Theoharidou, Kokolakis, Karyda, &

Kiountouzis, 2005). As such, the scope of IS security is broader than that of information security.

2.2 Threats to IS Security

An IS security threat is an object, person, or other entity that represents a constant danger to the security of information systems (Whitman & Mattord, 2003, p. 43). The identification and analysis of threats is considered to be an integral part of conventional risk management approaches (Alberts, Behrens, Pethia, & Wilson, 1999; NIST, 2001). In the IS security literature, there have been many ways of defining and classifying threats. This section gives an overview of these various terms.

Classification of Threats to IS Security

One approach to classifying IS security threats is a four-dimension model (Loch, Carr, & Warkentin, 1992). The four dimensions are: 1) sources, which could be internal or external to the organization in question; 2) perpetrators, which could be either human or non-human; 3) intents, which could be intentional or unintentional (accidental); and 4) consequences, which could be disclosure, modification, destruction, or denial of service.

Another approach to classifying IS security threats is the elaborated IS threat taxonomy (Im & Baskerville, 2005) shown in Table 1. With this approach, threats are first classified into two classes: accidental and deliberate. Accidental threats are those not intentionally caused by humans. These can be further broken down into two subtypes: human errors and catastrophes. Human errors can be skill-based (which is attributable to monitoring failures such as data input errors caused by inattention to a routine action

sequence), rule-based (which can be misapplication of good rules and application of bad rules, e.g. truncation or rounding errors), or knowledge-based (which are caused bounded rationality and the fact that knowledge relevant to the problem space is incomplete or inaccurate, e.g. several software malfunctions). Deliberate threats, on the other hand, are caused by the intentional behavior of the people who interact with the information systems. There are two dimensions of deliberate threats: mode and motive. Mode refers to a person's basic approach to creating the threat. There are four modes of deliberate threat: physical assault, falsification, malicious code, and cracking. The motive of a deliberate threat could be fraud, espionage, or vandalism.

Table 1: Classification of Threats to IS Security

Threat Type	Dimension	Threat Subtype
Accidental Threats	Non-human related	Catastrophe
	Human Error	Skill-based
		Rule-based
		Knowledge-based
Deliberate Threats	Mode	Physical assault
		Falsification
		Malicious code
		Cracking
	Motive	Fraud
		Espionage
		Vandalism

Sources of Threats

Natural disaster and the accidental actions of employees are among the top threats to IS security (Loch et al., 1992). It was found that the majority of the threats are human-initiated and of these, most are internal threats from within organizations (Loch et al., 1992). Examples of the most frequently reported internal threats in the survey included accidental entry of bad data, accidental destruction of data by employees, and unauthorized access by employees.

Other research reported similar findings. For example, one study found that accidental threats are the major source of unmanaged risk, which refers to those incidents for which the systems were vulnerable and unprepared (Im & Baskerville, 2005). Of these security accidents, human errors were found to be the major cause (Im & Baskerville, 2005).

These findings indicate the importance of "human factors" in IS security management. As Arce (2003) pointed out, information systems are designed and used by humans. Any security solutions that do not consider how users will react to and comply with them are likely to fail. From this point of view, security is not a technical issue but rather a management one (Dutta & McCrohan, 2002) and a social and organizational problem that involves people who operate and use the technical systems (Dhillon & Backhouse, 2000).

2.3 IS Security Management

To secure their information systems, organizations implement various security measures or controls such as firewalls and antivirus software, among others. IS security controls can be classified into three categories: technical, operational, and management (Stoneburner, Goguen, & Feringa, 2001). Technical controls include products and processes such as firewalls, antivirus software, and intrusion detection; operational controls focus on enforcement mechanisms such as backup procedures and physical access control; and management controls include measures such as disaster planning and employee training.

Prior research has found that antivirus controls, which are technical in nature, were perceived to have the highest quality of implementation while management controls such as training employees to prevent social engineering (i.e. being cheated by an attacker and revealing one's own credentials for accessing information systems) were rated the lowest (Baker & Wallace, 2007). This finding indicates that organizations may have viewed viruses and malicious codes as the most severe threat but at the same time underestimated human factors. As a result, organizations may invest more in technical solutions while paying less attention to management issues.

The management of IS security can be decomposed into four layers: organizational, workflow, information, and infrastructure (Weippl & Klemen, 2006). Infrastructure level security refers to traditional security aspects such as secure network and hardware; the information level encompasses access control and user rights; the

workflow level refers to secure business processes; and at the organizational level, IS security encompasses security strategy; corporate security culture, and risk management. A similar viewpoint is that IS security is an integral part of a 3D "enterprise security" pyramid, which encompasses technology, process, people, and organizational design/strategy (Kiely & Benzel, 2006). Technology involves the development and implementation of technological approaches for protecting information systems; processes refer to explicit means by which IS department and end users can do to keep the organization's information systems secure; people are the human resources of an organization, who must implement security processes and receive training for securing organizational data; and organizational design/strategy is the organizational structures and strategies that should put IS security to a top priority while enabling the organization to compete effectively in the marketplace.

Regardless of differences in terminology of these two viewpoints, one common argument is that security involves much more than just technical factors and IS security management must also consider human and organizational factors. It is generally realized that IS security is not so much a technical problem as a business and management issue (Dhillon & Backhouse, 2000; Dutta & McCrohan, 2002).

2.3.1 Security Policies and Guidelines

In most corporations, and public and government institutions, security policy guidelines and implementations are the responsibility of the chief information security officer (CISO). This is normally an executive position that reports to the chief

information officer (CIO), or the chief executive officer (CEO). In theory, this should ensure that IS security receives high level attention in the organization, although this is not always the case.

Security policies and guidelines are viewed as the starting point of IS security (Whitman, 2004). A security policy prescribes how an organization manages its information systems security. More specifically, it consists of a set of rules and practices that regulate how the organization manages, protects, and distributes its key information assets (Walker, 1985). Generally speaking, a good security policy should clarify the following aspects: individual responsibility, authorized and unauthorized uses of IS, how users report suspected threats, and penalties for violations (Whitman, 2004).

One useful classification scheme (although each type seems not mutually exclusive) is given by (Verdon, 2006): 1) Corporate security policy, which is a high-level corporate policy that serves as a legal protection against negligence; 2) acceptance-use policy, which regulates what users can and can't do; 3) privacy policy; 4) email policy; 5) information (systems) policy, which refers to operational procedures governing network access, firewall, and so on; 6) network security policy; 7) secure application development policy; 8) incident management policy; 9) data classification policy; and 10) policy exemption processes.

The above-mentioned classification is loosely based on the functional scope of the policy. Another classification of security policy is based on the level of analysis. A security policy can be at micro-, meso-, or macro-level (Marcinkowski & Stanton, 2003).

Micro-level policies emphasize on the human-technology interfaces; meso-level policies focus on what motivates end users to perform desirable actions and avoid undesirable ones; and macro-level policies deal with organizational-level controls. Alternatively, a security policy can be classified at information technology level, work system level, or organizational level (Karyda, Kiountouzis, & Kokolakis, 2005). The information technology level refers to the configuration of technical components of the IS, including software and hardware; the work system level refers to a set of different elements in an organization, including IS end users, business processes, and so on; and the organizational level refers to organizational structure and management style etc. A third approach is to classify a security policy as an organizational security policy or an automated security policy (Sterne, 1991). An organizational security policy refers to the set of laws and rules that governs how the organization manages security and how users exercise their authority; and an automated security policy refers to how computers and networks should be configured. The way these classifications tend to be roughly matched is shown in Table 2, although there are some subtle differences in their definitions.

Table 2: Classifications of Security Policy based on Level of Analysis

Classification			**Reference**
Macro level	Meso level	Micro level	(Marcinkowski & Stanton, 2003)
Organizational level	Work system level	Information technology level	(Karyda et al., 2005)
Organizational security policy		Automated security policy	(Sterne, 1991)

In sum, a policy can be one of the following: 1) security policies implemented by systems, e.g. a password longer than eight characters; 2) security policies regulating employees' action, e.g. what they should do and should not do; and 3) security policies regulating general security management, e.g. organizational structure, and decision-making processes. The current study focuses on the second type of policy, i.e. the kind of policies that regulate end user actions in using information technology.

2.4 Conceptualization of Security Misbehavior

In the present study, *security misbehavior* (SMB) is defined as *the behaviors engaged in by employees who voluntarily violate or bypass organizational information systems security policies with the intention of benefiting the performance of their work.* Organizational security policy in this study refers to the set of rules and regulations that govern employee actions related to security issues when using information systems for routine business tasks. SMBs have a number of characteristics:

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 information systems. The term "intentional" in this context implies that the actor makes some "conscious decisions" to follow a course of action.

Voluntary. SMBs are voluntary actions of users. Although organizational IS security policies are often mandatory, users may nevertheless voluntarily choose to violate such policies.

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 a malicious intent to harm the security or general business operations of the organization. Furthermore, SMBs do not include those actions that benefit the actors personally but clearly at the organization's cost. For example, stealing and selling information for personal profit are normally viewed as crimes that are subject to legal prosecution. SMBs on the contrary are handled internally within the organization.

Rule-breaking. When employees engage in security misbehavior, they actually violate the organization's policies to various degrees. In general, an IS security policy defines what users are allowed to do or what they are not allowed to do. The organization's security policy is the basis for the dissemination and enforcement of sound security practices within the organizational context (Baskerville & Siponen, 2002).

Possibly causing damage or security risk. In addition to rule-breaking, SMB is "misbehavior" in the sense that such behaviors are undesirable from an IS security perspective and may cause direct damage to the organizations' information systems or put the systems at risk, although the user in question may not have a malicious intent. As such, the term security misbehavior in this context is not the same as the behaviors with

malicious intention that are defined in the literature (Stanton, Stam, Mastrangelo, & Jolton, 2005).

2.5 Security Misbehavior and Related Concepts

In the IS literature, many terms have been proposed to describe "bad" behaviors that are deemed unacceptable and "good" behaviors that are viewed as beneficial from an organizational IS management perspective. Such terms include compliance, computer abuse, IS misuse, and unethical computer use, among others. Some of these terms are security-related while others reflect IS use behaviors in general, but such behaviors may have security implications. This section reviews and compares these terms with SMB.

2.5.1 Classification of User Security Behaviors

End user behaviors in using information systems affect security in various ways. Stanton et al (2005) developed a taxonomy to classify user security behavior on two dimensions: intentionality and level of expertise (Table 3). A user's behavior could be intentionally malicious, intentionally beneficial, or neutral (i.e. without explicit intention to help or harm security); the behavior could also require either high or low technical expertise.

Those "neutral" behaviors that do not involve the actors' clear malicious intention are of particular interest in the current study. If users do not have explicit intention to help or harm IS security, what are the factors that influence or motivate them to engage in security misbehaviors?

Table 3: Two Factor Taxonomy of Security Behaviors (Stanton et al., 2005)

Expertise	Intentions	Title	Description
High	Malicious	Intentional Destruction	Behaviors that require technical expertise and a strong intention to do harm to the organization's IS.
Low		Detrimental Misuse	Behaviors that require minimal technical expertise but the actor nonetheless has the intention to do harm through annoyance, harassment, etc.
High	Neutral	Dangerous Tinkering	Behaviors that require technical expertise but the actor has no clear intention to do harm to the organization's IS.
Low		Naïve Mistakes	Behaviors that require minimal technical expertise and the actor has no intention to do harm to the organization's IS.
High	Beneficial	Aware Assurance	Behaviors that require technical expertise together with the actor's strong intention to protect the organization's IS.
Low		Basic Hygiene	Behaviors that require no technical expertise but the actor has clear intention to protect the organization's IS.

2.5.2 Desirable Behaviors

Based on the two-factor taxonomy of security behaviors (Stanton et al., 2005), the two types of "beneficial" behavior – aware assurance and basic hygiene – can be viewed as desirable from an IS security management perspective. Examples of such behaviors include attending security training programs, reporting security vulnerabilities, and using excellent passwords, etc.

One of the desirable behaviors that has been studied more extensively is user compliance to security policies (Chan, Woon, & Kankanhalli, 2005; Pahnila, Siponen, & Mahmood, 2007; Son & Rhee, 2007). There is not, however, a clear definition of such compliant behavior, although the term may seem self-explanatory. Son and Rhee describe

it as "rule-following behaviors with respect to IT security" (2007). The behavior can be further broken down into two distinctive subtypes: compliance and deference (Tyler & Blader, 2005). Compliance refers to employee willingness to abide by or tolerate rules, while deference refers to voluntary and more discretionary acceptance rules. In the latter case, employees may still follow the rules even when their behaviors are not monitored.

2.5.3 Undesirable Behaviors

Some "undesirable behaviors" of end users using information systems have been discussed in the literature. Examples of such behaviors include computer misuse, computer crime, data theft, unethical computer use, and non-work related computing. Although the concept of SMB defined in this study shares some similarities with these terms, there are some important characteristics that differentiate them from SMB.

Computer Abuse

Computer abuse is defined as unauthorized, deliberate, and internally recognizable misuse of organizational assets by individuals (Kling, 1980; Straub, 1990; Straub & Nance, 1990). Possible abuses include theft or damage to hardware and software, modification of data, and disruption of computing services. One characteristic of computer abuse is that the actor has malicious intention to cause damages, although it is believed that the motivation behind some reported incidents is uncertain (Straub & Nance, 1990).

Some researchers have used the term computer abuse more broadly. For example, it may refer to writing virus codes, illegal software copying, and corporate sabotage by

using computers (e.g. hacking a competitor's network) (Harrington, 1996). These behaviors do not necessarily impact the information system and security of the actor's own employer. However, such behaviors may be counted as computer-related crimes. The term "IS misuse" is also used to describe any behaviors that are deemed as a misuse of IS resources owned by the organization in question (D'Arcy et al., 2009). Such behaviors may range from unethical and/or inappropriate uses (e.g. personal use of company email account) to illegal uses such as accessing confidential information.

A related concept is Internet abuse, which is defined as the "deviant use of Internet technology" in the workplace (Mahatanankook, 2006). Types of such deviant uses include: 1) property-related, where employees intentionally acquire intellectual properties or damage knowledge assets of the organization; 2) production-related, where employees violate organizational regulations regarding quality and quantity of work; 3) politically-related, where employees use the Internet as a tool for workplace politics such as spreading rumors and gossip; and 4) personal aggression, where employees use the Internet to "express aggression or hostility towards other individuals in the workplace".

The key difference between the above terms and SMB is whether the behavior implies or involves a deliberate intention to cause damage or is deemed to be inappropriate and illegal. These two characteristics do not apply to SMBs. On one hand, SMBs are defined as intentional behaviors. However, the intention is not malicious. Users may simply try to take shortcuts to do their jobs. On the other hand, SMBs are a

phenomenon within the scope of a specific organization and are not normally subject to the governance of the laws and regulations of society in general.

Unethical Computer Use

Unethical computer use broadly refers to "inappropriate uses" of computers (Banerjee, Cronan, & Jones, 1998). This term is also used interchangeably with terms such as "misuse", "unacceptable use", and "illegal use" (see for example, Leonard & Cronan, 2001). In both studies mentioned above, however, no clear definition or explanation was given regarding what behaviors can be deemed as inappropriate or unethical. Indeed, the concept of computer ethics is problematic in the IS literature, in the sense that an action can be deemed as ethical from the perspective of one theory (e.g. stockholder theory), but unethical from the perspective of another theory (e.g. social contract theory) (Smith & Hasnas, 1999). For example, a company that sells its customers' personal data may be ethical according to stockholder theory, because the sales would presumably increase the company's value; on the other hand, the action may be unethical according to social contract theory, because it would not provide meaningful benefits to its customers.

Similar ambiguity exists in the organizational behavior literature in general. The question of whether an action is good or bad is inherently a judgmental matter (Vardi & Wiener, 1996). For example, whistle-blowing may be viewed as ethical if it would be beneficial to society at large, but unethical or unacceptable from the viewpoint of the organization in question.

Nevertheless, SMBs as defined in this study are not necessarily unethical, because the actors may actually be trying to improve their job performance. From the stockholder perspective discussed above, SMBs may be beneficial to the organization because of improved employee job performance. Thus one may argue that SMBs are actually ethical behaviors despite the risk of causing damage to IS security.

Non-Work Related Computing

Non-work related computing refers to the use of organizational IS resources for personal purposes (O. K. Lee, Lim, & Wong, 2005) or "junk computing" that does not advance organizational goals (Guthrie & Gray, 1996).

Internet misuse, which is viewed as a "troubling transformation" of the workplace by the Internet (Anandarajan, Simmers, & Teo, 2006), is this type of behavior. One specific type of such behavior is cyberloafing, which is worker use of employer Internet access for visiting non-work related web sites (Lim & Teo, 2006). Although all these non-work related behaviors may have some security implications, the main concern is worker productivity. Thus these behaviors are different from SMBs in terms of intention and possible consequences.

Omissive Security Behavior

Omissive security behavior refers to the omission of information security measures among those people who know how to protect their systems but fail to do so (Workman, Bommer, & Straub, 2008). In other words, people who engage in such

omissive behaviors are "aware of IS security threats and countermeasures" but nevertheless choose to neglect them.

The concept of omissive security behavior is similar to that of SMB in that both are manifested in form of behaviors that are taken without security precautions and may result in security breaches. There is, however, a fundamental difference. The focus of omissive behavior is on the threats and relevant countermeasure, while that of SMB is security policy. Those who engage in SMBs are not necessarily aware of related threats or countermeasures. The security policy factor is not salient to the concept of omissive security behavior. Using the "knowing-doing gap" (Workman et al., 2008) as an analogy, people who engage in omissive behavior "know" the threats and countermeasures but choose to ignore them; people who engage in SMBs, however, "know" the security policy but nevertheless choose to violate or ignore it.

Security Contravention

Another category of undesirable behavior is the actions of users who try to contravene information security procedures (Workman & Gathegi, 2006). More specifically, contravention is associated with: 1) illegal copying of software (software piracy or soft-lifting); 2) breaking software license keys; 2) removing software from the office for personal use; 3) cracking passwords; and 4) committing fraudulent acts such as stealing information.

There are some key differences between SMBs and security contravention behaviors. The latter can better be categorized as malicious acts (intentional destruction

or detrimental misuse) based on the two-dimensional taxonomy (Stanton et al., 2005) shown in Table 3. Furthermore, these behaviors (e.g. software piracy and stealing information) are mostly illegal.

Exceptional Situations

SMBs should also be differentiated from other security rule-violating behaviors that may be "allowed" by the rules. Such behaviors often involve "exceptional situations", in which rigid compliance may prevent the organization from taking advantage of unanticipated business opportunities that may necessitate rule-breaking (Siponen & Iivari, 2006). In this case, such "temporary violation" (Siponen & Iivari, 2006) can be deemed as beneficial to the organization, as opposed to being beneficial individual employees. For example, a typical policy is that an employee's passwords should not be shared with other people. However, there may be some cases where temporary violation - sharing the employee's password with his or her coworkers – may be necessary. For example, the employee may have the sole control of some data that his or her coworkers need. The employee may need to share passwords with coworkers if he or she is on vacation and is not able to provide the data.

Behavior in Consumer Settings

Some studies have focused on behaviors (either desirable or undesirable) of individual computer use in consumer settings. Such consumer behaviors are beyond the scope of this study, which focuses on SMBs in organizational settings. Nevertheless,

these behaviors are briefly reviewed because they may be manifested in forms that are similar to that of SMBs.

One category of such behavior is conscious and voluntary use of protective technologies (Dinev, Goo, Hu, & Nam, 2009; Dinev & Hu, 2007), which refer to information technologies that can protect computer systems from disturbances such as viruses and spyware. A second category is risky user computing practices (Aytes & Connolly, 2005), which refer to some "low-level insecure behaviors" such as sharing passwords, using simple passwords, and opening email attachments without checking for viruses. A third category involves consumers succumbing to social engineering attacks (Workman, 2007). In comparison to the first two categories, this latter behavior is basically unintentional.

Another type of user behavior is software piracy (Peace, Galletta, & Thong, 2003), which is defined as the illegal copying of software. This type of behavior is different from SMB in two ways: 1) it is illegal and the actor in question is violating societal laws in addition to the policies of an organization; and 2) it does not have any direct or indirect impact on IS security of an organization.

2.5.4 Comparison to Organizational Misbehavior

Table 4 provides a comparison of intentional individual behaviors with similar types of organizational misbehavior (OMB), where OMB is defined as any intentional action by employees that defies and violates organizational norms or core societal values (Vardi & Wiener, 1996). Security misbehavior may be seen as a special form of OMB.

There are three basic types of OMB: Type S, Type O, and Type D (Vardi & Weitz, 2004). Type S reflects intention to benefit the individual rather than the organization; Type O reflects intention to benefit the organization rather than the individual directly; Type D, on the other hand, reflects intention to damage organizational assets. It can be argued that SMB can fall into both Type S and Type O organizational misbehaviors, as the intention of SMB is often to improve individual worker job performance, which is self-benefiting but at the same time can benefit the organization indirectly.

Table 4: A Comparison of Behaviors in IS and Organizational Misbehavior

Organizational Misbehavior	Intentional Behavior in IS	Reference
OMB Type S and Type O	Security Misbehavior (SMB)	(the present study)
OMB Type O	Temporary violation in exceptional situations	(Siponen & Iivari, 2006)
OMB Type D	Computer crime Computer misuse/abuse	(Harrington, 1996; Willison, 2006)
OMB Type S	Unethical computer use	(Banerjee et al., 1998)
OMB Type S	Non-work related computing	(Guthrie & Gray, 1996; O. K. Lee et al., 2005; Lim & Teo, 2006)

2.6 Antecedents of User Security Behaviors

This sub-section provides a review of prior research on the antecedents of security behaviors and identifies the gaps in the literature that the present study tries to address.

2.6.1 Deterrence Models

General Deterrence Theory (GDT), one of the theories in the criminology literature, builds on the assumptions that people are rational and they pursue their self-interest by minimizing cost or pain and maximizing benefit or happiness (Beccaria, 1986). According to this theory, wrongdoers should be punished so that the punishment can serve as an example to deter others from doing likewise (Beccaria, 1986). In practice, the theory serves as the guiding principle for various security management standards (Theoharidou et al., 2005), which include the British Standard BS7799 and its successor ISO17799 (ISO/IEC, 2000).

In the IS security literature, general deterrence theory has been applied to investigate the effect of organizational deterrent measures on computer abuse by employees. For example, the security impact model (Straub, 1990) suggests that deterrent measures can reduce computer abuse 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, and policies for system use, among others. Computer abuse is measured by number of incidents, actual dollar loss caused by security incidents, and opportunity dollar loss. This study suggested 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, Teo, Tan, & Wei, 2003). Deterrent severity, on the other hand, did not have a significant impact. In their study, preventive efforts refer to security software that can prevent security being breached; IS security effectiveness is the degree of security perceived by survey respondents.

In another study, physical security systems (e.g. physical entry control and secured computer rooms) negatively influenced on computer user self-defense intention, which is defined as the intention to install access control software and intrusion detection software (S. M. Lee, Lee, & Yoo, 2004). Two other factors - security policy and security awareness – do not have a significant impact, contrary to what is expected according to GDT.

In a more 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, 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 towards the policies influenced the relationship. Users may think the policies are just on paper and will not be

enforced, although the punishments due to violations may be severe. The factor of user attitude, however, has not been fully investigated in the IS security literature.

2.6.2 Ethical/Unethical Behavioral Models

Some studies have investigated user security behaviors from an ethics perspective. IS ethics, which refer to the ethical content of informal norms and behavior, may help deal with those situations where no formal rules or policies are in place (Dhillon & Backhouse, 2000). Harrington (1996) investigated the effect of codes of ethics on computer abuse judgment and intention. Overall, it found that codes of ethics have little effect on computer abuse judgment and intention relative to the psychological trait of responsibility denial. Two limitations of the study, however, may have reduced the explanatory power of the model. One limitation is that the study targeted IS employees such as programmers, system analysts, technical specialists, and security administrators. IS employees, who manage and implement systems (and IS security in particular) in organizations, may very well have different perspectives than end users. Indeed, the scenarios used in the study reflect those behaviors that may be engaged in by IS employees but not end users. Those behaviors, such as sabotaging a competitor's security system and writing and spreading viruses, require good technical knowledge and skills, which are not what end users are capable of doing. Secondly, employee awareness and perceptions of the codes of ethics were not measured in the study (Harrington, 1996). Thus the effect of the codes of ethics may be limited.

A different model was proposed to predict ethical behavior of IS personnel (Banerjee et al., 1998). The model suggests that intention to behave ethically or unethically is determined by the following factors: moral judgment, attitude towards ethical behavior, personal normative beliefs, ego strength, locus of control, and organizational ethical climate. Of these factors, only personal normative beliefs and organizational ethical climate were found to be significant, based on a survey of IS professionals. It was also found that ethical intention depends upon situational factors. The study was replicated with a student sample in a university setting (Leonard & Cronan, 2001). The findings, however, were not consistent with the previous study. A different set of factors, including attitude towards ethical behavior, personal normative beliefs, ego strength, and moral judgment, were found to be significant antecedents of ethical behavior intention, which was also situation-dependent.

One common limitation of ethical research is that the classification of ethical and unethical behaviors is not always straightforward and clear-cut. In fact, prior research found that some undesirable behaviors related to use of organizational IS were viewed as neutral, i.e. neither ethical nor unethical by survey participants (Calluzzo & Cante, 2004). One example of such behaviors is the downloading of files from the Internet on the job or at school from the Internet for personal use. Such behaviors can potentially compromise IS security if the files are infected with viruses.

2.6.3 Security Policy Compliance Models

Some studies have focused on user compliance to security policies. In one study, an IS security policy compliance model (Pahnila et al., 2007) suggested that user intention to comply with security policies is influenced by user attitude towards compliance. Both attitude and intention are influenced by a number of negative and positive reinforcements. Negative reinforcements include sanctions, threat appraisal (employee assessment of the threats to IS security), coping appraisal (employee assessment of whether complying with security policies is an effective mechanism for detecting a threat, whether they have the ability to cope with the security issues, and the costs associated with their actions), and normative beliefs (the normative expectation of peers or colleagues). Positive reinforcements included information quality of the policies, facilitation conditions (the resources and opportunities that employees possess for accomplishing a task), and habits (unconscious or automatic behavior, as opposed to intentions or conscious behavior). A survey of employees in a Finnish company indicated that attitude, normative beliefs, and habits have a significant effect on user intention to comply with security policies; and that threat appraisal and facilitation conditions have a significant influence on attitude towards complying. It is notable that, contrary to what was expected, coping appraisal did not have a significant impact on user attitude towards complying. Sanctions also did not have significant effect on user intention to comply, contrary to the predictions of 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 their self-efficacy (of breaching security). User perception of security climate was determined by individual observation of upper management practices, direct supervisory practices, and coworker socialization.

While having a security policy and guideline in place is one thing, the enforcement of such policies and guidelines is another. Many factors such as costs, employee resistance, and the phenomena of "everyone-breaks-the-law" may discourage organizations from enforcing security policy strictly, especially when stiff punishment is involved. One study found that top management support positively impacts the security culture and security enforcement in organizations (Knapp, Marshall, Rainer, & Ford, 2006). The enforcement in turn may impact employees' attitude towards security policies and guidelines.

2.6.4 Neutralization Model

Siponen and Vance (2010) proposed a neutralization model to investigate the problem of employee IS security policy violations. Based on neutralization theory in the 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 a

significant positive effect on employee intention to violate IS security policies. The effects of formal or informal sanctions, on the other hand, were not significant.

2.6.5 Password Use Model

Access control mechanisms that use passwords are probably the most widely adopted security measures. Together with the use of user names or identities (ID), it authenticates legitimate users before allowing them to access systems and resources. From a technical standpoint, a password-based access control is a low-cost security option for organizations (Sasse, Brostoff, & Weirich, 2001). Organizations tend to address security issues by enforcing more restrictive authentication policies (Anne Adams, Sasse, & Lunt, 1997), such as more frequent changes of password, longer and more complex passwords, and lockout of user accounts upon a maximum number of unsuccessful logons. However, the effectiveness of such policies is questionable because users tend to circumvent them by writing passwords down or choosing easy-to-guess ones (Zviran & Haga, 1999).

The problem of password write-down may be caused by a number of factors. Focusing on password characteristics and user practice, the password security model (Zviran & Haga, 1999) suggests that users write down passwords because of their difficulty in recalling them ("memorability"). The study also found that password write-down is significantly associated with how passwords are composed (alphabetic, numeric, alphanumeric, or ASCII). It also found that usage frequency is related to memorability

and write-down. In other words, infrequent use of a password could result in recall difficulty, causing the user to write it down.

Another factor that may cause users to circumvent security procedures is the incompatibility between workplace practices and security procedures (Anne Adams & Sasse, 1999; Anne Adams et al., 1997). For example, in a group-work setting where users work on the same data or information, users perceived the security mechanism of individually-owned passwords as incompatible with their work. As a result, they tended to reject individually-owned passwords and advocated shared group passwords.

2.6.6 Threat Control Model

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 "threat assessment" and "coping assessment", based on the assumption that, when a threat is perceived, people adjust their behavior according to an acceptable level of risk. Threat assessment includes user perceptions of threat severity and vulnerability (whether they perceive they are vulnerable to a security breach). Coping assessment involves user evaluation of their capability to deal with certain situations. It includes the assessment of locus of control, self-efficacy (of dealing with security issues), perceived response efficacy (whether security measures are effective), and response cost-benefit.

Both subjective and objective measurements of user omissive behavior were used in Workman et al (2008). Subjective measurement was self-reported frequency by survey

respondents; objective measurement was through the logs of computer use behaviors: password change, security patch updates, and backups. It found that both threat assessment and coping assessment significantly reduce user omissive behavior.

As previously discussed, similar concepts of threat appraisal and coping appraisal have been studied in security policy compliance models (Pahnila et al., 2007). The conclusions of the two studies, however, were inconsistent. In the study by Pahnila et al, it was found that coping appraisal did not have a significant effect on user attitude towards complying (which in turn is hypothesized to influence compliance intention and actual compliance).

2.7 Summary

This chapter set out to build the foundation and to define the scope of the present study. More specifically, it provided a review of the current literature on organizational IS security management. It clarified some related concepts and discusses different types of threats to IS security and different security policies for dealing with these threats. This chapter then provided a definition of "security misbehavior" (SMB) and comparison of this type of behavior with other conceptualizations of desirable and undesirable IS user behaviors reported in the literature such as computer abuse, Internet misuse, unethical computer use, among others. Finally, this chapter provided a thorough review of relevant theoretical models that have been proposed for studying the antecedents of these behaviors (or behavioral intention).

The literature review revealed that, while 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 are worth further investigation.

First of all, in the context of SMB, ethical/unethical behavioral models may not be directly applicable. Security misbehavior may not be intrinsically "unethical", as discussed in the previous section. Thus a code of ethics may not have a significant impact on user intention to engage in SMB, nor do these factors affect ethical behaviors. Furthermore, although SMB may trigger disciplinary actions that are often prescribed in security policies, such disciplinary actions may be deemed to be unfair because the actor may intend to improve job performance by engaging in SMB.

Secondly, security compliance models do not explain why users break rules. In general, compliance seems to represent the opposite of SMB, which is the focus of this thesis. These models may share some common antecedents such as threat appraisal. For example, someone who perceives a high security threat may tend to comply with the organization's security policies while others who perceive a low threat may actually engage in SMBs (or non-compliance). Despite this commonality, however, the antecedents of the two types of behaviors may be quite different. Following rules or policies could simply be common sense and may not require any salient cues. To break rules, on the other hand, actors may think about rule breaking and look for salient cues or purposes and excuses for themselves. Practically, it may be more worthwhile to investigate why employees misbehave rather than why they comply with policies, so that

proper measures could be put in place to discourage them from breaking the rules. When deviant behaviors (which refer to those behaviors that are not typical in comparison with what others would do in similar situations) are observed, it means that something surprising occurred and requires an explanation (Blanton & Christie, 2003; Hilton & Slugoski, 1986). In other words, deviant behaviors are more "informative" (Blanton & Christie, 2003). From this perspective, studying security misbehavior (a type of deviant behavior, may enable us to have some insightful understanding of employee actions in using organizational information systems. Another limitation of compliance models is that these models tend to view end users' compliance behavior as an end in itself. However, such view seems contrary to the reality in organizational settings. Using information systems (and dealing with security issues) is just a means for end users to accomplish business goals.

Third, somewhat in common with these 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 these rules or engage in SMB. Furthermore, the effect of deterrence is not conclusive. For example, contrary to what is predicted by GDT, prior studies indicated that perceived certainty of punishment as stipulated in security policies does not have a significant influence on user intentions to misuse information systems (D'Arcy et al., 2009). Further study is needed to understand the reasons why deterrent 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, these two behaviors 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. That is how users evaluate and cope with threats. Their model may not provide sufficient explanation about user behavior because security and the dealing with threats are perceived not to be user tasks or responsibilities (Besnard & Arief, 2004).

Fifth, although violation of IS security policies conceptualized in the neutralization model (Siponen & Vance, 2010) may be manifested in rule-breaking 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 focused on whether employees are aware of and understand the IS security policies in question. Furthermore, violations of IS security policies are generally not considered as crimes, although the two types of behaviors share some commonalities such as rule-breaking. Crimes are extremely bad behaviors that are condemned and prohibited by 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 into security policies to allow some violations under exceptional circumstances (Siponen & Iivari, 2006). Thus, applying criminological theories to IS security policies may not be straightforward. Another difference between violations of security policy (as defined by Siponen and Vance) and SMB is that SMBs

are voluntary actions. Violations of security policy can be mandatory in the sense that a user may be ordered to do so by his or her superior (as implied in the scenario used in Siponen and Vance's study).

Lastly, some studies investigated security behaviors of IS professionals (e.g. Banerjee et al., 1998; Harrington, 1996) while others used student samples (e.g. Leonard & Cronan, 2001). Arguably, the perspectives of IS professionals and students may be much different from those 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 efforts in studying user security behavior in the literature, some critical questions remain unanswered. In particular, there is the general question of why users engage in security misbehaviors that violate organizational security policies and rules and may result in punishments or disciplinary actions. It is the objective of this study to answer this question through the use of the composite behavior model developed by Eagly and Chaiken (1993).

Chapter 3

Theoretical Background and Hypothesis Development

3.1 The Composite Behavior Model

The composite behavior model (CBM) proposed by Eagly and Chaiken is an extension to the theory of planned behavior, or TPB (Ajzen, 1991). According to CBM (Figure 1), a person's attitude towards a behavior affects whether or not the person will engage in that behavior. Attitude is defined as "a psychology tendency that is expressed by evaluating a particular entity with some degree of favor or disfavor" (Eagly & Chaiken, 1993, p. 1). The impact of attitude on behavior is mediated by the person's intention. The person's attitude towards the behavior is in turn determined by a number of antecedents: 1) habit; 2) attitude towards target; 3) utilitarian outcomes; 4) normative outcomes; and 5) self-identity outcomes. The most noticeable differences between CBM and TPB are the inclusion of habit factor and the split of attitude into attitude towards target and attitude towards behavior. These two types of attitude impact the person's actions at different points of time in the behavioral decision process. Each of the antecedents is defined below.

Habit. This refers to the sequences of a person's behavior that have become relatively automatic and occur without the person's self-instruction. The inclusion of habit as an antecedent of attitude towards behavior is based on the argument that many everyday behaviors are controlled only partially by intentions and may be controlled in part by habit (Eagly & Chaiken, 1993, p. 181). According to the CBM model, a person's

habit has a direct impact on attitude towards target, attitude towards behavior, and actual behavior.

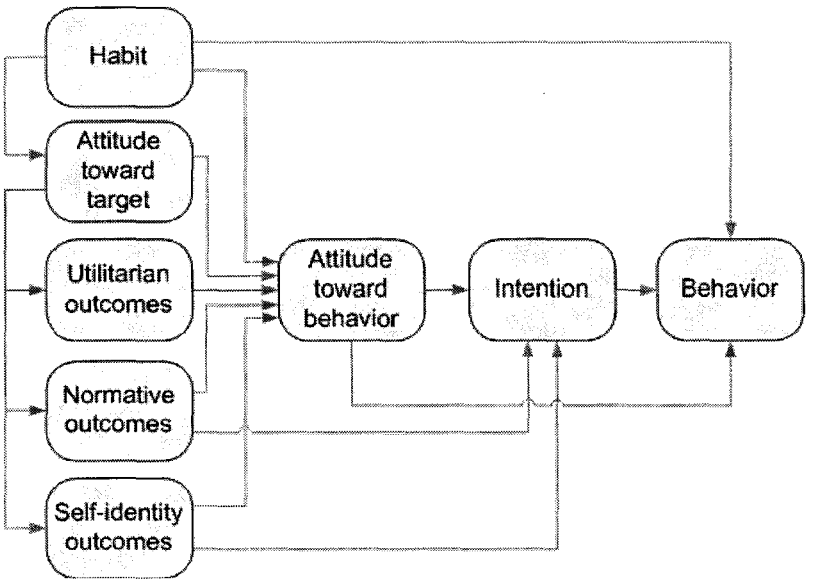


Figure 1: The Composite Behavior Model (Eagly & Chaiken, 1993)

Attitude towards target. 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. a thing or a person) towards which the behavior in question is directed. Take the action of attending university as an example. Persons can have certain attitudes towards the action of attending university. They can also have certain attitudes towards the university itself. In this case, the university is the target of the attitude.

Attitude towards behavior. As opposed to attitude towards target, attitude towards behavior is about the *action* that one may or may not take. In the above example, the

action is "attending university" and attitude towards behavior is "attitude towards attending university". As shown in Figure 1, attitude towards behavior is determined by habit, attitude towards target, and expected outcomes.

Expected outcomes. Expected outcomes are the anticipated consequences of a behavior. There are three types of outcome: utilitarian, normative, and self-identity. Utilitarian outcomes refer to either rewards or punishments that one expects from engaging in the behavior in question. Normative outcomes refer to the approval or disapproval by significant others of the behavior. In Eagly and Chaiken's terminology, this also refers to self-administrated rewards (pride) and punishments (guilt) that follow from the actor's internalized moral rules. Self-identity outcomes are either affirmations or repudiations of one's self-concept that are expected to follow from engaging in the behavior. The differentiation of these outcomes helps highlight various classes of consequences – rewards or costs – that are relevant to the behavior. All these outcomes have an impact on attitude towards a behavior. In addition, normative outcomes and self-identity outcomes influence behavior through their direct impact on intention.

3.2 Comparison of Competing Theories

3.2.1 User Acceptance Theories of Information Technology

The technology acceptance model (Davis, 1989; Davis, Bagozzi, & Warshaw, 1989) is one of the most influential theories in IS research (Y. Lee, Kozar, & Larsen, 2003). According to the technology acceptance model (TAM), user acceptance of technology is determined by two antecedents: perceived usefulness and perceived ease of

use. Security misbehaviors, to some extent, imply user resistance to (or not accepting) IS security measures. User acceptance theories, however, may not be applicable to security-related behaviors for the following reasons:

Assumption of full volitional control. One of the key assumptions of TAM is that the adoption of a technology is voluntary (Brown, Massey, Montoya-Weiss, & Burkman, 2002). In other words, users have full volitional control, which is in line with the assumption of the theory of reasoned action (TRA) (Ajzen & Fishbein, 1980; Madden, Ellen, & Ajzen, 1992) – the theoretical foundation of TAM. Security measures in organizations, however, are often enforced and not under a user's full volitional control (although in the case of SMB, the behavior of breaking security policy is voluntary). As such, security misbehaviors may not be explainable by TAM.

TRA was later modified and extended to the theory of planned behavior (TPB) (Ajzen, 1991). TPB explicitly incorporates a non-volitional control factor: perceived behavior control. In the IS field, there have many efforts to extend TAM, based on TPB. With the inclusion of non-volitional control factors in mandatory settings, research has found that perceived usefulness and perceived ease of use became statistically non-significant in predicting user acceptance of technology (Brown et al., 2002). This suggests that it is necessary to look beyond TAM in order to search for better models to explain security misbehaviors.

Security measures not directly useful for end-users. Security measures can be viewed as "protective technologies", which protect data and systems from disturbances

(Dinev & Hu, 2007). Rather than being useful as typical IS artifacts such as software, security measures may not be useful at all to end users. This is because, for ordinary end users, IS security has nothing to do with their job performance, which is often business-oriented. Instead, they may perceive security measures as causing inconvenience and hindering job performance (Post & Kagan, 2007). From their perspective, IS security is a task for system administrators rather than end users (Besnard & Arief, 2004). For end users, information technology is just a tool for them to carry out business activities. It is often the tasks of IS department to make sure proper technologies are implemented and secured.

3.2.2 Theory of Planned Behavior

The composite behavior model (CBM) is an extension to the theory of planned behavior (Ajzen, 1991). The most noticeable difference between CBM and TPB is that the former includes a habit factor and that it separates the attitude factor into attitude towards targets and attitude towards behavior. We contend that attitude towards targets, which is considered to be external to the TPB model, is important in the IS context because user security behavior is not an isolated act. It involves interaction with the IS department in an organization when users have to deal with security policies and measures. Thus, their attitudes towards these targets may be an important antecedent of their security behavior.

In light of these limitations, the present study turns to other avenues for theorizing the antecedents of SMB. More specifically, this study uses the composite behavior model (Eagly & Chaiken, 1993) as its theoretical foundation.

3.3 Proposed Security Misbehavior Model

Based on Eagly and Chaiken's Composite Behavior Model and other theoretical considerations discussed below, this research proposes the security misbehavior (SMB) model shown in Figure 2. Instead of studying actual behavior as in the CBM, this research focuses on intention (i.e. SMB intention is the dependent variable). This approach is chosen for two reasons. First, actual security misbehaviors are not readily observable or objectively measurable because they are "ideographic in nature" (Workman et al., 2008). One cannot practically observe or objectively measure every possible IS security behavior (Workman et al., 2008). Self-reported actual behavior may be an option. However, prior studies suggest that there is always discrepancy between what people report about their behaviors and what they actually do (Workman et al., 2008). The other reason is that the influence of intention on behavior has been rigorously tested and well established in the literature. Replicating this link (from intention to actual behavior) in the proposed model may not add much theoretical contribution.

Indeed, the intention-focused approach is not uncommon in the IS literature. Examples of studying behavioral intention as the dependent variable include knowledge sharing intention (Bock, Zmud, Kim, & Lee, 2005), IS misuse intention (D'Arcy et al., 2009), and IS use intention (Bhattacherjee & Sanford, 2006), among others. As such, this

research focuses on user SMB intention instead, by exploring and testing those antecedents that predict user intention to misbehave in the context of information security.

One notable difference between the proposed SMB model and CBM is that habit is not included in the proposed model. The main reason is that habits (if defined as previous behavior) have a tautological relationship with current or future behavior (Thompson, Higgins, & Howell, 1991). Furthermore, using prior behavior to predict future (the same) behavior does not add much theoretical value (Ajzen, 1991). In other words, it is roughly equivalent to predicting that someone will do something because they have done the same thing in the past.

Habit also implies that the behavior in question is automatic. If behavior has become routinized through repetition, the person does not make a conscious decision to act, yet still engages in the behavior in an automatic way. As such the behavior should be less affected by intention to the extent that the behavior is habitual (Eagly & Chaiken, 1993, p. 180). Because the proposed SMB model focuses on intention instead of actual behavior, inclusion of a habitual factor will be less likely to improve the explanatory power of the model. SMB implies rule-breaking, so individuals involved in SMB are more likely conscious of making such behavioral decisions. In other words, they are making conscious decisions and are self-instructed, unlike habitual situations that lack self-instruction.

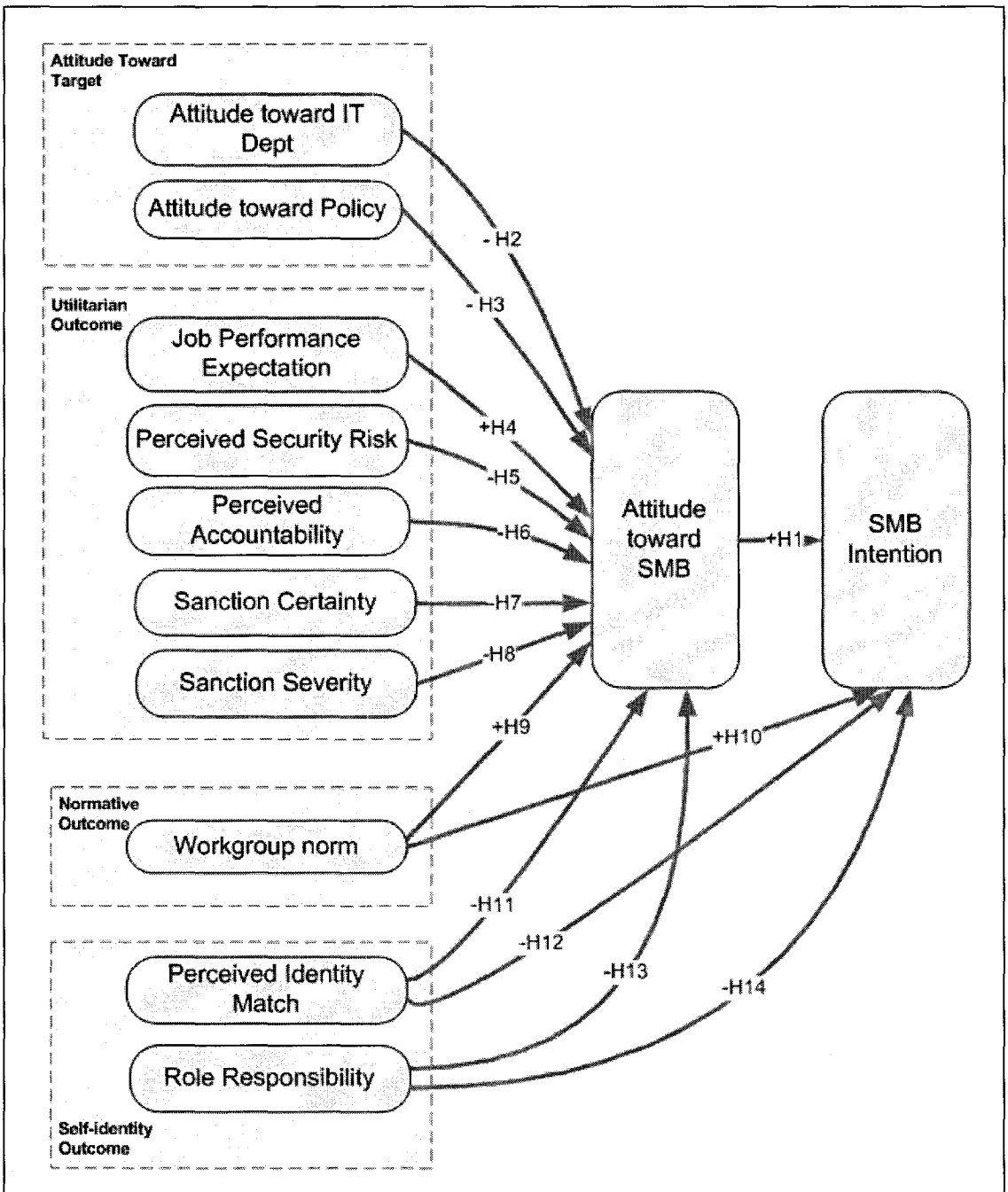


Figure 2: Security Misbehavior Model

Another difference between Eagly and Chaiken's composite behavioral model and the SMB model is that the latter does not include interrelationships among antecedents of attitude towards behavior. Interrelationships among the antecedents are excluded 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 the literature (e.g. Venkatesh, Morris, Davis, & Davis, 2003). It should be noted that the variance (R^2) explained by the model is not affected by indirect paths (Venkatesh et al., 2003).

3.3.1 SMB Intention

SMB intention in this study is defined as the extent to which an end user intends to voluntarily engage in actions that violate the organization's security policies. Intentions are assumed to be the indications of how hard end users are willing to try and how much of an effort they are planning to exert in order to perform the behavior (Ajzen, 1991). According to CBM, individuals' behavioral intention is partially determined by their attitude towards the behavior in question. Similarly, in the context of IS in organizations, this relationship should also apply to SMB. Based on Eagly and Chaiken's definition of the general term of attitude, *attitude towards SMB* defines an end user's evaluation of security misbehaviors in terms of the degree of favor or disfavor. Those users who hold a positive attitude towards SMB would have a greater intention to engage in such misbehavior. Hence it is hypothesized that:

H1: User attitude towards SMB has a positive effect on SMB intention, such that the more favorable the attitude towards SMB, the greater intention to engage in SMB.

3.3.2 Attitude towards SMB

In line with the CBM, it is posited that end user attitude towards SMB is in turn determined by four groups of antecedents: attitude towards target, utilitarian outcome, normative outcome, and self-identity outcome.

3.3.2.1 Attitude towards Target

In organizational settings, it is not uncommon that information technologies are managed by a single organizational unit, which is often the IS department. This organizational structure, however, creates an "obvious point of friction" between the IS department and end users because the IS department manages information systems while users are responsible for the business activities that the systems are intended to support (Applegate, McFarlan, & McKenney, 1996, p. 42). Such intergroup conflict is inevitable in organizations for various reasons such as differences in their perceptions of reality (Gibson, Ivancevich, & Donnelly, 1988, pp. 304-313), competing goals, competition for resources, and cultural differences (Cox, 2003). The conflict is also seen as a consequence of the organizational decision-making context, which includes the organization as a social system, the way the organization is structured, and others (Barclay, 1991). Tension and conflict between end users and the IS department is a challenging organizational issue in corporate information technology management

(Applegate et al., 1996, p. 166; McKeen & Smith, 1996). Such conflict may contribute to user resistance to the implementation of information systems in organizations (c.f. Bhattacherjee & Hikmet, 2007; Lapointe & Rivard, 2005).

One characteristic of user resistance is the change of object (i.e. what users are resisting) over the time period of implementation (Lapointe & 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, user resistance (as behavior) to these objects reflects their attitudes towards these objects. One of the reasons why users resist is that they "perceive a threat" from their interaction with these objects. In other words, they may have negative attitudes towards these objects (or "targets"). For example, in their study, Lapointe and Rivard cited user complaints about specific aspects of a computer system (the system itself), unfavorable power distribution caused by the system (the system's significance), and hospital administration (the system's advocate) trying to undermine the power of physicians (the users in this case). In essence, user resistance behavior can be in part attributed to unfavorable attitudes towards the system, its significance, and its advocates.

Similarly in the context of organizational IS security, users may resist the implementation and enforcement of security measures. It is often the case that the IS department (under the direction of the Chief Information Security Officer, or CISO) designs and enforces security policies, which define what users are allowed to do or are 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. Applying Lapointe and Rivard's terminology, security policies are the "system" and the IS department is its "advocate". Understandably, user attitudes towards the IS department and its security policies will affect their willingness to follow or their intention to violate the policies and measures.

Attitude towards the IS Department

Based on Eagly and Chaiken's definition of the general term of attitude, *attitude towards the IS department* is defined as end user evaluation of the IS department in terms of degree of favor or disfavor. In the IS security context, users may think that IS department tries to control everything about information by enforcing security policies. For users, such control may cause inconvenience, extra effort, and less freedom in using IS. Users may also develop stereotypes about IS people in terms of their business knowledge and skills. Indeed, prior research has found that IS professionals' business competence does influence the IS-business partnership (Bassellier & Benbasat, 2004). Based on this reasoning, it makes sense that the more negative user attitudes are towards IS department, the more the likelihood that users may ignore security policies. Therefore, it is hypothesized that:

H2: User attitude towards the IS department has a negative effect on attitude towards SMB, such that the more favorable their attitude is towards the IS department, the more unfavorable their attitude will be towards SMB.

Attitude towards Security Policy

Attitude towards security policy refers to the degree of favor or disfavor expressed by IS users about organizational information security policies. Users may have a negative attitude towards security policies because such policies may be seen as a tool used by the IS department to control information and the way users do their information-related work. Security measures may be seen as "barriers" or "obstacles" that create trouble for them rather than as a protective mechanism (A. Adams & Blandford, 2005; Dourish, Grinter, de la Flor, & Joseph, 2004). They may also perceive security as a "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 towards security policy has a negative effect on attitude towards SMB, such that the more favorable user attitude towards security policies, the more unfavorable their attitudes towards SMB.

3.3.2.2 Utilitarian Outcomes

According to goal-directed behavioral theories, people distinguish between positive and negative goals when engaging in certain behaviors (Klinger, 1977; Winell, 1987). Positive goals represent pleasant results to be attained and negative goals represent unpleasant results to be avoided. Negative goals can also be viewed as detrimental side effects that might occur when one pursues desired outcomes (Heckhausen & Kuhl, 1985).

One may refrain from any intention to engage in actions directed towards positive outcomes, if such positive outcomes are outweighed by undesirable side effects. Such behavior has been 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 & Scheier, 1998). Stated differently, people direct behavior ("approach") towards positive stimuli such as object, events, and possibilities and away ("avoidance") from negative stimuli (Elliot, 2006).

In the context of information systems security, the following utilitarian outcomes are posited to be salient to users when they are involved in SMB: 1) job performance expectation; 2) perceived security risk; 3) perceived accountability; and 4) sanction (certainty and severity). Job performance expectation is a positive outcome users pursue while the rest are negative outcomes or side effects that they want to avoid.

Job Performance Expectation

The first anticipated outcome is *job performance expectation*, which is defined as the extent to which users expect their actions to help them do their job. As discussed previously, security is often not seen as an end user task (Besnard & Arief, 2004). From their perspective, end 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 IS people, for guidance on IS security-related issues (Cisco, 2006). This may be an indication that job performance is more important for end users. Many of

the problems end users have with security measures can be explained in terms of the mismatch between the measures and user 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 & Kagan, 2007). In essence, end users care more about job performance than IS security. They will likely ignore policies and bypass security measures if doing so can help them do their work and improve their job performance. Hence it is hypothesized that:

H4: Job performance expectation as a result of SMB has a positive effect on user attitude towards SMB, such that the higher the job performance expectation, the more favorable is the user's attitude towards SMB.

Perceived Security Risk of SMB

The second anticipated outcome is *perceived security risk*, which refers to end user evaluation of the security risk that may be caused by their violation of security policies and rules. In this context, risk refers to the likelihood of unfavorable or negative outcomes, e.g. security breaches and data loss, as a result of SMB.

Prior research indicates that perception of risk has an impact on human behavior. For example, in the management literature, it is suggested that risk perception is negatively related to business managers' risky decision making behavior (Sitkin & Weingart, 1995). In the consumer behavior literature, perceived risk can explain

consumer 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 levels of risk (Dowling & Staelin, 1994). In the information systems literature, it has been found that perceived risk will decrease intended use of P2P (peer-to-peer) sharing software (Xu, Wang, & Teo, 2005) and affect consumer attitude towards shopping online and consequently their willingness/intention to buy (Grazioli & Jarvenpaa, 2000; Jarvenpaa, Tractinsky, & Vitale, 2000; Malhotra, Kim, & Agarwal, 2004; Pavlou, 2003; Pavlou & 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 may cause damage to overall IS security. If users perceive a lower security risk, they will likely form more favorable attitudes towards SMB (i.e. approve of SMB) and hence will be more likely to engage in SMB. On the other hand, if users perceive a higher security risk, they will be likely to form more unfavorable attitudes towards SMB (i.e. disapprove of SMB) and hence will be less likely to engage in SMB. As such, it is hypothesized that:

H5: Perceived security risk has a negative effect on user attitude towards SMB, such that the higher perceived security risk of SMB by end users, the more unfavorable their attitude towards SMB.

Perceived Accountability

In an organizational setting, accountability is often used as an element of management control (Dose & Klimoski, 1995). Accountability refers to being answerable to audiences for performing up to certain prescribed standards and the actor in question is subject to observation and evaluation by the audience (Schlenker, Britt, Pennington, Murphy, & Doherty, 1994). The overall effect of accountability is that, the more people feel accountable, the higher the likelihood they will act in a considered and motivated manner (Dose & Klimoski, 1995). Furthermore, according to Schlenker et al (1994), the evaluating audience could be either other people or oneself. In the latter case it can be viewed as a person's self-evaluation, judgment, and sanctioning of his or her own conduct.

The above accountability concept can be applied to IS security as well. In the present study, *perceived accountability* refers to the extent to which end users believe they are accountable for their IS security-related misbehaviors (i.e. SMB) and possible consequences. This accountability reflects user self-evaluation of behaviors (evaluation by other people will be discussed latter in this section as "sanctions"). Users may feel that they are not accountable for various reasons. For example, user actions may not be viewed as the causal factor for security incidents. Rather, end users may argue that it is the IS department that has not done a good job of managing IS security. Thus, despite the possibility of causing security problems, users may still engage in SMBs.

Based on the above reasoning, it is argued that perceived accountability plays an important role in influencing user attitude and behavior related to IS security. If perceived

accountability is low (i.e. when users believe they are not accountable), users will likely form a more favorable attitude towards SMB; on the other hand, if perceived accountability is high, they will likely form a more unfavorable attitude towards SMB. It is therefore hypothesized that:

H6: Perceived accountability has a negative effect on user attitude towards SMB such that the higher the perceived accountability, the more unfavorable user attitude will be towards SMB.

Sanctions

As opposed to perceived accountability, which is the evaluation by oneself, sanctions (or punishments) reflect the evaluation and judgment by other people and particularly the management in an organization. SMBs may cause damage to overall IS security of an organization. When that happens, the actors may be held accountable for their undesirable rule-breaking behaviors. They may be disciplined for their actions, depending on how the organization deals with violations. Thus sanctions can be viewed as negative outcomes that users may try to avoid. The above argument is basically consistent with the general deterrence theory (GDT), which posits that certain and severe sanctions deter individuals from targeted actions (Gibbs, 1975). The less certain and severe the sanctions are, the more the likelihood the action is. For example, many users misbehave even when they are aware that their behaviors do not fully comply with security policies because they do not expect to be sanctioned by the organization (Sasse et al., 2001).

As discussed previously in the literature review, some studies in the IS security literature have applied GDT to investigate undesirable user behaviors such as computer abuse (Straub, 1990) , IS misuse (D'Arcy et al., 2009), and violation of security policies (Siponen & Vance, 2010). Sanction (or punishment) is often conceptualized in terms of sanction certainty and sanction severity. Both terms are self-explanatory: sanction certainty refers to the certainty that violation of security policies will be subject to organizational reprimand; sanction severity refers to how severe the reprimand is. Prior studies have reported inconsistent findings regarding the effect of sanctions. For example, sanctions had no significant influence on user intention to violate security policies (Siponen & Vance, 2010); on the other hand, sanction severity but not certainty was found to significantly influence user IS misuse intention (D'Arcy et al., 2009). Despite these inconsistent empirical findings, we propose sanctions as an antecedent of user attitude towards SMB for a number of reasons. First, it is consistent with the two theories: GDT and CBM (composite behavioral model). Secondly, the mixed findings in prior studies may be due to other stronger factors that have or have not been accounted for. For example, it is argued that neutralization by excuses weakens the effects of sanctions (Siponen & Vance, 2010). This does not necessarily mean that sanctions do not have any effects at all, however. Lastly, following the practice in the literature, sanction is included in the proposed SMB model for the purpose of comparing with other studies (e.g. D'Arcy et al., 2009; Siponen & Vance, 2010). Based on GDT and CBM, it is therefore hypothesized that:

H7: *Sanction certainty has a negative effect on user attitude towards SMB such that the more certain the sanction is, the more unfavorable the user attitude will be towards SMB.*

H8: *Sanction severity has a negative effect on user attitude towards SMB such that the greater the severity of sanctions, the more unfavorable the user attitude will be towards SMB.*

3.3.2.3 Normative Outcome

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 & Chaiken, 1993). Arguably, people in the same workgroup, including supervisor and peers, have more influence on an employee's 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 of employees in the organization. In the present study, this type of approval or disapproval by a user's workgroup members, include supervisor and peers, is referred as *workgroup norm*.

Prior studies in IS use in organizations suggest that top management, supervisors, peers, and IS department are the salient referents for users to make decisions (Karahanna, Straub, & Chervany, 1999). In an IS security context, some studies have also investigated the impact of top management's support. It has been found that top management support is a significant predictor of an organization's security culture and the level of policy

enforcement (Knapp et al., 2006). In the present study, however, it is argued that top management may not have a significant influence on employee day-to-day IS security behaviors. Most employees do not have direct interactions with top management and do not have the opportunity 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 & Dansereau, 2002). Behaviors in organizations are inherently hierarchical (Ployhart & 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 than levels farther apart (e.g. individual and organization) (Ployhart & Schneider, 2002). Accordingly, the effect of a workgroup on individuals will be stronger than that of the organization as a whole (Ployhart & Schneider, 2005). Top management's support can be viewed as being at an organizational level factor, while one's supervisor and coworkers are at workgroup level. For end users, their supervisor and coworkers within the same workgroup are more relevant than top management. Prior research also indicates that workgroup-based social influence is a stronger predictor of individual attitudes and behaviors than influence from people in other social networks within the same organization (Fulk, 1993).

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 norms 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 & 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 & 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 their supervisor and peers, end users are more likely to form a negative attitude towards 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 towards SMB, and hence more likely to engage in SMB. It is therefore hypothesized that:

H9: Workgroup norm (framed as in favor of SMB) has a positive effect on user attitude towards SMB such that the greater the extent to which the SMB is approved by workgroup members, the more favorable the user attitude will be towards SMB.

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

H10: Workgroup norm (framed as in favor of SMB) has a positive effect on user SMB intention such that the greater the extent to which the SMB is approved by workgroup members, the greater the user intention will be to engage in SMB.

3.3.2.4 Self-Identity Outcomes

Self-identity outcomes refer to affirmations or repudiations of the self-concept that are anticipated to follow from engaging in a behavior (Eagly & Chaiken, 1993). In the IS security context, the following two types of self-identity outcomes are posited to be salient when end users make IS security related behavioral decisions: perceived identity match and role responsibility.

Perceived Identity Match

In organizations, IS security is often seen as the responsibility of IS 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 a degree, whether end users care about IS security or not does not affirm or repudiate their identity as business professionals – their "professional image" (Roberts, 2005) – vis-à-vis IS people. We define this perception of affirmation and non-repudiation as perceived identity match. For example, the professional status of salespersons is more likely to be judged on their knowledge and experience in sales and their job performance rather than on how well 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 a business professional. If employees believe that strictly following organizational security policies does not help improve their identities as business professionals, or doing otherwise (i.e. SMB) does not necessarily hurt their identities as business professionals, they are more likely to form a positive attitude towards SMB and ignore those security 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, Higgins, & Huff, 1999). That 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 computers may improve users' "IT competence" as perceived by others, it will be less likely to improve user image as "business professionals". In other words, users may very well form a negative attitude towards using computers (and hence use computers less) because using computers does not help improve their image or their identity of business professionals, although it may help build a positive image of their IT competence.

Other supporting evidence for this effect was also found 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 information systems were not welcomed. In a similar healthcare setting, physicians were found to resist the implementation of information systems at different levels (Lapointe & Rivard, 2005). One reason for the resistance was 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:

H11: Perceived match between user identity as a business professional and following security rules and policies has a

negative effect on user attitude towards SMB such that the greater the user perceived identity match, the more unfavorable the user attitude will be towards SMB.

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

H12: Perceived match between user identity as a business professional and following security rules and policies has a negative effect on user SMB intention such that the greater user perceived identity match, the less the user intention will be to engage in SMB.

Role Responsibility

Role responsibility refers to obligations or duties one has, based on his or her job function (Hart, 1968, p. 212). This also refers to "duty responsibility" (Corlett, 2009). In an organizational setting, IS security is often not seen as a user's task (Besnard & Arief, 2004). It is more likely viewed as the responsibility of the IS department in a typical organizational structure. Indeed, prior research has indicated that end users do not see themselves as primarily responsible for security problems (Gross & Rosson, 2007). In other words, end users may argue that dealing with security issues is not part of their roles in general business activities such as sales, accounting, operations management, etc. This perception is defined as "role responsibility" in this study.

If end users believe that a task is not their job or responsibility, they may not care about it, especially when the task is in conflict with their "main job" and requires extra effort. Similarly in the IS security context, if end users think security is not their job, they may not care about it; they may very well have a negative attitude towards security measures implemented by the IS department and consequently ignore or bypass security measures when necessary. Therefore, it is hypothesized that:

H13: Perceived role responsibility (in relation to IS security) has a negative effect on user attitude towards SMB such that the greater the extent to which users perceive IS security as their role responsibility, the more unfavorable their attitude will be towards SMB.

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

H14: Perceived role responsibility (in relation to IS security) has a negative effect on user SMB intention such that the greater the extent to which users perceive IS security as their role responsibility, the less user intention will be to engage in SMB.

3.4 Summary

In this chapter, an SMB model was proposed based on Eagly and Chaiken's composite behavioral model. More specifically, it is posited that user SMB intention is determined by attitude towards SMB, which in turn is predicted by four groups of

antecedents: 1) attitude towards targets (IS department and security policy), 2) utilitarian outcome expectations (perceived security risk, perceived accountability, and job performance expectation), 3) normative outcome (workgroup norm), and identity outcome (perceived professional identity match). Workgroup norm and perceived professional identity will also influence SMB intention directly.

Chapter 4

Research Design

4.1 Overview of Research Methods

A survey of currently employed computer users in the workplace was conducted to test the proposed SMB model. Because IS security is often seen as a sensitive matter, prior research in this field has reported issues such as low response rate (Kotulic & Clark, 2004). To overcome these difficulties, the survey used hypothetical scenarios ("vignettes") to solicit participant opinions 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 included some typical security misbehaviors. The use of vignettes has been recommended as one way to ask sensitive questions on surveys (R. M. Lee, 1993). One advantage of this method is that vignettes can present survey respondents with concrete and detailed situations (R. M. Lee, 1993). Watson et al (2002) present a good review and summarize the advantages of using vignettes vis-à-vis direct questions. They: 1) provide greater realism; 2) provide standardized stimuli to all subjects; 3) reduce social desirability bias; and 4) enhance subject involvement. Indeed, the use of vignettes in management and IS literature is not uncommon (Banerjee et al., 1998; D'Arcy et al., 2009; Harrington, 1996; James, Pirim, Boswell, Reithel, & Barkhi, 2008; Siponen & Vance, 2010; Webster & Trevino, 1995). In the organizational behavior literature, a similar method – policy capturing, where

respondents are asked to rate and react to a set of critical incidents or scenarios – was recommended to overcome the reluctance of research participants to reveal their deviant behaviors (Bennett & Robinson, 2003). The key research methods are highlighted in Table 5.

Table 5: Overview of Research Methods

Research Stages	Evaluation	Qualitative and Quantitative Procedures	Target Population
Scenario development	Representativeness, Importance	Interview Literature review	IS Professionals, Academic Experts, and PhD students in MIS
Measurement Item Development	Content validity, Convergent validity, Discriminant validity	Item creation (literature review, interview) Sorting Content validity ratio	IS Professionals, Academic Experts, and PhD students
Pilot Study	Reliability, Validity	Exploratory Factor Analysis (EFA)	MBA students who have prior working experience, employees at a local university Paper-based survey
Final Study	Common method bias	Harman's single factor test Construct-method effect check	
	Model testing	Partial Least Square (PLS)	Computer users in the workplace Paper- and web-based survey

4.2 Security Misbehavior Scenarios

There seems to be no agreement in the literature on the optimal number of scenarios to be included in one study. In a review of business ethics research, it was

found that the number of scenarios cover a wide range of from one to eighteen (Weber, 1992). Although there is no ideal number of scenarios to be used, Weber suggests that researchers should be cautious of having too few or too many scenarios. In the IS literature, the numbers vary from two to eight among sampled studies (Banerjee et al., 1998; D'Arcy et al., 2009; Ellis & Griffith, 2001; Harrington, 1996; James et al., 2008; Malhotra et al., 2004). In these studies, the number of scenarios that survey subjects responded to also varies. For example, in the study by Malhotra et al (2004), each subject responded to one of two scenarios; in the study by Banerjee et al, each subject responded to two of seven scenarios; in the study by James et al (2008), each subject responded to all eight scenarios; in the study by D'Arcy et al (2009), subjects responded to all four scenarios; lastly, in the study by Siponen and Vance (2010), subjects responded to one of three scenarios.

In the current study, participants were asked to respond to one of four scenarios (Appendix 1). The main reason for this approach is the length of the survey. Repeated questions to similar scenarios may cause participant boredom and low response quality.

Scenarios were developed according to guidelines suggested in the literature (Wason et al., 2002): 1) literature review (including academic journals and trade publications); 2) interviews with IS practitioners (including IS professionals at the local university and a large North American consumer electronics retailer); and 3) interviews with academic experts. During the process, the scenarios were chosen or revised so that they met the requirement of representativeness (Aiman-Smith, Scullen, & Barr, 2002),

relevance (Banerjee et al., 1998), and importance (Banerjee et al., 1998). Representativeness refers to the extent to which the scenarios capture real-life security issues; the issues described by the scenarios should also be important for IS security management.

Because the purpose of the scenarios was to provide a realistic and plausible context for survey subjects, the variation of factors in a factorial design (Wason et al., 2002) is not the focus of the current study. Nevertheless, the following elements were included in each scenario: actor (using unisex names), action, security policy, possible risks of the action, and a clear indication that the action violates the policy.

As a result of this process, four initial scenarios (Appendix 1) were developed, each of which reflected security issues related to user authentication and access control, hardware, software, and network, respectively.

Password write-down

The first scenario related to the improper use of passwords. As previously discussed, passwords are one of the most widely adopted security measures. Together with the use of user names or identifiers (ID), it authenticates and allows legitimate users to access systems and resources. A recent practitioner survey found that organizations overwhelmingly depend on this mechanism to manage system access (DTI-UK, 2006). Problems with passwords have been recognized by both practitioners and researchers. One particular problem is that users tend to write passwords down (Anne Adams & Sasse, 1999; Garfinkel, 2000; Stanton et al., 2005; Zviran & Haga, 1999). By doing so, users

risk the organizational data being accessed by unauthorized individuals and other potentially disastrous damages to security. This password-write-down problem was also echoed by practitioners and academic experts during the interview processes, conducted either face-to-face or through emails. For example, one practitioner commented:

"Probably the biggest one [of the problems] is users writing down their passwords somewhere, or organizations that do not enforce strong password will have users use very simple, guessable passwords. Even when strong passwords are enforced, some users will only change 1 letter or number in their passwords to make it easier to memorize."

Unauthorized portable devices for storing and transporting organizational data

The second scenario involves unauthorized mobile devices (hardware) for storing organizational data. There are many risks associated with the use of mobile devices such as USB drives for data storage. A mobile device can easily get lost (so does the data it carries); when infected, it can spread viruses to the organizational network. Security issues with mobile devices have drawn much media attention. For example, it is reported that a second-hand MP3 player bought by an Australian contained some US military data, although the nature and sensitivity of such data is unknown (Anonymous, 2009). There have also been discussions in the media about "the dark side of flash drives" (Ward, 2009). The problem of unauthorized mobile storage devices has also been highlighted in practitioner surveys (BERR, 2008; Cisco, 2006). As one practitioner commented in an

interview, "connecting unauthorized devices [such as USB thumb drives] to their laptops / workstations... [may help] spread [virus] around. This same method could be used to compromise security."

Installation and use of unauthorized software

The third scenario was the installation and use of software that is not authorized nor authenticated by the IS department. By installing unauthorized software, users may inadvertently bring viruses and other malicious software (malware) into the organization's computer network. Practitioner surveys indicated that infection by viruses and malware is one of the top security incidents (BERR, 2008; Richardson, 2007). IS security researchers have also studied this problem. A recent study found that unauthorized use of peer-to-peer (P2P) data sharing software leaked confidential data of financial institutions (Johnson, 2008). Similar security scenarios have been developed and studied in the literature (D'Arcy et al., 2009).

Using insecure public wireless network for business purposes

The fourth scenario was the usage of an insecure pubic wireless network for business purposes, e.g. remotely accessing the organizational network. While wireless connections are a convenient way to access corporate networks, there are security risks involved. Wireless signals may be intercepted by hackers who have the necessary knowledge and skills. It poses a particular risk when users access corporate networks through unsecured public wireless hotspots or a neighbor's open wireless network (BERR, 2008; Cisco, 2006).

4.3 Measurement Item Development Procedures

The survey instrument was adapted from two sources: 1) existing scale borrowed and adapted from relevant literature; 2) constructs that are unique to the IS security and not available in the literature were be developed from scratch. The instrument, including those items that were adapted from relevant literature, were validated to ensure validity and reliability based on the development and validation strategies recommended in the literature (Churchill, 1979; Gerbing & Anderson, 1988; Lewis, Templeton, & Byrd, 2005; Moore & Benbasat, 1991; Straub, 1989; Straub, Boudreau, & Gefen, 2004).

More specifically, the scale was developed in three steps: item creation, sorting, and item rating. In the first step, measurement items were pooled from two sources: existing items adapted from the literature and new items developed from scratch.

In the second step, a sorting procedure similar to the one implemented by Moore and Benbasat (1991) was conducted to select candidate items. The full set from the initial raw instrument was given to a panel of three persons (PhD students in MIS) without any specific order or indication of which construct the items were supposed to measure. Each person individually sorted the items and proposed a name for each construct (i.e. each group of items). They were also asked to give a brief definition of each construct. Based on their comments and suggestions, the items were further revised for the next step.

The last step of scale development was item rating. The items were given to eight persons (PhD students in the MIS and Human Resources Areas) for evaluation. Each was asked to evaluate the items individually and to rate each item on the extent to which the

item measured the construct it was supposed to measure. They were asked to rate each item as "essential", "useful but not essential", or "not useful". Their responses were then used to calculate content validity ratios (CVR) (Lawshe, 1975). Although the original method developed by Lawshe was intended to count only those items in the response category of "essential", in this study both the category of "useful but not essential" and "essential", were used. This less stringent method could be justified because the two response categories were positive indicators of an item's relevance to the construct (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. Some items were revised and new ones were added, based on rater feedback. For example, a new item was added to measure "attitude towards IS department". This item reflects user evaluation of how well the IS department meets their business needs.

4.4 Pilot Study

After the initial development process, a pilot study was conducted to validate the instrument and conduct a preliminary test of the proposed SMB model. Participants were employees and full-time graduate students (MBA and PhD) at the university. The sampled MBA and PhD students have prior working experience in the industry and use computers intensively in their work. Thus they are reasonably good candidates for completing the survey. The employees at the local university were from various administrative departments, including business management services (accounting, payroll, accounts payable etc), continuing education center, and student records. The survey was paper-based and had roughly an equal number of copies for each of the four scenarios.

Survey packages, each of which had a copy of the questionnaire, a Letter of Information/Consent Form, and a coffee card reward, were given to participants in person after the study was approved by the university's research ethics board. The distribution of the four scenarios was randomized in a way that they were first collated (i.e. in a sequence like Scenario 1, 2, 3, 4, 1, 2...) before being put into envelopes. The packages were then distributed sequentially from the stack.

Except for attitude towards SMB, which was measured on a semantic differential scale (1~7) using pairs of adjective words such as bad-good, all other constructs were measured on a Likert-type scale (1 – Strongly Disagree, 7 – Strongly Agree). In total, 104 usable cases were collected from the survey. Because new or modified measurement items are used in this study, several procedures are implemented to validate the scales. An overview of the procedures is shown in Table 6.

Table 6: Scale Validation Steps

Criteria	Quantitative Validation	Qualitative Validation
Face validity		Sorting*
Content validity	Content validity ratio*	Sorting
Reliability	Cronbach's alpha CFA: Composite reliability	
Convergent validity	EFA: factors, loadings CFA: AVE>.5	Sorting
Discriminant validity	EFA: factors, loadings CFA: Square root of AVE> construct correlations	Sorting

* Sorting and content validity ratios are discussed in previous section. CFA = confirmatory factor analysis; EFA = exploratory factor analysis; AVE = average variance extracted.

4.4.1 Reliability and Validity

Reliability was first tested with coefficients of internal consistency – Cronbach's Alpha (Cronbach, 1951). Items with low item-item and item-total correlation (which would raise Alpha if deleted) were to be dropped. The aim was to achieve a Cronbach alpha level of 0.7 or higher (Straub et al., 2004).

Construct validity (discriminant validity and convergent validity) was tested with the exploratory factor analysis (EFA) technique. EFA tests were carried out for each stage of the proposed causal model (Straub et al., 2004): 1) Factors were extracted with eigenvalue > 1; and 2) 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 level. Each EFA test is run with principal component analysis (PCA) and Varimax rotation. During each round of EFA test, if an item was dropped, the internal consistency reliability test was rerun to ensure the Cronbach alpha value met the minimum requirement. As a result of the EFA tests, ten items were subsequently dropped from the item pool.

A PLS-based confirmatory factor analysis (CFA) analysis was also completed to test the reliability and validity of the instrument. More specifically, the measurement model (or "outer model") of a PLS analysis shows 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.

Convergent validity is generally achieved if three criteria are met (Fornell & Larcker, 1981): 1) all item factor loadings should be significant and greater than .70; 2) the 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) the composite reliability index for each construct should be greater than .80. Based on these criteria, the PLS results indicated that a satisfactory level of convergent validity was achieved. All item loadings except one were greater than .70. The loading of the exceptional item (.59) was still considered acceptable given the high loadings of other items for the same construct (Chin, 1998). In addition, all item loadings were significant (two at the .01 and .05 levels; others at the .001 level). Furthermore, the square root of AVE was greater than .707 for each construct. The composite reliabilities of all constructs also met the minimum criterion of .80.

4.4.2 Measurement Items for Final Study

As a result of the above development procedures, two types of measurement items were adopted: general items and scenario-specific items. The difference between these two groups is that the latter was to be responded to by survey participants based on their opinion about specific scenarios. Except for attitude towards SMB, which was measured on a semantic differential scale (1~7) using pairs of adjective words such as bad-good, all other constructs were measured on a Likert-type scale (1 – Strongly Disagree, 7 – Strongly Agree). The complete list of items is provided in Appendix 2.

4.5 Differences among Security Scenarios

Because each participant responded to only one of the four security scenarios, it was necessary to check whether there was any difference among the results from these scenarios. Ideally, the difference should be minimal and all of the scenarios should equally represent typical security management issues.

For this purpose, a simple ANOVA test was conducted on all the constructs in the theoretical model. Indicator scores were averaged as the score of the corresponding construct. The ANOVA test revealed that one of the means – SMB Intention – was significantly different across the four scenarios while others were not. This indicated that the contexts depicted by the four scenarios may indeed have some influence on user SMB intention. In order to partial out this influence, scenarios were included as a control variable in the final study.

4.6 Summary

This chapter presented the overall research procedures and measurement scale development. Four security misbehavior scenarios were developed based on a literature review and input from IS professionals and academic experts. General and scenario-specific measurement items were developed in accordance with the strategies (such as sorting and quantitative content validity index) recommended in the literature. A pilot study was conducted to validate the measurement instrument. The analysis of the pilot study data indicated that the instrument is sufficiently reliable and valid.

Chapter 5

Data Collection and Analysis

5.1 Data Collection Procedures

As introduced in the previous chapter, the targeted population of this study was computer users in the workplace. Two methods were used to collect data: a paper-based survey and a web-based survey. The letter of information and the survey are shown in Appendix 3 and Appendix 4 respectively.

For the paper-based survey, potential participants were approached in person. The selected locations included office buildings and coffee shops in industrial zones. Potential participants were asked if they would be willing to participate in an academic survey. They were also briefed about the purpose of the survey and the compensation they would receive. If they were willing to participate, they would be given a survey package (including consent form, questionnaire, a $10-value coffee card, and a return envelope with mailing address and postage paid). In total, 250 surveys were distributed and 167 (67%) were returned.

For the web-based survey, email addresses were obtained from the websites of a provincial government and a recruiting agency. These email addresses are considered to be public information and thus obtaining consent from the two organizations was not necessary. In total, survey invitations, which explained the purpose of the survey, compensation, and other related information, were emailed to about 2500 individuals

(about 400 of whom were out of office at the time of survey). To address the concerns of privacy and email spam, individual responses were not tracked and no reminder emails were sent. Web-based survey participants were given the option to receive a $10-value coffee card or to enter a lucky draw (top prize $300). Among the targeted individuals, 212 visited the survey websites. However, only 168 of them proceeded to the final step (i.e. clicking the submit button). The response rate of the web-based survey was relatively low (6.5%). Due to the fact that the characteristics of the targeted population were unknown prior to the actual data collection processes, non-response bias is not assessed in this study.

For both paper- and web-based surveys, four different versions (with different security scenarios) were randomly distributed. In the case of the paper-based survey, packages for the four versions were first collated before being put into envelopes. The packages were then distributed sequentially from the stack. There were roughly equal numbers of copies for each of the four scenarios. In the case of the web-based survey, email addresses (without any sorting order) were first divided into four sets (with roughly equal sizes). They were then assigned to one of the four versions of the survey. To partial out potential influences of the two different survey methods on end user SMB intention, a control variable (survey method) will be included in the model testing.

In total, 335 responses were received and 306 of them are usable (data screening is discussed in the next section). Using a regression heuristic of 10 cases per predictor, the sample size requirement should be 10 times either one of the following, whichever is

the greater (Chin, 1998): 1) the block with the largest number of formative indicators, or 2) the dependent variable with the largest number of independent variables impacting it. Based on this heuristic, the required sample size for testing the SMB model would be 100 (attitude towards SMB has ten variables impacting it). Thus the sample size of the current study (N = 306) is sufficient.

5.2 Data Screening

Some responses were incomplete. To screen out unusable data, the following procedures were carried out to treat those cases that had one or more missing values. First, those cases that had more than three (>=4) missing values were dropped from the data set. The reason for this treatment is that the data point might not be reliable if there were too many missing values. Furthermore, if the values of a whole set of items for a single construct was missing, the case was dropped. After the unusable cases were dropped, the remaining incomplete cases were then processed as follows. For essential items (i.e. those items that are included in the main theoretical model), within-subject mean of a construct was used to replace missing values of the same construct. For example, suppose a construct has three items. If the value of Item 3 is missing, it was replaced with the average of Item 1 and 2. For non-essential variables (i.e. those variables, mostly demographic ones, that were not included in the main model), between-subject means were used to replace missing values. For example, if the age value of a case is missing, it will be replaced with the average of all the remaining cases in the sample (note that age is coded as the medium of an age group, e.g. 21 for age group 18-24).

As a result of the above data screening procedures, 29 cases were dropped. This resulted in a usable data set of 306 cases for testing the theoretical model. The demographic characteristics of the participants are summarized in Table 7.

Table 7: Demographic Characteristics of Participants

Demographic	Group	N	Percentage
Gender	Female	124	41%
	Male	182	59%
Survey Method	Online	141	46%
	Paper	165	54%
Age	18-24	21	7%
	25-34	86	28%
	35-44	101	33%
	45-54	63	21%
	55+	35	11%
Education	High School	12	4%
	College	212	69%
	Master's	77	25%
	Doctoral	5	2%
Industry	Education	15	5%
	Information Tech	21	7%
	Healthcare	23	8%
	Professional Services	26	8%
	Manufacturing	29	9%
	Government	45	15%
	Financial/Banking	66	22%
	Other	81	27%
Organization Size	100 or less	50	16%
	100 - 499	50	16%
	500 - 999	35	11%
	1000 - 4999	53	17%
	5000 or more	118	39%

5.3 Preliminary Reliability Check

SPSS procedures were conducted to check measurement reliabilities based on Cronbach's Alpha statistics (as shown in Table 8). Most constructs are reliable, based on the commonly used .70 criterion (ranging from .71 to .94) except for the following three constructs: attitude towards IS department (.64), role responsibility (.60), and severity of sanction (.59). These constructs were subsequently dropped from the model. Although it might affect the explanatory power of the research model, the treatment (i.e. dropping unreliable constructs) is consistent with the literature (Hullett, 2004; Lau & Ng, 2001; Narver & Slater, 1990). Furthermore, the dropped constructs represent a small portion of the original model, which has 12 constructs. The four blocks, i.e. attitude towards target, utilitarian outcomes, normative outcome, and self-identity outcomes remained largely unchanged.

Reexamination of the items in the dropped constructs revealed some possible causes of the low reliabilities. The first possible cause was reverse-coded items. Two of the above three constructs (attitude towards IS department and role responsibility) have two reverse-coded items (out of four respectively). These reverse-coded items may have been incorrectly interpreted by survey participants when they were in the mental flow of answering positively worded questions. For the construct of attitude towards IS department, another possible cause was the wording of the third item ("IT people in my organization know about computers but not business"). This item appears to be inadvertently double-barreled and as a result may have, to some extent, confused survey participants. For sanction severity, the low reliability may be due to the fact that the

evaluation of severity was conditional on the level of sanction certainty. For example, one of the item is "If the management decides to punish me, the punishment would be severe". The question of severity would be irrelevant if participants believed that they would not be punished. Thus the way how participants evaluate the question may have been inconsistent and caused the low reliability as a result.

The item-total statistics provided by the SPSS reliability procedures also revealed that the reliability of two constructs – attitude towards security policy and perceived security risk – could be improved by nearly 5% if an item was dropped from their respective item pool. More specifically, the Cronbach's Alpha level of attitude towards security policy could be improved from .853 to .901; for perceived security risk, it could be improved from .767 to .808. The improvement could be attributed to the fact that the two candidate items for dropping are reverse-coded – similar to the reverse-coding problem for the unreliable constructs discussed above. For these reasons, the two items were subsequently dropped from the item pools of their respective constructs.

Table 8: Preliminary Reliability Check

Construct	Item	Dropped	Cronbach's Alpha	
			Original	Final
Attitude towards IS Dept	AttitudeITD1	c	0.638	-
	AttitudeITD2	c		
	AttitudeITD3	c		
	AttitudeITD4	c		

Note: c: construct dropped; i: item dropped; n.c.: no change

Table 8: Preliminary Reliability Check (cont.)

Construct	Item	Dropped	Cronbach's Alpha	
			Original	Final
Perceived Security Risk	Risk1		0.767	0.808
	Risk2			
	Risk3	i		
	Risk4			
Job Performance Expectation	JobPerf1		0.935	n.c.
	JobPerf2			
	JobPerf3			
	JobPerf4			
Perceived Accountability	Accountability1		0.710	n.c.
	Accountability2			
	Accountability3			
Certainty of Sanction	Certainty1		0.829	n.c.
	Certainty2			
Severity of Sanction	Severity1	c	0.590	-
	Severity2	c		
Workgroup Norm	WrgpNorm1		0.818	n.c.
	WrgpNorm2			
	WrgpNorm3			
	WrgpNorm4			
SMB Intention	Intent1		0.836	n.c.
	Intent2			
	Intent3			
	Intent4			
Attitude towards SMB	AttitudeAcc1		0.939	n.c.
	AttitudeAcc2			
	AttitudeAcc3			
	AttitudeAcc4			
	AttitudeAcc5			
	AttitudeAcc6			

Note: c: construct dropped; i: item dropped; n.c.: no change

Table 8: Preliminary Reliability Check (cont.)

Construct	Item	Dropped	Cronbach's Alpha	
			Original	Final
Role Responsibility	RoleResp1	c	0.600	-
	RoleResp2	c		
	RoleResp3	c		
	RoleResp4	c		
Perceived Identity Match	IDMatch1		0.842	n.c.
	IDMatch2			
	IDMatch3			
	IDMatch4			
Attitude towards Security Policy	AttitudePol1		0.853	0.901
	AttitudePol2			
	AttitudePol3			
	AttitudePol4			
	AttitudePol5	i		

Note: c: construct dropped; i: item dropped; n.c.: no change

5.4 Descriptive Statistics

A summary of descriptive statistics for the remaining constructs is shown in Table 9. The skewness and kurtosis indices indicate that responses are not normally distributed in this study (Appendix 5 provides a comparison of response histograms by scenario). This is one of the reasons (non-normal distributions) why the PLS technique was chosen for model testing and analysis.

Table 9: Descriptive Statistics of Constructs

Construct	Mean	Std. Dev.	Skewness		Kurtosis	
(N=306)			Statistic	z-Score	Statistic	z-Score
Accountability	5.12	1.40	-0.51	-3.63	-0.24	-0.87
Attitude towards SMB	2.99	1.48	0.38	2.75	-0.54	-1.93
Attitude towards Security Policy	5.34	1.31	-0.95	-6.82	0.49	1.78
Sanction Certainty	4.80	1.47	-0.33	-2.37	-0.43	-1.54
Perceived Identity Match	5.63	1.17	-0.92	-6.61	0.98	3.54
SMB Intention	3.31	1.47	0.19	1.36	-0.51	-1.83
Job Performance Expectation	4.53	1.76	-0.47	-3.38	-0.71	-2.55
Perceived Security Risk	5.25	1.22	-0.59	-4.21	0.21	0.76
Workgroup Norm	3.10	1.38	0.30	2.16	-0.32	-1.14

5.5 Common-Method Bias Check

Common-method bias, i.e. variance being attributable to measurement method rather than the constructs, is a potential problem in behavioral research (Podasakoff, MacKenzie, Lee, & Podsakoff, 2003). In this study, such bias may be present because self-reported survey was the data collection method used. Although prior research indicates that the effect may not be substantial (Malhotra, Kim, & Patil, 2006), checking for such method bias is strongly recommended in MIS literature (Straub et al., 2004; Straub & Burton-Jones, 2007).

Two procedures were implemented in this study to check for common-method bias. First, a Harman's single-factor test (Podasakoff et al., 2003; Podasakoff & Organ, 1986) was applied. In this test, all the measurement items were included in a single

exploratory factor analysis (EFA). The unrotated factor solution indicated that: 1) no single factor emerged from the factor analysis; and 2) no single general factor accounted for the majority of the covariance (the most covariance explained by one factor was 34%). 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. In this test, a partial least square (PLS) model was created with a common method factor (construct). The measurement items of all the constructs in the theoretical model were included as the indictors of this method factor. Each indicator was also converted into a single-indicator construct. Thus in this model, the variance of a single-indicator construct is "caused" by two factors: the theoretical construct that the indicator is supposed to measure and the common method factor. Two criteria were used to judge whether common method bias was a serious problem: 1) whether the path coefficients of the method factor were significant; and 2) whether the differences between the variances explained by those theoretical constructs and by the common method factor were sufficiently large. The result is shown in Table 10.

Table 10: Common Method Bias Analysis

Construct	Items	(S)		Var. (S)	(M)		Var. (M)
Attitude toward SMB	AttAct1	0.895	***	0.801	0.012		0.000
	AttAct2	0.866	***	0.745	0.030		0.001
	AttAct3	0.929	***	0.862	-0.004		0.000
	AttAct4	0.925	***	0.862	-0.073		0.006
	AttAct5	0.822	***	0.680	0.028		0.001
	AttAct6	0.823	***	0.674	0.007		0.000

Note: S – Substantial factor (construct) loading; M – Method factor loading; Var – Variance.

Table 10: Common Method Bias Analysis (cont.)

Construct	Items	(S)		Var. (S)	(M)		Var. (M)
Attitude toward Security Policy	AttPol1	0.919	***	0.846	0.088		0.008
	AttPol2	0.882	***	0.769	-0.023		0.001
	AttPol3	0.910	***	0.820	0.137		0.017
	AttPol4	0.929	***	0.851	0.012		0.000
Perceived Accountability	Acc1	0.827	***	0.696	-0.016		0.000
	Acc2	0.629	***	0.389	-0.158		0.024
	Acc3	0.929	***	0.851	0.169		0.025
Sanction Certainty	Certainty1	0.944	***	0.890	0.040		0.001
	Certainty2	0.905	***	0.823	-0.040		0.001
Perceived Identity Match	IDMatch1	0.847	***	0.713	-0.046		0.002
	IDMatch2	0.897	***	0.802	-0.028		0.001
	IDMatch3	0.826	***	0.680	0.009		0.000
	IDMatch4	0.754	***	0.559	0.082		0.006
SMB Intention	Intent1	0.760	***	0.582	0.139		0.017
	Intent2	0.898	***	0.814	-0.081		0.007
Job Performance Expectation	JobPerf1	0.742	***	0.548	0.163		0.025
	JobPerf2	0.927	***	0.860	-0.020		0.001
	JobPerf3	0.997	***	0.993	-0.069		0.004
	JobPerf4	0.986	***	0.969	-0.057		0.003
Perceived Security Risk	Risk1	0.998	***	0.995	0.103		0.010
	Risk2	0.999	***	0.994	0.094		0.007
	Risk4	0.628	***	0.380	-0.065		0.004
Workgroup Norm	WkgpNorm1	0.666	***	0.443	0.131		0.014
	WorkNorm2	0.826	***	0.688	0.003		0.000
	WorkNorm3	0.979	***	0.948	-0.236		0.049
	WorkNorm4	0.758	***	0.573	0.090		0.007
Average		0.863		0.753	0.013		0.008

Note: S – Substantial factor (construct) loading; M – Method factor loading; Var – Variance.

The result indicated that common method bias was not a problem. On the one hand, the average of the variances explained by these theoretical constructs is .753, while the average of the variances explained by the method factor was .008. The ratio of these two types of variance is 100:1, 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 all loadings of the method factor are not significant.

5.6 Hypothesis Testing

The theoretical SMB model was tested using the partial least square (PLS) approach. This method was chosen for the following reasons: 1) it does not assume any distribution form for measure variables (Chin, 1998); 2) it has minimal demands on measurement scales, which could be interval or ratio (Chin, 1998); and 3) it can be used for both exploratory and confirmatory research (Chin, 1998; Gefen, Straub, & Boudreau, 2000).

As discussed earlier, the pilot study revealed that the influence of different scenarios on SMB intention was significant. As such, scenarios were included as a control variable in the final study. In addition, a number of other factors were also included as control variables: 1) age; 2) gender; 3) position, which is based on the assumption that the more senior positions end users hold, the more likely they are to violate security policies; and 4) research method, which is based on the fact that two survey methods – web-based and paper-based – were used in the final study and the influence, if any, should be partialed out.

Each of the control variables was modeled as follows. Age is a construct with a single indicator, which was coded as the medium point of an age group (e.g. 21 for the 18-24 age group). Both gender and research methods are also single-indicator constructs. Both indicators were coded as binary (female = 0, male = 1; online version = 0, paper version = 1). Scenario is a formative construct with three indicators, each of which represents one of the four scenarios. Each of the indicators was coded with binary values (0: the scenario was not used, 1: the scenario was used). Note that for the scenario construct, only three indicators (i.e. scenarios) were needed. The fourth one would only provide redundant information.

5.6.1 Measurement Model

The measurement model (or "outer model") shows 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.

Convergent validity is generally achieved if three criteria are met (Fornell & 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.

Table 11: PLS - Outer Loadings

Item <- Construct	Loading	T Stats	p
Accountability1 <- Accountability	0.80	9.24	0.000
Accountability2 <- Accountability	0.84	13.64	0.000
Accountability3 <- Accountability	0.72	5.31	0.000
AttitudeAcc1 <- AttAct	0.91	41.25	0.000
AttitudeAcc2 <- AttAct	0.89	30.56	0.000
AttitudeAcc3 <- AttAct	0.93	54.21	0.000
AttitudeAcc4 <- AttAct	0.86	26.91	0.000
AttitudeAcc5 <- AttAct	0.84	25.06	0.000
AttitudeAcc6 <- AttAct	0.83	15.39	0.000
AttitudePol1 <- AttPol	0.86	9.28	0.000
AttitudePol2 <- AttPol	0.91	9.85	0.000
AttitudePol3 <- AttPol	0.82	8.09	0.000
AttitudePol4 <- AttPol	0.93	12.20	0.000
Certainty1 <- Certainty	0.90	14.08	0.000
Certainty2 <- Certainty	0.95	16.86	0.000
IDMatch1 <- IDMatch	0.89	13.25	0.000
IDMatch2 <- IDMatch	0.92	19.25	0.000
IDMatch3 <- IDMatch	0.82	11.36	0.000
IDMatch4 <- IDMatch	0.68	5.43	0.000
Intent1 <- Intention	0.93	47.56	0.000
Intent2 <- Intention	0.88	19.20	0.000
JobPerf1 <- JobPerf	0.87	26.09	0.000
JobPerf2 <- JobPerf	0.90	21.24	0.000
JobPerf3 <- JobPerf	0.95	36.68	0.000
JobPerf4 <- JobPerf	0.94	34.34	0.000
Risk1 <- Risk	0.91	18.31	0.000
Risk2 <- Risk	0.92	24.00	0.000
Risk4 <- Risk	0.75	8.01	0.000

Table 11: PLS - Outer Loadings (cont.)

Item <- Construct	Loading	T Stats	p
WkgpNorm1 <- WkgpNorm	0.78	13.68	0.000
WkgpNorm2 <- WkgpNorm	0.82	15.48	0.000
WkgpNorm3 <- WkgpNorm	0.78	9.56	0.000
WkgpNorm4 <- WkgpNorm	0.84	20.93	0.000

As shown in Table 11, all but one item loading was greater than .70. The exception was IDMatch4, of which the loading (.68) was slightly lower than the .70 threshold. The loading was still considered acceptable given the high loadings of other items for the same construct (Chin, 1998). In addition, all item loadings, including that of IDMatch4, were significant ($p < .001$). Furthermore, as shown in Table 12, the square root of AVE was greater than .707 for each construct. The composite reliabilities of all constructs also met the criterion of .80. Based on the above criteria, the PLS results indicated that a satisfactory level of convergent validity was achieved.

Discriminant 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 & Larcker, 1981). As shown in Table 12, the highest construct correlation is .61 and the lowest square root of AVE is .79. Furthermore, item loadings on their corresponding constructs are greater than their cross loadings on other constructs (Table 13). Thus, the criterion for sufficient discriminant validity was also met in this study.

Table 12: PLS Measurement Model – Construct Correlations

Construct		CR	1	2	3	4	5	6	7	8	9
1	Acc	0.83	**0.79**								
2	AtA	0.95	-0.42	**0.88**							
3	AtP	0.93	0.53	-0.25	**0.88**						
4	Crt	0.92	0.46	-0.31	0.35	**0.92**					
5	IDM	0.90	0.27	-0.29	0.23	0.28	**0.83**				
6	Int	0.90	-0.41	0.62	-0.29	-0.30	-0.30	**0.91**			
7	Job	0.95	-0.41	0.39	-0.23	-0.08	-0.13	0.44	**0.92**		
8	Rsk	0.90	0.61	-0.36	0.61	0.45	0.26	-0.36	-0.21	**0.86**	
9	WN	0.88	-0.60	0.54	-0.52	-0.47	-0.25	0.54	0.47	-0.49	**0.81**

Note: CR = Composite Reliability; Off diagonal numbers are inter-construct correlations; Diagonal numbers are the square roots of AVE (average variance extracted). Construct: 1. Accountability 2. Attitude towards SMB 3. Attitude towards Security Policy 4. Sanction Certainty 5. Perceived Identity Match 6. SMB Intention 7. Job Performance Expectation 8. Perceived Security Risk 9. Workgroup Norm

Table 13: PLS – Cross Loadings

Construct & Item		1	2	3	4	5	6	7	8	9
1	Acc1	**0.80**	-0.29	0.48	0.48	0.22	-0.32	-0.32	0.57	-0.52
	Acc2	**0.84**	-0.42	0.39	0.30	0.24	-0.35	-0.37	0.42	-0.51
	Acc3	**0.72**	-0.23	0.42	0.36	0.17	-0.29	-0.25	0.51	-0.38
2	AtA1	-0.34	**0.91**	-0.26	-0.25	-0.29	0.61	0.35	-0.33	0.48
	AtA2	-0.38	**0.89**	-0.21	-0.31	-0.29	0.58	0.34	-0.33	0.48
	AtA3	-0.39	**0.93**	-0.24	-0.28	-0.26	0.60	0.33	-0.32	0.50
	AtA4	-0.35	**0.86**	-0.21	-0.27	-0.20	0.48	0.29	-0.31	0.45
	AtA5	-0.35	**0.84**	-0.19	-0.23	-0.18	0.50	0.45	-0.29	0.48
	AtA6	-0.38	**0.83**	-0.20	-0.31	-0.29	0.49	0.30	-0.29	0.46

Construct: 1. Accountability 2. Attitude towards SMB 3. Attitude towards Security Policy 4. Sanction Certainty 5. Perceived Identity Match 6. SMB Intention 7. Job Performance Expectation 8. Perceived Security Risk 9. Workgroup Norm

Table 13: PLS – Cross Loadings (cont.)

Construct & Item		1	2	3	4	5	6	7	8	9
3	AtP1	0.45	-0.19	**0.86**	0.27	0.27	-0.25	-0.15	0.51	-0.40
	AtP2	0.51	-0.26	**0.91**	0.31	0.21	-0.28	-0.24	0.59	-0.51
	AtP3	0.37	-0.18	**0.82**	0.27	0.11	-0.23	-0.19	0.44	-0.36
	AtP4	0.52	-0.24	**0.93**	0.37	0.21	-0.25	-0.20	0.59	-0.53
4	Crt1	0.37	-0.24	0.34	**0.90**	0.21	-0.27	-0.07	0.39	-0.42
	Crt2	0.47	-0.33	0.31	**0.95**	0.30	-0.28	-0.08	0.43	-0.45
5	IDM1	0.27	-0.29	0.21	0.25	**0.89**	-0.29	-0.14	0.25	-0.21
	IDM2	0.23	-0.29	0.22	0.28	**0.92**	-0.26	-0.14	0.25	-0.25
	IDM3	0.21	-0.21	0.21	0.24	**0.82**	-0.26	-0.07	0.23	-0.20
	IDM4	0.17	-0.12	0.09	0.15	**0.68**	-0.18	-0.07	0.10	-0.16
6	Int1	-0.41	0.64	-0.28	-0.23	-0.30	**0.93**	0.47	-0.33	0.52
	Int2	-0.33	0.47	-0.23	-0.32	-0.25	**0.88**	0.32	-0.33	0.45
7	Job1	-0.43	0.42	-0.26	-0.13	-0.13	0.47	**0.87**	-0.23	0.45
	Job2	-0.34	0.32	-0.21	-0.06	-0.12	0.38	**0.90**	-0.21	0.41
	Job3	-0.33	0.33	-0.18	-0.05	-0.10	0.37	**0.95**	-0.18	0.42
	Job4	-0.35	0.35	-0.18	-0.04	-0.13	0.38	**0.94**	-0.16	0.42
8	Rsk1	0.59	-0.31	0.60	0.37	0.23	-0.33	-0.16	**0.91**	-0.44
	Rsk2	0.60	-0.32	0.58	0.36	0.23	-0.33	-0.19	**0.92**	-0.44
	Rsk4	0.39	-0.30	0.39	0.42	0.21	-0.28	-0.20	**0.75**	-0.39
9	WN1	-0.44	0.43	-0.49	-0.52	-0.24	0.44	0.31	-0.47	**0.78**
	WN2	-0.54	0.41	-0.45	-0.49	-0.25	0.43	0.31	-0.49	**0.82**
	WN3	-0.45	0.39	-0.31	-0.26	-0.15	0.39	0.32	-0.28	**0.78**
	WN4	-0.49	0.50	-0.42	-0.25	-0.18	0.46	0.54	-0.35	**0.84**

Construct: 1. Accountability 2. Attitude towards SMB 3. Attitude towards Security Policy 4. Sanction Certainty 5. Perceived Identity Match 6. SMB Intention 7. Job Performance Expectation 8. Perceived Security Risk 9. Workgroup Norm

5.6.2 Structural Model

The hypotheses were assessed by examining the parameters provided by the PLS structural model. More specifically, R^2 values of the 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 re-sampling procedure (with 300 samples) was carried out to estimate the significance of paths in the structural model. The result is shown in Table 14.

Among the control variables, scenarios have a significant influence on end user SMB intention (beta = -.16, $p < .05$) as expected. The influences of other control variables, including age, gender, job position, and survey method, were not significant.

As shown Table 14, the R^2 value of .49 indicates that the theoretical model explained a substantial amount of variance in user SMB intention. In addition, 36 percent of the variance for attitude towards SMB is accounted for by the model. Given the minimum 10-percent criterion (Falk & Miller, 1992, p. 80), which suggests that the R^2 value of an independent variable should be at least 10% in order to make any meaningful interpretation, the theoretical model demonstrates substantive explanatory power.

Table 14: PLS - Path Coefficients

Dependent Variable (DV)	Independent Variable (IV)	Path Coefficient	T Stats	p Value	R^2
Attitude towards SMB	Accountability	-0.06	0.422	n.s.	0.36
	Attitude towards Security Policy	0.14	1.187	n.s.	
	Sanction Certainty	-0.05	0.370	n.s.	
	Perceived Identity Match	-0.14	1.316	n.s.	
	Job Performance Expectation	0.17	1.710	0.044	
	Perceived Security Risk	-0.13	0.868	n.s.	
	Workgroup Norm	0.38	3.177	0.001	
SMB Intention	Age*	-0.05	0.572	n.s.	0.49
	Attitude towards SMB	0.41	3.219	0.001	
	Gender *	0.04	0.493	n.s.	
	Perceived Identity Match	-0.10	1.292	n.s.	
	Position *	0.08	0.952	n.s.	
	Scenario *	-0.16	2.029	0.022	
	Survey Method *	0.03	0.411	n.s.	
	Workgroup Norm	0.24	1.870	0.031	

Notes: *: control variable.

Both attitude towards SMB and workgroup norm had strong direct effects on SMB intention, as demonstrated by the significant path coefficients (attitude towards SMB: beta = .41, $p < .001$; workgroup norm: beta = .24, $p < .05$). Thus, H1 and H10 are supported. H4 and H9 are also supported, suggesting that job performance expectation (beta = .17, $p < .05$) and workgroup norm (beta = .38, $p < .001$) are significant predictors of attitude towards SMB. The overall model is shown in Figure 3.

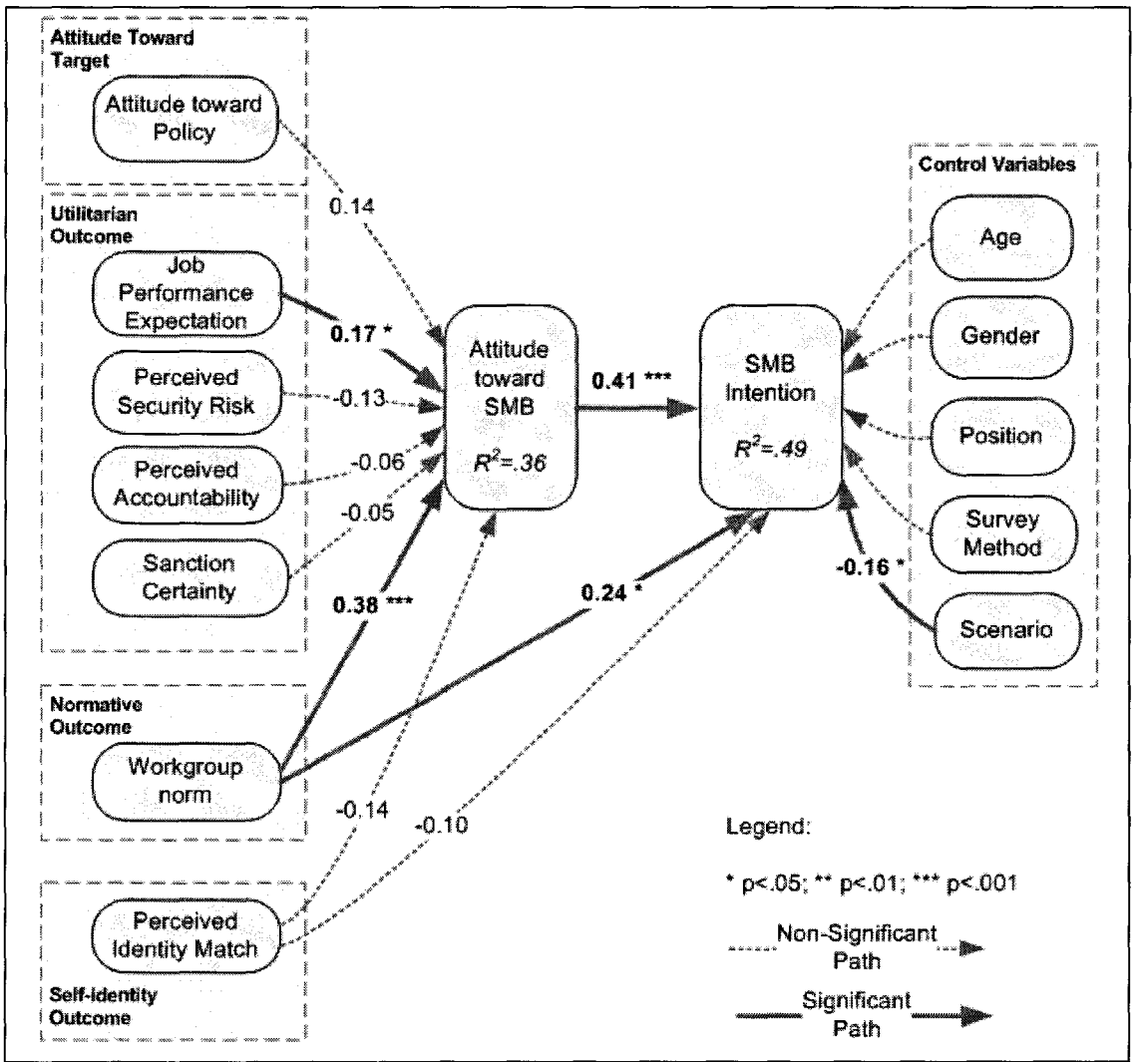


Figure 3: PLS Analysis Results

Contrary to what is predicted by the theoretical model, the following constructs do not have a significant impact on attitude towards SMB: attitude towards security policy, perceived security risk, perceived accountability, sanction certainty, and perceived identity match. Furthermore, perceived identity match does not have a

significant effect on SMB intention, contrary to what is expected. A summary of the hypothesis testing results is shown in Table 15.

Table 15: Summary of Hypothesis Testing

Hypotheses		**Supported**
H1:	User attitude towards SMB has a positive effect on SMB intention.	Yes
H2:	User attitude towards IS department has a negative effect on attitude towards SMB.	N.T.
H3:	User attitude towards security policy has a negative effect attitude towards SMB.	No
H4:	Job performance expectation as a result of SMB has a positive effect on user attitude towards SMB.	Yes
H5:	Perceived security risk has a negative effect on user attitude towards SMB	No
H6:	Perceived accountability has a negative effect on user attitude towards SMB.	No
H7:	Sanction certainty has a negative effect on user attitude towards SMB.	No
H8:	Sanction severity has a negative effect on user attitude towards SMB.	N.T.
H9:	Workgroup norm (framed as in favor of SMB) has a positive effect on user attitude towards SMB.	Yes
H10:	Workgroup norm has a positive effect on user SMB intention.	Yes
H11:	Perceived match between the identity as a business professional and following security rules and policies has a negative effect on user attitude towards SMB.	No
H12:	Perceived identity match has a negative effect on user SMB intention.	No
H13:	Perceived role responsibility has a negative effect on user attitude towards SMB.	N.T.
H14:	Perceive role responsibility has a negative effect on user SMB intention.	N.T.

Note: N.T.: not tested due to low construct reliability.

5.7 Effect Sizes and Saturated Model

The impact of a particular independent variable on a dependent variable can be determined by its effect size, which is calculated as $f^2 = (R^2_{included} - R^2_{excluded})/(1 - R^2_{included})$ (Chin, 1998). $R^2_{included}$ and $R^2_{excluded}$ are the R^2 on the dependent variable when the independent variable is included or excluded in the PLS model respectively. A pseudo F-test, $F = f^2 \times (n - k - 1)$, where n is the sample size and k is the number of independent variables, was then carried out to check whether the change of R^2 is significant (Mathieson, Peacock, & Chin, 2001). The results of each of the alternative models are shown in Table 16.

Table 16: Effect Sizes

Dependent Variable	Independent Variable	R^2		ΔR^2	f^2	F Test	P
		Excluded	Included				
SMB Intention	Scenario	0.47	0.49	0.02	**0.04**	11.76	0.001
	Attitude toward SMB	0.38	0.49	0.11	**0.22**	64.49	0.000
	Workgroup Norm	0.45	0.49	0.04	**0.08**	23.29	0.000
Attitude towards SMB	Job Performance Expectation	0.34	0.36	0.02	**0.03**	9.47	0.002
	Workgroup Norm	0.29	0.36	0.07	**0.11**	32.59	0.000

The following criteria can be used to interpret the effect sizes: 1) for a small effect size, $.02 < f^2 \leq .15$; 2) for a medium effect size, $.15 < f^2 \leq .35$, and 3) for a large effect size, $f^2 > .35$ (Chin, 1998; Cohen, 1988). Thus attitude towards SMB and workgroup norm have a medium and small effect on SMB intention respectively; job performance

expectation and workgroup norm have a small effect on attitude towards SMB respectively. Scenario has a small effect (.05) on SMB intention.

Following the practice in the literature (Anderson & Gerbing, 1988; Hassanein & Head, 2007; Karahanna & Straub, 1999), a saturated model was also tested. In this saturated model, new paths were added to link all independent variables to the two dependent variables: attitude towards SMB and SMB intention. The result suggested that none of the additional links was significant.

5.8 Post-Hoc Analysis

5.8.1 Comparison of Scenarios

As shown in the full model test, security scenarios had a significant influence on user SMB intention. For the purpose of comparing the differences among the four scenarios, the full model was also tested for each scenario (Table 17). The sample size for each scenario ranged from 73 to 79. Although the sample size requirement discussed earlier has been met (note the largest block in the tested model has seven independent variables), caution should be taken when interpreting the results as the samples are at the borderline of the requirement for PLS analysis. Nevertheless, the results shed some light on the context-dependent nature of security misbehaviors. In each of the four scenarios, different sets of factors have significant effect on attitude towards SMB and behavioral intention. However, the effect of job performance expectation and workgroup norm on attitude towards SMB and the effect of attitude towards SMB and workgroup norm on SMB intention were nearly universal across four scenarios..

Table 17: Full Model Testing by Scenario

Dependent Variable	Independent Variable	H (N=73)	P (N=77)	S (N=79)	W (N=77)	ALL (N=306)
Attitude towards SMB	Attitude towards Policy	**0.18**	**0.27**	-0.02	-0.06	0.14
	Job Performance Expectation	**0.13**	**0.21**	**0.25**	0.12	**0.17**
	Perceived Accountability	-0.13	0.12	**-0.20**	0.15	-0.06
	Perceived Identity Match	0.04	**-0.22**	-0.17	**-0.20**	-0.14
	Perceived Security Risk	0.12	-0.27	-0.13	-0.20	-0.13
	Sanction Certainty	-0.13	-0.04	0.04	-0.12	-0.05
	Workgroup Norm	**0.61**	**0.34**	0.16	**0.36**	**0.38**
SMB Intention	Attitude towards SMB	**0.50**	**0.42**	**0.41**	**0.45**	**0.41**
	Workgroup Norm	0.11	**0.29**	**0.24**	**0.30**	**0.24**
	Perceived Identity Match	-0.18	-0.04	-0.15	**-0.13**	-0.10
	Position^	0.12	0.08	**0.24**	-0.17	0.08
	Survey Method^	0.03	-0.06	**0.19**	-0.08	0.03
	Age^	**-0.15**	-0.01	-0.03	-0.05	-0.05
	Gender^	0.09	-0.09	0.10	-0.04	0.04
	Scenario^	-	-	-	-	**-0.16**

Note: H - Hardware scenario (USB); P - Password scenario; S - Software scenario; W - Wireless scenario; ^ Control variable. Bolded path coefficients are significant at .05 level; others are non-significant.

5.8.2 Asymmetric Effects of Independent Variables

Reexamination of the results of the model test suggested that the non-significant independent variables, including perceived security risk, sanction certainty, perceived accountability, perceived identity match, and attitude towards policy, might have asymmetric effects (Sirdeshmukh, Singh, & Sabol, 2002) on the dependent variables –

attitude towards SMB and SMB intention. For example, low perceived security risk and high perceived security risk might have a differential impact on end user attitude towards SMB. This differential impact can be best depicted in a diagram. As shown in Figure 4, end users who have a high security risk perception will very likely have an unfavorable attitude towards SMB (the right side) and the linear relationship between the two variables appears to be strong. However, those who have a low security risk perception may not have either favorable or unfavorable attitude towards SMB. Furthermore, the correlation between security risk perception and attitudes towards SMB was not clear. In other words, high security risk perception appears to have a strong impact on end user attitude towards SMB while low security risk perception does not. To put it in another way, high security risk perception may prevent end users from engaging in SMBs; however, low security risk perception does not necessarily cause or motivate end users to engage in SMBs. Other non-significant independent variables appear to have similar patterns (see Appendix 6 for details). These non-significant independent variables can be viewed as "inhibitors", which act solely to discourage the behavior (Cenfetelli, 2004a).

To demonstrate the asymmetrical effects of these inhibiting factors, the following two-step procedures (Cenfetelli, 2004b) were carried out. First, the sample was split into two sub-samples at the midpoint[2] (i.e. 4 on a 7-point Likert scale) of an inhibitor. For example, when the effect of perceived security risk was to be analyzed, one sub-sample

[2] The midpoint (4) of the 7-point Likert scales was chosen over samples means because the purpose was to compare two opposing groups, e.g. unfavorable vs. favorable and no risk vs. high risk. To use sample means is basically to compare "below average" and "above average". However, those who scored "below average" did not necessarily have an "unfavorable" attitude or a perception of "no risk". Thus midpoint was more appropriate than sample mean in this case.

would include those end users who perceived a "below or equal 4" security risk and the other sub-sample would include those end users who perceived an "above 4" security risk. Second, the bivariate correlation between the inhibitor and the dependent variable in question was analyzed for each of the sub-samples. For example, a correlation between perceived security risk and attitude towards SMB was calculated for each of the above two sub-samples. The two-step procedure was repeated for all other inhibiting factors. The results were shown in Table 18. For the two sub-samples, the probabilities of an end user engaging in the SMB are also provided.

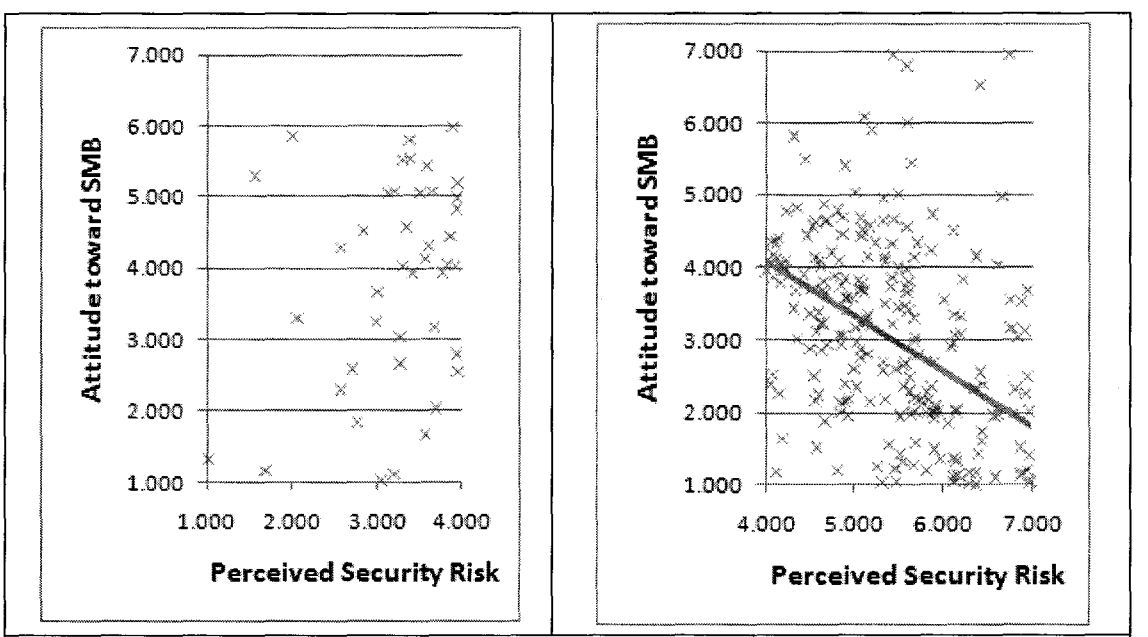


Figure 4: Matrix Plot – Perceived Security Risk vs. Attitude towards SMB

Table 18: Asymmetric Effects of Inhibitors

DV	IV	ALL	Sub-sample (Low, <=4)			Sub-sample (High, >4)		
		r	r	N	P_L	r	N	P_H
Attitude towards SMB	Perceived Accountability	**-0.39**	-0.12	76	0.34	**-0.40**	230	0.22
	Attitude towards Policy	**-0.31**	0.10	49	0.43	**-0.33**	257	0.22
	Sanction Certainty	**-0.30**	-0.12	110	0.34	**-0.28**	196	0.20
	Perceived Identity Match	**-0.27**	-0.15	33	0.27	**-0.23**	273	0.25
	Perceived Security Risk	**-0.41**	0.21	52	0.38	**-0.50**	254	0.22

Note: Boldface indicates significant at .05 level; r: Correlation; P_L: Conditional probability of SMB (i.e. Intention > 4) for below-midpoint sub-sample (i.e. IV<=4); P_H: Conditional probability of SMB (i.e. Intention > 4) for above-midpoint sub-sample (i.e. IV >4); N: sample size.

As demonstrated in Table 18, all correlations of the below-midpoint inhibitors with attitude towards SMB were not significant while all correlations of the above-midpoint inhibitors with attitude towards SMB were all significant. Thus, the results generally support the asymmetric effects of inhibitors such as perceived security risk. Furthermore, for all the inhibitors, end users in the high sub-sample were more likely to engage in SMBs (the conditional probabilities are all lower than that of the low sub-samples). This further supports the findings of asymmetric effects of the inhibitor independent variables.

5.9 Summary

This chapter presented statistical tests that were carried out on the data collected in the survey. Before testing the proposed SMB model, the data were first screened and

subjected to internal consistency reliability analysis and exploratory factor analysis for scale validation. The results suggest that the scales were sufficiently reliable and valid. Two tests – Harman's single-factor test (Podasakoff et al., 2003; Podasakoff & Organ, 1986) and construct-method variance analysis (Liang et al., 2007) – were conducted to check common method variance. Both tests verified that common method bias is not a problem in the current study.

The SMB model was tested with the PLS technique. The reliability and validity of the constructs were further verified in the PLS measurement model. The structural model suggested that attitude towards SMB and workgroup norm have a significant influences on end user SMB intention. Attitude towards SMB in turn is significantly influenced by workgroup norm and job performance expectation. Although other variables did not have a significant impact on SMB in the PLS model testing, some evidence was found to support the asymmetric effects of these variables.

Chapter 6

Discussion and Conclusions

Overall, the theoretical model was successful in capturing the main antecedents of user SMB intention. With the effects of age, gender, job position, survey method, and security scenario being controlled for, both attitudes towards SMB and workgroup norm have a significant influence on SMB intention. In turn, user attitude towards SMB is influenced by workgroup norm and job performance expectation. Furthermore, the significant effect of different security scenarios also suggests that end user decisions on security misbehavior may be context-dependent. In other words, users may behave differently under different circumstances involving information security. Contrary to the predictions of the composite behavioral model (CBM), however, several factors do not have a significant impact on either user attitude towards SMB or behavioral intention. These factors include user attitude towards security policy, perceived security risk, perceived accountability, sanction certainty, and perceived identity match. In the rest of this chapter, the above key findings are further discussed in terms of theoretical contributions and practical implications. It then concludes with a discussion of limitations and future research.

6.1 Key Findings

6.1.1 Antecedents of User SMB Intention

As predicted by the model, user intention to engage in SMB is influenced by *attitude towards SMB* and *workgroup norm*. The significant effect of attitude towards SMB suggests that the more favorable attitude users have towards SMBs, the more likely they will engage in such behaviors. This is consistent with prior technology-acceptance research based on the theory of planned behavior (Ajzen, 1991) and its variants. The significant effect of workgroup norm suggests that end users may simply follow the opinion and practices of their peers to engage in security misbehaviors. This is also consistent with prior technology-acceptance research based on the theory of planned behavior (Ajzen, 1991) and its variants, although this line of research typically conceptualizes the norm as "social norm" or "subjective norm" and is operationalized as the norms held by those people who are important to the actor in question. The finding is also consistent with other research in the IS security literature. For example, subjective norm was found to influence user intention to comply with security policies (Herath & Rao, 2009). Subjective norm was operationalized in Herath and Rao's study as the norm held by top management, boss, colleagues, IS security department, and other computer specialist. However, the weights of top management and IS security department were not significant. This essentially supports the conceptualization of workgroup norm in the present study. The finding appears to echo relevant research in the organizational behavior literature as well. For example, workgroups in organizational settings have the

ability to influence individual members' antisocial actions (Robinson & O'Leary-Kelly, 1998).

Taken together, the significant influences of these two factors suggest that two paths may lead to user security misbehavior. One path is where users have their own evaluation of security-related actions. They may have a favorable or unfavorable opinion about those actions. Either way, their own opinions will in part determine their decisions about whether or not to engage in those actions. The other path is where users simply follow the opinions and practices of their peers in the same workgroup. In this case, they may not have a clear attitude towards those behaviors. In other words, they may not know or do not care whether those behaviors are right or wrong as long as their peers are doing the same.

6.1.2 Antecedents of User Attitude towards SMB

The results indicate that user attitude towards SMB is significantly influenced by *job performance expectation* and *workgroup norm*. The significant influence of job performance expectation on attitude towards SMB confirms that job performance is an important decision factor when users deal with security issues during their routine business activities. If an action can help users carry out their business tasks and improve productivity, users will have a favorable attitude towards and subsequently engage in the action even if such an action violates organizational security policies. This finding is basically consistent with the theories in the technology adoption literature (e.g. Davis, 1989). This finding can also be explained from the goal-oriented behavioral perspective

(Heckhausen & Kuhl, 1985). Job performance is the goal that users try to accomplish by using necessary means. For them security is often seen as a non-task and thus not a goal that they will try to pursue. Thus violating security measures or policies would not be a big problem for users if such actions can help them do their job. In other words, such actions (i.e. violating security policies) may be seen as legitimate means to their desired ends (i.e. job performance).

Perhaps the most interesting findings of this study about the antecedents of attitude towards SMB are the strong and significant effects of workgroup norm in comparison to the relatively small impact of utilitarian outcome expectations (except job performance expectation) and attitude towards security policies. Although it seems to be surprising at first glance, the different effects are not totally inconsistent with other research in the information systems literature. This may be explained by the impact of job relevance and user expertise. Literature suggests that these two factors moderate the way in which users evaluate the use of information technology (Bhattacherjee & Sanford, 2006). The less relevant an IS application is to their job and the less expertise they have, the more likely they will 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 a system) by themselves. This is arguably applicable in an IS security context. End users often lack security knowledge and skills and they may also view security 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 at hand. In fact, it has been

suggested that users may be more inclined to follow practices and advice of their coworkers (Dourish et al., 2004; Wood, 2000). In particular, users tend to "delegate" security issues to other individuals they know (Dourish et al., 2004).

6.1.3 Contextual Factors

The data analysis revealed that situational contexts also have significant effect on user SMB intention. As indicated in the model testing, in each of the four scenarios, different sets of factors have significant effect on attitude towards SMB and behavioral intention. However, the effect of job performance expectation and workgroup norm on attitude towards SMB and the effect of attitude towards SMB and workgroup norm on SMB intention are nearly universal across the four scenarios. A simple ANOVA analysis indicated that the means of SMB intention across the four scenarios are significantly different (USB drive: 4.1; Password: 2.7; Software: 3.2; and Wireless 3.3; $p < .001$). It appeared that end users are more likely to engage in SMB in the USB drive scenario.

While further research is required to investigate the effect of situational context, it suggests that some other factors embedded in the security scenarios are unaccounted for by the proposed SMB model. One possible explanation is the different views of whether a behavior can be deemed as a "security issue" held by IS managers and users. For example, users may believe that there is nothing wrong in using a USB drive for work purposes while IS managers may view such an action as a threat to security. Even if the security risk of using a USB drive is high, users may believe that it is the job of the IS department to manage the risk rather than simply ban the use of such technology. Future

research may be conducted to identify the behaviors deemed as SMBs not only from IS management perspective but also from the user's perspective.

6.1.4 Other Factors

The empirical test with PLS method indicated that several factors in the original proposed model are not significant. These non-significant factors include attitude towards security policy, perceived identity match, perceived security risk, perceived accountability, and sanction certainty. It is premature, however, to dismiss the effects of these factors all together. As demonstrated by the post-hoc analysis, the effects of these factors on end users attitude towards SMB may be asymmetric in nature. For example, end users who perceive a high security risk may have an unfavorable attitude towards SMB and thus may be discouraged from engaging in the behavior. However, those who perceive a low security risk may not necessarily have a favorable attitude towards SMB and thus may not necessarily be encouraged to engaging in the behavior. Because of their asymmetric nature, the PLS method may not detect the effects of these factors in their entirety.

In addition to the asymmetric effects, there are some other plausible explanations for the non-significant impact of these factors, as explained in the following.

Attitude toward security policy. The non-significant effect (beta = .14) of attitude toward security policy appeared to be consistent with other research in the literature. For example, Herath and Rao (2009) found that user attitude toward policy does not influence their intention to comply with the policy. The positive, albeit non-significant, effect of

attitude towards security policy is somewhat surprising. One possible explanation is that, although end users may have a general attitude toward a security policy, there might be some exceptional situations where the action (i.e. SMB) is necessary. In this case, end users will still have a favorable attitude toward the action, even if they are also in favor of the security policy (which prohibits the action). This appears to be in line with the recommendation of considering such exceptions in the design of security policies (Siponen & Iivari, 2006). In other words, sometimes a "temporary violation" of predefined security policies is required.

It should be noted, however, that the correlation between attitude toward security policy and attitude toward SMB is actually negative (r = -.25), i.e. a favorable attitude toward security policy is associated with an unfavorable attitude toward SMB. The direct effect of attitude toward security policy on attitude toward SMB becomes positive only when other factors in the model are taken into account. Such change of direction, i.e. from one direction of bivariate correlation to the opposite direction of direct effect in a research model, is not completely impossible. For example, the change of direction was found between personal outcome expectation and system use (Compeau et al., 1999), and between formal sanctions and user intention to violate security policy (Siponen & Vance, 2010).

Utilitarian outcomes. Non-significant utilitarian factors include *perceived security risk*, *perceived accountability*, and *sanction certainty*. From a goal-directed behavioral

perspective, these are negative consequences to be avoided. There are some plausible explanations for their non-significant effects.

The positive outcome – job performance expectation – may be more salient than these non-significant outcomes. For end users, job performance is likely to be their top priority. Thus, their attitude toward SMB will be influenced more by job performance expectation than by non-significant outcomes.

The non-significant effect (beta = -.13) of perceived security risk appeared to be contradictory to the findings of some studies in the management, consumer, and information systems literature. For example, risk perception is negatively related to business managers' decision-making behavior (Sitkin & Weingart, 1995); consumers increase risk-reduction activities when they perceive high risks (Dowling & Staelin, 1994); and perceived risks affect consumer attitude toward online-shopping and subsequently the intention to buy (Jarvenpaa et al., 2000; Malhotra et al., 2004; Pavlou, 2003; Pavlou & Gefen, 2004). Reexamination of these studies suggested that the different effects may be due to different relationships between risks and individuals. For example, business managers are *directly* responsible for the decisions they make and the risk of loss. In consumer e-commerce settings, security risks also have a *direct* impact on individual personal information or financial security if they use credit cards on the Internet. Thus the influence of risks on individual attitudes and behavioral intentions may be significant because of these direct links. In the organizational IS security setting, the link between risk and individual users may be different. Usually it is the responsibility of

the IS department to secure organizational information systems. Thus the link between security risk and users is rather an *indirect* one. Even if they believe that security risk posed by an action is high, end users may not necessarily have an unfavorable attitude toward the action. Instead, they may not care about information security risk and argue that IS people should deal with the risk. For example, prior research has found that apathy (lacking of motivation or enthusiasm about information security) significantly reduces user intention to take security precautions (Boss, Kirsch, Angermeier, Shingler, & Boss, 2009).

From the perspective of risk-taking behavior, the presence of job performance expectation and workgroup norm may increase the level of risk tolerance. It was suggested that a more risk tolerant user can endure more threatening malicious technology (e.g. viruses) than will a less risk tolerant user (Liang & Xue, 2009). It is possible that users are willing to take risks (i.e. tolerate more risks) when they are motivated to accomplish business tasks and their peers are doing the same.

For similar reasons, the effects of perceived accountability and sanction certainty may also be reduced by the presence of the two significant factors – job performance expectation and workgroup norm. End users may argue that they engage in SMB for a good reason (i.e. for increased job performance). The effects of perceived accountability and sanction certainty may be outweighed by the importance of good job performance. Furthermore, they may also try to attribute any security risks or damage to IS people (e.g. to argue that IS people have not done a good job). In other words, users may believe that

they are indeed accountable and likely to be punished. But at the same time, they may argue that IS people share the same responsibility if not more. Workgroup norm may also help explain the non-significant effects of perceived accountability and sanction certainty. It may well be that, even if punishment is certain, it may not matter when everyone else is violating security policies. In other words, laws and regulations do not work when a majority of the population breaks them. It has been suggested that people of high moral commitment may be very sensitive to sanction certainty because they would find it unpleasant even to be accused of any socially undesirable act (D'Arcy et al., 2009). The presence of workgroup norm may reduce such sensitivity and unpleasantness. In other words, users may believe that there is nothing to be ashamed of because their coworkers are doing the same thing.

It should be noted that the non-significant effect of sanctions is consistent with the findings of some studies in the IS literature (e.g. D'Arcy et al., 2009; Siponen & Vance, 2010). However, it contradicts the findings of other research (Herath & Rao, 2009). The mixed findings regarding the general deterrence theory (GDT) in security management in general (a discussion of GDT-based security research is presented in the literature section) suggest that additional factors need to be integrated with GDT for better prediction and explanation of SMB in future research.

Perceived identity match. Three possible reasons may have contributed to the non-significant effect of perceived identity match on both attitude toward SMB and SMB intention. First, end users are pragmatic about security rules and policies. When dealing

with a security issue, they may care more about the job tasks that they need to finish right away. Their image as business professionals may appear to be "remote" to them and thus have a lower priority, even if following security policies is important to them as business professionals. The low priority may be in part explained by the goal-shielding effect (Shah, Friedman, & Kruglanski, 2002), which suggests that the focal goals committed to by individuals inhibit the accessibility of alternative goals. In the context of security misbehavior, job performance expectation can be seen as a focal goal, which may be more important to end users. The attention end users pay to job performance may make them "forget" about how security misbehaviors affect their professional image. The second possible reason for the non-significant impact of perceived identity match on both attitude toward SMB and SMB intention is that violating security rules as described in the scenarios may be seen as trivial by end users. In other words, they may believe that such violations do not hurt their image as business professionals, even if they believe that dealing with security problems match their images as business professionals. Third, in the present study, perceived identity match is measured at the "general" level. That is how following security rules in general appears to affect end user professional image. Attitude toward SMB and SMB intention, on the other hand, are measured at the "specific" level, i.e. about a specific action. According to the theory of planned behavior, this type of "general-to-specific" prediction may not be as strong as expected. Thus in future similar studies, the measurement of perceived identity match might be revised to reflect specific security behaviors rather than following security policies in general.

6.2 Contributions

The current study has several important contributions to IS security research. First, it provides a clear conceptualization of security misbehavior (SMB), which refers to those actions engaged in by employees who voluntarily violate or bypass their organization's rules and policies governing the security of information systems. Their intent in doing so is to benefit themselves (i.e. to help do their jobs). This can help to clarify some confusion and the loosely defined uses of general terms such as IS misuse, computer abuse, and security contravention, among others. Many of these terms refer to criminal activities (in which actors' malicious intention to cause damage or steal information is implied) or unethical behaviors. This research contributes to the literature by focusing on undesirable behaviors in which the actor may not have malicious intentions and may not be necessarily unethical. Such behaviors may be more pervasive than criminal activities in organizations and thus should draw more attention from both researchers and practitioners.

This research is also differentiated from prior studies on security compliance, which may be seen as "desirable" or "good" behaviors. Although the two types of behaviors – SMB and security compliance – may be viewed as opposite to each other on the same continuum, the antecedents may be quite different. Following rules and policies may be common sense and thus may not require salient cues. In other words, one may not need explicit reasons to follow rules. Breaking rules, on the other hand, often necessitates explicit reasoning by the actors. This study, by focusing on undesirable behaviors, advances our understanding of why users want to break security rules and provides a

unique perspective that helps complete our view of behavioral issues in security management.

In the IS security literature, end user attitude towards SMB and its antecedents have not been fully addressed. For example, general deterrence theory-based research focused on the effect of punishment on *reducing* misuse behavior or behavior intention. What *motivates* users to engage in these behaviors has not been rigorously investigated. This research fills the gap by integrating both inhibiting and motivating factors based on the composite behavioral model – CMB (Eagly & Chaiken, 1993). These factors include job performance expectation, perceived security risk, perceived accountability, workgroup norm, and professional identity match. These constructs were either newly introduced or reconceptualized from existing literature. In particular, although security risk has been widely examined in electronic commerce settings, this study is the first known effort to investigate the effect of user perceived security risk in organizational IS security management. Some other research has studied the effect of threats (e.g. Workman et al., 2008). However, such threats were conceptualized as an assessment of the external environment, which is different from user security risk perception associated with actions. Furthermore, in this study, normative outcome was conceptualized as the norm within a workgroup. This is different from the widely used term "social norm", which is often operationalized as the norm held by those people who are important to the actor in question. The advantage of workgroup norm is that it provides a more accurate representation of the norms held by people at work, particularly when the issue at hand is

work-related. In a sense, the usual conceptualization of social norm may be too broad for research in organizational settings.

From a methodology perspective, this study also developed and validated new measurement scales for several constructs, including attitude towards security policy, perceived accountability, perceived security risk, workgroup norm, attitude towards SMB, and SMB intention. Satisfactory levels of psychometric properties have been achieved in the constructs developed for the model. The validated scales can provide some valuable input for future research on user behavior related to information systems security.

Lastly, the study contributes to the literature by expanding our understanding of the factors that influence end user security misbehaviors in organizational settings. Security misbehaviors in organizations appear to be depend on the strengths of the driving forces (job performance expectation and workgroup norm) and the inhibiting factors (attitude toward security policy, perceived security risk, sanction certainty, perceived accountability, and perceived identity match) (as shown in Figure 5). Those driving forces are much stronger that those inhibiting factors. First, the results of the study demonstrated that end users of organizational IS are indeed goal-oriented. They strive to meet their job performance expectations, even if to do so may require them to violate organizational rules and policies. This positive outcome strongly influences their attitude towards security misbehaviors. Taken this finding into consideration, the non-significant influences of the negative utilitarian outcomes (sanction certainty, perceived security risk, and perceived accountability) indicated that these factors should not be

examined in isolation. From the perspective of general deterrence theory, a behavior is punishable because it causes (or has the potential to cause) damages and is universally viewed as a crime in a society. In general, there is no possible legitimate reason behind the crime. In the case of SMB, however, job performance is a very legitimate goal for users. It is often job performance that employees are evaluated for. Thus the general deterrence theory may not provide valuable insight about security misbehavior without the consideration of organizational settings. Similarly, perceived security risks do not prevent users from engaging in security misbehaviors when other factors are considered. It may well be that the goal – job performance expectation – makes users to take risks rather than to shy away from risks. The results of this study also demonstrated that end users are strongly influenced by workgroup norms, which not only influence how they view security misbehaviors in general but also impact directly on their intention to engage in such behaviors. This finding has important theoretical implications. It suggests that security misbehavior 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 reasons why users engage in such behaviors.

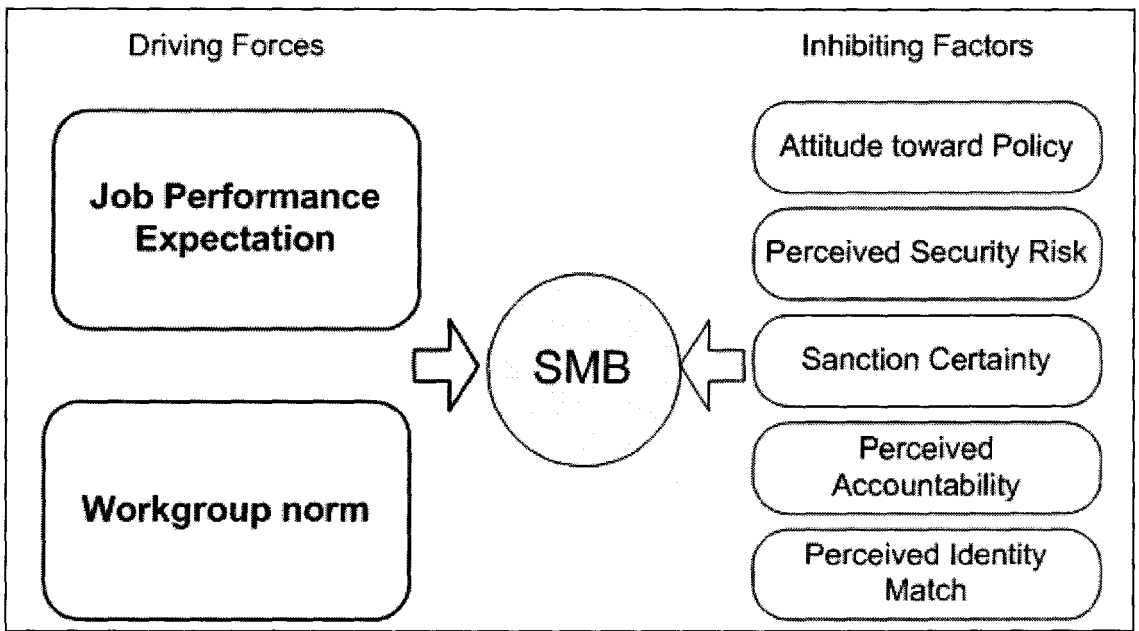


Figure 5: Summary of Driving Forces and Inhibiting Factors of SMB

6.3 Implications for Practice

This study has several important implications for IS security management practice. The results of this study suggest that a shift of IS security management strategy may be necessary. Although it is important to obtain top management support, raise user security awareness, and nurture a security-friendly organizational culture, these strategies appear to be narrowly focused on "IS security" as an end in itself. The mindset for these strategies may be best described as "what top management and end users should know or should do to improve security". A better strategy may be a "user-centered" one, which raises the question, "what IS management should do to help end users do their job without implicating IS security?"

First of all, end users are pragmatic and they care about their job performance more than IS security. When implementing a security policy, IS management should first address what the policy mean for end users. Does it require extra effort or help them do their job? The answer to this question will ultimately influence whether end users will comply with the policy. A good example is the password-protected computer screen saver implemented at a hospital (A. Adams & Blandford, 2005). The screen saver was implemented as part of the hospital's policy to lock unattended computers so that sensitive data are protected. One particular reason for the successful implementation of the policy was that, the screen saver did more than just blocking access when a computer was left unattended. It also conveyed some very important messages abut the hospital's up-to-date status (e.g. patient admission), in which end users were interested.

Secondly, this study indicated that, how end users evaluate the security risk associated with their actions does not have a significant influence on their attitude towards these actions. This suggests that the practice of user security training and education may need a shift of focus. The common wisdom is that the IS department should provide sufficient training and education so that end users are aware of potential security risk. However, security risk in itself may be too vague for end users. IS management (with the support of senior management and in collaboration with user management) should instead try to build links between security risk and end user job performance. In other words, security training and education programs should "crystallize" the risk that end user actions would pose on their own job performance, rather than simply treating security risk in vacuum. In this way, end users would develop some

vested interests in IS security. This in turn would encourage end users to take partial ownership of IS security rather than attribute all the responsibility entirely to the IS department. With vested interests and ownership in mind, end users would more likely think twice about risky security actions when using information systems.

Third, the present study did not find evidence to support the influence of deterrent measures on end user attitude towards SMB when other motivating factors such as job performance expectation are considered. Similar conclusions have been made by other studies, e.g. D'Arcy et al on punishment certainty (2009) and Siponen and Vance (2010) on formal sanctions. Although researchers (Siponen & Vance, 2010) cautioned that it may be premature to draw a decisive conclusion about the ineffectiveness of deterrent measures, the findings of the present study and others (e.g. Siponen & Vance, 2010) do raise some serious questions about the practical effectiveness of those measures in IS security management. Particularly, despite giving organizations some legal ground to discipline violators (Harrington, 1996), deterrent measures are often very difficult to enforce in practice. If end users are trying to achieve legitimate ends (e.g. job performance), prohibiting certain means of using IS (e.g. SMB) will be problematic. Thus it is important for IS security management to align security objectives with end user objectives. This requires IS management to take into consideration end user objectives when managing IS security. This also necessitates some changes of security management strategy of using deterrent measures. Instead of outright banning of certain actions that may pose security risks, IS management should provide alternative means that meet both end user job objectives and security objectives. Such alternative means would be more

acceptable to end users and thus would reduce the likelihood that end users would engage in undesirable security misbehaviors.

Finally, IS management should try to disseminate security awareness through exemplary day-to-day secure computing behaviors rather than simply through security awareness training programs. In other words, IS people should be part of the users' inner circle (workgroup) and act as a "role model" in dealing with IS security issues. Organizations may consider embedding IS people as end user support within other business functions such as accounting, human resources, among others. Another possible strategy is to train "power users" – who have relatively stronger IS and security knowledge than other users – in business departments. These power users then can be role models and act as a resource for other people in the same workgroup when they deal with IS security issues. To a certain extent, security awareness should be more about an understanding of what actions are acceptable and what are not than about proper evaluation of security risks. Furthermore, although end users should know "who to turn to when things go wrong" (Guzman, Stam, Hans, & Angolano, 2009), perhaps more importantly, the IS function should be easily accessible to end users. It should not be isolated in terms of physical location and daily operations. Help should be available and easy to access when users face any IS-related issues. End users should be able to turn to IS people (in addition to power users) rather than their supervisors and coworkers for advices on these issues, particularly those related to IS security. This would also help build a security-friendly organizational culture in a bottom-up fashion at the local workgroup level.

6.4 Limitations and Future Research

Several limitations of the current study should be taken into account for the interpretation of the findings.

Limitations of the Research Method

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, for many constructs the survey data is not normally distributed. Although the statistical method – partial least squares – is assumed to be able to handle such deviation from normal distribution (Chin, 1998), future research may consider using different analytical methods. For example, data mining techniques such as classification and decision trees may be used to identify those users who are most likely to engage in security misbehaviors. Such analyses may provide some useful insights for security management practice.

Fourth, this study used four specific security scenarios to solicit participant responses. Although this scenario-based method is commonly accepted in the literature (e.g. IS, organizational, and marketing), a limitation of this method is that the scenarios do not include every possible type of security misbehavior. Future research should include more types of SMBs to further test the proposed model.

Finally, the measurement of several constructs (attitude towards IS department, role responsibility, and sanction severity) was not reliable based on the commonly accepted criterion of Cronbach's Alpha indices (between .6 and .7). The unexpected low reliability was somewhat surprising given the fact that the scale was pretested in a rigorous pilot study. These items were either adopted from the literature or developed in accordance with recommended methods in the literature. Nevertheless, the omission of these constructs may affect the explanatory power of the theoretical model.

Limitations of the Theoretical 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 to improve the model's external validity and generalizability.

Furthermore, some elements of the composite behavioral model (CBM) (Eagly & Chaiken, 1993) were purposefully excluded as discussed earlier. For example, the

relationships between the antecedents were omitted in order to make the proposed model more parsimonious. Future research may be conducted to include these relationships in order to get a complete picture of the mechanism that forms security misbehaviors.

Lastly, as demonstrated by the post-hoc analysis, those non-significant factors found in the PLS model testing have asymmetric effects on end user attitude towards SMB. The finding is basically consistent with the literature. For example, Cheung and Lee (2009) found a positive-negative asymmetry in a user satisfaction model, where negatively perceived performance of an information-quality attribute had stronger impact than positively perceived performance. Ziekel (2008) also found that consumer price perception have an asymmetric impact on price satisfaction. Such asymmetric effects may not be sufficiently accounted for with a simple linear and additive model where inhibitors (such as perceived security risk) are modeled alongside enablers (such as job performance expectation). Relying solely on symmetric and linear models may run the risk of systemically misestimating the impact of independent variables on user perception or behavior (Cheung & Lee, 2009). Thus, future studies may be conducted to investigate alternative models such as moderation (where inhibitors moderate the effects of enablers on a dependent variable) and mediation (where the effects of inhibitors are mediated by enablers) (Cenfetelli, 2004a, 2004b). Another approach is to use negative-positive bipolar rating scales to test the asymmetric effects (Cheung & Lee, 2009).

6.5 Conclusions

The current study aimed to answer the following research question: why do users intend to engage in insecure use of IS although such use may violate the organization's policy? To achieve this end, this study developed and tested an initial theoretical model to explain the antecedents of user security misbehavior (SMB) based on the composite behavior model – CBM (Eagly & 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 towards SMB and workgroup norm have a significant influence on SMB intention. In turn, user attitude towards SMB is influenced by two factors: workgroup norm and job performance expectation. Contrary to the predictions of CBM, however, user attitude towards target (security policy), some utilitarian outcome expectations (perceived security risk, perceived accountability, and sanction certainty), and perceived professional identity match did not have a significant influence on user attitude towards security misbehavior. However, these non-significant factors in the PLS analysis have demonstrated asymmetric effects. In sum, the results suggest that workgroup norm and job performance expectation are the key determinants of user SMB intention, given their strong direct and indirect effects.

References

Adams, A., & Blandford, A. (2005). Bridging the gap between organizational and user perspectives of security in the clinical domain. *International Journal of Human-Computer Studies, 63*, 175-202.

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM, 42*(12), 41-46.

Adams, A., Sasse, M. A., & Lunt, P. (1997). Making passwords secure and usable. In *People and Computers XII: Proceedings of HCI'97* (pp. 1-19). Berlin: Springer.

Aiman-Smith, L., Scullen, S. E., & Barr, S. H. (2002). Conducting studies of decision making in organizational contexts: A tutorial for policy-capturing and other regression-based techniques. *Organizational Research Methods, 5*(4), 388-414.

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

Ajzen, I. (2006). Constructing a TPB Questionnaire: Conceptual and Methodological Considerations. from http://people.umass.edu/aizen/pdf/tpb.measurement.pdf

Ajzen, I., & Fishbein, M. (1980). *Understanding Attitudes and Predicting Social Behavior*. Englewood Cliffs, NJ: Prentice-Hall.

Alberts, C. J., Behrens, S. G., Pethia, R. D., & Wilson, W. R. (1999). *Operationally Critical Threat, Asset, and Vulnerability Valuation (OCTAVE) Framework.* Pittsburgh, PA: Carnegie Mellon Software Engineering Institute.

Anandarajan, M., Simmers, C. A., & Teo, T. S. H. (2006). The Internet and workplace transformation: An introduction. In M. Anandarajan & T. S. H. Teo (Eds.), *The Internet and Workplace Transformation* (pp. 3-11). Armonk, NY: M.E. Sharpe.

Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin, 103*(3), 411-423.

Anonymous. (2009). Man 'find US troop data' on MP3. Retrieved January 27, 2009, from http://news.bbc.co.uk/go/pr/fr/-/2/hi/asia-pacific/7853213.stm

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

Aytes, K., & Connolly, T. (2005). Computer security and risky computing practices: A rational choice perspective. In M. A. Mahmood (Ed.), *Advanced Topics in End User Computing*. Hershey, PA, USA: IGI Publishing.

Baker, W. H., & Wallace, L. (2007). Is information security under control? - Investigating quality in information security management. *IEEE Security & Privacy, 5*(4), 36-44.

Banerjee, D., Cronan, T. P., & Jones, T. W. (1998). Modeling IT ethics: A study in situational ethics. *MIS Quarterly, 22*(1), 31-60.

Barclay, D. W. (1991). Interdepartmental conflict in organizational buying: The impact of the organizational context. *Journal of Marketing Research, 28*(2), 145-159.

Baskerville, R. L., & Siponen, M. T. (2002). An information security meta-policy for emergent organizations. *Logistics Information Management, 15*, 337-346.

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

Beccaria, C. (1986). *On Crime and Punishmens* (D. Young, Trans.). Indianapolis, Indiana, USA: Hackett Publishing Company.

Bennett, R. J., & Robinson, S. L. (2003). The past, present, and future of workplace deviance research. In J. Greenberg (Ed.), *Organizational Behavior: The State of the Science* (pp. 247-281). Mahwah, NJ. USA: Lawrence Erlbaum.

BERR. (2008). *Information security breaches survey*. London: Department for Business Enterprise & Regulatory Reform (BERR)(UK).

Bertino, E., & Sandhu, R. (2005). Database security - concepts, approaches, and challenges. *IEEE Transactions on Dependable and Secure Computing, 2*(1), 2-19.

Besnard, D., & Arief, B. (2004). Computer security impaired by legitimate users. *Computer & Security, 23*, 253-264.

Bhattacherjee, A., & Hikmet, N. (2007). Physicians' resistance toward healthcare informaiton technology: A theorectical model and empirical test. *European Journal of Information Systems, 16*, 725-737.

Bhattacherjee, A., & Sanford, C. (2006). Influence processes for information technology acceptance: An elaboration likelihood model. *MIS Quarterly, 30*(4), 805-825.

Blanton, H., & Christie, C. (2003). Deviance regulation: A theory of action and identity. *Review of General Psychology, 7*(2), 115-149.

Bock, G.-W., Zmud, R. W., Kim, Y.-G., & 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), 87-111.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems, 18*, 151-164.

Brown, S. A., Massey, A. P., Montoya-Weiss, M. M., & Burkman, J. R. (2002). Do I really have to? User acceptance of mandated technology. *European Journal of Information Systems, 11*, 283-295.

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

Carver, C. S. (2006). Approach, avoidance, and the self-regulation of affect and action. *Motivation and Emotion, 30*(2), 105-110.

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

Cenfetelli, R. T. (2004a). Inhibitors and enablers as dual factor concepts in technology usage. *Journal of the Association for Information Systems, 5*(11-12), 472-492.

Cenfetelli, R. T. (2004b). *The Inhibitors of Technology Use.* The University of British Columbia, Vancouver, BC.

Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of information security at the workplace: Linking information security climate to compliant behavior. *Journal of Information Privacy and Security, 1*(3), 18-41.

Cheung, C. M. K., & Lee, M. K. O. (2009). User satisfaction with an Internet-based portal: An asymmetric and nonlinear approach. *Journal of the American Society for Information Science and Technology, 60*(1), 111-122.

Chin, W. W. (1998). The partial least squares approach to structural equation modeling. In G. A. Marcoulides (Ed.), *Modern Methods for Business Research* (pp. 295-336). Mahwah, NJ, USA: Lawrence Erlbaum Associates.

Churchill, G. A., Jr. (1979). A paradigm for developing better measures of marketing constructs. *Journal of Marketing Research, 16*(1), 64-73.

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

Cohen, J. (1988). *Statistical Power Analysis for the Behavioral Sciences*. Hillsdale, NJ: Lawrence Erlbaum.

Compeau, D. R., Higgins, C. A., & Huff, S. (1999). Social cognitive theory and individual reactions to computing technology: A longitudinal study. *MIS Quarterly, 23*(2), 145-158.

Corlett, J. A. (2009). *Responbility and Punishment*. Dordrecht, The Netherlands: Springer.

Cox, T., Jr. (2003). Cultural diversity in organizations: Intergroup conflict. In J. S. Ott, S. J. Parkes & R. B. Simpson (Eds.), *Classic Readings in Organizational Behavior* (3rd ed., pp. 263-273): Thomson Learning.

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika, 16*(3), 297-334.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20*(1), 79-98.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 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*(8), 982-1003.

Dhillon, G., & Backhouse, J. (2000). Information systems security management in the new millennium. *Communications of the ACM, 43*(7), 125-128.

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User behaviour towards protective information technologies: The role of national cultural differences. *Information Systems Journal, 19*(4), 391-412.

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association of Information Systems, 8*(7), 386-408.

Doherty, N. F., & Fulford, H. (2005). Do information security policies reduce the incidence of security breaches: An exploratory analysis. *Information Resources Management Journal, 18*(4), 21-39.

Doolin, B., & McLeod, L. (2007). Information technology at work: The implications for dignity at work. In S. C. Bolton (Ed.), *Dimensions of Dignity at Work* (pp. 154-175). Oxford, UK: Butterworth-Heinemann.

Dose, J. J., & Klimoski, R. J. (1995). Doing the right thing in the workplace: Responsibility in the face of accountability. *Employee Responsibilities and Rights Journal, 8*(1), 35-56.

Dourish, P., Grinter, R. E., de la Flor, R. D., & Joseph, M. (2004). Security in the wild: User strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing, 8*(6), 391-401.

Dowling, G. R., & Staelin, R. (1994). A model of perceived risk and intended risk-handling activity. *Journal of Consumer Research, 21*(1), 119-134.

DTI-UK. (2006). Information Security Breaches Survey 2006: Technical Report: Department of Trade and Industry (United Kingdom).

Dubie, D. (2007, December 10). End users behaving badly. *Network World*, from http://www.networkworld.com/slideshows/2007/120707-end-users-behaving-badly.html

Dutta, A., & McCrohan, K. (2002). Management's role in information security in a cyber economy. *California Management Review, 45*(1), 67-87.

Eagly, A. H., & 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), 111-116.

Ellis, T. S., & Griffith, D. (2001). The evaluation of IT ethical scenarios using a multidimensional scale. *The DATA BASE for Advances in Information Systems, 32*(1), 75-85.

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

Finch, J. (1987). The vignette technique in survey research. *Sociology, 21*(1), 105-114.

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

Fulk, J. (1993). Social construction of communication technology. *Academy of Management Journal, 36*(5), 921-950.

Garfinkel, S. (2000). *Database nation: the death of privacy in the 21st century*. Sebastopol, CA, USA: O'Reilly.

Garg, A., Curtis, J., & Halper, H. (2003). The financial impact of IT security breaches: What do investors think? *Information Systems Security, 12*(1), 22-33.

Gefen, D., Straub, D. W., & Boudreau, M. (2000). Structural equation modeling and regression: Guidelines for research practice. *Communications of the AIS, 4*(7), 1-78.

Gerbing, D. W., & Anderson, J. C. (1988). An updated paradigm for scale development incorporating unidimensionality and its assessment. *Journal of Marketing Research, 25*(2), 186-192.

Gibbs, J. P. (1975). *Crime, Punishment, and Deterrence*. New York: Elsevier North-Holland.

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

Grazioli, S., & 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), 395-410.

Gross, J. B., & Rosson, M. B. (2007). *Looking for trouble: Understanding end-user security management.* Paper presented at the The Symposium on Computer Human Interaction for the Management of Information Technology (CHIMT'07).

Guthrie, R., & Gray, P. (1996). Junk computing: Is it bad for an organization? *Information Systems Management, 13*(1), 23-28.

Guzman, I. R., Stam, K., Hans, S., & Angolano, C. (2009). Human factors in security: The role of information security professionals within organizations. In K. J. Knapp (Ed.), *Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions* (pp. 184-200). Hershey, PA: IGI Global.

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), 257-278.

Hart, H. L. A. (1968). *Punishment and Responsibility.* Oxford: Oxford University Press.

Hassanein, K., & Head, M. (2007). Manipulating perceived social presence through the web interface and its impact on attitude towards online shopping. *International Journal of Human-Computer Studies, 65*, 689-708.

Heckhausen, H., & Kuhl, J. (1985). From wishes to action: The dead ends and short cuts on the long way to action. In M. Frese & J. Sabini (Eds.), *Goal Directed Behavior: The Concept of Action in Psychology* (pp. 134-159). Hillsdale, NJ: Lawrence Erlbaum Associates.

Herath, T., & Rao, H. R. (2009). Protection motivation an deterrence: A framework for security policy compliance in organizations. *European Journal of Information Systems, 18*, 106-125.

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

Hullett, C. R. (2004). A test of the initial processes of the goal-planning-action model of interpersonal influence. *Communication Studies, 55*(2), 286-299.

Im, G. P., & Baskerville, R. L. (2005). A longitudinal study of information system threat categories: The enduring problem of human error. *The DATA BASE for Advances in Information Systems, 36*(4), 68-79.

ISO/IEC. (2000). Information Technology - Code of Practice for Information Security Management (ISO/IEC 17799). Geneva, Switzerland: International Organization for Standardization.

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., & Barkhi, R. (2008). An extension of the technology acceptance model to determine the intention to use biometric devices. In S. Clarke (Ed.), *End User Computing Challenges and Technologies: Emerging Tools and Applications* (pp. 57-78). Hershey, PA, USA: IGI Global.

Jarvenpaa, S. L., Tractinsky, N., & Vitale, M. (2000). Consumer trust in an Internet store. *Information Technology and Management, 1*, 45-71.

Jehn, K. A., Northcraft, G. B., & Neale, M. A. (1999). Why differences make a difference: A field study of diversity, conflict, and performance in workgroups. *Administrative Science Quarterly, 44*, 741-763.

Johnson, M. E. (2008). Information risk of inadvertent disclosure: An analysis of file-sharing risk in the financial supply chain. *Journal of Management Information Systems, 25*(2), 97-123.

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.

Karahanna, E., & Straub, D. W. (1999). The psychological origins of perceived usefulness and ease-of-use. *Information & Management, 35*(4), 237-250.

Karahanna, E., Straub, D. W., & Chervany, N. L. (1999). Information technology adoption across time: A cross-sectional comparison of pre-adoption and post-adoption beliefs. *MIS Quarterly, 23*(2), 183-213.

Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). Information systems security policies: a contextual perspective. *Computer & Security, 24*, 246-260.

Kiely, L., & Benzel, T. V. (2006). Systemic security management. *IEEE Security & Privacy, 4*(6), 74-77.

Kling, R. (1980). Computer abuse and computer crime as organizational activities. *Computer/Law Journal, 2*(2), 186-196.

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., & Ford, F. N. (2006). Information security: Management's effect on culture and policy. *Information Management & Computer Security, 14*(1), 24-36.

Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. *Information & Management, 41*(597-607).

Lapointe, L., & Rivard, S. (2005). A multilevel model of resistance to information technology implementation. *MIS Quarterly, 29*(3), 461-491.

Lau, G. T., & Ng, S. (2001). Individual and situational factors influencing negative word-of-mouth behavior. *Canadian Journal of Administrative Sciences, 18*(3), 163-178.

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

Lee, O. K., Lim, K. H., & Wong, W. M. (2005). *Why employees do non-work-related computing: An exploratory investigation through multiple theoretical perspectives.* Paper presented at the 38th Hawaii International Conference on System Sciences, Hawaii.

Lee, R. M. (1993). *Doing research on sensitive topics*. London ; Newbury Park, Calif.: Sage Publications.

Lee, S. M., Lee, S. G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management, 41*, 707-718.

Lee, Y., Kozar, K. A., & Larsen, K. R. T. (2003). The technology acceptance model: Past, present, and future. *Communications of the AIS, 12*, 752-780.

Leonard, L. N. K., & 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., & Byrd, T. A. (2005). A methodology for construct development in MIS research. *European Journal of Information Systems, 14*(4), 388-400.

Liang, H., Saraf, N., Hu, Q., & Xue, Y. (2007). Assimilation of enterprise systems: The effect of institutional pressures and the mediating role of top management. *MIS Quarterly, 31*(1), 59-87.

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly, 33*(1), 71-90.

Lim, V. K. G., & Teo, T. S. H. (2006). Cyberloafing and organizational justice. In M. Anandarajan, T. S. H. Teo & C. A. Simmers (Eds.), *The Internet and Workplace Transformation* (pp. 241-258). Armonk, NY: M.E. Sharpe.

Lindqvist, U., & Jonsson, E. (1997). *How to systematically classify computer security intrusions.* Paper presented at the IEEE Symposium on Security and Privacy.

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly, 17*(2), 173-186.

Madden, T. J., Ellen, P. S., & Ajzen, I. (1992). A comparison of the theory of planned behavior and the theory of reasoned action. *Personality and Social Psychology Bulletin, 18*(1), 3-9.

Mahatanankook, P. (2006). Internet abuse in the workplace: Extension of workplace deviant model. In M. Anandarajan, T. S. H. Teo & C. A. Simmers (Eds.), *The Internet and Workplace Transformation* (pp. 41-62). Armonk, NY: M.E. Sharpe.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336-355.

Malhotra, N. K., Kim, S. S., & Patil, A. (2006). Common method variance in IS research: A comparison of alternative approaches and a reanalysis of past research. *Management Science, 52*(12), 1865-1883.

Marcinkowski, S., & Stanton, J. M. (2003). *Motivational aspects of information security policies.* Paper presented at the IEEE International Conference on Systems, Man and Cybernetics.

Mathieson, K., Peacock, E., & Chin, W. W. (2001). Extending the technology acceptance model: The influence of perceived user resources. *The Data Base for Advances in Information Systems, 32*(3), 86-112.

McKeen, J. D., & Smith, H. (1996). *Management challenges in IS : successful strategies and appropriate action.* Chichester ; New York: Wiley.

Mitchell, V.-W. (1999). Consumer perceived risk: Conceptualisations and models. *European Journal of Marketing, 33*(1/2), 163-195.

Moore, G. C., & Benbasat, I. (1991). Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information Systems Research, 2*(3), 192-222.

Narver, J. C., & Slater, S. F. (1990). The effect of a market orientation on business profitability. *Journal of Marketing, 54*(4), 20-35.

NIST. (2001). Risk management guide for information technology systems: National Institute of Standards and Technology (USA).

Pahnila, S., Siponen, M. T., & Mahmood, A. (2007). *Employees' behavior towards IS security policy compliance.* Paper presented at the 40th Annual Hawaii International Conference on System Sciences, Hawaii.

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), 69-103.

Pavlou, P. A., & Gefen, D. (2004). Building effective online marketplaces with institution-based trust. *Information Systems Research, 15*(1), 37-59.

Peace, A. G., Galletta, D., & Thong, J. Y. L. (2003). Software piracy in the workplace: A model and empirical test. *Journal of Management Information Systems, 20*(1), 153-177.

Perry, W. E. (1985). *Management Strategies for Computer Security*. Stoneham, MA: Butterworth Publishers.

Ployhart, R. E., & Schneider, B. (2002). A multi-level perspective on personal selection research and practice: Implications for selection system design, assessment, and construct validation. In F. J. Yammarino & F. Dansereau (Eds.), *The Many Faces of Multi-Level Issues* (pp. 95-140). Oxford, UK: Elsevier Science.

Ployhart, R. E., & Schneider, B. (2005). Multilevel selection and prediction: Theories, methods, and models. In A. Evers, O. Omit-Voskuyl & N. Anderson (Eds.), *The Blackwell Handbook of Personnel Selection* (pp. 495-516). Malden, MA, USA: Blackwell Publishing.

Podasakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & 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), 879-903.

Podasakoff, P. M., & Organ, D. W. (1986). Self-reports in organizational research: Problems and prospects. *Journal of Management, 12*(4), 531-544.

Post, G. V., & Kagan, A. (2007). Evaluating information security tradeoff: Restricting access can interfere with user tasks. *Computer & Security, 26*, 229-237.

Richardson, R. (2007). *CSI computer crime and security survey*: Computer Security Institiute (CSI).

Richardson, R. (2008). *CSI Computer Crime & Security Survey*: Computer Security Institute.

Roberts, L. M. (2005). Changing Faces: Professional Image Construction in Diverse Organizational Settings. *Academy of Management Review, 30*(4), 685-711.

Robinson, S. L., & 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), 658-672.

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the "weakest link" - A human/computer interaction approach to usable and effective security. *BT Technology Journal, 19*(2), 122-131.

Schlenker, B. R., Britt, T. W., Pennington, J., Murphy, R., & Doherty, K. (1994). The triangle model of responsibility. *Psychological Review, 101*(4), 632-652.

Schneier, B. (2000). *Secrets and Lies*: John Wiley and Sons.

Shah, J. Y., Friedman, R., & Kruglanski, A. W. (2002). Forgetting all else: On the antecedents and consequences of goal shielding. *Journal of Personality and Social Psychology, 83*(6), 1261-1280.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8*(1), 31-41.

Siponen, M. T., & Iivari, J. (2006). Six design theories for IS security policies and guidelines. *Journal of the Association of Information Systems, 7*(7), 445-472.

Siponen, M. T., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *The DATA BASE for Advances in Information Systems, 38*(1), 60-80.

Siponen, M. T., & Vance, A. (2010). Neutralization: New insight into the problem of employee information systems security policy violation. *MIS Quarterly, forthcoming.*

Sirdeshmukh, D., Singh, J., & Sabol, B. (2002). Consumer trust, value, and loyalty in relational exchanges. *Journal of Marketing, 65*(1), 15-37.

Sitkin, S. B., & 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), 1573-1592.

Smith, H. J., & Hasnas, J. (1999). Ethics and information systems: The corporate domain. *MIS Quarterly, 23*(1), 109-127.

Son, J. Y., & Rhee, H. S. (2007). *Out of fear or desire: Why do employees follow information systems security policies?* Paper presented at the Americas Conference on Information Systems, Keystone, Colorado, USA.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computer & Security, 24*(2), 124-133.

Sterne, D. F. (1991). On the buzzword "security policy", *IEEE Symposium on Security and Privacy* (pp. 219-230).

Stoneburner, G., Goguen, A., & Feringa, A. (2001). *Risk Management Guide for Information Technology Systems*: National Institute of Standard and Technology (U.S.A.).

Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly, 13*(2), 147-169.

Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research, 1*(3), 255-276.

Straub, D. W., Boudreau, M., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the Associations of Information Systems, 13*, 380-427.

Straub, D. W., & Burton-Jones, A. (2007). Veni, vidi, vici: Breaking the TAM logjam. *Journal of the Association for Information Systems, 8*(4), 223-229.

Straub, D. W., & Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: A field study. *MIS Quarterly, 14*(1), 45-60.

Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computer & Security, 24*, 472-481.

Thompson, R. L., Higgins, C. A., & Howell, J. M. (1991). Personal computing: Toward a conceptual model of utilization. *MIS Quarterly, 15*(1), 125-143.

TJX. (2007a). Annual Report of 2006: The TJX Companies, Inc.

TJX. (2007b). Quaterly Report of The TJX Companies, Inc (SEC Form 10-Q, for the Quaterly Period Ended April 28, 2007).

Triandis, H. C. (1977). *Interpersoal Behavior*. Monterey, CA: Brooks/Cole Publishing Company.

Tyler, T. R., & Blader, S. L. (2005). Can Businesses Effectively Regulate Employee Conduct? The Antecedents of Rule Following in Work Settings. *Academy of Management Journal, 48*(6), 1143-1158.

Vardi, Y., & Weitz, E. (2004). *Misbehavior in Organizations: Theory, Research, and Management*. Mahwah, NJ: Lawrence Erlbaum Associates.

Vardi, Y., & Wiener, Y. (1996). Misbehaviors in organizations: A motivational framework. *Organization Science, 7*(2), 151-165.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*(3), 425-478.

Verdon, D. (2006). Security policies and the software developer. *IEEE Security & Privacy, 4*(4), 42-49.

Walker, S. T. (1985). *Network security overview*. Paper presented at the IEEE Symposium on Security and Privacy.

Ward, M. (2009). The dark side of the flash drive. Retrieved January 27, 2009, from http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/7807999.stm

Wason, K. D., Polonsky, M. J., & Hyman, M. R. (2002). Designing vignette studies in marketing. *Australasian Marketing Journal, 10*(3), 41-58.

Weber, J. (1992). Scenarios in business ethics research: Review, critical assessment, and recommendations. *Business Ethics Quarterly, 2*(2), 137-160.

Webster, J., & 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), 1544.

Weippl, E. R., & Klemen, M. (2006). Implementing IT security for small and medium enterprises. In M. E. Warkentin (Ed.), *Enterprise Information Systems Assurance and Systems Security*. Hershey, PA: Idea Group Publishing.

Whitman, M. E. (2004). In defense of the realm: Understanding the threats to information security. *International Journal of Information Management, 24*, 43-57.

Whitman, M. E., & Mattord, H. J. (2003). *Principles of Information Security*. Boston: Thomson.

Willison, R. (2006). Understanding the perpetration of employee computer crime in the organisational context. *Information and Organization, 16*(4), 304-324.

Winell, M. (1987). Personal goals: The key to self-direction in adulthood. In M. E. Ford & D. H. Fort (Eds.), *Humans as Self-Constructing Living Systems: Putting the Framework to Work* (pp. 261-287). Hillsdale, NJ, USA: Lawrence Erlbaum.

Wood, C. C. (2000). An unappreciated reason why information security policies fail. *Computer Fraud & Security*(10), 13-14.

Workman, M. (2007). Gaining Access with Social Engineering: An Empirical Study of the Threat. *Information Systems Security, 16*(6), 315-331.

Workman, M., Bommer, W. H., & 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), 2799-2816.

Workman, M., & 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), 212-222.

Xu, H., Wang, H., & Teo, H.-H. (2005). *Predicting the usage of P2P sharing software: The role of trust and perceived risk.* Paper presented at the The 38th Hawaii International Conference on System Sciences, Hawaii.

Yammarino, F. J., & Dansereau, F. (Eds.). (2002). *The Many Faces of Multi-Level Issues* (Vol. 1). Oxford, UK: Elsevier Science.

Zielke, S. (2008). Exploring asymmetric effects in the formation of retail price satisfaction. *Journal of Retailing and Consumer Services, 15*, 335-347.

Zviran, M., & Haga, W. J. (1999). Passwrod security: An empirical study. *Journal of Management Information Systems, 15*(4), 161-185.

APPENDIX 1.

SECURITY SCENARIOS

Survey participants were given one of the following security misbehavior scenarios:

Scenario 1 - Password Write-Down

Alex is a senior manager at your organization, which recently installed a computer system for customer record management. The information technology (IT) department gave users their own usernames and passwords. Different users have different levels of access to the system (e.g. what they can see and what they can do). For security and privacy reasons, the IT department implemented a policy stating that users are accountable for the information they access. Users are required to keep their passwords to themselves and not let other people know or use. Users who fail to follow the policy may be subjected to disciplinary actions ranging from warning to termination of employment. Finding it difficult to remember the password, Alex wrote down her username and password on a sticker and attached it to the computer she usually uses.

Scenario 2 - Unauthorized portable devices for storing and carrying organizational data

Chris is a business manager at your organization. Periodically Chris makes presentations to your organization's business partners or works from home. As a result, Chris often uses personal USB drives to copy data back and forth. Your organization's IT policy, however, prohibits users from attaching unauthorized devices to the corporate network and computers. The IT department argues that the use of unauthorized devices can cause security problems, e.g. loss and disclosure of confidential corporate data and spreading of computer virus. Employees who fail to follow the policy may be subjected to disciplinary actions ranging from warning to termination of employment.

Scenario 3 - Installation and use of unauthorized software

Jordan is a business analyst at your organization. Jordan uses computers on a daily basis to do financial analysis and prepare management report. Jordan recently was given a new computer. However, the new computer is missing a piece of software that Jordan needs for preparing reports. Believing that purchasing one may take some time, Jordan managed to download and install an open source but similar software (free of charge) from the Internet. Installation of unauthorized software, however, is not permitted according to your organization's policy. The IT department insists that unapproved open-source software may damage the security and expose the corporate network to external attacks. Users who fail to follow the policy may be subjected to disciplinary actions ranging from warning to termination of employment.

Scenario 4 - Using insecure public wireless network for business purposes

Kelly is an accounting manager at your organization. Kelly uses a corporate laptop while traveling to other sites or working from home. Kelly often brings the laptop and do some work when having a coffee at coffee shops. One thing that Kelly likes much is that many coffees shops nowadays offer free wireless Internet access. The IT policy of your organization, however, does not allow its employees to use public free wireless connection for business purposes due to security reasons. Most free wireless connections are not encrypted and may be intercepted by hackers. Users who violate the policy may be subjected to disciplinary actions ranging from warning to termination of employment. Although aware of the security policy, Kelly continues to use free public wireless access when working out of office.

Instructions

Following each scenario, participants were given instructions similar to the following statement (revised for each scenario):

"Based on the information described in the above scenario, please indicate the extent (on a 1-to-7 scale) to which you agree with the statements if you were Kelly. 1=Strongly Disagree; 7=Strongly Agree. The expressions of "the action" and "the behavior" refer to the action of using unsecure public wireless network for business purposes by Kelly as described in the scenario."

APPENDIX 2.

MEASUREMENT ITEMS

General Items

The following are general items that are shown before the security scenario:

Attitude towards IT Department

Four items were developed to reflect user evaluation of the role, knowledge/skills, stereotype, and functions of the IT department in an organization:

[AtttudeITD1]:	The IT department in my organization tries to control too much about how we use computers.
[AtttudeITD2]:	IT people in my organization have a good understanding of users' needs.
[AtttudeITD3]:	IT people in my organization know about computer but not business.
[AtttudeITD4]:	The IT department in my organization does not always meet our business needs.

Perceived Role Responsibility

Four items are developed to reflect user opinion about whether they, as end users, should be held accountable for IS security in general:

[RoleResp1]:	As an end-user, I am not responsible for computer security problems.
[RoleResp2]:	End users like me should be accountable for computer security.
[RoleResp3]:	It is fair to discipline users for causing computer security problems.
[RoleResp4]:	End users like me should not to be blamed for computer security breaches.

Professional Identity Match

For the measurement of identity match, two items (IDMatch1 and IDMatch4) ("As a non-IT business user, ...") were adapted from the social identity literature (Triandis, 1977). The other two items were newly created.

[IDMatch1]: As a business professional, I have to do certain things on my job. Strictly following computer security policies is one of them.
[IDMatch2]: Following computer security rules and policies is an important part of me as a business professional.
[IDMatch3]: Breaking security policies hurts my image as a business professional.
[IDMatch4]: As a business professional, I have to do certain things. Taking care of computer security issues is one of them.

Scenario-Specific Items

The following are scenario-specific items that are shown after the security scenario:

Attitude towards IS Security Policy

Five new items were created to reflect user evaluation of the IS security policy that is described in a specific scenario:

[AttitudePol1]: This security policy helps secure computer systems.
[AttitudePol2]: This security policy is absolutely necessary.
[AttitudePol3]: This security policy is effective for securing computer systems.
[AttitudePol4]: This security policy is important.
[AttitudePol5]: This security policy causes too much inconvenience for computer users to do their job.

Perceived Security Risk of SMB

Four items were created to measure user evaluation of the risk associated with the behavior (SMB) in question:

[Risk1]: The action can cause damages to computer security.
[Risk2]: The action can put important data at risk.
[Risk3]: The action does not cause any problems to computer security.
[Risk4]: The action will most likely cause security breaches.

Job Performance Expectation

Four items were used to capture user expectation of job performance. Three items were adapted from literature on the measurement of "relative advantage" of using

technology (Moore & Benbasat, 1991). A new item (JobPerf4) was created to reflect the convenience aspect of SMB.

[JobPerf1]:	The action helps improve my job performance.
[JobPerf2]:	The action makes it more convenient for to do my job.
[JobPerf3]:	The action would enable me to accomplish tasks more quickly.
[JobPerf4]:	The action would make it easier to do my job.

Perceived Accountability

Three items were developed to measure user perceived accountability about their actions (as described in the scenarios):

[Accountability1]:	I should be held accountable for violating this security policy.
[Accountability2]:	I should not be blamed if my action causes any damages to computer security.
[Accountability3]:	I should be held accountable if my action causes any negative consequences.

Sanction Severity

The following items were adapted from (D'Arcy et al., 2009; Siponen & Vance, 2010) to measure user evaluation about sanction severity:

[Severity1]	If the management decides to punish me, the punishment would be (not severe at all … very severe).
[Severity2]	It would be a big problem for me if the management decides to punish me for my action.

Sanction Certainty

The following items were adapted from (D'Arcy et al., 2009) to measure users' evaluation about the certainty of sanction:

[Certainty1]	The likelihood my organization would punish me for engaging in the action is (very low … very high).
[Certainty2]	I will be reprimanded eventually if my organization is aware of my action.

Workgroup Norm

Consistent with the literature, a workgroup is operationally defined as the functional unit (e.g. department) in which all personnel report directly to the same supervisor (or manager) and interact to complete unit tasks (Fulk, 1993; Jehn, Northcraft, & Neale, 1999). Four items were created to measure workgroup norm perceived by users:

[WkgpNorm1]: My coworkers will believe it is wrong to engage in this action.
[WkgpNorm2]: My supervisor will disapprove this action.
[WkgpNorm3]: My supervisor will not object this action.
[WkgpNorm4]: My coworkers will think that I should do this action.

Attitude towards SMB

The items for measuring user attitude towards SMB are created in accordance with the structure recommended by Ajzen (2006). The following six adjective pairs were used to form the items by completing the sentence: "For me to engage in the action is …":

[AttitudeAcc1]: a (bad … good) idea.
[AttitudeAcc2]: (harmful … beneficial).
[AttitudeAcc3]: (wrongful…rightful).
[AttitudeAcc4]: (unethical … ethical).
[AttitudeAcc5]: (worthless … valuable).
[AttitudeAcc6]: (illegitimate … legitimate).

SMB Intention

Two items were created to measure user intention to engage in the behavior described in each scenario:

[Intent1]: I would do [the behavior] if I were the person.
[Intent2]: I would do [the behavior] if I were in a similar situation.

APPENDIX 3.

LETTER OF INFORMATION AND CONSENT FORM

A Study of Computer Use and Information Security

Investigators

Principal Investigator:	Dr. Yufei Yuan DeGroote School of Business McMaster University Hamilton, Ontario, Canada Tel.: (905) 525-9140 ext. 23982;
Student Investigator:	Ken Guo DeGroote School of Business McMaster University Hamilton, Ontario, Canada Tel: (905) 525-9140 ext. 26216

Purpose of the Study

The purpose of this study is to investigate user behavior in using information technologies (IT) in organizations. More specifically, we aim to understand how employees make the decisions to use IT in certain ways that may have positive or negative impacts on the security of organizational information systems. Thanks to the Internet, both organizational and individual information are at risk of being stolen or abused. Your participation in this study will greatly help us gain a better understanding of the current status of information security issues.

Procedures involved in the Research

You will be asked to complete a questionnaire about your experience of using information technology at your current organization (or your prior employer if you are not currently working), your opinion about information security in general, and your opinion about a hypothetical computer use scenario related to security. The survey takes about 15 to 30 minutes.

Potential Harms, Risks or Discomforts

There are no known physical risks of participating in the study. You might worry that others in your organization will find out your opinion of the IT department or its policies. To prevent such risk, we will not be asking you for any identifying information and we will keep your responses confidential. You may skip any question that makes you uncomfortable or withdraw from the study at any time.

Potential Benefits to the Participants and/or Society

The result of this research will help organizations have a better understanding of why employees often break security rules. Based on the result, they may implement relevant measures to encourage employees to follow security rules or discourage them from engaging in security misbehavior that could damage the overall IS security.

The research will not benefit you directly.

Payment or Reimbursement [Paper version]

We appreciate your time and effort on completing the survey! A complimentary coffee card is enclosed in the survey package you receive.

Payment or Reimbursement [Web version]

We appreciate your time and effort on completing the survey! If you complete the survey, you will be eligible to enter a lucky draw or to receive a $10 coffee card at your choice. In both cases, you only need to email us your contact information at the end of this survey (further instruction will be provided to you when you complete the survey). If you choose to enter the lucky draw, you will have the chance to win one of the following prizes:

* First prize: $300 gift card (odds to win: 1/300);

* Second prize: $100 gift card (odds to win: 1/100);

* Third prize: $20 gift card (odds to win: 1/20)

Note that the odds to win are approximate because they depend on the number of responses we receive. You may also opt out of the lucky draw or decline the complimentary coffee card by not providing us your name and contact information.

Confidentiality and Anonymity

Anything that you say or do in the study will not be told to anyone else. Anything that we find out about you that could identify you will not be published or told to anyone else, unless we get your permission. Your privacy will be respected. We will not be asking you to provide your name or any personal information other than some demographic information.

Participation

Your participation in this study is voluntary. If you decide to participate, you may choose to stop at any time during the study and there will be no consequences to you. Should you be interested in finding out the result of the research, please do not hesitate to contact us. A summary of the research results will also be posted on the website of McMaster eBusiness Research Centre.

Consent

By turning in your completed the survey questionnaire, you indicate your consent for us to use your responses in our research.

Rights of Research Participants

If you have questions or require more information about the study itself, please contact Dr. Yufei Yuan.

This study has been reviewed and approved by the McMaster Research Ethics Board. If you have concerns or questions about your rights as a participant or about the way the study is conducted, you may contact:

McMaster Research Ethics Board Secretariat

Telephone: (905) 525-9140 ext. 23142

c/o Office of Research Services

E-mail: ethicsoffice@mcmaster.ca

APPENDIX 4.

SURVEY QUESTIONNAIRE

A Study on Computer Use and Information Security

Thank you for taking time to complete this survey. There are five types of questions: 1) demographic information about you; 2) information about your organization; 3) information about your job; 4) your experience of information technology (IT) use and your opinion about information security in general; and 5) your opinion about a computer use scenario related to security.

PART 1: Information about You

1. What is your age? ☐ 18-24 ☐ 25-34 ☐ 35-44 ☐ 45-54 ☐ 55 or above

2. What is your gender? ☐ Female ☐ Male

3. What's your highest level of education? ☐ High school ☐ College/University ☐ Master's ☐ Doctoral ☐ None of the above

4. How long have you been working on your current job? ☐ (Years)

5. How many years of working experience do you have? ☐ (Years)

6. On average, how much time per day do you spend on using computers at home? ☐ (hours per day)

The following questions ask about your preference regarding coffee consumption. Please indicate the extent (on a 1-to-7 scale) to which you agree with the statements. 1=Strongly Disagree; 7=Strongly Agree. Please note that these questions are for our internal testing purpose and have nothing to do with the Starbucks Company per se. No information of any kind will be provided to the company.

Coffee Preference	Strongly Disagree	<---------->					Strongly Agree
7. I consider myself to be loyal to Starbucks Coffee.	1	2	3	4	5	6	7
8. Starbucks would be my first choice for coffee.	1	2	3	4	5	6	7
9. As far as coffee concerned, I would not buy other brands if Starbucks Coffee is available.	1	2	3	4	5	6	7

PART 2: Information about Your Organization

10. What industry is your organization in?

- ☐ Automotive manufacturing
- ☐ Eduction
- ☐ Financial/banking
- ☐ Healthcare
- ☐ Information Technology
- ☐ Other manufacturing
- ☐ Professional services
- ☐ Public sector
- ☐ Retail/wholesales
- ☐ Other(Please specify)

11. How many employees does your organization have?

- ☐ 100 or less
- ☐ 100 - 499
- ☐ 500 - 999
- ☐ 1000 - 4999
- ☐ 5000 or more

12. How many employees are there in your workgroup, including you, your supervisor, your coworkers who report to the same supervisor as you do, and those people who report directly to you?

- ☐ 5 or less
- ☐ 6 - 19
- ☐ 20 - 49
- ☐ 50 or more

PART 3: Information about Your Job and Computer Skills

13. On average, how much time do you spend on using computers at work everyday? ☐ (hours)

Your General Computer Skills	Novice <----------> Expert						
14. How would your supervisor rate your general computer skills at work (on a 1-to-7 scale, 1=Novice; 7=Expert)?	1	2	3	4	5	6	7
15. How would you rate your general computer skills at work (on a 1-to-7 scale, 1=Novice; 7=Expert)?	1	2	3	4	5	6	7

16. What is your job function?

- ☐ General management
- ☐ Sales/marketing
- ☐ Accounting
- ☐ Auditing
- ☐ Logistics/production
- ☐ Administration
- ☐ Informaiton Technology
- ☐ Physician/nurse
- ☐ Other (Please specify)

17. What is the position of your current job?

- ☐ Senior manager
- ☐ Middle manager
- ☐ Staff
- ☐ Other (Please specific)

Your Specific Computer Skills	Strongly Disagree <----------> Strongly Agree						
18. I believe I have the ability to describe how a computer works.	1	2	3	4	5	6	7

19. I believe I have the ability to install new software applications on a computer.	1	2	3	4	5	6	7
20. I believe I have the ability to identify and correct common operational problems with a computer.	1	2	3	4	5	6	7
21. I believe I have the ability to unpack and set up a new computer.	1	2	3	4	5	6	7
22. I believe I have the ability to remove information from a computer that I no longer need.	1	2	3	4	5	6	7
23. I believe I have the ability to use a computer to display or present information in a desired manner.	1	2	3	4	5	6	7
24. I am able to identify a breach in information security even if there is no one to help me.	1	2	3	4	5	6	7
25. I am able to identify a breach in information security, even if I do not have a copy of written procedures and rules to refer to.	1	2	3	4	5	6	7
26. I am able to identify a breach in information security even if I have not seen a similar situation occurring before.	1	2	3	4	5	6	7
27. I am aware of what to do in the event of an information security breach even if there is no one to tell me what to do.	1	2	3	4	5	6	7
28. I am aware of what to do in the event of an information security breach, even if I do not have a copy of written procedures and rules to refer to.	1	2	3	4	5	6	7

PART 4: Your Experience of Computer Use at Work

A) How would you describe the IT department of your organization?	Strongly Disagree	<---------->				Strongly Agree
29. The IT department in my organization tries to control too much about how we use computers.	1	2	3	4	5	6	7
30. IT people in my organization have a good understanding of end-users' needs.	1	2	3	4	5	6	7

31. IT people in my organization know about computers but not business.	1	2	3	4	5	6	7
32. The IT department in my organization does not always meet our business needs.	1	2	3	4	5	6	7
B) What is your opinion about the relationship between end users and information security?	Strongly Disagree	<---------->				Strongly Agree	
33. As an end-user, I am not responsible for computer security problems.	1	2	3	4	5	6	7
34. Users like me should be accountable for computer security.	1	2	3	4	5	6	7
35. It is fair to discipline users for causing computer security problems.	1	2	3	4	5	6	7
36. End-users like me should not be blamed for computer security breaches.	1	2	3	4	5	6	7
C) What is your opinion about dealing with information security policies and rules?	Strongly Disagree	<---------->				Strongly Agree	
37. As a business professional, I have to do certain things. Strictly following computer security policies is one of them.	1	2	3	4	5	6	7
38. Following computer security rules and policies is an important part of me as a business professional.	1	2	3	4	5	6	7
39. Breaking computer security rules hurts my image as a business professional.	1	2	3	4	5	6	7
40. As a business professional, I have to do certain things. Dealing with IS security issues is one of them.	1	2	3	4	5	6	7
D) What is your opinion about risks in general?	Strongly Disagree	<---------->				Strongly Agree	
41. I enjoy taking risks.	1	2	3	4	5	6	7
42. I try to avoid situations that have uncertain outcomes.	1	2	3	4	5	6	7
43. Taking risk does not bother me if the gains involved are high.	1	2	3	4	5	6	7
44. People have told me I seem to enjoy taking chances.	1	2	3	4	5	6	7

45. I rarely, if ever, take risks when there is another alternative.	1	2	3	4	5	6	7
E) How would you describe the IT management of your organization?	Strongly Disagree		<---------->			Strongly Agree	
46. My organization has specific guidelines that describe acceptable use of e-mail.	1	2	3	4	5	6	7
47. My organization has established rules of behavior for use of computer resources.	1	2	3	4	5	6	7
48. My organization has a formal policy that forbids employees from accessing computer systems that they are not authorized to use.	1	2	3	4	5	6	7
49. My organization has specific guidelines that describe acceptable use of computer passwords.	1	2	3	4	5	6	7
50. My organization has specific guidelines that govern what employees are allowed to do with their computers.	1	2	3	4	5	6	7
51. My organization has specific guidelines that govern what employees are allowed to do with wireless network connections.	1	2	3	4	5	6	7

PART 5: Computer Use Scenario

Please read the following scenario and the respond to each statement below.

[Note: one of the four scenarios will be shown here. The following is an example. This paragraph will not appear on the actual survey.]

Alex is a senior manager at your organization, which recently installed a computer system for customer record management. The information technology (IT) department gave users their own usernames and passwords. Different users have different levels of access to the system (e.g. what they can see and what they can do). For security and privacy reasons, the IT department implemented a policy stating that users are accountable for the information they access. Users are required to keep their passwords to themselves and not let other people know or use. Users who fail to follow the policy may be subjected to disciplinary actions ranging from warning to termination of employment. Finding it difficult to remember the password, Alex wrote down her username and password on a sticker and attached it to the computer she usually uses.

[Note: the instruction will include information about the actor, action, and policy described in the scenario. The following is an example. This paragraph will not appear on the actual survey.]

Based on the information described in the above scenario, please indicate the extent (on a 1-to-7 scale) to which you agree with the statements if you were Alex. 1=Strongly Disagree; 7=Strongly Agree. The expressions of "the action" and "the behavior" refer to the action of writing down user name and password and posting somewhere by Alex as described in the scenario.

A) What is your opinion about the policy?	Strongly Disagree		<---------->				Strongly Agree
52. The policy helps secure computer systems.	1	2	3	4	5	6	7
53. The security policy absolutely necessary.	1	2	3	4	5	6	7
54. The security policy is effective for securing information systems.	1	2	3	4	5	6	7
55. The security policy is important.	1	2	3	4	5	6	7
56. The security policy causes too much inconvenience for computer users to do their job.	1	2	3	4	5	6	7
B) What do you think about the benefits and negative consequences of the action?	Strongly Disagree		<---------->				Strongly Agree
57. The action can cause damages to computer security.	1	2	3	4	5	6	7
58. The action can put important data at risk.	1	2	3	4	5	6	7
59. The action does not cause any problems to computer security.	1	2	3	4	5	6	7
60. The action will most likely cause security breaches.	1	2	3	4	5	6	7
61. The action helps improve my job performance.	1	2	3	4	5	6	7
62. The action makes it more convenient for me to do my job.	1	2	3	4	5	6	7
63. The action would enable me to accomplish tasks more quickly.	1	2	3	4	5	6	7
64. The action would make it easier to do my job.	1	2	3	4	5	6	7
65. I should be held accountable for violating this security policy.	1	2	3	4	5	6	7
66. I should not be blamed if my action causes any damages to computer security.	1	2	3	4	5	6	7
67. I should be held accountable if my action causes any negative consequences.	1	2	3	4	5	6	7

68. It is likely that my organization will punish me for engaging in the action.	1	2	3	4	5	6	7
69. I will be reprimanded eventually if my organization is aware of my action.	1	2	3	4	5	6	7
70. If the management decides to punish me, the punishment would be severe.	1	2	3	4	5	6	7
71. It would be a big problem for me if the management decides to punish me for my action.	1	2	3	4	5	6	7
C) What would other people think about the action?	Strongly Disagree		<----------				Strongly Agree
72. My coworkers will believe it is wrong to engage in this action.	1	2	3	4	5	6	7
73. My supervisor will disapprove this action.	1	2	3	4	5	6	7
74. My supervisor will not object to this action.	1	2	3	4	5	6	7
75. My coworkers will think that I should do this action.	1	2	3	4	5	6	7
D) What would you and your coworkers do in a similar situation?	Strongly Disagree		<----------				Strongly Agree
76. I would do the same if I were the person.	1	2	3	4	5	6	7
77. I would not do the same if I were in a similar situation.	1	2	3	4	5	6	7
78. My coworkers would do same if they were the person.	1	2	3	4	5	6	7
79. My coworkers would not do the same if they were in a similar situation.	1	2	3	4	5	6	7

For the following questions, please complete the statements by indicating the extent (on a 1-to-7 scale) to which you would describe the subject.

E) What is your opinion about the action in general?	<----------							
80. For me to engage in the action is a ( ) idea.	Bad	1	2	3	4	5	6	7	Good
81. For me to engage in the action is:	Harmful	1	2	3	4	5	6	7	Beneficial
82. For me to engage in the action is:	Wrongful	1	2	3	4	5	6	7	Rightful
83. For me to engage in the	Unethical	1	2	3	4	5	6	7	Ethical

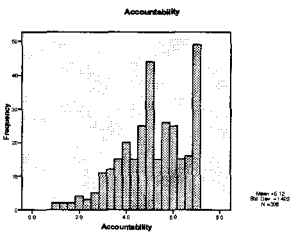
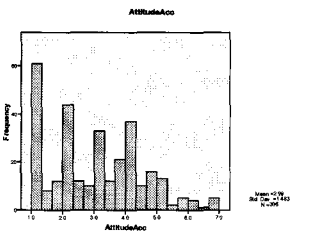
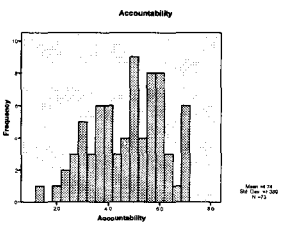
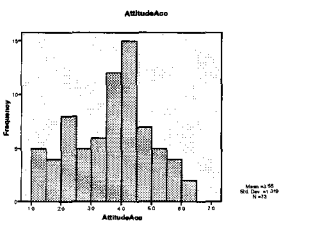
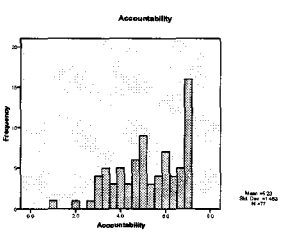
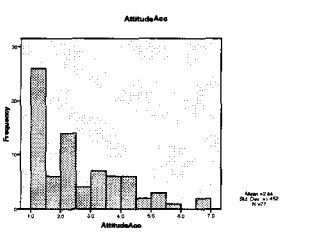
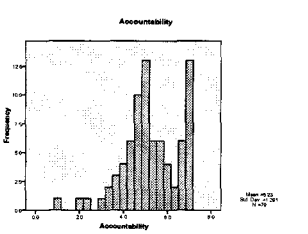
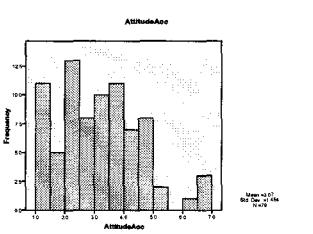
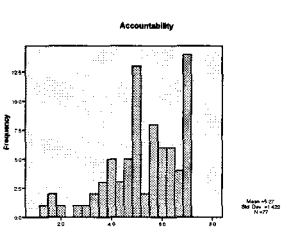
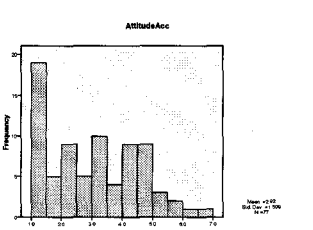
action is:

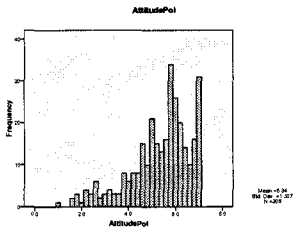
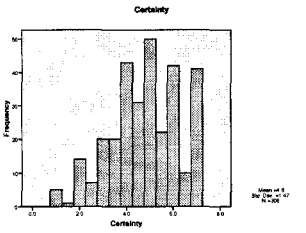
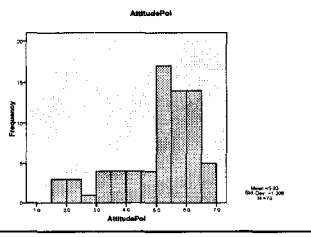
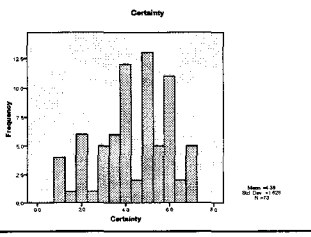
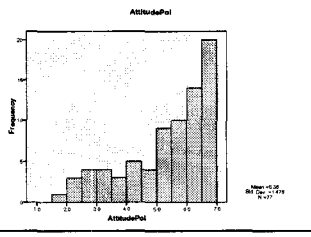
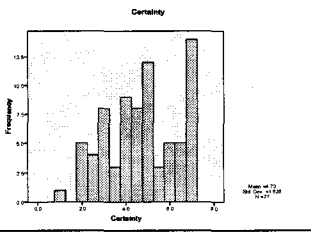
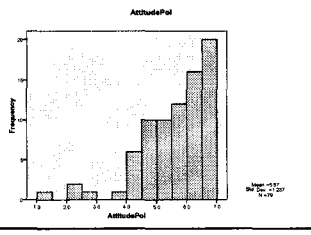
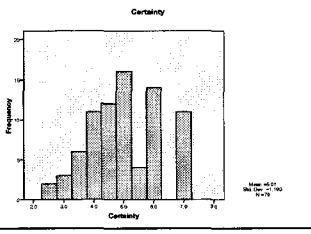
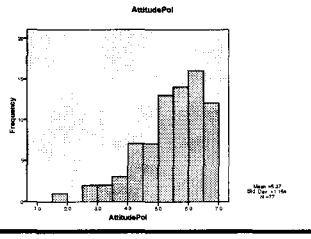
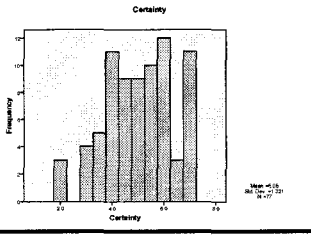
84. For me to engage in the action is:	Worthless	1	2	3	4	5	6	7	Valuable
85. For me to engage in the action is:	Illegitimate	1	2	3	4	5	6	7	Legitimate

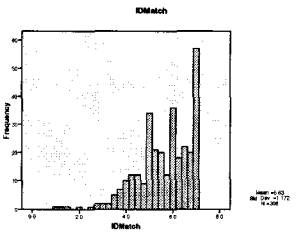
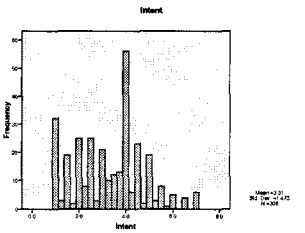
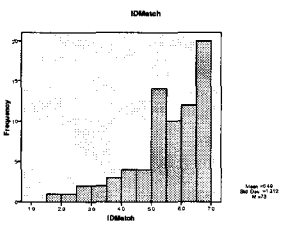
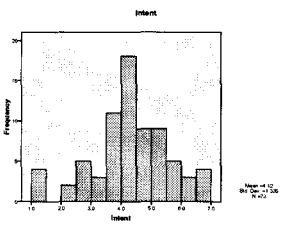
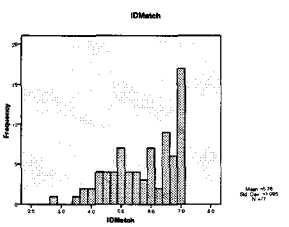
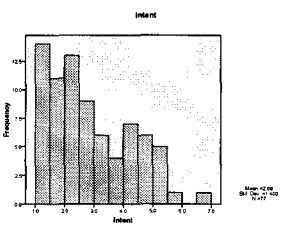
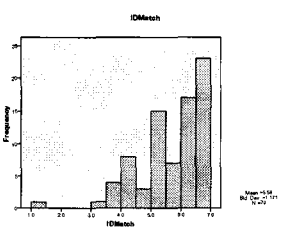
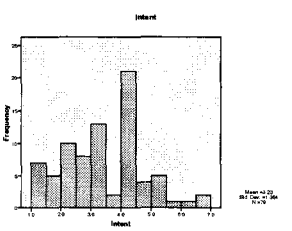
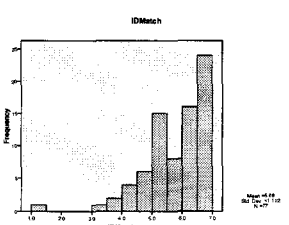
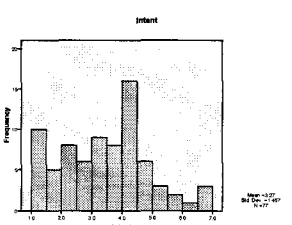
[End of questionnaire. Thank you very much for your time!]

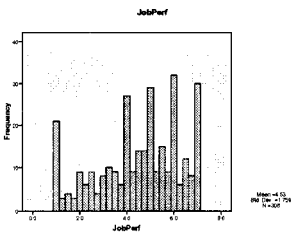
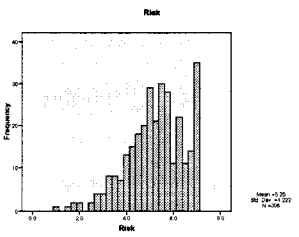
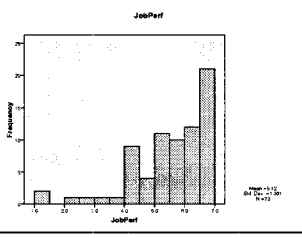
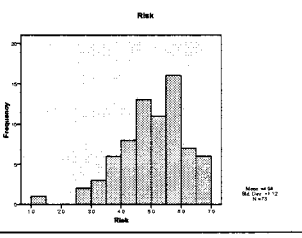
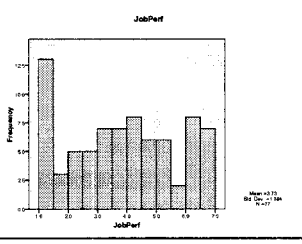
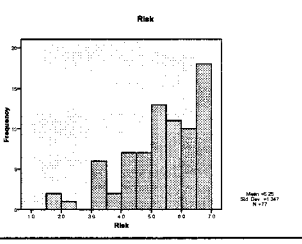
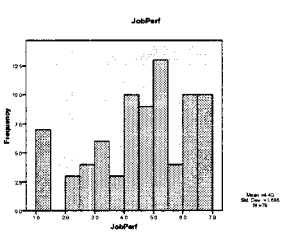
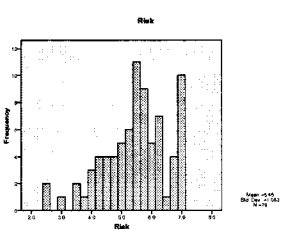
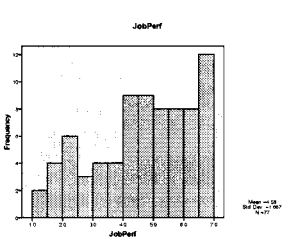
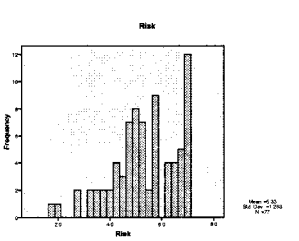
APPENDIX 5.

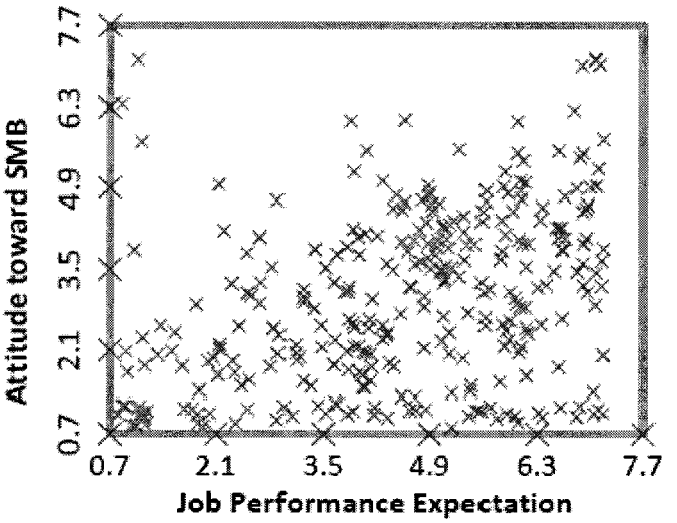
COMPARISON OF HISTOGRAMS BY SCENARIO

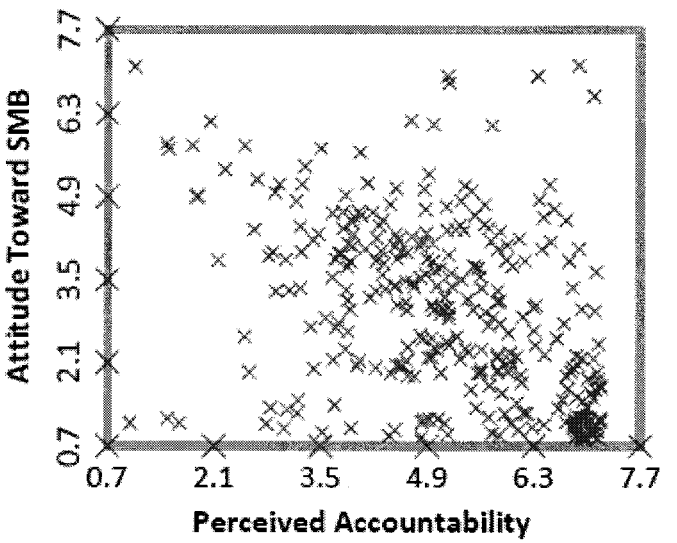
Scenario	Perceived Accountability	Attitude towards SMB
Combined (N=306)		
Hardware (N=73)		
Password (N=77)		
Software (N=79)		
Wireless (N=77)		

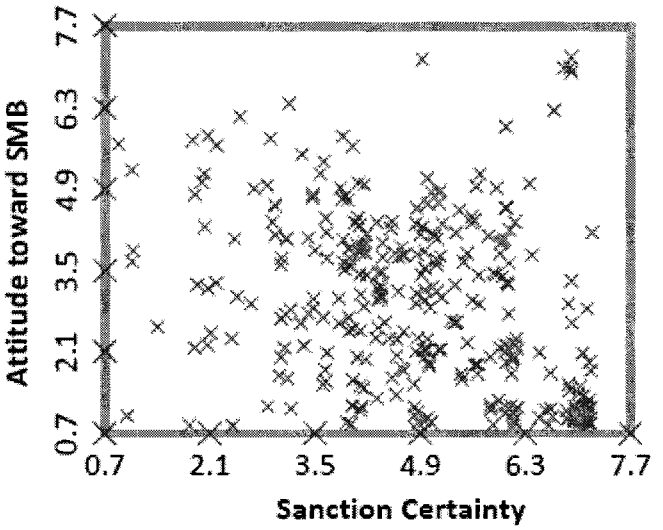
Scenario	Attitude towards Policy	Sanction Certainty
Combined (N=306)		
Hardware (N=73)		
Password (N=77)		
Software (N=79)		
Wireless (N=77)		

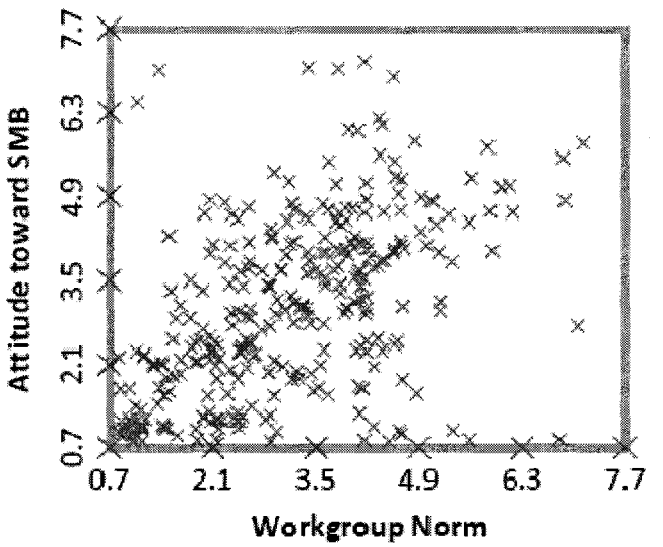
Scenario	Perceived Professional Identity Match	SMB Intention
Combined (N=306)		
Hardware (N=73)		
Password (N=77)		
Software (N=79)		
Wireless (N=77)		

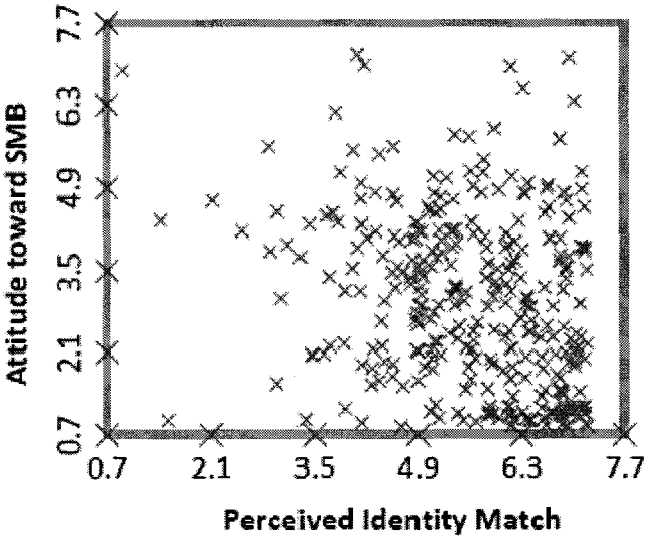
Scenario	Job Performance Expectation	Perceive Security Risk
Combined (N=306)		
Hardware (N=73)		
Password (N=77)		
Software (N=79)		
Wireless (N=77)		


Attitude toward SMB
0.7
2.1
3.5
4.9
6.3
7.7
Job Performance Expectation

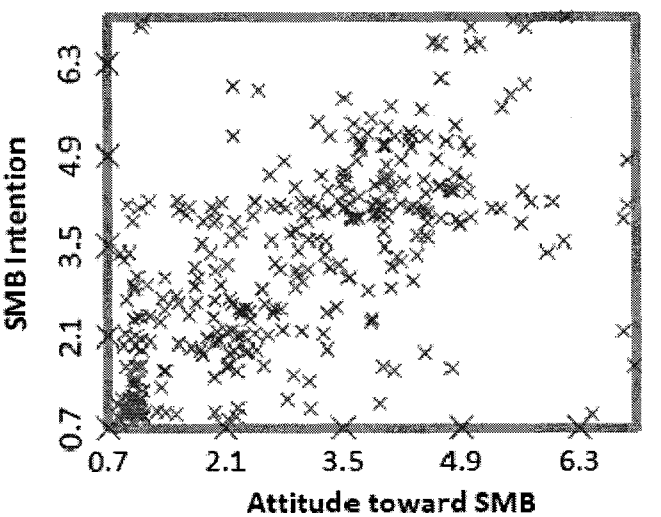

Attitude Toward SMB
0.7
2.1
3.5
4.9
6.3
7.7
Perceived Accountability

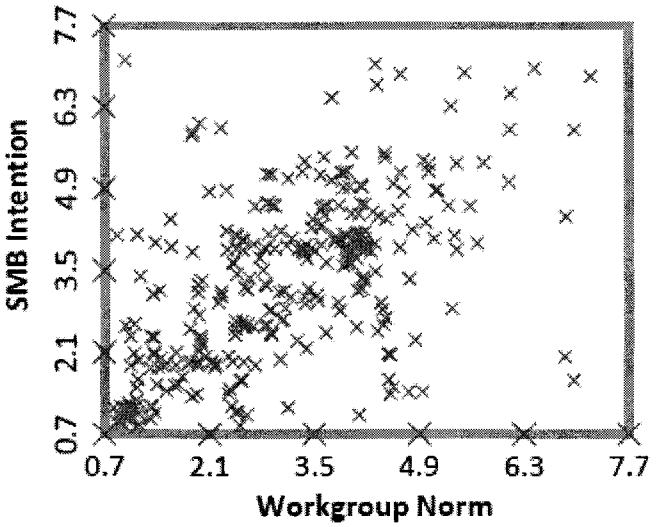

Attitude toward SMB
0.7
2.1
3.5
4.9
6.3
7.7
Sanction Certainty

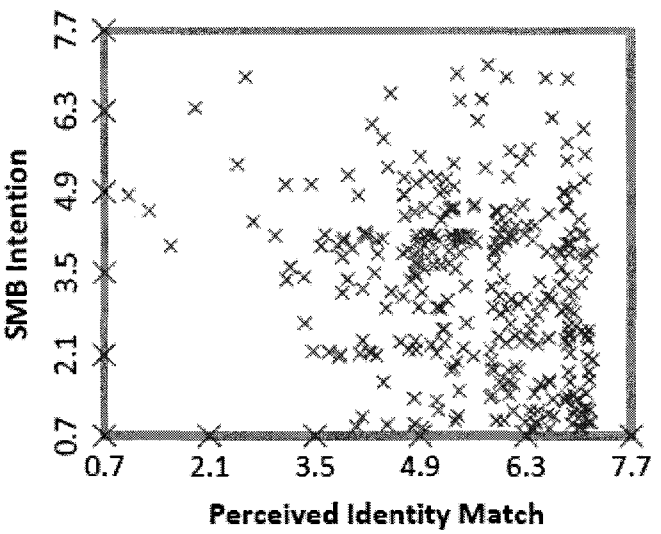

Attitude toward SMB
0.7
2.1
3.5
4.9
6.3
7.7
Workgroup Norm



SMB Intention and Its Antecedents




SMB Intention
0.7
2.1
3.5
4.9
6.3
7.7
Workgroup Norm


SMB Intention
0.7
2.1
3.5
4.9
6.3
7.7
Perceived Identity Match