Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model

KEN H. GUO, YUFEI YUAN, NORMAN P. ARCHER, AND CATHERINE E. CONNELLY

KEN H. GUO is an assistant professor of accounting in the College of Business at Western New England University. He holds a B.A. in economics (Zhejiang University), an M.Sc. in business (University of British Columbia), and a Ph.D. in information systems (McMaster University). He is a certified management accountant (British Columbia, Canada). His research interests include information systems security, IT auditing, behavioral accounting, forensic accounting, and accounting information systems.

YUFEI YUAN is a professor of information systems in the DeGroote School of Business at McMaster University, Canada. He received his Ph.D. in computer information systems from the University of Michigan and his B.S. in mathematics from Fudan University, China. His research interests are in the areas of mobile commerce, emergency response systems, Web-based negotiation support systems, security and privacy, business model of electronic commerce, fuzzy logic and expert systems, matching problems, and information systems in health care. He has more than 70 papers published in journals such as *MIS Quarterly, Management Science, Journal of Management Information Systems, Communications of the ACM, IEEE Security and Privacy, International Journal of Mobile Communications, Group Decision and Negotiation, Decision Support Systems, Information & Management, Fuzzy Sets and Systems, International Journal of Human–Computer Studies, European Journal of Operational Research,* and *Decision Sciences*.

NORMAN P. ARCHER is Professor Emeritus in the DeGroote School of Business at McMaster University, and a special adviser to the McMaster E-Business Research Centre. His current research interests are in the adoption and use of electronic health records, including issues of interoperability, electronic medical record system adoption by physicians, and personal health record systems for consumers. He and his colleagues and students have jointly published more than 100 articles in journals such as the *Communications of the AIS, Communications of the ACM, International Journal of Medical Informatics,* and *INFOR* and conference proceedings.

CATHERINE E. CONNELLY is an associate professor of organizational behavior in the DeGroote School of Business at McMaster University. She has a Ph.D. in organizational behavior and management information systems from Queen's University. Her research deals primarily with workers who have ‘‘nonstandard'' employment arrangements (e.g., mobile workers, contractors, volunteers, and temporary workers). Her research has appeared in several journals, including the *Journal of Management Information Systems, Journal of Applied Psychology, Journal of Management, Journal of Vocational*

Journal of Management Information Systems / Fall 2011, Vol. 28, No. 2, pp. 203–236.

0742–1222 / 2011 $9.50 + 0.00.
DOI 10.2753/MIS0742-1222280208

Behavior, and *IEEE Transactions on Engineering Management.* She currently serves on the editorial board of *Human Relations.*

Abstract: End users are said to be "the weakest link" in information systems (IS) security management in the workplace. They often knowingly engage in certain insecure uses of IS and violate security policies without malicious intentions. Few studies, however, have examined end user motivation to engage in such behavior. To fill this research gap, in the present study we propose and test empirically a nonmalicious security violation (NMSV) model with data from a survey of end users at work. The results suggest that utilitarian outcomes *(relative advantage for job performance, perceived security risk),* normative outcomes *(workgroup norms),* and self-identity outcomes *(perceived identity match)* are key determinants of end user intentions to engage in NMSVs. In contrast, the influences of *attitudes toward security policy* and *perceived sanctions* are not significant. This study makes several significant contributions to research on security-related behavior by (1) highlighting the importance of job performance goals and security risk perceptions on shaping user attitudes, (2) demonstrating the effect of workgroup norms on both user attitudes and behavioral intentions, (3) introducing and testing the effect of perceived identity match on user attitudes and behavioral intentions, and (4) identifying nonlinear relationships between constructs. This study also informs security management practices on the importance of linking security and business objectives, obtaining user buy-in of security measures, and cultivating a culture of secure behavior at local workgroup levels in organizations.

Key words and phrases: information systems security, nonlinear construct relationships, nonmalicious security violation, perceived identity match, perceived security risk, relative advantage for job performance, workgroup norms.

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. In the 2010 Computer Security Institute (CSI) survey of computer security practitioners in U.S. organizations, more than 41 percent of the respondents reported security incidents [68]. In the United Kingdom, a similar survey found that 45 percent of the participating companies had security incidents in 2008 [37]. While the causes for these security incidents may be difficult to fully identify, it is generally understood that insiders from within organizations pose a major threat to IS security [36, 55]. For example, peer-to-peer file-sharing software installed by employees may cause inadvertent disclosure of sensitive business information over the Internet [41]. Employees writing down passwords on a sticky note or choosing easy-to-guess passwords may risk having their system access privilege be abused by others [98]. The 2010 CSI survey found that nonmalicious insiders are a big issue [68]. According to the survey, more than 14 percent of the respondents reported that nearly all their losses were due to nonmalicious, careless behaviors of insiders. Indeed, end users are often viewed as "the weakest link" in the IS security chain [73], and fundamentally IS security has a "behavioral root" [94].

A frequently recommended organizational measure for dealing with internal threats posed by end user behavior is security policy [6]. For example, a security policy may specify what end users should (or should not) do with organizational IS assets, and it may also spell out the consequences of policy violations. Having a policy in place, however, does not necessarily guarantee security because end users may not always act as prescribed [7]. A practitioner survey found that even if end users were aware of potential security problems related to their actions, many of them did not follow security best practices and continued to engage in behaviors that could open their organizations' IS to serious security risks [62]. For example, the survey found that many employees 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 [22]. This phenomenon raises an important question: What factors motivate end users to engage in such behaviors? The role of motivation has not been considered seriously in the IS security literature [75] and our understanding of the factors that motivate those undesirable user behaviors is still very limited.

To fill this gap, the current study aims to investigate factors that influence end user attitudes and behavior toward organizational IS security. The rest of the paper is organized as follows. In the next section, we review the literature on end user security-related behaviors. We then propose a theoretical model of nonmalicious security violation and develop related hypotheses. This is followed by discussions of our research methods and data analysis. In the final section, we discuss our findings, implications for research and practice, limitations, and further research directions.

Literature Review

Conceptualization of Nonmalicious Security Violation

In the present study, we conceptualize insecure uses of IS as *nonmalicious security violation* (NMSV). More specifically, NMSV is defined as the behaviors engaged in by end users who knowingly violate organizational IS security policies without malicious intents to cause damage. NMSVs have a number of characteristics:

- *Intentional.* NMSVs are intentional end user behaviors. Thus, such behaviors should be differentiated from accidental events that may lead to breaches of IS security rules and policies. Examples of accidental events include human error and power outages that may damage the operation of IS. The term "intentional" in this context implies that end users make "conscious decisions" to follow a course of action.
- *Self-benefiting without malicious intent.* End users who engage in NMSVs may try to help themselves, for example, by saving time and effort that may be required in order to follow specific rules and policies. It should be noted, however, that end users who engage in NMSVs do not necessarily have malicious intents to harm the security or general business operations of the organization. Furthermore,

NMSVs do not include unethical actions that benefit end users at the organization's expense. For example, stealing and selling company information for personal profit is normally viewed as a crime that is subject to legal prosecution. NMSVs, in contrast, are noncriminal transgressions that are handled within the organization.

- *Voluntary rule breaking.* When end users engage in NMSVs, they voluntarily violate the organization's policies, which define what users are allowed to do or not do. Although organizational IS security policies are often mandatory, end users may nevertheless choose to violate such policies at their own will.
- *Possibly causing damage or security risk.* In addition to rule breaking, NMSVs may cause damage to the organizations' IS or put organizational information at risk. This is probably one of the main reasons that organizations implement security policies in the first place to prevent undesirable NMSVs.

Undesirable security-related behaviors have been conceptualized in the IS security literature from different perspectives, such as computer abuse [45, 81, 82], IS misuse [18], security contravention [94], unethical use [5, 52], IS security policy violation [76], and security omissive behavior [95]. NMSVs defined in the present study differ from these concepts in many ways. For example, NMSVs are not illegal and malicious (in comparison to computer abuses, IS misuses, and security contravention). NMSVs as defined in this study are not necessarily unethical (in comparison to unethical computer use). The scope of NMSVs is narrower than that of violations of security policies [76], which include both malicious and nonmalicious behaviors.[1] In the current study, we explicitly limit NMSVs to end user intentional and nonmalicious actions, which according to the 2010 CSI survey [68] are one of the most serious problems in security management. A summary of these differences is shown in Table 1.

Prior Research on End User Security-Related Behaviors

In the IS security literature, deterrence theory has been applied to investigate the effects of organizational deterrent measures on employee computer abuses. For example, the security impact model [81] 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 a recent study, an extended deterrence model [18] was proposed to examine 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 in the deterrence theory.

Some studies have investigated user security behaviors from an ethics perspective [5, 30, 52, 58]. IS ethics, which refers to the ethical content of informal norms and behavior, may help deal with those situations where no formal rules or policies are in place [19]. Other studies have focused on user compliance to security policies. In one study, an IS security policy compliance model [59] suggests that user intentions to comply with security policies are influenced by user attitudes toward compliance. The

Table 1. Comparison of NMSV and Other Security Behavior Concepts

Concepts	Key difference from NMSVs	Examples	References
Computer abuses	Illegal	Data theft, unauthorized use	[45, 81, 82]
IS misuse	Illegal, unethical, not limited to security policy	E-mail jokes, use unlicensed software, access confidential information	[18]
Security contravention	Illegal, mostly malicious	Software piracy, steal information, crack passwords	[94]
Unethical use	Unethical, not limited to security policy	Illegal software copying, hacking competitors' systems, writing viruses	[5, 52]
Violation of policy	Does not clearly differentiate malicious and nonmalicious behavior	Copy sensitive data to USB drives, disabling security configurations, revealing confidential information to outsiders	[76]
Omissive security behavior	Aware of threat and countermeasure but choose to ignore, policy violation is not the focus	Do not change passwords, do not back up, do not update security patches	[95]

study found that, contrary to what was expected, coping appraisal (a three-dimensional construct composed of response efficacy, self-efficacy, and response cost) did not have a significant effect on user attitudes. Sanctions also did not have a significant effect on user intentions to comply, contrary to the predictions of the deterrence theory. In another study [12], it was found that compliant behavioral intentions are influenced by the IS security climate perceived by users and their self-efficacy of breaching security. From a rational-choice perspective, Bulgurcu et al. [10] found that the costs/benefits of compliance and costs of noncompliance are key factors influencing user attitudes toward compliance and intention to comply. Herath and Rao [32, 33] also examined user motivations to comply with security policies.

Siponen and Vance [76] 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 using a number of neutralization techniques such as defense of necessity. The study found that neutralization techniques had a significant positive effect on employee intentions to violate IS security policies. The effects of formal or informal sanctions, on the other hand, were not significant. Workman et al. [95] 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 user omissive behaviors depend on their "threat assessments" and "coping assessments," based on the assumption that when a threat is perceived, people adjust their behaviors according to an acceptable level of risk.

The literature review revealed that although prior studies have provided some valuable insights on the conceptualization of user security-related behaviors and the antecedents of such behaviors, there are some limitations and gaps that warrant further investigations. First, in the context of NMSV, ethical/unethical behavioral models may not be directly applicable. NMSVs may not be intrinsically "unethical." For example, one may write down a password and post it on the computer screen. Thus, a code of ethics may not have a significant effect on end user intentions to engage in NMSVs, nor do those factors that affect ethical behaviors. Furthermore, although NMSVs may trigger management disciplinary actions that are often prescribed in security policies, such disciplinary actions may be deemed to be unfair because end users may intend to improve their job performance by engaging in NMSVs.

Second, security compliance models do not explain why users break rules. In general, compliance seems to represent the opposite of NMSVs. However, these two types of behaviors are qualitatively different and the antecedents of each type of behavior 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, end users 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 end users violate rather than why they comply with policies. Focusing on policy violations may help to ensure that proper measures are put in place to discourage end users from breaking security 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 [9, 34]. In other words, deviant behaviors are more "informative" than normal or good behaviors [9]. From this perspective, studying NMSVs (a type of deviant behavior) may help further our understanding of employee actions in using organizational IS.

Although we did not find empirical evidence in the IS literature that specifically differentiates "policy violation" and "policy compliance," there is ample empirical evidence in the organizational behavior and management literature that differentiates similar concepts. For example, Tyler and Blader [89] found that "rule following" and "rule breaking" are distinct forms of behavior. Kelloway et al. [44] suggested that counterproductive behaviors and organizational citizenship behaviors are empirically distinct. Tyler and Blader's study is particularly relevant. They focused on general policies that govern employee behavior in the workplace. Our study focused on a specific set of policies—IS security policies—that govern how employees behave to deal with security issues.

Third, somewhat in common with compliance models, deterrence models may help explain why users comply with computer use or security rules (by not engaging in NMSVs), but not why they break these rules or engage in NMSVs. For example, D'Arcy et al. [18] examined the effect of deterrence on preventing IS misuse. Furthermore, the effects of deterrence are not conclusive. For example, contrary to what is predicted by the deterrence theory, prior studies have indicated that perceived certainty of punishment did not have a significant influence on user intentions to misuse IS [18]. Further study is needed to understand the reasons why deterrent security policies do not work, even when punishment is certain.

Finally, omissive security behavior [95] is similar to NMSVs in that both behaviors are undesirable from a security management perspective. However, these two behaviors are qualitatively different. The term "omissive behavior" assumes that users "do not do what they are supposed to do," whereas NMSVs assume that users "do what they are not supposed to do." Furthermore, in their study, Workman et al. [95] considered the factor of threat only (i.e., how users evaluate and cope with threats). Their model does not provide a sufficient explanation for user NMSVs because maintaining security and dealing with threats are not perceived to be user tasks or responsibilities [7].

In summary, despite the growing interest and research efforts in studying user security-related behaviors in the IS security literature, some critical questions remain unanswered. In particular, our understanding of the factors that motivate end users to engage in NMSVs is still limited. It is the objective of this study to fill this research gap by proposing and testing empirically an NMSV model based on the composite behavior model developed by Eagly and Chaiken [23].

Research Model and Hypotheses Development

The composite behavior model (CBM) proposed by Eagly and Chaiken is an extension to the theory of reasoned action (TRA) [4] and the theory of planned behavior (TPB) [2]. The model suggests that *intention* is the immediate cause of *behavior;* and intention is influenced by *attitude toward behavior,* which is in turn determined by the following antecedents: (1) *habit* (the sequences of a person's behavior that have become relatively automatic and occur without the person's self-instruction), (2) *attitude toward target* (attitude toward the particular target that is the object of a behavior), (3) *utilitarian outcomes* (either rewards or punishments that one expects from engaging in the behavior in question), (4) *normative outcomes* (the approval or disapproval by significant others of the behavior), and (5) *self-identity outcomes* (either affirmations or repudiations of one's self-concept that are expected to follow from engaging in the behavior). Furthermore, the CBM also suggests that (1) habit and attitude toward behavior have a direct effect on behavior, (2) normative outcomes and self-identity outcomes have a direct effect on intention, (3) habit influences attitude toward target, and (4) attitude toward target has an effect on utilitarian outcomes, normative outcomes, and self-identity outcomes.

For the purpose of the present study, we apply and test a trimmed CBM with the following modifications. First, instead of studying actual behaviors, we focus on behavioral intentions of users (i.e., NMSV intention as the dependent variable). This approach is chosen because actual IS security violations are not readily observable or objectively measurable as they are “ideographic in nature” [95]. One cannot practically observe or objectively measure every possible IS security behavior [95]. Self-reported actual behaviors may be an option; however, prior studies suggest that there is always a discrepancy between what people report about their behaviors and what they actually do [95]. Further, the influence of intention on behavior has been rigorously tested and is well established in the literature. Replicating this link (from intention to actual behavior) in the proposed model may not add much theoretical contribution. Second, habit is not included in the proposed model since habit implies that the behavior in question is automatic. If a 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 the person’s intention to the extent that the behavior is habitual [23]. Because the proposed NMSV model focuses on intentions instead of actual behaviors, inclusion of a habitual factor will be less likely to improve the explanatory power of the model. Furthermore, NMSVs imply rule breaking, so end users involved in NMSVs 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. Finally, the model also does not consider interrelationships among antecedents of user attitudes toward NMSVs. The interrelationships are excluded because the aim of this study is to predict attitudes and behavioral intentions. As such, only direct effects are modeled and analyzed in order to make the research model more parsimonious. This approach is consistent with the IS literature (e.g., [90]). It should be noted that the variance (R^2) explained by a model is not affected by indirect paths [90].

Based on Eagly and Chaiken’s CMB and other theoretical considerations discussed below, we propose the NMSV model shown in Figure 1. In line with the CBM model, it is posited that user intentions to engage in NMSVs are determined by their attitudes toward the behavior, normative outcomes, and self-identity outcomes; and user attitudes toward NMSVs are in turn determined by four groups of antecedents: attitude toward target, utilitarian outcomes, normative outcomes, and self-identity outcomes. Further, the following utilitarian outcomes are posited to be salient to users when they are involved in NMSVs: (1) relative advantage for job performance, (2) perceived security risk, and (3) perceived sanctions. Relative advantage for job performance is a positive outcome that users pursue, whereas the rest are negative outcomes or side effects that they want to avoid.

Behavioral Intentions and Attitudes Toward NMSV

NMSV intentions, in this study, are defined as end user tendencies to voluntarily engage in actions that violate the organization’s security policies. Intentions are the indications of how much of an effort end users are planning to exert in order to perform the behavior [2]. According to CBM, individual behavioral intentions are partially determined by attitudes toward the behavior in question. Similarly, in the context of IS security in organizations, this relation between attitudes and behavioral intentions should also apply to NMSVs. Based on Eagly and Chaiken’s [23] conceptualization,

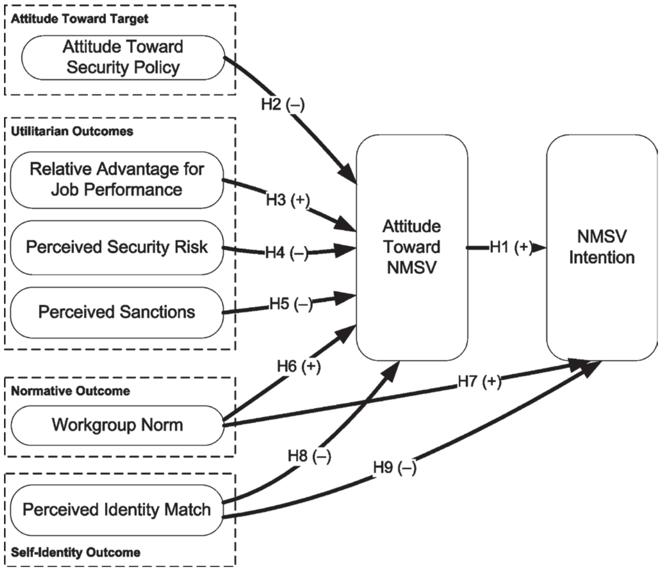

Figure 1. Nonmalicious Security Violation (NMSV) Model

attitude toward NMSV is defined as end users' evaluation of security violations in terms of their degree of favor or disfavor. Users who have a positive attitude toward an NMSV would have a greater intention to engage in such violations. Hence, it is hypothesized that:

> *Hypothesis 1: End users' attitudes toward NMSVs are positively associated with their NMSV intentions.*

Attitudes Toward Target

Targets refer to the entities to which behaviors are directed [23]. In the context of organizational IS security, policies are one of the key targets. *Attitude toward security policy* refers to the degree of favor or disfavor expressed by end users about organizational IS security policies. Users may have a negative attitude toward 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. In Lapointe and Rivard's terminology [50], security policies are the "system" that end users may resist. Users may see security measures as barriers or obstacles that create trouble rather than as a protective mechanism [1, 21]. Users may also perceive security as "futile" [21] and may believe that violating policies and bypassing security measures are justified. It is therefore hypothesized:

> *Hypothesis 2: End users' attitudes toward security policy are negatively associated with their attitudes toward NMSVs.*

Utilitarian Outcomes

Relative Advantage for Job Performance

Relative advantage for job performance is defined as the extent to which users expect their actions to help them do their job (e.g., carrying sensitive business data on an unencrypted USB (universal serial bus) memory device for convenience). As discussed previously, security is often not seen as an end user task [7]. From their perspective, end users are evaluated by how well they perform on their job role (e.g., sales revenue for a salesperson), not how secure the IS is, or how well they follow security rules. A recent survey found that users often look to their managers, rather than IS personnel, for guidance on information security–related issues [62]. This may be an indication that job performance is more important for end users (in the sense that they might consult their managers on whether they should sacrifice job performance, e.g., late submission of a business report, for security rules). Many of the problems, such as difficulties in following security rules, that end users have with security measures can be explained in terms of the mismatch between the measures and user goals and tasks [72]. End users often talk of IS security in terms of costs and benefits, and frame security measures as interference with their job responsibilities and the practical accomplishment of their work [21, 67]. In essence, end users may 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

> *Hypothesis 3: End users' evaluation of the relative advantage for job performance as a result of NMSVs is positively associated with their attitudes toward NMSVs.*

Perceived Security Risk

Perceived security risk refers to end users' evaluation of the security risk that may be caused by their violations of security policies and rules. Prior research indicates that perceptions of risk affect human behavior. In the IS literature, it has been found that perceived risk will decrease intended use of P2P (peer-to-peer) sharing software [96] and affect consumer attitudes toward online shopping and consequently their willingness and intention to buy [29, 39, 56, 60, 61].

In the context of IS security, end user perceived risk may play a similar role in affecting NMSVs. Organizational security policies are put in place to secure IS. Any actions that violate the policies may cause damage to overall IS security. If end users perceive a lower security risk, they will likely form more favorable attitudes toward an NMSV (i.e., approve of the NMSV) and hence will be more likely to engage in the NMSV. On the other hand, if users perceive a higher security risk, they will be likely to form more unfavorable attitudes toward the NMSV (i.e., disapprove of the NMSV) and hence will be less likely to engage in the NMSV. As such, it is hypothesized that

> *Hypothesis 4: End users' perceived security risk is negatively associated with their attitudes toward NMSVs.*

Perceived Sanctions

Perceived sanctions are negative outcomes that end users may try to avoid. According to the deterrence theory, assured and severe sanctions deter individuals from targeted actions [28]. The less certain and severe the sanctions, the more likely is the action. 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 [72]. In the IS security literature, sanctions have been studied in combination with other theoretical perspectives. For example, Siponen and Vance [76] examined the effect of sanctions (based on deterrence theory) along with user neutralization techniques (based on neutralization theory). Bulgurcu et al. [10], however, investigated the effects of sanctions along with costs/benefit factors (based on rational choice theory).

The deterrence theory and CBM represent different but complementary perspectives. Whereas deterrence theory focuses on investigating the security countermeasure factors that may deter security policy violation behaviors, CBM focuses on the factors end users may have in their mind that may lead to certain security violations. Based on the CMB and deterrence theory, it is therefore hypothesized that

> *Hypothesis 5: End users' perceived sanctions are negatively associated with their attitudes toward NMSVs.*

Normative Outcomes

Normative outcomes refer to the approval or disapproval that end users' significant others are expected to express in relation to the behavior in question [23]. Arguably, people in the same workgroup, including supervisor and peers, have more influence on end user behaviors than others in the organization because end users interact with their supervisor and peers on a daily basis. End users therefore have more opportunities to observe and understand their colleagues' attitudes and behaviors than they would with other employees in the same organization. In the present study, this type of approval or disapproval by a user's workgroup members (i.e., supervisor and peers) is referred to as *workgroup norm.*

Prior studies in IS use suggest that top management, supervisors, peers, and the IS department are the salient referents for users when they make decisions [43]. 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 [46]. In the present study, however, we argue that top management may have less influence than coworkers and peers do on employee day-to-day IS security-related behaviors. Social norms require an extended socialization process to learn and understand [17]. 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. Behaviors in organizations are inherently hierarchical [63]. A minimum of three levels may be considered: individual, group (e.g., department and workgroup), and organizational. Adjacent levels (e.g., individual and group) are more highly interrelated than levels farther apart (e.g., individual and organization) [63]. Accordingly, the effect of a workgroup on individuals will be stronger than that of the organization as a whole [64]. Top management can be viewed as being an organizational level factor, whereas one's supervisor and coworkers are at the workgroup level. For end users, their supervisor and coworkers within the same workgroup are more relevant than top management. They will likely use other members as role models for analyzing the appropriateness of particular beliefs, attitudes, and behaviors [71]. 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 [26]. Based on the above reasoning, we offer the following hypotheses (according to the CBM model, normative outcome expectations also have a direct effect on behavioral intention):

> *Hypothesis 6: Workgroup norms are positively associated with user attitudes toward NMSV.*

> *Hypothesis 7: Workgroup norms are positively associated with user NMSV intentions.*

Self-Identity Outcomes

Self-identity outcomes refer to affirmations or repudiations of an individual's self-concept that are anticipated to follow from engaging in a behavior [23]. Self-identities provide individuals with a sense of meaning and purpose ("who he or she is") and behavioral guidance ("how he or she ought to behave") [85, 86]. In general, individuals tend to engage in those behaviors deemed as consistent with their self-identities. For example, individuals who regard recycling as an important component of their self-identity are more motivated to engage in the behavior than those who do not [84], and individuals may donate blood partly because they believe giving blood is an important part of their self-identity as blood donors [13]. Such behaviors may be seen as "identity-enhancing events" that are associated with improved psychological well-being [85]. Conversely, individuals tend to avoid those behaviors that are deemed as inconsistent with their self-identities. Such behaviors may be seen as "identity-threatening events" that may lead to decreased psychological well-being [85]. For example, tasks (e.g., cleaning a desk) in organizational settings may be regarded as outside the range of one's profession and thus deemed unreasonable or illegitimate. Individuals may try to resist such illegitimate tasks or engage in some forms of counterproductive behaviors that may help release the "stress" caused by those tasks [74].

In the context of IS security, how end users perceive dealing with security issues and following security polices as related to their identity as business professionals (their "professional image" [70]) vis-à-vis IS employees will likely play a role in influencing their security-related behaviors. We define this perception as *perceived identity match.* In organizations, IS security is often seen as the responsibility of IS personnel. For ordinary end users, who are typically businesspeople, IS security may not really matter in the sense that it is not in their job descriptions. For example, the professional status of salespeople is more likely to be judged on their knowledge and experience in sales and their sales performance rather than on how well they are at following security rules or performing information security–related actions. In Blanton and Christie's terms [9], security-related behaviors do not "stick" to the identity of a business professional. If end users believe that strictly following organizational security policies does not improve their identities as business professionals, or doing otherwise (i.e., engaging in NMSVs) does not necessarily hurt their professional identities, they are more likely to form a positive attitude toward NMSVs and ignore these security policies.

Prior studies in the IS literature also support the above arguments. In a study of the implementation of nursing IS, Doolin and McLeod [20] found that the new systems challenged a strong professional nursing culture and a distinctive collective identity held by nurses. As a result, the new IS were not welcomed. In a similar health care setting, physicians were found to resist the implementation of IS at different levels [50]. As Lapointe and Rivard [50] suggested, user resistance can be passive (e.g., complain), active (e.g., voice objection and attempt to stop the use of a system), and aggressive (e.g., rebel and refuse to use the system). Rule breaking can best be compared to active and aggressive resistance. One reason for resistance was that the new system was perceived by physicians as a threat to their "professional status" [50]. According to the CBM model, identity outcome expectation also has a direct effect on behavioral intention. Based on the above reasoning, it is hypothesized that

> *Hypothesis 8: End users' perceived match between their identities as business professionals and following security rules and policies is negatively associated with their attitudes toward NMSVs.*
>
> *Hypothesis 9: End users' perceived match between their identities as business professionals and following security rules and policies is negatively associated with their intentions to engage in NMSVs.*

Research Method and Data Analysis

A survey of computer end users in the workplace was conducted to test the proposed NMSV model. Because IS security is often seen as a very sensitive matter, prior research in this field has faced many challenges such as low survey response rates and organizations' unwillingness to discuss security matters [49]. To overcome these difficulties, our survey used hypothetical NMSV scenarios. One advantage of this method is that scenarios can present survey respondents with concrete and detailed situations [51]. Indeed, the use of scenarios in management and IS literature is not uncommon (e.g., [5, 18, 30, 38, 76, 92]).

We developed NMSV scenarios according to guidelines suggested in the literature [91]: (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. As a result of this process, four scenarios were developed, each of which reflected security issues related to user authentication and access control (writing down passwords), hardware (using portable USB drives to carry sensitive business data), software (downloading and installing free software from the Internet), and the network (using insecure public wireless connections), respectively (see Appendix A). The survey instrument was developed from two sources: (1) existing scales borrowed and adapted from relevant literature, and (2) constructs that are unique to IS security, not available in the literature but developed specifically for this study. The instrument, including those items that were adapted from the relevant literature, was validated to ensure validity and reliability based on the development and validation strategies recommended in the literature [16, 27, 53, 57, 80, 83]. After the initial development process, a pilot study involving end users in several administrative units at a university was conducted to validate the instrument. The results of the pilot study suggested that the instrument was reliable and valid. The final list of items is provided in Appendix B.

Data Collection Procedures

Two methods were used to collect data: a paper-based survey and a Web-based survey. One of the four scenarios was randomly given to targeted participants. This approach is consistent with other research in the IS literature (e.g., [76]). For the paper-based survey, potential participants were approached in person at locations such as office buildings in business districts and industrial zones. Potential participants were asked if they are employed and use computers on a daily basis before survey packages were given to them. In total, 250 surveys were distributed and 167 (67 percent) were returned. For the Web-based survey, e-mail addresses were obtained from the Web sites of a local government and a recruiting agency. In total, survey invitations were e-mailed to 2,543 individuals (418 of whom were not available as indicated by the automatic "out of the office" e-mail replies at the time of survey). To address the concerns of privacy and e-mail spam, individual responses were not tracked and no reminder e-mails were sent. Of the targeted individuals, 168 proceeded to the final step to submit the survey. The response rate of the Web-based survey was relatively low (6.5 percent). Low response rates are not usual with mass e-mail surveys (e.g., [79]). In total, 335 responses were received and 306 of them were usable after incomplete responses were deleted. Two procedures were implemented in this study to check for common method variance (CMV): Harman's single-factor test [65, 66] and the statistical approach developed by Liang et al. [54]. The results indicated that common method bias was not a serious problem.

Hypothesis Testing

The NMSV model was tested using the partial least squares (PLS) approach. Because four different scenarios were used, we included a control variable to account for their possible influence. In addition, a number of other factors were also included as control variables, including participant age, gender, position, and data collection method, to control for their possible effects on survey responses.

We initially assumed that all hypothesized relations are linear, and therefore tested the model using standard linear PLS software.[2] According to these preliminary analyses, some of our hypotheses were unsupported.[3] However, an examination of the bivariate data plots suggested the presence of nonlinear relationships or asymmetric effects [77]. Further correlation analysis on split samples[4] also revealed such nonlinearity. For example, high security risk perceptions may prevent end users from engaging in NMSVs; however, low security risk perceptions do not necessarily cause or motivate end users to engage in NMSVs. The existence of nonlinear effects is not unusual; for example, Cheung and Lee [14] found a positive–negative asymmetry in a user satisfaction model, where negatively perceived performance of an information-quality attribute had a stronger effect than positively perceived performance. Zielke [97] found that consumer price perceptions have an asymmetric effect on price satisfaction; more specifically, price level, value for money, and special offers are both satisfiers and dissatisfiers, whereas price fairness, price perceptibility, and price processibility tend to be dissatisfiers only.

Because of the possible nonlinear relationships that may be present in the current study, standard PLS software packages based on a linear assumption may not be appropriate for testing the proposed model. Following the recommendation of an anonymous reviewer, we chose WarpPLS software (version 1.0) [47] to analyze our data because of its capability to test both linear and nonlinear relationships (e.g., U-shaped and S-shaped functions) in an integrative manner.

The results of the WarpPLS analysis provided some evidence that suggests a pattern of nonlinear effects. All the relationships among latent variables were shown as "warped" (i.e., nonlinear). Although the extent of nonlinearity varies, the plot of the relationship between perceived security risk and attitude toward NMSV (as shown in Figure 2) depicts a clear and strong nonlinear pattern: high security risk perceptions appear to have a strong impact on end users' attitudes toward NMSVs, whereas low security risk perceptions do not.

Measurement Model

The measurement model shows how each block of items relates to its construct or latent variable [15]. Convergent validity is generally achieved if three criteria are met [25]:

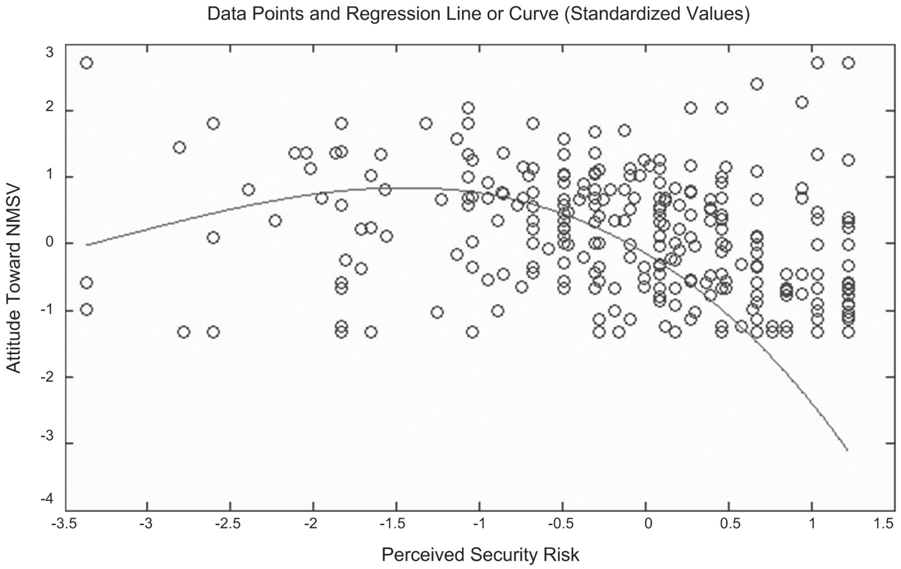

Figure 2. Example of Nonlinear Relationship

(1) all item factor loadings should be significant and greater than 0.70, (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 0.50 (or square root of AVE > 0.707), and (3) the composite reliability index for each construct should be greater than 0.80.

Based on the above criteria, the PLS results indicated that a satisfactory level of convergent validity was achieved. As shown in Table 2, all but one item loading were greater than 0.70 (all significant, $p < 0.001$).[5] The exception was the first item of *workgroup norm* (WkgpNorm1), of which the loading (0.57) was lower than the 0.70 threshold. This item was retained because (1) according to Chin [15], a loading would be considered acceptable if the loadings of other items for the same construct are high, and (2) the loading was still higher than the cutoff point of 0.4 recommended by some scholars [35, 83]. Furthermore, as shown in Table 3, the square root of AVE was greater than 0.707 for each construct and the composite reliabilities of all constructs also exceeded the minimum criterion of 0.80.

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 [25]. As shown in Table 3, the criterion for sufficient discriminant validity was also met in this study.

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

Table 2. Item Loadings and Cross-Loadings

	1	2	3	4	5	6	7	8	*p*-value
Intent1	**0.77**	0.16	–0.03	0.02	0.10	0.03	0.08	–0.03	< 0.001
Intent2	**1.05**	–0.16	0.03	–0.02	–0.10	–0.03	–0.08	0.03	< 0.001
AttSV1	0.13	**0.87**	–0.03	–0.04	0.10	0.01	–0.04	–0.08	< 0.001
AttSV2	0.07	**0.84**	–0.02	–0.03	–0.03	–0.03	–0.03	0.04	< 0.001
AttSV3	0.10	**0.91**	0.00	0.03	0.07	0.02	–0.06	–0.03	< 0.001
AttSV4	–0.12	**0.95**	0.04	0.01	–0.02	–0.02	–0.02	0.01	< 0.001
AttSV5	–0.12	**0.83**	0.08	0.03	–0.04	–0.02	0.17	0.07	< 0.001
AttSV6	–0.08	**0.86**	–0.07	0.00	–0.08	0.04	–0.01	0.00	< 0.001
IDMatch1	0.02	–0.09	**0.86**	0.12	0.02	0.05	–0.06	0.03	< 0.001
IDMatch2	0.09	–0.08	**0.90**	0.03	0.06	0.00	–0.04	0.01	< 0.001
IDMatch3	–0.07	0.06	**0.80**	0.01	0.01	0.01	0.08	0.03	< 0.001
IDMatch4	–0.06	0.14	**0.77**	–0.19	–0.11	–0.06	0.04	–0.08	< 0.001
WkgpNorm1	0.03	–0.04	0.03	**0.57**	–0.27	–0.01	–0.06	–0.10	< 0.001
WkgpNorm2	0.03	–0.08	–0.01	**0.78**	–0.15	–0.11	–0.07	0.06	< 0.001
WkgpNorm3	0.04	0.01	–0.03	**1.05**	0.22	0.09	–0.08	0.08	< 0.001
WkgpNorm4	–0.10	0.11	0.01	**0.82**	0.20	0.04	0.20	–0.05	< 0.001
Sanction1	–0.05	0.04	–0.04	0.03	**0.93**	–0.05	0.01	0.07	< 0.001
Sanction2	0.08	–0.06	0.08	–0.12	**0.77**	0.09	0.05	–0.09	< 0.001
Sanction3	–0.03	0.02	–0.03	0.10	**0.92**	–0.04	–0.07	0.02	< 0.001
Risk1	–0.06	0.01	0.00	–0.01	–0.11	**0.92**	0.05	0.07	< 0.001
Risk2	–0.04	–0.01	0.01	0.00	–0.12	**0.94**	0.01	0.06	< 0.001
Risk3	0.13	0.00	–0.01	0.01	0.30	**0.72**	–0.07	–0.18	< 0.001
JobPerf1	0.12	0.07	0.03	0.01	0.05	0.01	**0.75**	–0.07	< 0.001
JobPerf2	–0.01	–0.04	0.00	–0.01	–0.03	–0.02	**0.94**	0.02	< 0.001
JobPerf3	–0.05	–0.03	0.00	0.01	–0.01	–0.02	**0.98**	0.04	< 0.001
JobPerf4	–0.05	0.01	–0.03	–0.01	–0.01	0.03	**0.98**	0.00	< 0.001
AttPol1	–0.06	0.03	0.12	0.03	–0.09	0.00	0.05	**0.90**	< 0.001
AttPol2	0.05	0.00	–0.01	–0.06	–0.01	0.09	–0.02	**0.81**	< 0.001
AttPol3	–0.08	–0.02	–0.10	0.18	0.08	–0.13	–0.07	**0.96**	< 0.001
AttPol4	0.08	–0.01	–0.01	–0.13	0.02	0.03	0.03	**0.87**	< 0.001

Notes: Factor loadings greater than 0.40 are shown in boldface. Factors: 1 = NMSV Intention, 2 = Attitude Toward NMVS, 3 = Perceived Identity Match, 4 = Workgroup Norm, 5 = Perceived Sanction, 6 = Perceived Security Risk, 7 = Relevant Advantage for Job Performance, 8 = Attitude Toward Security Policy.

predictiveness of the theoretical model and standardized path coefficients indicate the strength of the relationship between the independent and dependent variables [15]. In this study, a bootstrapping resampling procedure (with 500 samples) was carried out to estimate the significance of paths in the structural model. The results are shown in Figure 3.

The R^2 value of 0.49 indicates that the theoretical model explained a substantial amount of variance in *NMSV intention.* In addition, 37 percent of the variance for *attitude toward NMSV* is accounted for by the model. Given the minimum 10 percent criterion [24], which suggests that the R^2 value of a dependent variable should be at

Table 3. PLS Measurement Model—Construct Correlations

Latent variable correlations	1	2	3	4	5	6	7	8
1 NMSV Intention	0.91							
2 Attitude Toward NMSV	0.61	0.88						
3 Perceived Identity Match	–0.30	–0.28	0.83					
4 Workgroup Norm	0.53	0.54	–0.25	0.81				
5 Perceived Sanctions	–0.30	–0.30	0.26	–0.47	0.87			
6 Perceived Security Risk	–0.36	–0.35	0.25	–0.49	0.44	0.86		
7 Relative Advantage for Job Performance	0.43	0.38	–0.13	0.46	–0.08	–0.20	0.92	
8 Attitude Toward Security Policy	–0.28	–0.25	0.22	–0.51	0.35	0.61	–0.22	0.88
Composite reliability	0.90	0.90	0.95	0.90	0.88	0.91	0.90	0.96
Cronbach's alpha	0.78	0.78	0.94	0.85	0.82	0.85	0.82	0.94
Average variances extracted	0.82	0.82	0.77	0.69	0.65	0.77	0.75	0.84

Notes: Off diagonal numbers are interconstruct correlations; diagonal numbers are the square roots of AVE (average variance extracted).

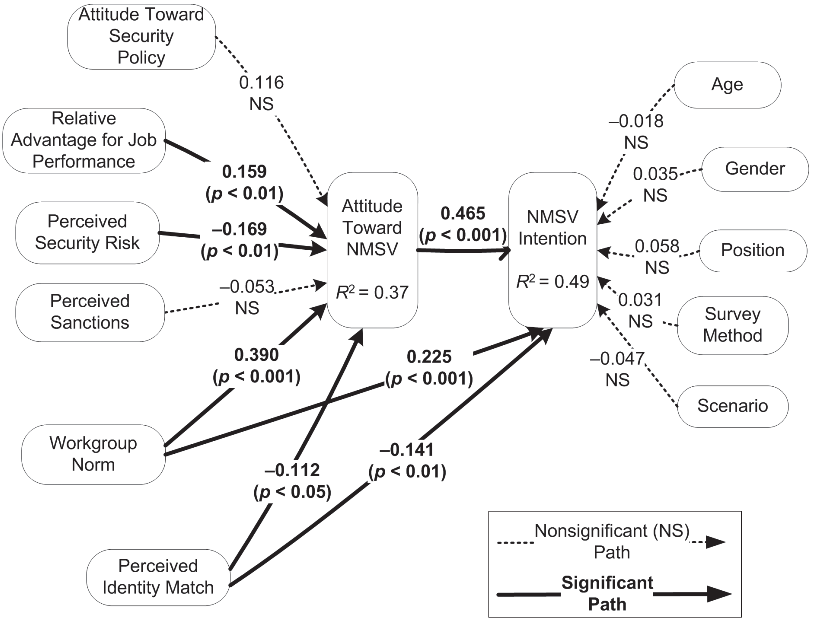

Figure 3. Nonlinear PLS Analysis Results

least 10 percent in order to make any meaningful interpretation, the theoretical model demonstrated substantive explanatory power.

Consistent with the CBM, *attitude toward NMSV* (β = 0.465, p < 0.001), *workgroup norm* (β = 0.225, p < 0.001), and *perceived identity match* (β = –0.141, p < 0.01) had significant effects on *NMSV intention,* thereby supporting Hypotheses 1, 7, and 9. In addition, *relative advantage for job performance* (β = 0.159, p < 0.01), *perceived security risk* (β = –0.169, p < 0.01), *workgroup norm* (β = 0.390, p < 0.001), and *perceived identity match* (β = –0.112, p < 0.05) had significant effects on *attitudes toward NMSV,* demonstrating support for Hypotheses 3, 4, 6, and 8. Contrary to what is predicted by the theoretical model, *attitude toward security policy* and *perceived sanctions* did not have significant effects on *attitudes toward NMSV.* Thus, Hypotheses 2 and 5 were not supported. The influences of all the control variables, including scenario, age, gender, job position, and data collection method, were not significant.

Discussion and Conclusions

Key Findings

What are the factors influencing end user intentions to engage in NMSVs*?* Consistent with Eagly and Chaiken's theory [23], our empirical results demonstrated that *relative advantage for job performance, perceived security risk, workgroup norm,* and *perceived identity match* are the key predictors after the effects of age, genders, job positions, survey methods, and scenarios are controlled for.

Relative advantage for job performance and perceived security risk are utilitarian outcomes in Eagly and Chaiken's theory [23]. Relative advantage for job performance can be seen as a positive outcome that end users try to achieve. The significant influence of relative advantage for job performance confirms that job performance is an important decision factor when end users deal with security issues. If an action can help them carry out their business tasks and improve productivity, users will likely engage in the action even if such an action violates organizational security policies. The importance of job performance can also be explained from the goal-oriented behavioral perspective [31]. Job performance is the goal that users try to accomplish by using necessary means. For them, security is often seen as a nontask 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). Perceived security risk can be seen as a negative outcome that end users try to avoid. Our results confirm that security risk is an important factor influencing users' behavioral decisions. The higher the security risk users perceive, the less likely they will engage in NMSVs. This is consistent with other risk-related research in the IS literature (e.g., [29, 39, 56, 60, 61]). Consistent with the CBM, the effects of relative advantage for job performance and perceived security risk are fully mediated by user attitudes toward NMSVs.

The significant influence of workgroup norms (normative outcome) may be explained by the impact of job relevance and user expertise on security and IS in general. These two factors moderate the way in which end users evaluate the use of information technology (IT) [8]. The less relevant an IS application is to their job and the less IS 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. Similarly, in an IS security context, end users often lack security knowledge and skills and they may also view security as irrelevant to their jobs. It is not surprising that they turn to their supervisors and coworkers for guidance and advice on how to deal with security-related issues rather than to depend on their own evaluation of the situation at hand. In fact, it has been suggested that users may be more inclined to follow the practices and advice of their coworkers [21, 93]. In particular, end users tend to "delegate" security issues to other individuals they know [21]. This finding is consistent with other research in the IS security literature. For example, subjective norm was found to influence user intention to comply with security policies [10, 33]. 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 [71].

As confirmed by the empirical results, workgroup norms influence user NMSV intentions both indirectly and directly. On the one hand, the effect of workgroup norms is mediated by user attitudes toward NMSV. In this case, users may have a favorable opinion if their workgroups favor the NMSV in question. Such an effect is independent of user evaluation of the utilitarian consequences (relative advantage for job performance and perceived security risk). On the other hand, workgroup norms also influence user NMSV intentions directly. In this case, they may not have a clear attitude toward those behaviors. In other words, they may not know or do not care whether those behaviors are right or wrong as long as they are doing the same thing as their peers.

Our results suggest that perceived identity match (self-identity outcome) is another key predictor of end user intentions to engage in NMSVs. More specifically, end users' perceived match between their images of business professionals and strictly adhering to IS security policies plays an important role in preventing their NMSVs. This finding is consistent with previous research in the human behavior literature. For example, perceptions of self-identity was found to be a significant factor influencing decisions to donate blood [13] or to engage in household recycling [84]. Similar to the effect of workgroup norms, perceived identity match influences user NMSV intentions both indirectly and directly. On the one hand, the effect of perceived identity match is mediated by user attitudes toward NMSV. In this case, if users believe that dealing with security issues and following security policies is an important part of them being business professionals, they will likely form an unfavorable opinion of NMSVs, and may subsequently refrain from engaging in NMSVs. On the other hand, perceived identity match directly influences user NMSV intentions. Users may refrain from engaging in an NMSV because it does not match their image of business professionals even if the behavior may be a good idea from a utilitarian perspective.

Our empirical results also indicated that two factors in the original proposed model were not significant. The first factor is attitudes toward security policies. One plausible explanation for its nonsignificant influence is the "relevance principle" [23, 78], which suggests that the link between "attitude toward target" and "attitude toward behavior" may require that people perceive that the behavior provides a means of expressing their attitudes toward the target. In our study, this principle suggests that the link may be significant only when users perceive NMSVs as a way to express their attitudes toward the policy. This condition may not always be met in the sense that users do not necessarily need to violate a policy in order to express their opinions about the policy. The nonsignificant effect of attitudes toward security policy was consistent with other research in the IS literature. For example, Herath and Rao [33] found that users' attitudes toward a policy did not influence their intention to comply with the policy. The second nonsignificant factor was perceived sanctions. From a goal-directed behavioral perspective, it is a negative consequence that end users desire to avoid. The negative effect of perceived sanctions may be outweighed by the importance of good job performance. It should be noted that the nonsignificant effect of sanctions is consistent with the findings of some studies in the IS literature (e.g., [18, 76]).

Theoretical Contributions

The current study makes several significant contributions to the IS security literature. First, in the IS security literature, end users' attitudes toward NMSV and its antecedents have not been fully addressed. This research fills the gap by integrating both inhibiting and motivating factors, including relative advantage for job performance, perceived security risk, workgroup norms, and perceived identity match. These constructs were either newly introduced or reconceptualized from existing IS and related literature. To the best of our knowledge, our study is the first to apply Eagly and Chaiken's [23] CBM to the examination of NMSVs issues. This new theoretical perspective helps to advance our understanding of user motivations to engage in NMSVs in addition to what was offered by the deterrence [18] and neutralization [76] perspectives that have been studied in the IS literature.

Second, the present 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. Such expectations strongly influence their attitudes toward NMSVs. Taking this finding into consideration, the nonsignificance of perceived sanctions should not be examined in isolation. From the perspective of deterrence theory in criminology, a behavior is punishable because it causes (or has the potential to cause) damage 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 NMSVs, however, job performance is a very legitimate and important goal for users. End users are usually evaluated on their job performance and not as heavily on how well they follow security procedures. Thus, deterrence theory only may not provide sufficient explanations about NMSVs without a consideration of organizational settings.

Third, the relationship between normative outcomes and attitudes toward behavior has been largely ignored in the current IS security literature or at best has been assumed to independently affect intentions (an exception is Titah and Barki [87], who examined the interaction between social norms and attitudes, but not how one influences the other). Our results suggest that user attitudes toward NMSVs are indeed influenced by perceived norms. Furthermore, in the present study, normative outcomes were conceptualized as the approval or disapproval of NMSVs expressed by people within a workgroup. This is different from the widely used terms of "social norm" and "subjective norm," which are often broadly operationalized as the opinions held by those people who are important to the end user 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. For example, subjective norm was operationalized in Herath and Rao's study [33] as the opinions held by top management, supervisors, colleagues, IS security department, and other computer specialists. However, the influence of top management and the IS security department on the views of end users were not significant. This essentially supports the conceptualization of workgroup norm in the present study. Our approach is also in line with prior research in the management and human behavior literature. For example, Fulk [26] differentiated "workgroup" and "ego network" and found that these two groups had different influences on member decisions to use communication technology; Terry et al. [84] differentiated "group norm" and "subjective norm" and found that group norm was related to behavioral intention for those who identified strongly with the group. The finding of the workgroup norm's strong effect (both direct and indirect) on end user NMSV intentions has an important theoretical implication. It suggests that NMSVs may not be just an individual-level phenomenon but more importantly a group-level consensus. Future group-level studies may provide a better understanding of the reasons why users engage in such behaviors.

Fourth, to the best of our knowledge, the present study is the first to empirically test the effects of self-identity outcomes in the IS security literature. Our results suggest that self-identity outcomes (operationalized as perceived identity match) did have a significant influence on user attitudes and NMSV intentions. In other words, end users will consider not only the short-term consequences of NMSVs but also how their own behaviors are related to their long-term self-images as business professionals (or "who they are" as business professionals). This finding raises an interesting question that warrants future research. Self-identity can be seen as a long-term and enduring factor (as compared to situational factors). People may not easily change their perceptions about who they are. The subsequent question is then, how does self-identity influence repeated NMSVs by end users? We suspect that self-identity and other significant factors found in the present study may play out differently. Prior research provided initial evidence for such differences. For example, Charng et al. [13, p. 310] found that long-term blood donors are influenced by self-identity more than social norm, which actually becomes a negative factor; Karahanna et al. [43] found that the effect of social norms diminishes with continued use of IT.

Finally, the findings of the present study also have an implication for research methodology. We found that most of the relationships proposed in our study are nonlinear. Such nonlinear effects may not be sufficiently accounted for with a simple additive linear model. Relying solely on linear models may run the risk of systematically misestimating the impact of independent variables on user perceptions or behaviors [14]. Our results demonstrated that directly testing such effects in PLS models may be a viable option, given the built-in capabilities of handling nonlinearity in computer software such as WarpPLS.

Practical Implications

This study has several important implications for IS security management practice. The results suggest that a shift in 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 mind-set for these strategies may be best described as "what should top management and end users know or do to improve security." A better strategy may be a "user-centered" one, which raises the question, "what should IS management do to help end users do their job without focusing exclusively on IS security?"

First, end users are pragmatic and they care about their job performance more than they care about IS security. When implementing a security policy, IS management should first address what the policy means for end users. Does it require extra effort to help them do their jobs? The answer to this question will ultimately influence whether end users will comply with the policy. Perhaps a more important question is, how should the enforcement of security policies be reflected in employee performance evaluation? Employees will likely ignore security policies if they are solely evaluated based on their job or business outcomes. At the same time, if employees are to be evaluated on behavior (what they do with IS) as well, then organizations need to set a balance between IS and business needs.

Second, this study has indicated that end users' evaluation of the security risks associated with their actions has a significant influence on their attitudes toward these actions. This suggests that the practice of user security training and education may need to shift focus. The common wisdom is that the IS department should provide sufficient training and education to make end users aware of potential security risks. However, security risk in itself may be too vague for end users and mere "awareness" may not be sufficient. More importantly, security training and education should enable end users to have a good understanding of how NMSVs will affect their job performance and business performance of the organization. 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. From an end user professional self-identity perspective, security training and education should emphasize that there is no "IS security" per se, but rather "business security." At the organizational level, eliminating the IS versus business division and integrating the two functions may be a better option, albeit a difficult one.

Third, the findings of the present study and others [18, 76] raise some serious questions about the practical effectiveness of measures used in IS security management, although researchers caution that it may be premature to draw a decisive conclusion about the ineffectiveness of deterrent measures [76]. If end users are trying to achieve legitimate ends (e.g., job performance), prohibiting certain means of using IS (e.g., NMSVs) will be problematic. Thus, it is important for IS security management to align security objectives with end user objectives. For example, instead of the 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 security policy violations.

Finally, IS management should try to disseminate security awareness through exemplary day-to-day secure computing behaviors. Organizations may consider embedding IS personnel as end user support within other business functions. Another possible strategy is to train "power users"—who have relatively strong IS and security knowledge—in business departments. These power users could be role models and act as a resource for other people in the same workgroup when they need to deal with IS security issues. Furthermore, 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 IS-related issues. End users should be able to turn to IS personnel (in addition to power users) rather than their supervisors and coworkers for advice 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.

Limitations and Future Research

Certain limitations of this study should be considered when interpreting the results. First, as for 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. Longitudinal research with multiple sources of measurement may help alleviate this problem and further validate the causal relationships. Second, this study used four specific security scenarios to solicit participant responses. Although this scenario-based method is commonly accepted in the literature, a limitation of this method is that the scenarios do not include every possible type of security violation. Future research should include more types of NMSVs to further test the proposed model. Third, the model focuses on NMSV intention as the ultimate independent variable. Although this practice is not uncommon in the IS literature, future research should try to measure actual security violations in a field setting to improve the model's external validity and generalizability. Finally, in the current study we limited our scope to NMSVs, which is one of the possible ways of how users deal with IS security issues at work. Future research should investigate how NMSVs relate to other types of security behavior. One particular issue is the investigation of the similarity and differences between NMSVs and malicious violations. For example, do they share any common antecedents? Can the two types of violations be explained from the same theoretical perspective? Another issue is the relationship between security violations and security compliance. In the current study, we argued that NMSVs and security compliance are distinct behaviors that have different antecedents. Future research should look at how the two types of behaviors can be integrated in a single model, which would advance our understanding of user security behavioral issues and provide some important guidance for security management practice.

Acknowledgments: This study was funded by the Social Sciences and Humanities Research Council of Canada. The authors are grateful to Editor-in-Chief Vladimir Zwass and four anonymous reviewers for their invaluable suggestions and insightful comments, which helped to improve the paper significantly.

Notes

1. In their study, Siponen and Vance [76] did not provide an explicit definition or scope of "violation of security policies," although they provided a list of commonly reported violations.

2. We used SmartPLS 2.0 M3 Release [69] for our initial linear model testing.

3. In this paper, we only report the data analysis results by using nonlinear algorithm provided by WarpPLS software. As a comparison, the results of our initial analysis were as follows. Variance explained: NMSV intention (0.49), attitude toward NMSV (0.36), which were the same as the nonlinear model; significant paths ($p < 0.05$): relative advantage for job performance → attitude toward NMSV ($\beta = 0.18$), workgroup norm → attitude toward NMSV

(β = 0.39), workgroup norm → NMSV intention (β = 0.24), attitude toward NMSV → NMSV intention (β = 0.41). However, the paths perceived security risk → attitude toward NMSV, perceived identity match → attitude toward NMSV, and perceived identity match → NMSV intention were not significant under the linear relationship assumption but significant under the nonlinear relationship assumption.

4. The method of splitting samples and correlation analysis is discussed in detail elsewhere in the literature (e.g., [11, 77]).

5. The loadings of two items, Intent1 (1.05) and WkgpNorm3 (1.05), were greater than one. According to Jöreskog [42] and Kock [48], standardized coefficients can be larger than one when the oblique rotation method is used (this is the case for WarpPLS).

References

1. Adams, A., and Blandford, A. Bridging the gap between organizational and user perspectives of security in the clinical domain. *International Journal of Human–Computer Studies, 63,* 1–2 (2005), 175–202.

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

3. Ajzen, I. Constructing a TPB questionnaire: Conceptual and methodological considerations. University of Massachusetts, Amherst, 2006 (available at http://people.umass.edu/aizen/pdf/tpb.measurement.pdf).

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

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

6. Baskerville, R.L., and Siponen, M.T. An information security meta-policy for emergent organizations. *Logistics Information Management, 15,* 5–6 (2002), 337–346.

7. Besnard, D., and Arief, B. Computer security impaired by legitimate users. *Computers & Security, 23,* 3 (2004), 253–264.

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

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

10. Bulgurcu, B.; Cavusoglu, H.; and Benbasat, I. Information security policy compliance: An empirical study on rationality-based beliefs and information security awareness. *MIS Quarterly, 34,* 3 (2010), 523–548.

11. Cenfetelli, R.T. The inhibitors of technology use. Ph.D. dissertation, University of British Columbia, 2004.

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

13. Charng, H.W.; Piliavin, J.A.; and Callero, P.L. Role identity and reasoned action in the prediction of repeated behavior. *Social Psychology Quarterly, 51,* 4 (1988), 303–317.

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

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

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

17. Coleman, J.S. *Foundations of Social Theory.* Cambridge, MA: Belknap Press, 1990.

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

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

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

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

22. Dubie, D. End users behaving badly. *Network World,* December 10, 2007 (available at www.networkworld.com/slideshows/2007/121007-end-users-behaving-badly.html).

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

24. Falk, R.F., and Miller, N.B. *A Primer for Soft Modeling.* Akron, OH: University of Akron Press, 1992.

25. Fornell, C., and Larcker, D.F. Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18,* 1 (1981), 39–50.

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

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

28. Gibbs, J.P. *Crime, Punishment, and Deterrence.* New York: Elsevier, 1975.

29. Grazioli, S., and Jarvenpaa, S.L. 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 (2000), 395–410.

30. Harrington, S.J. The effects of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly, 20,* 3 (1996), 257–278.

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

32. Herath, T., and Rao, H.R. Encouraging information security behaviors in organizations: Role of penalties, pressures, and perceived effectiveness. *Decision Support Systems, 47,* 2 (2009), 154–165.

33. Herath, T., and Rao, H.R. Protection motivation an deterrence: A framework for security policy compliance in organizations. *European Journal of Information Systems, 18,* 2 (2009), 106–125.

34. Hilton, D.J., and Slugoski, B.R. Knowledge-based causal attribution—The abnormal conditions focus model. *Psychological Review, 93,* 1 (1986), 75–88.

35. Hulland, J. Use of partial least squares (PLS) in strategic management research: A review of four recent studies. *Strategic Management Journal, 20,* 2 (1999), 195–204.

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

37. Information security breaches survey 2008. Department for Business Enterprise & Regulatory Reform (BERR), London, 2008 (available at www.bis.gov.uk/files/file45714.pdf).

38. James, T.; Pirim, T.; Boswell, K.; Reithel, B.; and Barkhi, R. 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.* Hershey, PA: IGI Global, 2008, pp. 57–78.

39. Jarvenpaa, S.L.; Tractinsky, N.; and Vitale, M. Consumer trust in an Internet store. *Information Technology and Management, 1,* 1–2 (2000), 45–71.

40. Jehn, K.A.; Northcraft, G.B.; and Neale, M.A. Why differences make a difference: A field study of diversity, conflict, and performance in workgroups. *Administrative Science Quarterly, 44,* 4 (1999), 741–763.

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

42. Jöreskog, K.G. How large can a standardized coefficient be? Scientific Software International, Chicago, 1999 (available at www.ssicentral.com/lisrel/techdocs/HowLargeCana StandardizedCoefficientbe.pdf).

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

44. Kelloway, E.K.; Loughlin, C.; Barling, J.; and Nault, A. Self-reported counterproductive behaviors and organizational citizenship behaviors: Separate but related constructs. *International journal of Selection and Assessment, 10,* 1–2 (2002), 143–151.

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

46. Knapp, K.J.; Marshall, T.E.; Rainer, R.K.; and Ford, F.N. Information security: Management's effect on culture and policy. *Information Management & Computer Security, 14,* 1 (2006), 24–36.

47. Kock, N. WarpPLS 1.0 user manual. ScriptWarp Systems, 2010 (available at www.scriptwarp.com/warppls/UserManual.pdf).

48. Kock, N. Why are cross-loadings so low in WarpPLS? WarpPLS, 2010 (available at http://warppls.blogspot.com/2010/01/why-are-cross-loadings-so-low-in.html).

49. Kotulic, A.G., and Clark, J.G. Why there aren't more information security research studies. *Information & Management, 41,* 5 (2004), 597–607.

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

51. Lee, R.M. *Doing Research on Sensitive Topics.* Newbury Park, CA: Sage, 1993.

52. Leonard, L.N.K., and Cronan, T.P. Illegal, inappropriate, and unethical behavior in an information technology context: A study to explain influences. *Journal of the Association for Information Systems, 1,* 1 (2001), Article 12.

53. Lewis, B.R.; Templeton, G.F.; and Byrd, T.A. A methodology for construct development in MIS research. *European Journal of Information Systems, 14,* 4 (2005), 388–400.

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

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

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

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

58. Myyry, L.; Siponen, M.; Pahnila, S.; Vartiainen, T., and Vance, A. What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems, 18,* 2 (2009), 126–139.

59. Pahnila, S.; Siponen, M.T.; and Mahmood, A. Employees' behavior towards IS security policy compliance. In R.H. Sprague (ed.), *Proceedings of the 40th Annual Hawaii International Conference on System Sciences.* Los Alamitos, CA: IEEE Computer Society Press, 2007.

60. Pavlou, P.A. Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce, 7,* 3 (2003), 69–103.

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

62. Perceptions and behaviors of remote workers: Keys to building a secure company. White Paper, Cisco Systems, San Jose, CA, 2006.

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

64. Ployhart, R.E., and Schneider, B. Multilevel selection and prediction: Theories, methods,

and models. In A. Evers, O. Omit-Voskuyl, and N. Anderson (eds.), *The Blackwell Handbook of Personnel Selection.* Malden, MA: Blackwell, 2005, pp. 495–516.

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

66. Podasakoff, P.M.; MacKenzie, S.B.; Lee, J.-Y.; and Podsakoff, N.P. Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88,* 5 (2003), 879–903.

67. Post, G.V., and Kagan, A. Evaluating information security tradeoff: Restricting access can interfere with user tasks. *Computers & Security, 26,* 3 (2007), 229–237.

68. Richardson, R. CSI computer crime and security survey. Computer Security Institute, New York, 2010.

69. Ringle, C.M.; Wende, S.; and Will, S. SmartPLS 2.0 (M3) beta. Hamburg, 2005.

70. Roberts, L.M. Changing faces: Professional image construction in diverse organizational settings. *Academy of Management Review, 30,* 4 (2005), 685–711.

71. Robinson, S.L., and O'Leary-Kelly, A.M. Monkey see, monkey do: The influence of work groups on the antisocial behavior of employees. *Academy of Management Journal, 41,* 6 (1998), 658–672.

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

73. Schneier, B. *Secrets and Lies: Digital Security in a Networked World.* Indianapolis: Wiley Computer, 2000.

74. Semmer, N.K.; Tschan, F.; Meier, L.L.; Facchin, S.; and Jacobshagen, N. Illegitimate tasks and counterproductive work behavior. *Applied Psychology: An International Review, 59,* 1 (2010), 70–96.

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

76. Siponen, M.T., and Vance, A. Neutralization: New insight into the problem of employee information systems security policy violation. *MIS Quarterly, 34,* 3 (2010), 487–502.

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

78. Snyder, M., and Kendzierski, D. Acting on one's attitudes: Procedures for linking attitude and behavior. *Journal of Experimental Social Psychology, 18,* 2 (1982), 165–183.

79. Spears, J.L., and Barki, H. User participation in information systems security risk management. *MIS Quarterly, 34,* 3 (2010), 503–522.

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

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

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

83. Straub, D.W.; Boudreau, M.; and Gefen, D. Validation guidelines for IS positivist research. *Communications of the Association for Information Systems, 13,* 1 (2004), 380–427.

84. Terry, D.J.; Hogg, M.A.; and White, K.M. The theory of planned behaviour: Self-identity, social identity and group norms. *British Journal of Social Psychology, 38,* 3 (1999), 225–244.

85. Thoits, P.A. Multiple identities and psychological well-being: A reformulation and test of the social isolation hypothesis. *American Sociological Review, 48,* 2 (1983), 174–187.

86. Thoits, P.A. On merging identity theory and stress research. *Social Psychology Quarterly, 54,* 2 (1991), 101–112.

87. Titah, R., and Barki, H. Nonlinearities between attitude and subjective norms in information technology acceptance: A negative synergy? *MIS Quarterly, 33,* 4 (2009), 827–844.

88. Triandis, H.C. *Interpersonal Behavior.* Monterey, CA: Brooks/Cole, 1977.

89. Tyler, T.R., and Blader, S.L. Can businesses effectively regulate employee conduct? The antecedents of rule following in work settings. *Academy of Management Journal, 48,* 6 (2005), 1143–1158.

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

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

92. Webster, J., and Trevino, L.K. Rational and social theories as complementary explanations of communication media choices: Two policy-capturing studies. *Academy of Management Journal, 38,* 6 (1995), 1544–1572.

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

94. Workman, M., and Gathegi, J. Punishment and ethics deterrents: A study of insider security contravention. *Journal of the American Society for Information Science and Technology, 58,* 2 (2006), 212–222.

95. Workman, M.; Bommer, W.H.; and Straub, D.W. Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24,* 6 (2008), 2799–2816.

96. Xu, H.; Wang, H.; and Teo, H.-H. Predicting the usage of P2P sharing software: The role of trust and perceived risk. In R.H. Sprague (ed.), *Proceedings of the 38th Annual Hawaii International Conference on System Sciences.* Los Alamitos, CA: IEEE Computer Society Press, 2005.

97. Zielke, S. Exploring asymmetric effects in the formation of retail price satisfaction. *Journal of Retailing and Consumer Services, 15,* 5 (2008), 335–347.

98. Zviran, M., and Haga, W.J. Password security: An empirical study. *Journal of Management Information Systems, 15,* 4 (Spring 1999), 161–185.

Appendix A: Security Scenarios

Each survey participant was given one of the following NMSV scenarios.

Scenario 1: Writing Down the Password

Alex is a senior manager at your organization, which recently installed a computer system for customer record management. The IT department gave users their own user names 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 them. 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 user name 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, such as loss and disclosure of confidential corporate data and spreading of computer viruses. 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 reports. 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 the software 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 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 to do some work when having a coffee at coffee shops. One thing that Kelly likes 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 connections for business purposes due to security reasons. Most free wireless connections and communications 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 the 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 Kelly's action of using an unsecure public wireless network for business purposes as described in the scenario.

Appendix B: Measurement Items

General Items

The following are general items that are shown to participants before the security scenario.

Perceived 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 [88]. 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 my work 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 Toward Security Policy

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

AttPol1: This security policy helps secure computer systems.
AttPol2: This security policy is absolutely necessary.
AttPol3: This security policy is effective for securing computer systems.
AttPol4: This security policy is important.

Perceived Security Risk of NMSV

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

Risk1: The action can cause damages to computer security.
Risk2: The action can put important data at risk.
Risk3: The action will most likely cause security breaches.

Relative Advantage for Job Performance

Four items were used to capture user evaluation of the relative advantage for job performance. Three items were adapted from literature on the measurement of "relative advantage" of using technology [57]. A new item (JobPerf4) was created to reflect the convenience aspect of NMSV.

JobPerf1: The action helps improve my job performance.
JobPerf2: The action makes it more convenient for me 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 Sanctions

Perceived sanctions can be conceptualized in terms of sanction certainty and sanction severity (e.g., [18]) or as a single latent variable (e.g., [10]). In this paper, we follow the second approach. The following items were adapted from D'Arcy et al. [18]:

Sanction1: The likelihood my organization would punish me for engaging in the action is (very low . . . very high).
Sanction2: I will be reprimanded eventually if my organization is aware of my action.
Sanction3: If the management decides to punish me, the punishment would be (not severe at all . . . very severe).

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 [26, 40]. 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 of this action.
WkgpNorm3: My supervisor will not object to this action.
WkgpNorm4: My coworkers will think that I should do this action.

Attitude Toward NMSV

The items for measuring user attitude toward NMSV are created in accordance with the structure recommended by Ajzen [3]. The following six adjective pairs were used to form the items by completing the sentence: "For me to engage in the action is . . .":

AttSV1: a (bad . . . good) idea.
AttSV2: (harmful . . . beneficial).

AttSV3: (wrongful . . . rightful).
AttSV4: (unethical . . . ethical).
AttSV5: (worthless . . . valuable).
AttSV6: (illegitimate . . . legitimate).

NMSV 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.