OULU 2011
A 578

ACTA UNIVERSITATIS OULUENSIS

Gregory Moody

A MULTI-THEORETICAL PERSPECTIVE ON IS SECURITY BEHAVIORS

UNIVERSITY OF OULU,
FACULTY OF SCIENCE,
DEPARTMENT OF INFORMATION PROCESSING SCIENCE

ACTA UNIVERSITATIS OULUENSIS
A Scientiae Rerum Naturalium 578

GREGORY MOODY

A MULTI-THEORETICAL PERSPECTIVE ON IS SECURITY BEHAVIORS

Academic dissertation to be presented with the assent of the Faculty of Science of the University of Oulu for public defence in OP-sali (Auditorium L10), Linnanmaa, on 21 October 2011, at 12 noon

UNIVERSITY OF OULU, OULU 2011

Acta Univ. Oul. A 578, 2011

Supervised by
Professor Mikko Siponen
Doctor Seppo Pahnila

Reviewed by
Professor H. R. Rao
Associate Professor Sung Kim

ISBN 978-951-42-9560-7 (Paperback)
ISBN 978-951-42-9561-4 (PDF)

ISSN 0355-3191 (Printed)
ISSN 1796-220X (Online)

Cover Design
Raimo Ahonen

JUVENES PRINT
TAMPERE 2011

Moody, Gregory, A multi-theoretical perspective on IS security behaviors.
University of Oulu, Faculty of Science, Department of Information Processing Science, P.O. Box 3000, FI-90014 University of Oulu, Finland
Acta Univ. Oul. A 578, 2011
Oulu, Finland

Abstract

Increasingly, organizations and individuals rely upon technologies and networks more and more. Likewise, these environments are infested with more dangers, which could be avoided if computer users were to follow general security guidelines or procedures. Despite the ever-increasing threat, little research has addressed or explained why individuals purposefully engage in behaviors that make them more vulnerable to these threats, rather than avoiding or protecting themselves from such threats. Despite the advantage that could be afforded by understanding the motivations behind such behaviors, research addressing these behaviors is lacking or focused on very specific theoretical bases.

This dissertation addresses this research gap by focusing on security-related behaviors that have yet to be addressed in this research stream, and by using novel theoretical perspectives that increase our insight into these types of behaviors. Four studies (n = 1,430) are tested and reported here that support the four behaviors and theoretical perspectives that are of focus in this dissertation.

By considering additional theories, constructs, and theoretical perspectives, this dissertation provides several important contributions to security-related behaviors. The results of this study provide new insights into the motivations behind the purposeful enactment of behaviors that increase one's vulnerability to technological threats and risks.

Keywords: anonymity, behavior, control, control balance theory, extended parallel processing model, risk, security, theory of interpersonal behavior, trust, whistle blowing

Moody, Gregory, Moniteoreettinen näkökulma tietoturvakäyttäytymiseen.
Oulun yliopisto, Luonnontieteellinen tiedekunta, Tietojenkäsittelytieteiden laitos, PL 3000, 90014 Oulun yliopisto
Acta Univ. Oul. A 578, 2011
Oulu

Tiivistelmä

Organisaatiot ja ihmiset ovat yhä enenevissä määrin riippuvaisia teknologiasta ja tietoverkoista. Tällöin he myös kohtaavat entistä enemmän tietoturvariskejä, joita olisi mahdollista välttää noudattamalla tietoturvaohjeita ja -politiikkoja. Huolimatta näistä jatkuvasti yleistyvistä riskeistä, tähän mennessä ei juurikaan ole tehty tutkimusta, joka selittää ihmisten tietoista tietoturvaohjeiden ja -politiikkojen laiminlyöntiä, joka altistaa heidät tietoturvariskeille. Aikaisempi ihmisten tietoturvakäyttäytymisen syiden ymmärtämiseen keskittyvä tutkimus tarkastelee ilmiötä yksipuolisesti tiettyihin teoreettisiin lähtökohtiin nojautuen.

Tämä väitöskirjatyö tarkastelee ihmisten tietoturvakäyttäytymisen syitä uudesta teoreettisesta näkökulmasta. Väitöskirja sisältää neljä tutkimusta (n = 1430), jotka tarkastelevat erityyppistä tietoturvakäyttäytymistä erilaisista teoreettisista lähtökohdista. Väitöskirja täydentää olemassa olevaa tietoturvakäyttäytymisen tutkimusta uusien teorioiden, käsitteiden ja teoreettisten näkökulmien avulla.

Asiasanat: tietoturva, tietoturvakäyttäytyminen, tietoturvariskit

Dedication

I dedicate this work to my family. Kelly and Ryan were brave and willing enough to brave the beginnings of a Finnish winter so that I could work at the Information Systems Security Research Center at the University of Oulu. It was a great experience and I was only able to complete this work due to the dedication of my wife, Kelly.

I also dedicate this work to Mikko Siponen, my advisor for this work. Mikko was a gracious host and provided me with this excellent opportunity to work for the ISSRC and to further advance my research agenda in regards to IS security research. Those few months were very helpful for my career and I am grateful for the experiences that I obtained during my time at the University of Oulu.

Preface

This compilation of research studies explores the behavioral side of IS security compliance. Despite the body of research focused on this area, this dissertation extends the body of knowledge by introducing theories from criminology and health research that introduce other motivations and explanations as to why individuals fail to protect themselves from the risks that are engendered through nonsecure behaviors.

I first explore emotional antecedents of behavior in the context of cyberloafing. This offers two important contributions to the security field by explicating how important affect is when explaining why employees engage in nonsecure behaviors. Second, the concept of cyberloafing is relatively understudied given the large cost that it introduces to the organizations through lost worktime, introduction of viruses and malware, etc.

The second study expands our understanding of security behaviors by applying the Extended Parallel Processing Model from health research. Most studies in IS security have relied on Protection Motivation Theory, which overlooks the emotional responses (*e.g.*, fear, avoidance, reactance) that individuals use to cope with fears evoked by technological threats. This model is further expanded with other constructs used in IS security research. Also, we explore an understudied context of home-users, which are the largest users of computers, despite the pausity of research focused on this segment of the population.

The third study applies Control Balance theory from the field of criminology. Unlike other theories from IS security, this approach explains that individuals engage in deviant behaviors, such as violating IS security policies, because they desire to regain more control over their lives, or exert even further control over others. Rather than exploring the rational or cognitive responses to threats, this theory explores the opportunities afforded by technological threats that an individual can use to better his or her life in comparison to his or her peers.

Lastly, we explore the motivations that lead one to whistle-blow with an anonymous online reporting tool. Little research has focused on such behaviors in IS, and this provides a first and novel view of this important area by exploring how aspects of the tool, and its ability to engender trust effect the individual's intention to engage in whistle-blowing of specific incidents.

This body of research focuses on novel contexts that have largely been overlooked or entirely ignored by the extant literature on security in IS. Further,

by introducing novel theories, this dissertation provides many unique perspectives that can further explain why secure behaviors are difficult to motivate and ensure.

Acknowledgements

I would like to acknowledge the help that Mikko Siponen has provided for the body of this work. Most of these studies are projects that have been done by the two of us. With his insights, especially into criminology, of the security research we have been able to examine several important aspects of security behavior.

I would also like to thank the two reviewers of these studies who provided helpful feedback for eventual publication in quality IS journals.

Last but not least, I would like to thank the external reviewers of this thesis, namely Professor H.R. Rao and Dr. Sung Kim, for their insightful comments concerning my doctoral thesis.

Table of Contents

1 Introduction

Individuals' compliance with security policies and guidelines is a major concern for organizations (D'Arcy *et al.* 2009; Pahnila *et al.* 2007; Siponen & Livari 2006). Failure to comply with security policies and guidelines costs organizations and individuals billions of dollars per year (Anandarajan 2002; Mesa 1999; Yasin 2000). However, despite the general awareness of standard security behaviors and policies, individuals continue to engage in risky behaviors or violate security policies and guidelines (Culnan & Williams 2009; Myyry *et al.* 2009). This dissertation attempts to explore this main research question by looking at a variety of security-related behaviors from different theoretical perspectives.

1.1 Research Gaps

Given the importance of security-related behaviors for both individuals, in order to protect their own property and information, and organizations, it is unclear why so little research has explored why individuals purposefully engage in behaviors that make them vulnerable to potential harmful actions from others. Although security related research has been reported in IS literature, the majority of this has focused on the abuse of IT resources, rather than exploring why individuals purposefully engage in non-secure behaviors (See for example, D'Arcy & Hovav (2007); D'Arcy *et al.* (2009); Straub & Goodhue (1991)). These approaches have generally relied upon the general deterrence theory to explain their respective behaviors (Straub & Goodhue 1991).

Alongside with the initial computer abuse and deterrence theory research, security-related research has also heavily explored how threat appeals can be used to explain the usage of threat-related technologies, such as anti-malware that help to secure individuals' information (Boss & Galletta 2008; Chenoweth *et al.* 2009; Galletta 2008; Herath & Rao 2009; Johnston & Warkentin 2010; Liang & Xue 2009; Liang & Xue 2010). However, research exploring the motivations and antecedents for individual performance of non-secure behaviors outside of these main research streams is greatly lacking.

This dissertation expands upon the current theoretical understandings of non-security related behaviors by adopting novel theories that can be used to explain behaviors that may increase the security of the individual and personal information.

1.2 Overview of Chapters

The objective of this dissertation is to explore the motivations and antecedents to security-related behaviors and how these can be explained through novel perspectives offered by theories that have yet to be applied in IS security research. To this end, four studies were designed and to directly examine four different security related behaviors, each from its own theoretical perspective. Each of these studies is briefly summarized here.

The first study explores cyberloafing of employees in a work situation using the theory of interpersonal behavior (Triandis 1977). The theory of interpersonal behavior is a complementary, more expansive, theory of behavior as it expands upon the antecedents of behavior predicted by the two most widely used models of behavior: theory of reasoned action (Fishbein & Ajzen 1975), and the theory of planned behavior (Ajzen 1985). The models uses affect, attitude and social influence to predict intentions and subsequent behaviors. This model was tested using 238 professionals from a Finnish organization.

The second study explores why individuals use anti-malware applications within their homes. Given the paucity of research regarding behaviors in the home, this study is distinct from the large majority if IS security research. This study explains the usage of anti-malware applications through the perspectives of the extended parallel processing model (Witte 1992; Witte *et al.* 1996) and the theory of habit (Verplanken 2006; Verplanken *et al.* 1997). The model explores whether individuals use anti-malware applications in order to protect themselves from the perceived threat brought by malware, or whether the individual attempts to rationalize away their own fears. The model was tested using a 285 sample of Chinese university students.

The third study examines the omission of prescribed software development tests by software developers using the control balance theory (Tittle 1995; Tittle 2004). This study proposes that individuals that feel that they are controlled more than they are able to control others, or individuals that control others more than they are controlled are likely to engage in deviance against the organization by omitting prescribed software development tests. The model is tested through an online survey of 136 professionals, employed in a variety of Finnish organizations.

The last study explores antecedents of whistle blowing behavior. Building on traditional whistle blowing theory (Miceli & Near 1985; Near *et al.* 1993; Near &

Miceli 1995), this study asserts that trust in the reporting system and individual receiving the report and the level of perceived anonymity afforded by the system all predict an individual's intention to predict wrong-doings occurring within his or her organization. This model is tested using students from several US universities (n = 569) and 202 professionals hired by a third-party research marketing company.

1.3 Study 1. Using the Theory of Interpersonal Behavior to Explain Cyberloafing

1.3.1 Research Gap

As organizations become ever more reliant on computers and networks, their usage within organizations will only continue to grow. However, the use of such technologies at work for personal reasons would diminish organization productivity, and increase the vulnerabilities to the organization through increased exposure risks to unsecure Web sites, connections, and malware (D'Arcy & Hovav 2007; Galletta & Polak 2003; Lim *et al.* 2002). Research on the motivations for cyberloafing (*i.e.*, using technical organizational resources for personal purposes) has produced conflicting findings. Several studies find that cyberloafing is predicted by employee attitudes towards cyberloafing, workplace norms, conditions that allowed cyberloafing (*i.e.*, lack of monitoring and low perceived consequences) (Blanchard & Henle 2008; Galletta & Polak 2003; Lim & Teo 2005; Manrique de Lara 2007; Pee *et al.* 2008; Woon & Pee 2004). However, these studies report different and in some cases, conflicting findings.

This study attempts to address these conflicting findings by using the theory of interpersonal behavior (Triandis 1977), which uses the majority of constructs in the extant literature. By comparing all of the constructs in one model, this study attempts to resolve conflicting findings by analyzing the results of all constructs in one model. This study attempts to provide a more comprehensive analysis of the motivations to engage in cyberloafing and thereby aid to current debate regarding these effects.

1.3.2 Theory of Interpersonal Behavior Overview

The theory of interpersonal behavior (TIB) (Triandis 1977), posits that three main antecedents predict behaviors: facilitating conditions, habits and the behavior's intention. Behaviors are more likely to occur when the individual already has a habit of performing the behavior, conditions allow for the behavior and the individual intends to act as such. This portion of the model expands beyond TRA (Fishbein & Ajzen 1975) or TPB (Ajzen 1985) by considering the habits behind behaviors, and looking at the interaction of intentions, facilitating conditions (akin to subjective controls in TPB) and habit.

Additionally, TIB expands further than TRA and TPB in the number of antecedents for behavioral intentions: affect and social factors. The attitude antecedent chain for intentions is similar to TRA and TPB, but the inclusion of affect allows this model to consider non-rational, goal-oriented, and time-limiting behaviors that may not necessarily apply to TRA.

Similarly, this model incorporates a broader consideration of the intentional process by considering how the individual is influenced by the social context. TIB proposes that individuals will form intentions based on the influence of others, norms and how the individual is positioned, within the context, in comparison to others.

The inclusion of all these variables is predicted, and shown in other studies, to allow powerful prediction of a wide variety of behaviors (Bamberg & Schmidt 2003; Bergeron *et al.* 1995).

1.3.3 Theoretical Model

The theoretical model tested in this study is shown in Figure 1. This model is based on TIB as proposed by (Triandis 1977), with further adaptations of the theory proposed by Bamberg and his associates (Bamberg *et al.* 2003; Bamberg & Schmidt 2003).

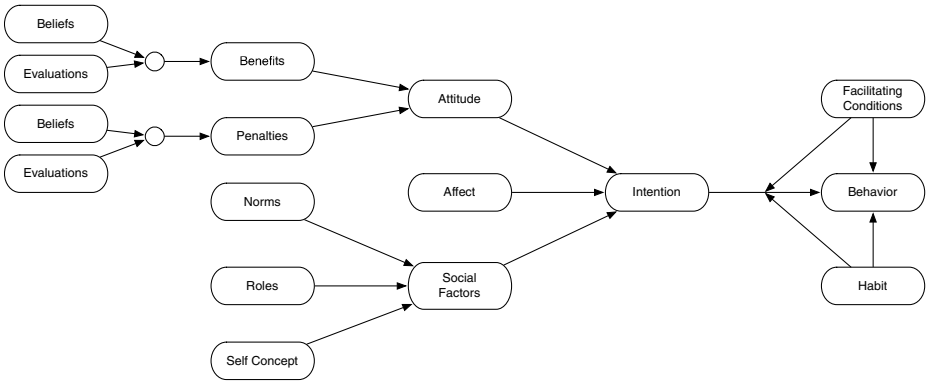

Fig. 1. Theory of Interpersonal Behavior for Cyberloafing.

1.3.4 Contributions

This chapter has four major contributions to IS security research. First, this is the first such study to report the interactive, powerful effects that habits, facilitating conditions and intentions have on cyberloafing. This is a significant finding for researchers as habit has been largely missing from the debate concerning the motivations for cyberloafing. Further, habit is largely outside the control of researchers or managers to control or alter, thus this work highlights the importance of intention as the most practical way to minimize cyberloafing for those that already have these habits.

Second, this model includes more antecedents than any previous studies. The inclusion of these many antecedents into the model makes it possible to compare each of these antecedents to each other. This builds on previous research by including multiple antecedents that have not been studied together (*i.e.*, benefits, penalties, attitudes, social factors, norms and intentions) and also antecedents that have not been studied in prior studies (*i.e.*, affect, habit, roles and self-concept). Our model shows that most of these antecedents are important predictors of cyberloafing behaviors and should be considered in future research.

Third, the results indicate that penalties for cyberloafing provide little ability to reduce cyberloafing or its intention. Thus, unlike previous research that focuses on the deterrence of security-related behaviors through penalties (Gibbs 1975), this study highlights how other motivations are able to overcome these managerial controls and sanctions.

Fourth, this study provides, to date, the most predictive model of cyberloafing, indicating the effectiveness of TIB in predicting a desired behavior. Unlike previous work that has used intentions as the dependent variable, this study also measures behaviors and shows the strong relationship between intentions and behaviors, implied by previous studies.

1.4 Study 2. Why Home Computer Users Use Anti-malware Tools: The Extended Parallel Processing Model

1.4.1 Research Gap

Malware; including spyware, viruses, and all kinds of unwanted software; is an increasing problem for home users. Several studies have highlighted that most home computers are affected by malware (Chenoweth *et al.* 2009; Litvinoff 2008). On a related note, these threats and problems can readily be resolved through the use of very accessible, and in many cases free, tools and applications. However, research investigating the use of such tools is sparse.

We further argue that findings on "computer abuse" or "employee compliance with IS security policies" in an organizational context, regarding such behavior as the use of anti-malware tools, may not translate into the home user context and vice versa. We thus focus on the use of anti-malware usage in the home user context. The home user differs in important and significant ways from the organization context in the lack of IT resources and support, and in the oversight provided by management and IT regarding organizational security policies, which do not exist in the home user context.

This study attempts to increase our understanding of home users' usage of anti-malware applications, this study adopts the extended parallel processing model (EPPM) (Witte 1992; Witte *et al.* 1996), which has yet to be applied in the IS security domain. This model is better situated to focus on the differences afforded to home users by identifying on two general coping mechanisms to threat, as opposed to the one used in the dominant theory in the research, protection motivation theory (PMT) (Maddux & Rogers 1983; Rogers 1975).

1.4.2 Extended Parallel Processing Model Overview

The extended parallel processing model is based on one of the first modern threat theories, the parallel response model (Leventhal 1970), which was also used as the foundation for the more known protection motivation theory (Maddux & Rogers 1983; Rogers 1975). Whereas protection motivation theory only focused on one of the coping routes predicted in the parallel response model, the extended parallel response model uses both coping routes, and further augments the original theory by adding additional antecedents to the original model, along with the construct of fear. Essentially, EPPM proposes that when an individual perceives a threat as severe and that it could happen to him or her, the individual will respond in one of two manners.

The first coping response route is engaged when the individual believes that an indicated response can diffuse the threat, and that the person is able to complete the desired response. By believing that a workable solution to the threat exists, the individual intends to behave in a fashion that protects the individual from the threat. The protective behavior is also predicted by the costs and benefits associated with the behavior.

The second coping response route is engaged when the individual perceives more threat and feels that there is no workable solution to the threat. When this occurs, the individual will enter a state of fear, and attempt to manage this fear through emotion-coping responses. Two such common responses, used in this study, are: avoidance and reactance. Avoidance is used to discount and ignore the threat, in order to reduce fear by removing it from conscious thought. The second method is reactance, wherein the individual discounts the credibility of the message itself or its source in order to minimize the potential severity of the threat, or discount the likelihood of encountering the threat. By these mechanisms, the individual is able to reduce the level of fear, which is the objective of this coping response route.

1.4.3 Theoretical Model

The model for this study is depicted in Figure 2. This model is mainly based on the EPPM as proposed by Witte and his colleagues (Witte 1992; Witte *et al.* 1996), with the addition of habit theory, as represented by the habit construct (Aarts *et al.* 1998).

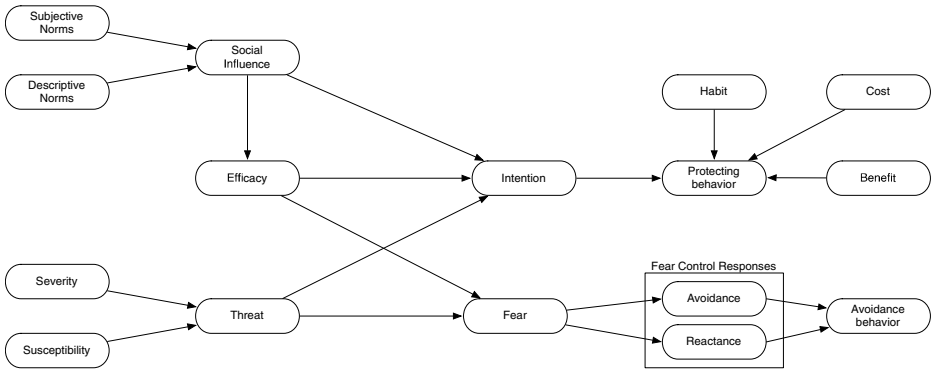

Fig. 2. The Extended Parallel Processing Model for Anti-malware Application Usage.

1.4.4 Contributions

This study provides several important contributions for research. Primarily, this is the first study to introduce and show support for the extended parallel processing model. This is an important contribution for research as the EPPM extends our understanding of threat-related behaviors by expanding the responses to threat to include not only protecting behaviors, as done in PMT (Maddux & Rogers 1983; Rogers 1975), but also emotion-coping responses. This route is marked by the presence of fear, which although intuitively relates to threats, IS security research has not reported any studies that predict or measure fear. The results also strongly support EPPM and validates the use of this model in IS security research.

The inclusion of fear into this context is important as it strongly predicts the emotion-coping response route, while efficacy predicts the problem-coping route (*i.e.*, protective behaviors). This extends our understanding of security-related behaviors involving threat as it emphasizes the importance of emotional responses for predicting behaviors.

Finally, the inclusion of habit into the theoretical network of EPPM was effective as habit was shown to, once again, be a powerful predictor of behaviors. However, expected relationships of cost and benefit with behaviors were insignificant, which calls attention to the inability to artificial reward or penalize behaviors that would encourage an individual to behave in a manner that will protect him or her from a perceived threat.

1.5 Study 3. Control Imbalances: Explaining Why Software Developers Skip Prescribed Testing Procedures

1.5.1 Research Gap

It is very common to find errors or bugs in software (Gibson & Senn 1989; Kafura & Reddy 1987). However, there are no silver bullets in software development. There are and always will be software errors, owing to software complexity (Brooks 1987). It is reported that competition to hit the market no later than competitors, tight deadlines, and a tendency to cut "unnecessary" documentation, push software developers toward trading quality for speed (Ahonen & Junttila 2003; Baskerville & Pries-Heje 2001; Baskerville & Pries-Heje 2001; Baskerville & Pries-Heje 2002; Baskerville & Pries-Heje 2004; Baskerville *et al.* 2003). In fact, it is estimated that inadequate testing of software in the USA alone could cost as much as $60 billion yearly in repairs and downtime (Ahonen & Junttila 2003).

Despite of all this hype on the need to have fast release cycles in software development, we find no studies that focus on the reasons as to why software developers omit prescribed tests that could potentially detect and correct errors and bugs (Agrawal & Chari 2007; Anquetil *et al.* 2007). Given that the detection of bugs by software developers can potentially minimize or avoid the negative outcomes from bugs and errors, it is important to determine why developers omit such tests. By elucidating the motivations behind such behaviors serves as the first step for managerial intervention to prevent and or correct such intentions before they occur.

Managers have long attempted to identify ideal portfolios of control or monitoring procedures that would allow them adequate oversight throughout the software development process (Kirsch 1996; Kirsch 1997; Kirsch 2004; Kirsch *et al.* 2002). With the focus of this literature being on the types of controls (*e.g.*, informal, process, or outcome) that would allow managers to increase overall software quality and also completing projects on time, in budget and providing all desired features, little research has explored how this type of oversight may provide detrimental outcomes to their very endeavor. This work provides the insight that the use of controls and monitoring in software development may have detrimental outcomes and effects on those being controlled.

1.5.2 Control Balance Theory Overview

Control balance theory (CBT) (Tittle 1995; Tittle 2004), proposes that individuals attempt to achieve a sense of balance in terms of the control that they exert over others, and the control that is exerted upon them. As individuals become more imbalanced in their control ratios (exerted control compared to felt control), they are more likely to engage in deviant behaviors (*i.e.*, behaviors that break organizational rules or norms) in order to gain a more a balanced control ratio. Additionally, individuals with a strong imbalance in favor of their increased control over others have increased motivations to further increase this imbalance and have even greater control over more aspects of their lives.

When this control imbalance also exists, other antecedents of deviant behavior are also more likely to occur. Namely, situational cues that trigger opportunities for deviance become more salient, and the motivation to engage in deviance becomes stronger. Further, perceived constraints that would curtail deviant behaviors are seen as weaker or less likely to be enacted against the individual if he or she were to be caught.

As a counter-balance to the control imbalance, (Tittle 2004) augmented the original theory to include self-control. Individuals with higher levels of self-control are better equipped to manage their short-term desires for justice, wherein control balances can be restored, and instead focus on the long-term objectives that may restore balance. These long-term goals and objectives are less likely to be forms of deviance, which serve as short-cuts to long-term desires. As such, individuals with higher levels of self-control are less likely to perceive the main antecedents of deviance that are affected by control imbalances.

1.5.3 Theoretical Model

The model used for this study is depicted in Figure 3. The model is based on control balance theory as proposed, and modified by several studies in this theories research stream (Curry 2005; Piquero & Hickman 2003; Tittle 1995; Tittle 2004).

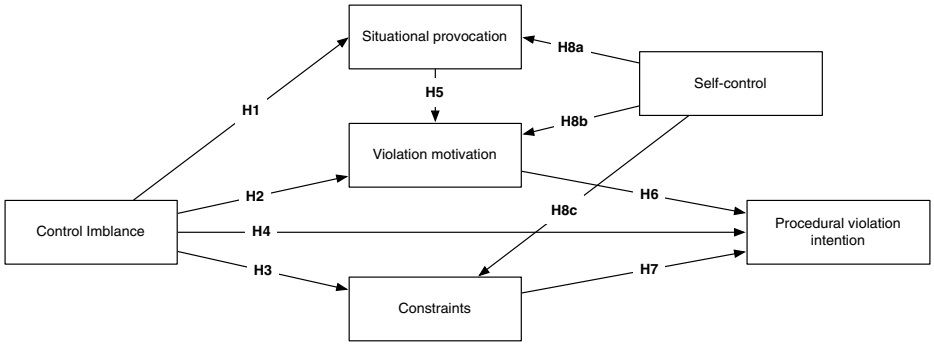

Fig. 3. Cognitive Balance Theory in Omission of Software Development Tests.

1.5.4 Contributions

This study has several important contributions for IS security research. First, it is the first such study to explain and introduce control balance theory to IS research. This has important implications for IS research in general due to the importance of control theory, which has been an important stream regarding the management of software projects (Kirsch 1996; Kirsch 1997; Kirsch 2004; Kirsch *et al.* 2002). The entire control research stream has focused on how to better apply controls, and how they are able to manage employees and the software development process. However, the literature does not consider the effects that control has on those being controlled, and how the process of controlling employees may sow the very seeds of deviance within the ranks of those being controlled. This novel insight opens up a wide avenue of research that could further explore this unique perspective that control balance theory offers to the control research stream.

Further, the focus on deviance on a software development context has been largely overlooked in IS security research. By promoting the importance of deviance and delineating several of its motivations, research can continue to explain why individuals engage in deviance, and how managers can potentially defuse deviant motivations. Additionally, the results indicate that constraints had no significant effect on deviant intentions, implying that planned interventions or monitoring programs have little affect on whether an individual will commit deviance.

Lastly, this study shows how deviant behaviors are in fact rational and not based on emotional outbursts. This implies that future research could further explore these motivations and ascertain when such rational deviance is most

likely to occur, and when opportunistic, and unplanned forms of deviance occur. By further exploring the specific control balance ratio in the context, CBT will be better equipped to explain and predict when such deviance will occur.

1.6 Study 4. Blowing the Whistle on Computer Abuse: Extending Whistle-Blowing Theory Using Anonymity, Trust, and Perceived Risk with Whistle-blowing Systems

1.6.1 Research Gap

In recent years, legislation such as the Sarbanes-Oxley Act in the United States and similar legislation in other countries have required public companies to establish channels through which whistle-blowers can anonymously report abuses[1]. In order to better understand whistle-blowing behavior, researchers have developed whistle-blowing theory (Near & Miceli 1995). A key distinction of this theory is that it explains that an individual does not choose to whistle-blow based on a traditional cost-benefit calculus (as widely seen in risk-related IS literature) because there are few, if any, personal benefits of whistle-blowing. Although whistle-blowing theory has been shown to be robust across a variety of settings, the theory has not been applied to the phenomenon of online whistle-blowing report systems[2], which are an increasingly prevalent and important means of receiving whistle-blowing reports (Ernst & Young 2009). Given the even sharing of information, increased likelihood of conflict, and a lack of a shared context, online whistle blowing systems have additional hurdles to overcome than the traditional means for whistle blowing.

We expect three factors in particular—namely anonymity, trust, and risk—to be salient in usage of an online whistle-blowing system because of their heightened effects in other online systems as compared to traditional whistle blowing mechanisms (*e.g.*, Gefen *et al.* 2003; Jarvenpaa & Tractinsky 1999b; Pinsonneault & Heppel 1998). First, *anonymity* is widely assumed and accepted to be a critical factor in individuals' decisions to use whistle-blowing systems (Ernst & Young 2009). We were thus surprised to learn that although previous

1 For the U.S., see the Sarbanes-Oxley Act, Section 301; in Canada, see Multilateral Instrument 52-110 section 2.3; in the U.K., see the Combined Code for Corporate Governance C.3.4.
2 For examples of whistle-blowing systems, see http://silentwhistle.com or http://clearviewconnects.com.

treatments of whistle-blowing theory tacitly acknowledge the importance of anonymity (Near and Miceli 1995), its effects on whistle-blowing behavior have neither been directly theorized nor examined empirically in the literature.

Second, another implicit factor in many whistle-blowing studies is *trust*: people are believed to be more likely to whistle-blow if they feel they can trust the authority to which they report (Smith and Keil 2003). Again we were surprised to learn that trust has not been explicitly theorized or tested in the context of whistle-blowing. Further, the criticality of trust may be even more salient in online settings, given research findings showing the importance of trust in users' interaction with e-commerce systems (Gefen *et al.* 2003).

Third, perceived risk is central to whistle-blowing because of the high-risk nature of whistle-blowing (Miceli and Near 1984)—with retaliation being the foremost risk (Miceli and Near 1985). Research in IS has consistently shown the substantial effects of perceived risk (Dinev and Hart 2006; Grazioli and Jarvenpaa 2000; Malhotra *et al.* 2004), and yet, despite the central role of risk, whistle-blowing theory literature does not explicitly describe the effects of perceived risk.

1.6.2 Whistle-blowing Theory Overview

Basic whistle-blowing theory was first expounded by (Miceli & Near 1985), and later modified to the IS software development by (Park *et al.* 2008), the only such study in IS literature. This basic model proposes that the willingness to report perceived wrongdoings of peers is based on two assessments in a causal chain. First, the individual has to believe that a problem ought to be reported. Without this initial assessment, an individual will never blow the whistle. A variety of studies have explored factors that manipulate this assessment that range from organization roles, demographic characteristics and the nature of the violation (Arnold & Ponemon 1991; Miceli & Near 1985; Miceli & Near 1984; Miceli & Near 1988; Near *et al.* 1993; Trevino & Victor 1992).

Having assessed that a violation ought to be reported, the individual will then assess whether he or she feels any personal responsibility to report this violation to the appropriate entity/individual. Again, the same studies above have explored a variety of covariates that have shown an impact on this construct, and thereby increased its relative impact on the intention to engage in whistle-blowing. Based on TRA (Fishbein & Ajzen 1975), the intention to whistle-blow serves as an antecedent to actual whistle-blowing.

1.6.3 Theoretical Model

Our theoretical model is depicted in Figure 4 (Note, the original whistle blowing theory is depicted as the shaded-in constructs). This study greatly extends the basic whistle-blowing model, shown in the top of the figure, in two general ways. First, constructs that focus on the anonymity of the individual have been incorporated into the theory: public-self awareness and anonymity. Based on research in this area, we propose that the perceived risk of reporting a violation through an online system will be altered by whether an individual feels that he or she could be identified and be connected with their report by others in the organization.

Second, we synthesize trust into the model through trust in the tool, trust in the party that monitors/controls the system, and one's general disposition to trust others. We posit that perceptions of trust with both the tool, and with relevant others are able to overcome the perceived risks of reporting a violation through the online whistle-blowing system.

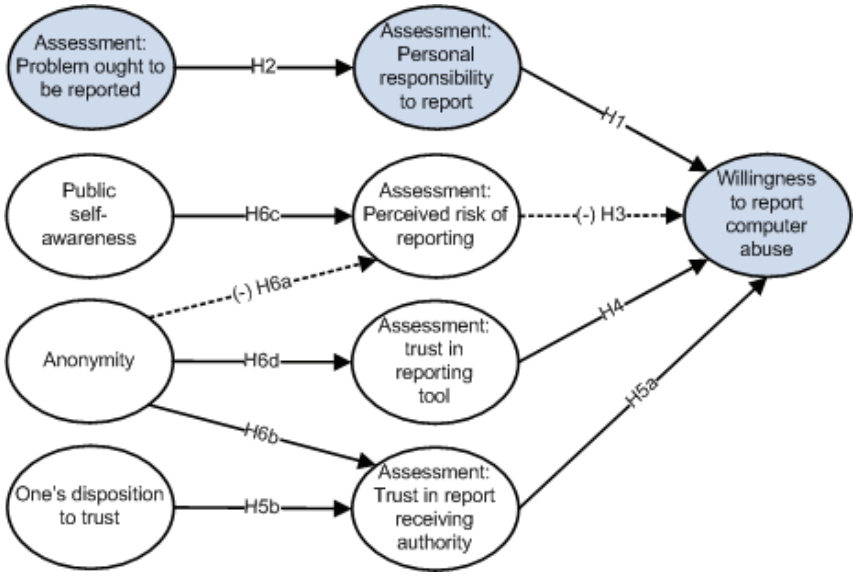

Fig. 4. Extended Theoretical Model of Whistle-blowing through an Online System.

1.6.4 Contributions

This study provides several important contributions to IS security research. First, this is the second such study in IS to focus on whistle-blowing, which is an important topic given the increased emphasis on whistle-blowing created through legislation around the globe. By promoting future research on this topic, this study increases the relevancy of IS security research by focusing on issues that are of high importance in contemporary society and of managerial concern.

Second, the inclusion of trust into the research model shows the advantages that trust research can have in this domain. This initial study shows that trust has importance effects that alter the intention to whistle-blow. We show that all three forms of trust are important and as such future research could highlight how the trust in the reporting authority and the system could be further augmented to encourage whistle-blowing.

Third, the presence of anonymity in the model is important as it is able to alter the levels of trust in the reporting authority and in the tool. Thus the ability of the online reporting tool to anonymize data is thus an important feature that could serve as a point for future research.

Lastly, previous research on whistle-blowing in other fields has long proposed that such an endeavor is risky due to retaliation by the organization or the reporters peers. However, despite our predictions, the perceived risk of reporting a violation through an online system that allows for anonymity has no impact on the intention to report. This is an interesting finding that shows the importance for using such systems as they have compensated for retaliation risks that are commonly found when researching whistle-blowing studies in offline channels (Arnold & Ponemon 1991; Gundlach *et al.* 2003; Miceli & Near 1985; Miceli & Near 1984).

1.7 Publication Status of Dissertation Chapters

Each chapter in this dissertation is its own independent study, all of which will eventually be published. Table 1 summarizes the current status of each chapter.

Table 1. Publishing Status of Dissertation Chapters.

Chapter	Co-Author(s)	Status
1	Mikko Siponen	Submitted
2	Mikko Siponen, Xiaosong Zheng	Submitted
3	Mikko Siponen	Submitted
4	Paul B. Lowry, Dennis F. Galletta, Anthony Vance	Submitted

1.8 Contributions

This dissertation provides four principal contributions from its study that extend the IS security understanding of security-related behaviors. First, the initial study on cyberloafing highlights several reasons why individuals engage in non-secure behaviors. Namely, they find these behaviors beneficial, positive, fitting with their roles and they have become habituated to performing these behaviors. An important conclusion provided by this study is the ineffectiveness of penalties to deter these types of behaviors. Non-secure behaviors are thus deeply entrenched in the daily life of individuals, and are self-rewarding insomuch that typical controls meant to deter such behaviors are generally ineffective.

Second, the study on anti-malware usage highlights the importance of threat, efficacy and fear in predicting security-related behaviors. Namely, if the individual, when confronted with a threatening message will endeavor to either 1) resolve the threat by removing it through protective behaviors that are believed to be effective and possible or 2) managing the fear that is produced by the threat through mental processes that are able to minimize fear. This is the first study in IS that has predicted and shown that fear plays an important role in determining whether individuals will attempt to protect themselves from harm, or rather accept that nothing can protect them and instead manage the internal outcomes of fear. This provides a unique and novel contribution to IS security research be providing a fear management route that is lacking from protection motivation theory-based work (Maddux & Rogers 1983; Rogers 1975).

Third, the study on omitted software tests provides a completely novel point of view for researchers to consider. Namely, rather than attempting to control processes and outcomes of employees (Kirsch 1997; Kirsch *et al.* 2002), care should be taken to consider how such controls impact the targets of said controls. This study emphasizes that when controlled individuals experience an imbalance between the control they exert on others, and the control that is exerted on them,

they have increased tendencies to engage in deviance. Further, this imbalance also affects other antecedents of deviance. By expounding on the detrimental impacts that controlling and monitoring mechanisms may have on individuals, this study provides novel insights into control portfolios and how they should be calibrated within an organization.

Finally, the fourth study highlights how trust in individuals and systems, and the anonymity provided by a system are able to increase the intentions to engage in whistle blowing. This yields to main implications for research. First, the study of whistle-blowing has been largely overlooked in general IS research, and in security research too. Whistle-blowing is strongly linked to these types of studies as it involves the informal controls that encourage others to behave appropriately and ethically in the work place, which may often involve concerns and issues that are studied in security research. Second, this is the first such study on whistle blowing to link its basic model to the constructs of trust and anonymity, which have been assumed to play a role in this process, but never empirically tested until this study. By combining these three research streams into one study, this studies provides greater elucidation into the motivations and antecedents that encourage whistle-blowing.

1.9 Conclusion

Security-related behaviors that protect both individuals and organizations from malicious attacks from both insiders and outsiders is an important topic for both researchers and practitioners. Such behaviors result in billions of dollars in lost time, infected hardware, buggy code, etc. (Anandarajan 2002; Straub & Goodhue 1991). This dissertation advances the security research stream by focusing on relatively understudied behaviors and adopting novel theoretical perspectives to provide additional insights into why individuals behave in manners that increase their vulnerability from digital attacks.

2 Using the Theory of Interpersonal Behavior to Explain Cyberloafing

2.1 Abstract

The use of the Internet at work for personal reasons (*i.e.*, cyberloafing) entails a number of problems from the viewpoint of organizations, including decreased efficiency of work output, increased risk of getting viruses and spyware and waste of IT resources. Previous research has examined the reasons as to why employees engage in cyberloafing. However, results from these studies have reported conflicting findings. In this study, we propose to build on previous research by examining multiple motivations for cyberloafing within one theoretical paradigm, the theory of interpersonal behavior (TIB). This theory expands upon TRA and TPB by also considering an individual's emotions, habits, and additional sources of social influence when predicting an individual's intentions and eventual behaviors. Based on TIB, we developed a model and test it in an organization in Finland (N = 238). Our results suggest that the model highly predicts cyberloafing. Our results indicate that the benefits regarding cyberloafing is positively related to the attitude towards the cyberloafing. Also, social norms and organizational roles within the organization as well as self-concepts regarding cyberloafing are positively related to the overall social factors regarding cyberloafing. Attitudes and affect regarding cyberloafing is positively related to the intention to engage cyberloafing. In addition, social factors regarding cyberloafing is positively related to the intention to engage in cyberloafing. Also, the interactive effect of intentions and habit predict cyberloafing. Finally, penalties and control have no significant influence on cyberloafing. Implications for research and practice are suggested based on the findings.

2.2 Introduction

Organizations have increased the usage and their reliance on computers and networks. With the increased availability of computers and the Internet at work, employees also have an increased opportunity to use these same devices for personal reasons (Anandarajan 2002; Lim *et al.* 2002). The term *cyberloafing* has been coined as the use of the Internet at work for personal reasons (Lim 2002). Research has highlighted than when employees use the Internet and related

applications (*e.g.*, messenger and email applications) they suffer from a drop in efficiency of work output (D'Arcy & Hovav 2007; Galletta & Polak 2003; Lim *et al.* 2002). This reduction in efficiency is costly for the organization in terms of reduce employee output, and also in terms of costs associated with the potential for increased spyware, viruses, security leaks, and use of IT resources (*e.g.*, the use of bandwidth for skype, video or Internet radio) (Mesa 1999; Yasin 2000). Estimates have placed this loss in the billions of dollars annually (Anandarajan 2002).

Research on the motivations cyberloafing has produced conflicted findings. Earlier work on this phenomenon focused on providing ways to profile these frequent users with some success (Anandarajan 2002; Lim *et al.* 2002; Stanton 2002; Urbaczewski & Jessup 2002). These studies were able to provide profiles of current cyberloafers, but these profiles lack the predictive power that would allow management to identify and thereby remedy such unwanted practices of their employees. Later work focused on the antecedents or motivations for cyberloafing, but the results are in conflict with each other (Chang & Cheung 2001; Cheung *et al.* 2000; D'Arcy & Hovav 2007; Galletta & Polak 2003; Pee *et al.* 2008; Woon & Pee 2004). By understanding the motivations behind the personal use of the organization's resources, organizations will be able to adopt practices, procedures, and develop training methods to reduce the amount of cyberloafing that is taking place in the organization. With the conflict in the current empirical findings, it is important to continue work in this area to determine which motivations lead to cyberloafing. We seek to increase our understanding of cyberloafing by proposing and testing a theoretical model that compares multiple motivations for cyberloafing concurrently, rather than separately as done in previous work on cyberloafing (D'Arcy & Hovav 2007; Galletta & Polak 2003; Lim 2002; Lim *et al.* 2002; Manrique de Lara 2007; Woon & Pee 2004).

Further, this study expands upon previous research by including novel theoretical antecedents of cyberloafing that have not yet been studied in previous research. Rather than relying upon the theory of reasoned action (TRA) (Fishbein & Ajzen 1975) or the theory of planned behavior (TPB) (Ajzen 1985), this study utilizes a comparable theory of interpersonal behavior, originally proposed by (Triandis 1977). The theory of interpersonal behavior (TIB) expands upon the same concepts of TRA and TPB (*i.e.*, attitudes, social influence and intentions), but it also includes emotional factors, habits and expands upon the sources of

social influence upon the individual. TIB provides a broader understanding of what may lead to cyberloafing at the workplace.

By understanding the motivations behind an individual's cyberloafing behaviors, this study provides several important contributions. First, our study shows that an individual's habit of cyberloafing is the strongest predictor of actual cyberloafing behavior. Further, this effect is further enhanced when the individual has an intention to engage in cyberloafing. Second, this model reports the effects of more antecedents to cyberloafing than any other model to date. This allows the comparison of several motivations to cyberloaf in comparison to other motivations, which has not been possible to date. Third, this study is the first to show the effects of affect, habit, roles and self-concept on cyberloafing behavior. Fourth, our results show that generally accepted methods of control or deterrence are unable to reduce cyberloafing behaviors. Lastly, this research reports the strongest predictive model of cyberloafing that has been reported to date.

The remainder of this paper is structured as follows. We first review the literature and findings regarding cyberloafing. We then review the theory of interpersonal behavior. Using this theoretical basis, we explicate our model and its hypotheses. We then described our study and the analysis of the subsequent data. Results are provided, along with implications for research and practice.

2.3 Literature Review

This section will briefly describe two main literature streams that are relevant for this study. First, we will describe the literature related to cyberloafing. Second, we will explain the theory of interpersonal behavior. For the purposes of this study, we define *cyberloafing* as any usage of a computer that is not for purpose of completing work-related tasks (Lim 2002). Such usage may include web surfing, chatting, online shopping, etc. This definition is more expansive than previous work in this area by including behaviors that use other applications (*e.g.*, messengers, video conferencing, skype, online gaming, online communities, etc.) rather than focusing only on the usage of the Internet browser for personal use while at work (Galletta & Polak 2003; Lim *et al.* 2002; Seymour & Nadasen 2007; Simmers 2002).

2.3.1 The Use of the Internet at Work for Personal Reasons—Cyberloafing

With the increasing presence of the Internet in the workplace, researchers initially focused on the extent to which personal use of the Internet was prevalent in the workplace. This type of research typically highlights that businesses should be aware of employees' cyberloafing and the detrimental effects that it has on the organization (Lim *et al.* 2002; Simmers 2002). This types of studies found support that at least 20% of employees in an organization engage in such an action, and posit that it subsequently lowers the performance and productivity of employees.

This line of research provided advice as to how cyberloafing could be reduced. Researchers, and practitioners, at this point advised organizations to adopt Internet usage policies (Siau *et al.* 2002) that would help employees understand what constituted suitable use of the Internet, and thereby deter its occurrence within the organization. The other common advice of this earlier work on cyberloafing prescribed the use of monitoring tools, reports, and devices to ensure the compliance of said policies (Panko & Beh 2002; Simmers 2002; Urbaczewski & Jessup 2002). However, empirical work found that the use of monitoring did lower the overall job satisfaction of the employees being monitored (Urbaczewski & Jessup 2002).

Building on the initial studies that found the prevelance of cyberloafing, later studies began the process of profiling personal Internet users in an attempt to provide tools and procedures for managers to use in identifying such users. It was hoped that by providing tools and procedures to identifying personal users of the Internet that it would allow management to proactively address, training, and punishing continued cyberloafing. Most approaches focused on varying dimensions of satisfaction or attitudes held towards the organization (Lim *et al.* 2002; Stanton 2002). These studies found that various attitudes towards the organization and social norms do in fact alter the levels of cyberloafing in the organization. (Simmers 2002) also reported a neural network approach based on genetic algorithms that would capture usage statistics of the users to predict their inclinations towards cyberloafing.

More recent work has attempted to use theoretical approaches to predict and understand why individuals engage in cyberloafing. The main approaches have depended on specifying antecedents of attitudes and social norms from the

behavior of planned behavior (Galletta & Polak 2003; Seymour & Nadasen 2007). These studies have found that the employee's attitude towards cyberloafing and norms at the workplace have strong predictive power on employees' intentions and actual cyberloafing. Further, building on concepts from interpersonal behavior, Pee and colleagues (Pee *et al.* 2008; Woon & Pee 2004) along with Cheung and colleagues (Chang & Cheung 2001; Cheung *et al.* 2000) have shown that consequences, habit, facilitating conditions and the emotions of the employees also strongly predict the personal use of the Internet at work. A summary of this work is shown in Table 2.

The later theoretical work on the use of the Internet at work for personal reasons has resulted in conflicting empirical results. Despite replications from two theoretical bases (*i.e.*, TPB: (Galletta & Polak 2003; Seymour & Nadasen 2007); and TIB: (Chang & Cheung 2001; Cheung *et al.* 2000; Pee *et al.* 2008; Woon & Pee 2004), the results are not consistent. In the first theoretical study of workplace Internet abuse, (Galletta & Polak 2003) find that only certain attitudes (*i.e.*, job satisfaction, and Internet addiction) and subjective norms are able to predict the use of the Internet at work for personal reasons. However, using the same theoretical approach (Seymour & Nadasen 2007) find that no attitudes or subjective norms are able to predict abuse. Instead (Seymour & Nadasen 2007) find that only the perceived supervision of managers is able to reduce abuse. Further, Pee and his colleagues (Pee *et al.* 2008; Woon & Pee 2004), using portions of TIB, report conflicting findings. The initial study (Woon & Pee 2004) reports that habits, intentions and facilitating conditions all negatively impact behavior, whereas the later study (Pee *et al.* 2008), reports the opposite. Meanwhile, (Chang & Cheung 2001; Cheung & Limayem 2005) report that near-term consequences and facilitating conditions are conducive to the intention to use the Internet at work (Note, these studies are not focused on cyberloafing but on whether the Internet would be adopted by the individual to aid him or her in their job functions) and have mixed results regarding the complexity of the application, social factors, and affect felt towards Internet usage. As a result of these mixed empirical findings, it is difficult to understand what motivates individuals to engage in cyberloafing

This study seeks to expand upon these studies and to provide a more complete view of the antecedents of cyberloafing in several ways. First, we use the Theory of Interpersonal Behavior, which has been shown to account for more variance in a model when compared to TRA and TPB (Bamberg & Schmidt 2003). Second, we expand the scope of cyberloafing to include not only personal use

related to the use of Internet browsers, but to include all applications that utilize networking or telecommunications abilities at a computer. Third, we specifically expand upon the work of Pee and his colleagues (Pee *et al.* 2008; Woon & Pee 2004) and Cheung and his colleagues (Chang & Cheung 2001; Cheung *et al.* 2000), by including all of the constructs from TIB, with their respective antecedents as specified by Triandis (Triandis 1977).

Table 2. Summary of Research on Cyberloafing

Author	Year	Theory Base	Methodology	Findings
Cheung *et al.*	2000	TIB	Survey	Using the Internet at work is more likely to occur when the Internet is not viewed as complex, the individual perceives near-term consequences from their behaviors, if cyberloafing is socially accepted at the organization, and whether the individual the individual has access to the Internet at work
Chang and Cheung	2001	TIB	Survey	Using the Internet at work is more likely to occur when the individual perceives near-term consequences, they feel good about using the Internet, and when the organization provides access to the Internet and its usage is socially acceptable.
Anandarajan	2002	Artificial Neural Networks	Simulation. Survey for testing the simulation	AI-based behavior models, can be used to profile employees' Web usage behavior, a priori
Simmers	2002	None	Case studies	Internet policies and monitoring of employee behavior will lead to optimal levels of employee freedom, while minimizing costs and risks for the organization
Oravec	2002	Social capital theory	None	Argues that workplace recreation through the use of the Internet can increase employee morale, creativity and therefore productivity

Author	Year	Theory Base	Methodology	Findings
Lim *et al.*	2002	None	Survey & focus groups	Cyberloafing is fairly common in the workplace. Individuals are more prone to this type of abuse if they perceive that the organization overworks them or does not provide adequate compensation
Stanton	2002	None	Survey	Frequent cyberloafers have higher levels of job and pay satisfaction, satisfaction with promotion opportunities and higher ratings of organizational support than non-abusers
Urbaczewski and Jessup	2002	Theory X/Y	Observation and Experiment	Monitoring decreases cyberloafing, but it also decreases the user's level of satisfaction
Galletta and Polak	2003	TPB	Survey	Cyberloafing was most predicted by employees' attitudes (job satisfaction and Internet addiction) towards cyberloafing, and norms within the workplace environment
Woon and Pee	2004	TIB	Survey	Cyberloafing was found to be decreased when employees had intentions to cyberloaf, a habit of cyberloafing, and conditions that increased the likelihood of cyberloafing. Further, job satisfaction, affect towards cyberloafing, social factors were all found to increase these mediating constructs while perceived consequences reduced cyberloafing intentions
Seymour and Nadasen	2007	TPB	Survey	Only managerial supervision affects the level of cyberloafing, other hypothesized TPB constructs were not significant
Pee *et al.*	2008	TIB	Survey	Habit, intention and facilitating conditions all increased cyberloafing, which were subsequently increased by affect, social factors and perceived consequences

2.3.2 The Theory of Interpersonal Behavior

The Theory of Interpersonal Behavior was first specified by (Triandis 1977), as a theoretical alternative to TRA and TPB (See Figure 5). (Triandis 1977) argued that TRA and TPB both suffer from several weaknesses that are overcome by this model. TRA and TPB are focused on the prediction of behaviors as predicted by the intentions to perform the given behavior. Further, the intentions are predicted by the individual's beliefs regarding the behavior and subjective norms that are relevant for the behavior (Ajzen 1985). TIB builds upon this work and further proposes several additions to the underlying model proposed by TRA and TPB. Each of these additions are discussed in turn.

First, both TRA and TPB, by focusing on the cognitive aspects of behavior, do not account for the emotions involved in eventual behavior. He argues that individuals often arrive at decisions not only by focusing solely on the cognitive aspects of a situation, but also by relying on their feelings. Thus, he poses that affect serves as an input into the decision-making process. For this paper, we define *affect* as the emotional response to a particular situation that is based on instinctive and unconscious processes in the mind (Triandis 1977).

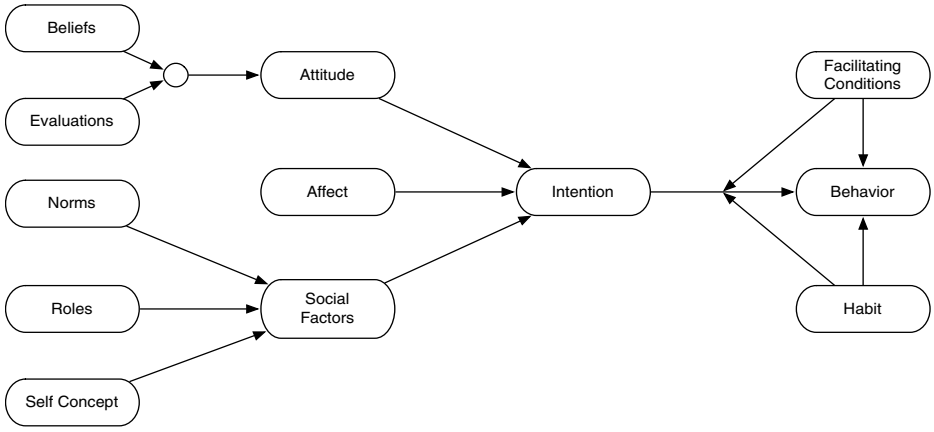

Fig. 5. Summary of the Theory of Interpersonal Behavior (Triandis 1977).

Second, TRA and TPB assume that intentions lead to behavior without any consideration as to the previous occurrence of the same behavior (Sheppard *et al.* 1988). TRA and TPB both pose that intentions predict behavior without considering whether this behavior has been so often repeated by the individual to

become automatic and thus will be performed without the conscious deliberation assumed by both TRA and TPB. This type of automated response to a situation to behave in a given manner is referred to as *habit* (Verplanken & Orbell 2003). For example, when someone arrives at a stop sign it does not require deliberate and conscious reasoning to decide to slow down and stop, but this action is rather dictated and automated due to the numerous times that the individual has performed this exact same behavior. Thus, it is not merely the intention that someone may create that dictates whether a behavior will occur, but how habitual this behavior has become. The relationship between intention and behavior is proposed to be altered by the level of habit that the person has towards the behavior. Specifically, the behavior is to be more pronounced when intention and habit are both present than either one in isolation resulting in an additive interaction effect (Gagnon *et al.* 2003).

Third, like the theory of planned behavior (Ajzen 1985), TIB proposes that the decision to engage in a behavior will be affected by the ability of the individual to perform the behavior. *Facilitating conditions* refers to lack of environmental or situational constraints that may prevent the individual from performing the desired behavior. Even if a person commonly performed a behavior, and had an intention to engage in the behavior, if the behavior is not possible due to some extenuating circumstances, it would be impossible to perform the behavior. Thus, TIB proposes that facilitating conditions will serve as a moderator of the interacted relationship between intentions and behavior (Gagnon *et al.* 2003; Triandis 1977).

Fourth, building on concepts from neoclassical criminology (Gibbs 1975), TIB proposes that attitudes are formed based on the beliefs that individuals hold, and the evaluations of these beliefs. *Beliefs* refer to internally held information that one holds to be true (Fishbein & Ajzen 1975), whereas the *evaluation* refers to the internal calculation of the individual which determines how relevant the belief is when forming an attitude in a given circumstance (Fishbein & Ajzen 1975; Triandis 1977). Even though an individual may hold several beliefs regarding an attitude object, each of these beliefs may be of different importance in a given situation. Thus, only beliefs that are evaluated to be relevant will have significant impacts on the formation of the attitude towards the given object. Thus, TIB proposes that the attitude is formed by an interaction of relevant beliefs and their respective evaluations (Triandis 1977). In this study we focus on two specific beliefs regarding the benefits and costs of cyberloafing. Thus, we

ascertain both the beliefs and the evaluation of these beliefs for each construct in our study.

Fifth, TIB proposes a more detailed explanation as to how the individual's environment will influence intentions and behaviors. TIB expands upon the role of social influences through the use of roles, self-concepts, and social norms. Like TRA and TPB, *social norms* are included in this model and refer to the pressures and expectations of others that pressure an individual to behave in a given manner (Triandis 1977). Like TRA and TPB, TIB proposes that social norms increase the inclination of individuals to behave in manners that will increase conformity with the known social group. However unlike TRA and TPB, TIB also proposes that social influences come from sources beyond the norms of the group where the behavior is performed. *Roles* refers to the sets of actions that are deemed appropriate for individuals occupying a given position within the group, whereas *self-concept* refers to concept that individuals have their own internal goals and values regarding what behaviors are appropriate (Bamberg & Schmidt 2003; Triandis 1977). Whereas norms equally apply to all individuals in a group, the insertion of roles into the model allows for the variability that groups experience due to the unique positions and functions of individuals within the group. For example, although a group may have a norm for individuals to be silent unless called upon, it is considered appropriate for the group leader to lead discussion and to speak during the majority of the meaning without being called upon. Additionally, the insertion of self-concept into the model accounts for individual differences due to values of the individual, which may be more important than desires for inclusion within a group. For example, consider a group that normally celebrates successes by attending a local bar for happy hour. However, one of the group members, due to religious convictions, although a long-standing and reputable member of the group, does not attend these celebrations. Personal convictions and central values may override social pressures to conform to desired group behaviors when such behaviors challenge central and salient values of an individual (Bamberg *et al.* 2003).

By incorporating these additional constructs in the prediction of intentions, TIB provides a more comprehensive theoretical model for the prediction of behaviors (Triandis 1977). Due to the conflicting findings in previous literature regarding the antecedents or motivations for employees to engage in cyberloafing (Galletta & Polak 2003; Pee *et al.* 2008; Woon & Pee 2004), TIB is an ideal theory for examining the antecedents of cyberloafing. TIB examines cognitive,

affective, social and habitual factors that may influence cyberloafing rather than only a subset of this list.

2.4 Model Development

Having reviewed the relevant literature and provided the background of the theory of interpersonal behavior, we now explain our theoretical model (See Figure 6). We first explain the two antecedents of attitude followed by the antecedents of social factors. Next, we explain how attitudes, affect and social factors influence intentions. Lastly, we propose how habit, intentions and facilitating conditions impact actual cyberloafing behavior.

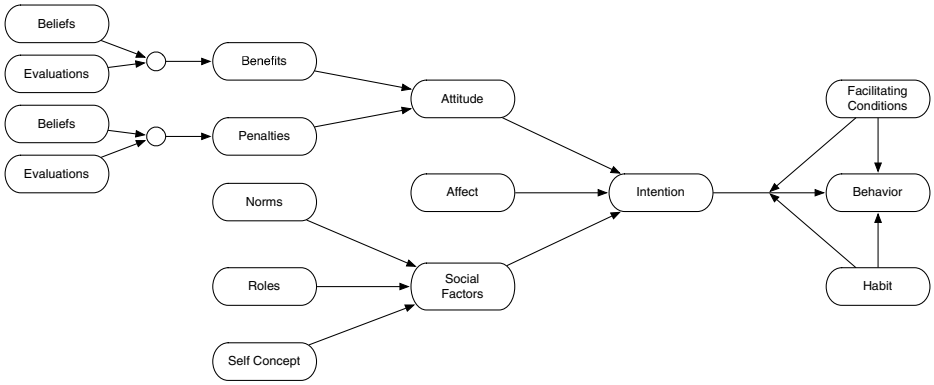

Fig. 6. Theoretical Model.

2.4.1 Attitude

The neoclassical view in the criminology is that people select to engage in behaviors that go against the established procedures, rules and guidelines (*i.e.*, cyberloafing in the context of this study) when it pays off, *i.e.*, people commit these behaviors when the benefits are high and the risk of sanctions is low (Miller 2008; Roshier 1989). Thus, this study adopts benefits and penalties as positive and negative antecedents of attitude respectively. We propose that the expectation of positive outcomes due to cyberloafing should result in more favorable attitudes towards cyberloafing. First, beliefs regarding future potential outcomes serve as motivation to engage in a given behavior (Bandura 1977). This motivation is based on the attitude that the benefits are relevant, possible and will help the

individual achieve their desired goals. If an individual believes that benefits are possible, and likely, their attitude towards the behavior should increase in an effort to achieve the benefits (Cofer & Appley 1967).

The connection between perceived beliefs regarding potential benefits from a behavior and the attitude towards engaging in the behavior has long been proposed and supported in prior literature in different application of neoclassical theory of crime and motivation research (Ajzen & Fishbein 1977; Cofer & Appley 1967; D'Arcy *et al.* 2009; Straub 1990; Theoharidou *et al.* 2005). We extend these findings to cyberloafing, and propose:

> *H1: The perceived benefits regarding cyberloafing will be positively related to the attitude towards the use of the Internet at work for personal reasons.*

As individuals are attempting to maximize benefits and minimize penalties (Theoharidou *et al.* 2005), the perception of penalties associated with cyberloafing should also alter an individual's attitude towards future loafing. Further, prior work has already indicated that individuals tend to be more averse to loss and punishments than rewards (Kahneman & Tversky 1979). While benefits should increase an individual's attitudes towards engaging in the behavior, perceived penalties associated with this behavior should have a stronger and negative impact on the individual's attitude towards the same behavior. In line with the neoclassical theory of crime (Roshier 1989), we propose that individuals will avoid negative outcomes and punishments by forming negative attitudes towards engaging in a punishable behavior. As such, we propose:

> *H2: The perceived penalties regarding cyberloafing will be negatively related to the attitude towards the use of the Internet at work for personal reasons.*

2.4.2 Social Factors

Triandis (1977) defines *social factors* as the individual's assessment of the reference group's culture, and the specific interpersonal agreements that the individual has made with others, in specific social situations (Woon & Pee 2004). TIB is more social oriented than either TRA or TPB and proposes several sources of social influence beyond those of social norms (Bamberg & Schmidt 2003). Although other sources of social influence could be proposed and tested, this paper tests those as proposed by (Triandis 1977).

First, (Triandis 1977) proposed that the first major source of social influence is due to the presence of social norms within referent groups. Social norms influence individuals by increasing the desire and pressure to conform to the expected behavior from a reference group. Individuals within the group, or being observed by a group, follows these unwritten rules to conform to the pressures of the group, and thereby perform in accordance with the norms of the relevant referent group (Ajzen 1985). Although individuals may break norms and behavior contrary to norms, the presence of norms serve as a cue or pressure that increases the likelihood of the individual to behave in accordance with the given norm (Madden *et al.* 1992).

Norms are known to influence behavioral intentions of individuals in groups, as this is also a central tenet of both TRA and TPB (Ajzen 1985; Fishbein & Ajzen 1975; Leone *et al.* 1999; Madden *et al.* 1992). However, social norms are only one source of influence that can occur within the social context of a given situation. Thus, in accordance with TIB, we propose that each of these social factors should be considered jointly rather than separately. Thus, although social norms have been shown to directly impact behavioral intentions from researched based on TRA and TPB. In accordance with TIB, we propose that the joint effects of all social factors will mediate the relationships between each source of social influence and abuse intentions. Social norms produce an effect upon the influence that the individual feels from social sources for a specific situation, which are then used to create behavioral intentions. Thus, we propose:

> *H3: Social norms within the organization regarding cyerloafing will be positively related to the social factors regarding cyberloafing.*

Roles refer to the idea of what is normal and proper behavior as determined by the position of the individual within the relevant social group (Triandis 1977). Like social norms, this type of idea can only be considered within the social situation where the individual is deciding how to behave. Roles are socially construed and understood (Aarts *et al.* 1997; Aarts *et al.* 1998; Bamberg & Schmidt 2003; Verplanken *et al.* 1997). When deciding how to behave, the consideration of the individual's roles can only be understood by considering the social role of relevance within the group. For example, an individual's role as sister may not be relevant in deciding whether to cyberloaf unless her sister happens to be her boss at the company.

As individuals have numerous roles, and functions, it is only possible to understand the impact of roles on eventual behavior by considering the relevant

group that is involved with the given role (Ashforth & Mael 1989; Turner 1985). Individuals will consider the various roles that are deemed to be relevant for the given context and determine what type of influence this role has on that behavior (Bamberg & Schmidt 2003; Triandis 1977). Thus, an individual's roles within the organization should significantly impact the overall felt social influence that an individual feels towards cyberloafing. As such, we propose:

> *H4: Organizational roles within the organization will be positively related to the overall social factors regarding the use of the Internet at work for personal reasons.*

Lastly, (Triandis 1977) proposes that the individual's self-concept regarding the behavior should also affect the amount of social influence perceived by the individual. Self-concept is proposed to impact social factors due to the ability of significant and known others to observe behaviors. For example, if an individual strongly believes that it is important to himself to reduce his carbon footprint on the world, he would have a strong pressure from known others to engage in behavior that supports this known self-concept. He would have an increased likelihood to ride a bike to work or use a hybrid car in order to publicly conform to his own internal value system. Individuals often assess themselves based on the opinions and feedback that they receive from others (Passos & Caetano 2005; Robinson & Weldon 1993). Thus, in deciding how to behave in a given situation, the potential social consequences and the impact of relevant social others on the individual and his or her self-concept will alter how an individual will decide to behave. Thus, we propose:

> *H5: Self-concepts regarding cyberloafing will be positively related to the overall social factors regarding the use of the Internet at work for personal reasons.*

2.4.3 Antecedents of Intention

Previous work has long proposed and found that attitudes, emotions and social factors influence behavioral intentions (Bamberg & Schmidt 2003; Fishbein & Ajzen 1975; Leone *et al.* 1999; Pee *et al.* 2008; Petty & Wegener 1998; Triandis 1977). As the relationship between attitude and emotions on intentions is well known and specified in prior literature, we will briefly explain the relationship between social factors and intentions as this relationship is only mentioned in TIB.

As previously stated, TIB expands upon the social influences that may alter an individual's behavioral decisions by including other social factors beyond social norms. In the previous section we described these sources of social factors and explained how they would impact behavior by means of altering the leave of social influence felt by an individual in the given situation. Thus, the connection between social factors and behavioral intentions is based on the same reasoning given for each factor, or those common to social norms in TRA and TPB. Essentially, individuals are influenced by pressures that they perceive from relevant social groups where the behavior would be performed (Leone *et al.* 1999; Sheppard *et al.* 1988). These sources of social influence increase the likelihood that an individual will desire to conform to known group norms, internal value structures or roles that the individual is expected to adhere to.

As these relationships have all been found in prior literature, we merely extend these previous findings to fit the context of our study and propose the following:

H6: Attitudes regarding the use of the Internet at work for personal reasons will be positively related to the intention to engage in cyberloafing.

H7: Affect regarding the use of the Internet at work for personal reasons will be positively related to the intention to engage cyberloafing.

H8: Social factors regarding the use of the Internet at work for personal reasons will be positively related to the intention to engage in cyberloafing.

2.4.4 Predicting Cyberloafing Behavior

Previous research has long proposed and found that both the intention to engage in a behavior and a habit of performing a behavior are strong predictors of behavior (Aarts *et al.* 1998; Bamberg & Schmidt 2003; Gagnon *et al.* 2003; Leone *et al.* 1999; Malle 1999; Sheppard *et al.* 1988; Valois *et al.* 1988; Verplanken *et al.* 1997; Verplanken & Orbell 2003). However, the theory of interpersonal behavior builds upon this research by proposing an interaction of these constructs on eventual behavior (Bamberg *et al.* 2003; Bamberg & Schmidt 2003; Gagnon *et al.* 2003; Triandis 1977). (Triandis 1977) originally explained that the intention to behave in a given fashion would be strongly influenced by the previous frequency of the behavior. For example, if an individual has no habit of checking his email at work, it is unlikely that the individual will check his

email, despite a strong intention to do so at a given point in time. Likewise, if the individual has a strong habit of checking his email on an hourly basis, it is very likely that he will continue to check his email at work despite an intention to not do so. However, the effect of each will be magnified when they are in the same direction. If the individual has an intention to check his email and he usually does, it is even more likely that he will do so, than if he did not have the habit, or the intention. In other words, TIB proposes that future behavior is not only a function of what the individual intends to do but also what the individual typically does.

However, even though this interaction was proposed by (Triandis 1977), later empirical tests of the theory in this context have not considered the interaction of these constructs on behavior (Chang & Cheung 2001; Cheung *et al.* 2000; Pee *et al.* 2008; Woon & Pee 2004). We thus, extend the proposed interaction of intention and habit on behavior from the theory of interpersonal behavior as found in prior research (Bamberg & Schmidt 2003) to the context of cyberloafing:

H9a: The intention to use the Internet at work for personal reasons will be positively related to actual cyberloafing.

H9b: The habit of using the Internet at work for personal reasons will be positively related to actual cyberloafing.

H9c: The interactive effect of intentions and habit will strongly predict the use of the Internet at work for personal reasons.

In accordance with neoclassical theories of crime (Roshier 1989), like Rational Choice Models, facilitating conditions should moderate the relationship between intentions and habit on behavior (Gibbs 1975; Lee *et al.* 2004; Straub 1990). If an individual has an intention to engage in the use of the Internet at work for personal reasons, but does not have the means or opportunity to easily perform the behavior, it is not likely the personal use of Internet will take place (Willison & Siponen 2009). By controlling and monitoring workstations and network traffic, organizations can decrease the facility with which individuals may engage in cyberloafing and avoid punishment. Thus, the presence of controls and monitoring functions within the network would likely deter abuse behaviors of individuals. This has been proposed in prior work (D'Arcy *et al.* 2009; Lee *et al.* 2004; Theoharidou *et al.* 2005) and we likewise replicate this prediction:

H10a: Having ready access to the Internet at work will be positively related to actual cyberloafing.

H10b: Having ready access to the Internet at work will negatively impact the relationship between intentions and actual cyberloafing.

2.5 Methodology

2.5.1 Method and Data Collection

This study utilized a survey methodology. Data were collected during a two-week period from a service company based in Finland. The company employs 1150 employees, of whom 238 submitted completed, with a usable response rate of 21%. The survey was anonymous; no identifying information of any kind was gathered from the participants. It was also clearly communicated to the respondents, that independent university researchers would analyze the results.

The reliability of constructs can be improved by using previously validated and tested questions (Straub 1989; Boudreau *et al.* 2001). Accordingly, we used items that were taken from previously validated and reported instruments (with some minor wording adjustment to fit the context of this study). Appendix 1 provides a detailed list of the scales that were used for this study. Participants were asked to report their personal use of the Internet at work for non-work purposes using. Participants were then asked to provide answers for the remaining constructs in the theory. These include: attitude (Pennington *et al.* 2004), beliefs and evaluations about the outcome of their behaviors (Pee *et al.* 2008), norms (Gagnon *et al.* 2003), roles (Bamberg & Schmidt 2003), self-concept (Gagnon *et al.* 2003), social factors (Pee *et al.* 2008), affect (Pee *et al.* 2008), habit (Verplanken and Orbell 2003), facilitating conditions (Pee *et al.* 2008), intentions (Pee *et al.* 2008) and behavior (Pee *et al.* 2008).

Given that we used TIB in new context, we used a pilot test to ensure the readability and validity of the questions. The pilot population consisted of staff members at a public university in Finland. The pilot respondents included IT support staff, lecturers, secretary, administrative and educational planners. We obtained 43 usable responses. Our pilot study used a paper-based questionnaire, which consisted of 65 questions, including an area where respondents could leave remarks and feedback about the questions that were asked. We used these responses to ascertain the validity of the questions, and to identify any points of confusion within the survey. Based on feedback, and initial statistical analysis, several questions were slightly modified prior to the final data collection.

2.5.2 Construction of Benefits and Penalties

This section will briefly highlight how the benefits and penalties were created from their respective beliefs and matching evaluations. TIB proposes that weighted beliefs form initial attitudes that serve as antecedents for intentions. For each relevant belief in this context, participants were asked to judge the likelihood of the benefit or penalty occurring and the magnitude of its impact on the participant. The two scores (*i.e.*, belief and evaluation) for each item were then multiplied to form an evaluated belief score for each respective item. For example, suppose a participant gave a score of 6 (Fairly likely) that she would receive a warning for using the Internet at work for non-work related purposes, and she also rated that the severity of this warning as a 2 (lenient). Her evaluated belief score would be 12 (6 x 2). These formed scores were then loaded on to their respective construct (*i.e.*, benefits or penalties) as described by the literature on TIB (Gagnon *et al.* 2003; Triandis 1977).

2.6 Data Analysis

2.6.1 Establishing Factorial Validity

Before assessing the hypotheses, several steps were taken to assure the reliability and accuracy of the collected data. First, we ascertained the types of constructs used in this study. Using (Diamantopoulos & Winklhofer 2001), and the sources of the instruments, we ascertained whether constructs were formative or reflective. The remainder of this section will report our procedures for establishing factorial validity tests for reflective and formative constructs using their respective tests.

2.6.2 Reflective Constructs

To analyze the factorial validity of the constructs, we used partial least squares (PLS), using SmartPLS version 2.0 (Ringle *et al.* 2005). To establish the validity of our reflective indicators, we followed the procedures outlined by (Gefen & Straub 2005). To establish convergent validity, we generated a boostrap with 200 resamples and examined the t-values of the outer model loadings. All retained items were significant at the .05 α level (See Table A2.1 in Appendix 2). This demonstrates strong convergent validity for the reflective constructs.

We then used two established methods for establishing discriminant validity: correlating the latent variable scores against the indicators (see Table A2.2), and calculating the AVE (see Table A2.3). Both of these demonstrated strong convergent validity for all retained items.

Finally, to establish reliability, PLS computes a composite reliability score as part of the model analysis (See Table 3). This score is a more accurate assessment of reliability than Cronbach's alpha because it does not assume that loadings or error terms of the items to be equal (Chin *et al.* 2003). Each reflective construct in our research model demonstrates high composite reliability that exceeds standard thresholds.

Table 3. Composite Reliability

Construct	Composite Reliability
Affect	0.962
Attitude	0.910
Behavior	0.952
Habit	0.959
Intention	0.970
Roles	0.911
Self Concept	0.895

2.6.3 Measures

Validating formative indicators is more challenging than validating reflective indicators, because the established procedures exist to determine the validity of reflective measures do not apply to formative measures (Petter *et al.* 2007), and the procedures validating formative measures are less known and established (Diamantopoulos & Winklhofer 2001). Researchers have generally used theoretical reasoning to support the validity of formative constructs (Diamantopoulos & Winklhofer 2001), although there are approaches that can be used beyond theoretical reasoning alone (Marakas *et al.* 2007; Petter *et al.* 2007). Though no technique is widely established for validating formative measures, the modified multitrait-multimethod (MTMM) approach, as presented in (Loch *et al.* 2003; Lowry *et al.* 2009; Marakas *et al.* 2007), is a promising solution that we followed.

For each formative item, we created new values that were the product of the original item values by their respective PLS weights (representing each item's

weighted score). We then created a composite score for each construct by summing all the weighted scores for a construct. We then produced correlations of these values, providing inter-measure and item-to-construct correlations (see Table A2.4).

To test convergent validity, we checked whether all the items within a construct highly correlate with each other, and whether the items within a construct correlate with their construct value. This was mostly true in all cases, inferring convergent validity. While we would ideally want inter-item correlations to be higher within a given construct, this cannot be strictly enforced as there are exceptions depending on the theoretical nature of the formative measure (Diamantopoulos & Winklhofer 2001; Loch *et al.* 2003). Thus, we believe the most meaningful discriminant validity check with formative measures is to look at the degree to which items within a construct correlate to a given construct.

Finally, we used another approach to assess formative validity as suggested by (Petter *et al.* 2007) that involves testing the multicollinearity among the indicators. This is particularly important with formative indicators because multicollinearity poses a much greater problem than with reflective indicators. Hence, low levels of multicollinearity are usually indicated with levels of the variance inflation factor (VIF) below 10, but in the case of formative indicators, the VIF levels need to be below 3.3 as a more stringent test (Petter *et al.* 2007). In our case, the VIF for five indicators (an item from benefits, from penalties, two from norms and one from social factors) was above 3.3, and these were all subsequently dropped from the final analysis.

In sum, using MTMM analysis and assessing VIF levels, we conclude reasonable discriminant validity exists with our formative constructs. Finally, because of the nature of formative measures, reliability checks cannot be reasonably made (Diamantopoulos & Winklhofer 2001).

2.6.4 Testing for Common Methods Bias

Given that data was collected using one method, we used two methods to ascertain to establish the presence of common methods bias. First, we used the Harman's single factor (Podsakoff *et al.* 2003). This test required that we run an exploratory unrotated factor analysis on all of the first-order constructs. The aim of the test is to see if a single factor emerges that explains the majority of the variance in the model. If so, then common-method bias likely exists on a

significant level. The result of our factor analysis for our study produced 35 distinct factors, the largest of which only accounted for 15.8% of the variance of the model.

Second, we examined a correlation matrix of our latent constructs to determine if any of the correlations were above .90, which is strong evidence that common methods bias exists (Pavlou *et al.* 2007). None of the correlations were near this threshold.

Given that our data passed both tests for common methods bias, we conclude that there is little reason to believe that our data exhibits any of the negative effects from common methods bias.

2.6.5 Results of Hypotheses Testing

Given that our data displays factorial validity and does not display common methods bias, we tested our model, which is displayed in Figure 7. The results of our hypotheses, as based on the model testing are shown in Table 4.

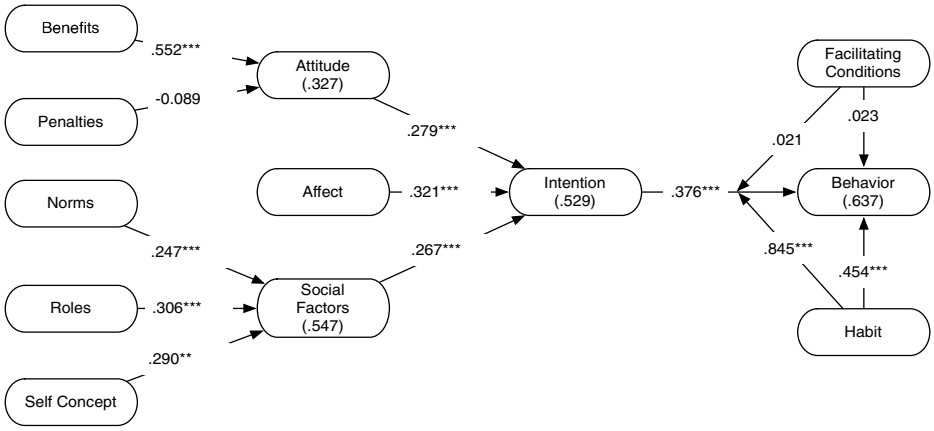

Fig. 7. Model Results.

Table 4. Summary of Model Results.

#	Hypothesis	Coef.	Supported?
1	Benefits → Attitude	.552 ***	Yes
2	Penalties → Attitude	-0.089 ns	No
3	Norms → Social factors	.247 ***	Yes
4	Roles → Social factors	.306 ***	Yes
5	Self concept → Social factors	.290 **	Yes
6	Attitude → Intention	.279 ***	Yes
7	Affect → Intention	.321 ***	Yes
8	Social factors → Intention	.267 ***	Yes
9a	Intention → Behavior	.376 ***	Yes
9b	Habit → Behavior	.454 ***	Yes
9c	Intention x habit → Behavior	.845 ***	Yes
10a	Facilitating conditions → Behavior	.023 ns	No
10b	Facilitating conditions x intention → Behavior	.021 ns	No

*** p < .001; ** p < .01; * p < .05; ns—not significant

2.7 Discussion

2.7.1 Summary of Findings

We would like to briefly highlight a number of findings based on our empirical study. First, our results indicate that affect is the strongest antecedent of the intention to engage in cyberloafing. Individuals that have positive emotions regarding the use of the Internet are more likely to use it at work for non-work purposes. This is consistent with the TIB (Triandis 1977) and previous studies on cyberloafing by (Pee *et al.* 2008) and (Chang & Cheung 2001).

Second, our results show that one's attitude towards cyberloafing as the next important antecedent of one's intention to cyberloaf. Further, attitude is strongly predicted by the benefits that one associates with cyberloafing. However, the individual's attitude towards cyberloafing is not predicted by penalties that an individual may receive when caught cyberloafing. The importance of both benefits and attitude are in support of TIB (Bamberg & Schmidt 2003; Pee *et al.* 2008; Triandis 1977). However, previous research by (Seymour & Nadasen 2007) found that attitudinal variables do not promote cyberloafing. We explain these differences by different operationalization of the attitude construct. For (Seymour & Nadasen 2007), attitude includes low job satisfaction, inadequate rewards and

long working hours. We utilized a measure for attitude and furthermore, attitude was predicted by perceived benefits and penalties associated with cyberloafing. By directly measuring attitude, we believe that this construct is more accurately operationalized as specified by TIB.

Third, we found that social factors is also a significant antecedent of the intention to cyberloaf. Further, we find that all three predicted antecedents of social factors are significant in predicting this construct. This is consistent with the TIB (Triandis 1977). Related studies on cyberloafing have reported mixed findings regarding social factors. (Galletta & Polak 2003) reported that subjective norms, operationalized in terms of peer culture and supervisor culture, increase cyberloafing. However, (Seymour & Nadasen 2007) found that supportive peer and supervisor cultures do not lead to an increased intention to cyberloaf. We expand upon this previous work by exploring not only the norms associated with cyberloafing, but also the role that an individual has within the organization and the individual's concept regarding cyberloafing.

Fourth, our results show that, as predicted by TIB, TRA and TPB, the intention to engage in cyberloafing is strongly predictive of actual cyberloafing behavior. Previous work on cyberloafing also found support for this relationship (Pee *et al.* 2008; Woon & Pee 2004). However, unlike predicted by TIB, the facilitating conditions that would more easily to enable an individual to engage in cyberloafing show no significant effects on actual cyberloafing behaviors, or interact with the intention to cyberloaf.

Finally, our results indicate that an individual's habitual cyberloafing is a very important and strong indicator to consider when predicting actual cyberloafing behaviors. An individual's habit to cyberloaf in the past is the strongest antecedent of current, actual cyberloafing behavior. This is in alignment with previous research on habits (Verplanken *et al.* 1997; Verplanken & Orbell 2003). Additionally, we found that the interactive effect of intentions and habit strongly predict actual cyberloafing behavior. Our finding is consistent with TIB (Triandis 1977). We find no studies that have studied the interaction effect between intention and habit in relation to cyberloafing. Previous related research that built upon TIB did not investigate this interaction (Pee *et al.* 2008; Woon & Pee 2004) or ignored the effect of habit as the work by Cheung and colleagues (Chang & Cheung 2001; Cheung *et al.* 2000) was focused on the adoption of the Internet in the function of the employees' role within the organization.

2.7.2 Contributions

Our study has five important contributions to the literature on cyberloafing. First, our model indicates that the strongest predictor of cyberloafing behavior is based on an interaction of an individual's habits regarding cyberloafing and the individual's intention to cyberloaf. Specifically, individuals that have the intention to cyberloaf and have a habit of cyberloafing are even more prone to cyberloaf than either of these indicators when considered separately. This interaction is important for future research in that both management and researchers are unable to directly alter the habits that individuals may have towards cyberloafing, but it is possible to alter the organizational environment and thereby reduce the intention to engage in cyberloafing. This interaction increases both the importance of habit and intention constructs when attempting to predict or control cyberloafing behaviors.

Second, our study shows that the largest predictor of actual cyberloafing behavior is an individual's habit of cyberloafing. This is important for two reasons. First, previous research has not found support for the importance nor strength of this relationship. Habits are strong predictors of behaviors and should be considered in future work on this phenomenon. Second, given the strong effect of habit on cyberloafing, it would stand as a primary candidate for interventions to reduce cyberloafing. However, habit research (Verplanken *et al.* 1997; Verplanken & Orbell 2003) has found that deprogramming habits are very difficult and that interventions that attempt to reduce the habit strength are likely to fail. Due to the difficulty involved with reducing habit strength, it is more important to prevent habits from forming regarding cyberloafing.

Third, this model includes more antecedents than any previous studies. The inclusion of these many antecedents into the model makes it possible to compare each of these antecedents to each other. This builds on previous research by including multiple antecedents that have not been studied together (*i.e.*, benefits, penalties, attitudes, social factors, norms and intentions) and also antecedents that have not been studied in prior studies (*i.e.*, affect, habit, roles and self-concept). Our model shows that most of these antecedents are important predictors of cyberloafing behaviors and should be considered in future research.

Fourth, our model indicates that interventions may have limited abilities to reduce cyberloafing in an organization. First, we see that the effect of penalties is non-significant indicating that deterrent methods of controlling cyberloafing have

no impact on eventual cyberloafing. This finding is rather interesting as it is contrary to the general approach to reducing undesired behaviors as proposed by both control and deterrence theories (Gibbs 1975; Ouchi & Maguire 1975). Second, the affect that an individual has towards cyberloafing is largely outside of the ability of organizational interventions to alter. Affect is an internal construct that is formed from prior experience and based on the motional make-up of the individual (Staw *et al.* 1994). However, organizational interventions generally are not able to alter these types of emotions. Rather, emotional-based training would need to be implemented that could alter affect over time.

Lastly, our model reports the highest R squared in regards to cyberloafing behavior that has been reported to date in an IS journal. Much of the previous work on cyberloafing has stopped at the intention to cyberloaf, and when actual behavior has been collected lower R squareds were reported than in this study. By building on previous research and including many of the antecedents reported in their studies we report the most powerful model for predicting cyberloafing to date.

2.7.3 Implications for Research

Given that employees rationalize their personal use of Internet at work by saving their personal time and expenses by using company Internet resources at work, there is a need to obtain a deeper understanding on what types of services the employees use, and more importantly, why employees see that they are able to save time by cyberloafing. For example, is the reason for this behavior that the employees would rather save their personal time, and use working time for personal use of Internet at work, instead of their personal time. This information is important in further understanding these reasons, which in turn, help to design education and campaigning sessions aimed at overcoming these rationalizations.

Again, given that employees feel that cyberloafing increases their work motivation, and also increase their work productivity, qualitative interviews are needed to obtain a deeper understanding on these phenomena ((Myers & Newman 2007). For example, the interview should examine why employees think that such browsing increases work productivity? Here the idea is that after when we know the underlying rationalizations as to why employees belief that the action increases work productivity, we can design training and campaigning interventions that tries to overcome these rationalizations.

Given that employees sees cyberloafing as acceptable and according to the their principles, we suggests that future research should obtain a deeper insights on these reasons in general and the underlying rationalizations in particular. In addition, given these results, future research should examine the role of moral persuasion in changing the employees' views that the action is acceptable. This entails two kinds of studies. First, there is a need to examine to which extent different moral qualifiers influence cyberloafing. The most well-known and holistic theory in this area is Kohlberg's theory of cognitive moral development (Kohlberg 1984) (see (Siponen & Vartiainen 2004). Then, if these studies suggest that moral decision-making explains cyberloafing, the second stream of studies should focus on how to influence such behavior by appealing to employees' moral responsibility. The moral persuasions intervention could be based on Kohlberg's theory of cognitive moral development (Kohlberg 1984), and should address all stages of moral development and decision-making. Such an education intervention should come with pre-then-post research settings, along with a control group that do not receive the intervention.

Given that employees perceive cyberloafing is appropriate and fits to their work role, qualitative interviews are needed to further understand these reasons. For example, interviews should find out why employees sees that, due to their certain work role, it is justified to engage in personal use of Internet at work. Interviews should also examine why employees feel that it is appropriate to use Internet for personal purposes at work. This information is needed to design education interventions aimed at attempting to overcome employees' rationalizations, like that such an action is acceptable from the viewpoint of employees' work role.

Also, there is a need to study whether an education intervention stressing the potential harms caused by cyberloafing is efficient in changing employees' behavior. Such an intervention should state to the employees that cyberloafing increases risks for viruses and spyware, windows registry modifications, increases IT traffic, and the sites may require installation of software components and plug-ins (that may results malfunctions or increase malware risks). In addition, cyberloafing may increase spam and non-work related emails, given that employees provide their work email addresses to all kinds of services. Finally, the education program should provide examples to the employees, which shows that cyberloafing has decreased the public image of the company.

Other possibility to design an intervention is to use fear appeals (Johnston & Warkentin 2010), Following this idea, future research could investigate the influence of fear appeals on cyberloafing. The research design would entail pre-test, fear appeal, and then post-test.

Given that cyberloafing is habitual behavior, if not addictive behavior, we call for research that attempts to change habitual behavior. The use of "pre-then-post" research setting is preferred, along with control groups.

Finally, all the previous studies on the topic use self-reports. We suggest that future studies should also use of objective data to measure the actual behavior.

2.7.4 Implications for practice

Regarding our results on affect, practitioners need to stress that although cyberloafing is pleasant and interesting, it has a number of negative implications for the organization. We also challenge the organizations to emphasize ways to increase work motivation by other means, and ensuring through recruitment and work assignments, that organization have motivated work force in each organizational role.

Our results suggest that employees feel that cyberloafing is beneficial for them. To be more precise, employees see that they are able to save their personal time and expenses by using company Internet access for personal purposes. The employees also feel that the use of such applications make their work more interesting and convenience, and also increase their work productivity. To tackle such a view that cyberloafing is beneficial for employees, we suggest the use of education sessions and sessions led by supervisors and managers. The aim of these sessions is to explain the employees the ways in which cyberloafing is risky for the organization, and decrease work productivity.

Our results suggest that cyberloafing is habitual behavior to our respondents. This is challenging for practitioners, provided that habits are automatic behavior. Hence, habitual behavior calls for long-term training and campaigning programs.

Our results also suggest that social factors, like approval by family, friend, co-workers, supervisors and top management, increase the intention to cyberloaf. Overcoming these factors require number of actions. For example, supervisors and managers need to take a strong position that cyberloafing is not acceptable and professional behavior at the company.

Our results show that supportive normative culture influence employees' cyberloafing. Here it is important to stress to the employees by IT staff and

managers that cyberloafing is not acceptable, even it could be encouraged by family members and friends.

Given that employees perceive that cyberloafing fits to their roles as employees, we suggests that organizations recruit supervisors and managers to spread to word to their employees that cyberloafing is not appropriate. The supervisor and managers need to also convince their employees that, from the viewpoint of the organizational roles to which the employees occupy, the personal use of Internet at work is not justified. For example, the supervisors could inform the employees that the work tasks performed by the employees do not require them to visit the non-work related web sites. Also, superiors could state that such activity is not professional, and its may decrease work efficiency by interrupting work. Also, the supervisors could stress that such an activity is a source of viruses and spyware, and finally, it is a waste of company IT resources.

Our results also show that penalties and controls have limited effects on cyberloafing. This can be seen as good news to the companies, given that sanctions require monitoring, which requires resources.

2.8 Conclusion

Cyberloafing is a significant problem that annually results in the loss of billions of dollars (Anandarajan 2002). With more and more organizations increasing their use of computers, the cost of cyberloafing will only increase with time. Research has focused on understanding both the type of individual that is likely to engage in this behavior, and to reveal what leads to these acts (Anandarajan 2002; Chang & Cheung 2001; Cheung *et al.* 2000; Galletta & Polak 2003; Lim *et al.* 2002; Pee *et al.* 2008; Seymour & Nadasen 2007; Stanton 2002). However, these findings have reported conflicted results. We build on previous research by including these antecedents into one model in an attempt to compare their effects on cyberloafing. Without being able to understand why employees engage in cyberloafing, organizations are unable to modify their practices to reduce the likelihood of cyberloafing and reduce its subsequent cost to the organization.

This study utilized a theoretical approach to explore the various motivations that may lead to cyberloafing. We found that organizations need to consider several factors when attempting to reduce this behavior. Specifically, companies should attempt to reduce the perceived benefits involved with cyberloafing, the emotional attached to engaging in this act, and the habit that these employees

have to continue to behave in this fashion. In more practical terms, organizations should ensure through recruitment that they have highly motivated and committed employees to each work role. Also, there is need to establish education sessions and campaigns stressing that cyberloafing has a number of negative implications for organizations. Also, managers need to explain to their employees the reasons why cyberloafing decreases work productivity, is insecure, takes IT resources, and hence, it is not acceptable. Interestingly, our results show that penalties and controls have limited effects on cyberloafing.

Future research should use interviews in the order to obtain a deeper understanding on the reasons as to why the employees feel that they are able to save time and increase work productivity by cyberloafing. Also interviews should examine why the employees sees that cyberloafing fits their work roles. This information is important in order to design education interventions, aimed at persuade employees to avoid future cyberloafing.

3 Why Home Computer Users Use Anti-malware Tools: The Extended Parallel Processing Model

3.1 Abstract

Previous studies have reported that most home computers are infected by malware, a term that includes viruses and all unwanted malicious software. Even though massive numbers of home computers are infected the security behavior of these home users has received comparatively little empirical research. Previous studies in the area have applied TAM, TRA, TPB, and the protection motivation theory. To contribute to the current understanding of home computer user information security behavior, we apply a theory called the extended parallel processing model (EPPM), not previously used in this field. We test this theory in the context of Chinese home users (N = 285). Our results largely support the model, and based on EPPM, we present 10 new relationships, which have not been examined in the IS context, and discuss their implications for research and practice.

3.2 Introduction

Malware, including spyware, viruses and all kinds of unwanted software, is an increasing problem for home users. Several studies have highlighted that most home computers are affected by malware (Chenoweth *et al.* 2009; Litvinoff 2008). In addition to direct problems caused by malware, such as the loss of personal data, such as credit card numbers, and reduced computer speed for applications, malware also causes indirect problems. These indirect problems include using infected or hijacked home computers as a breeding ground for launching attacks against other Internet users and companies and distribution of questionable material through the infected computers. Besides attacking organizations, infected home computers may infect corporate users in several ways. For example, much work is now done outside of the workplace, with employees using non-organizational or family computers for work purposes, not to mention using memory sticks in different computers, which can easily propagate malware from computer to computer.

Keeping these threats and the many problems that can be caused by malware in mind, it is interesting to note that many of these threats and problems can be resolved with readily available free tools. It is very important to study the factors explaining how home users use such anti-malware tools and the factors that inhibit their adoption.

Due to the threats attributed to malware, employee security behavior with regard to information systems (IS) in organizations is well studied in IS security literature in terms of computer abuse, misuse and employee compliance with IS security policies (Myyry *et al.* 2009); however, little empirical research has focused on home computer information security behavior. We argue that findings on "computer abuse" or "employee compliance with IS security policies" in an organizational context, regarding such behavior as the use of anti-malware tools, may not translate into the home user context and vice versa—the organizational context differs considerably from that of the home user. For example, companies can use centralized anti-malware solutions, offer limited user privileges, have competent IT support available, and provide guidelines and policies for safe computing practices. Home users, however, operate in a totally different environment: no one forces them to adopt anti-malware software and there is no IT support available—not to mention the lack of security awareness and the training efforts enjoyed by corporate workers. Hence, home computers provide an easy target for malicious people operating through malware.

To contribute to our understanding of why home users adopt anti-malware tools, we apply the extended parallel processing model (EPPM), which is a new theory in this domain. We test this theory in the context of Chinese home computer users.

The rest of this paper is organized as follows: the second section reviews previous research on home information security behavior; the third and fourth sections discuss the EPPM theory and its development; the fifth section describes the research methodology; and the sixth section provides data analysis describing the results of the paper. The seventh section discusses the implications of the findings for research and practice.

3.3 Literature Review

Previous work on home computer information security behavior has focused on three areas: (1) password psychology, (2) models aimed at explaining and

predicting why home users install or use information security features, such as firewalls or anti-virus programs, and (3) how to persuade or manipulate home users into behaving in a more secure manner.

In password psychology, (Bryant & Campbell 2005) carried out a descriptive study of home users' password memorization. They concluded that most users select passwords based on their personal details, with the result that these passwords are easy to guess. These results led the authors to question whether there are different password techniques that one could easily memorize. Accordingly, (Bunnell *et al.* 1997) examined the recall and guessing rates of cognitive, associative, and conventional (self-selected) passwords using home users (university students). An example of cognitive passwords is a fact-based question, such as: "What is your mother's maiden name?" or "the make or model of your first car?" In the case of an associative password approach, respondents generated up to 20 pairs of cue and response words, with the suggestion that a theme be used to aid memory (Bunnell *et al.* 1997). Conventional passwords are self-generated passwords, which meet some minimum requirements (*e.g.*, are at least eight characters long and contain both letters and numbers).

Bunnell *et al.* (1997) reported that conventional passwords have a high recall rate and quite low guessability; the guessability of cognitive items was high and received the highest recall rate; word associations produced the lowest guessability rate but were difficult to recall.

Regarding the second area of related work, *i.e.*, models aimed at explaining why home users use information security features, such as anti-virus or anti-malware software, studies include (Aytes & Connolly 2004), (Ng & Rahim 2005), (Rhee *et al.* 2005) and (Woon & Pee 2004). Ng and Rahim (2005) integrated TAM, self-efficacy, TPB, and facilitating conditions into one model to predict the intention of a home user to update an anti-virus application. (Ng & Rahim 2005) reported that attitude and subjective norm determined intention to update anti-virus software. They further found that perceived usefulness, family and mass media, as well as self-efficacy, influence the intention of home users to update anti-virus software.

Aytes and Connolly (2004) studied the risky computing behavior of home users (undergraduate university students). To be more precise, they studied why home users, even when they are aware of their insecure practices (*e.g.*, the failure to backup work and disclosing their passwords) continue to engage in such insecure practices. Aytes and Connolly (2004) reported that they could not predict a students' engagement in risky computing behavior merely from knowing how

much the students know about protecting themselves or how the students perceived the negative consequences (Aytes & Connolly 2004). As a result, they postulate that home user security behavior is unlikely to be changed by providing information on the risks and secure practices through security awareness programs.

Rhee *et al.* (2005) tried to explain that, while information security breaches have given probabilities of occurring, the estimation of a security breach occurring for an individual is usually underestimated. They examined whether the optimistic bias from the field of psychology could explain this tendency. They found that the optimistic bias explains information security behavior: home users believe that negative events are more likely to happen to other people rather than them. In other words, everyone believes that he or she is able to beat the odds.

Chan *et al.* (2005) examined the extent to which protection motivation theory (PMT) (Rogers 1975) explains the behavior of home computer users on wireless networks, in terms of using information security features. They found that the perceived severity of an IS security threat, the effectiveness of response, the perceived capability of using the security features (self-efficacy), and the cost of using security features (response cost) affect decisions on whether to use security features.

Finally, the third area focuses on examining how home users can be persuaded or manipulated to behave in a more secure manner. (Anderson & Agarwal, Forthcoming) examined the extent to which message manipulation can influence a home users' intention to take information security measures to protect their home computer. They found that positive motivational messages are more effective than messages stressing negative consequences. While (Anderson & Agarwal, Forthcoming) used university students, (Johnston & Warkentin 2010) used both students and faculty members of the university to examine the effect of fear appeals, which are persuasive messages designed to change home user behavior by suggesting negative consequences if they do not behave as suggested by the message (Johnston & Warkentin 2010). The fear appeal message was based on the PMT. They found that message elements containing response efficacy, social influence, and self-efficacy have a positive influence on a user's intention to use anti-spyware tools.

Among the three areas of related research: 1) password psychology; 2) models aimed at explaining and predicting why home users install or use information security features, such as firewalls or anti-virus programs; and 3)

how to persuade or manipulate home users to behave in a more secure manner), our study contributes to the second area—models aimed at explaining and predicting why home users install or use information security features. The literature review shows that previous studies in this area have applied TAM, TRA, TBP, and PMT. In this study, we apply EPPM, a new theory in this area, which is more comprehensive. In the next section, we describe the EPPM (Witte 1992; Witte *et al.* 1996) and the extent to which it is more comprehensive than previous theories applied in this area in general, and PMT in particular.

3.4 Theoretical Framework

The theoretical framework of this paper is based on the EPPM, which was first proposed by Witte (Witte 1992; Witte *et al.* 1996) (Figure 8). EPPM is an extension and explication of the parallel response model (PRM) (Leventhal 1970), which was used to explain how individuals respond to threats. *Threats* are defined as an individual's perception that something or someone has the intention to cause them harm (Witte 1992). EPPM explains that individuals typically exhibit two types of responses to a threatening situation: to control the danger within the threat or control the fear arising from the threat. This response duality has been found in other research areas and is further explained and defended by (Liang & Xue 2009).

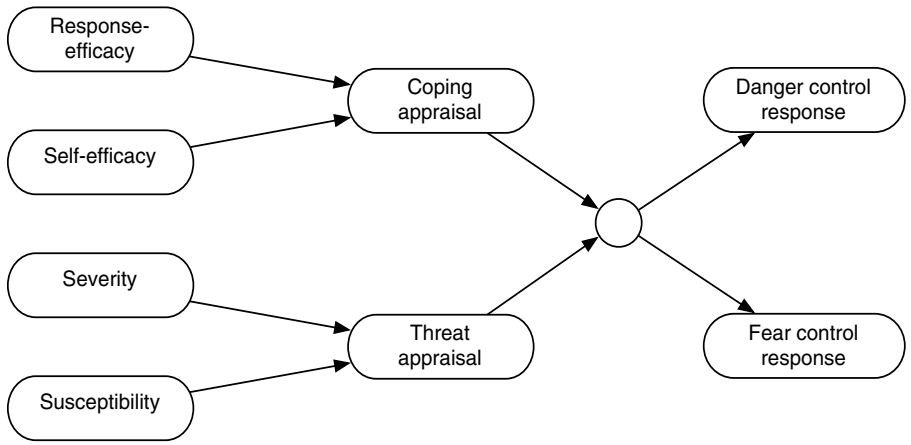

Fig. 8. Simplfied EPPM Model Overview.

When individuals attempt to control the danger within a threatening situation, they are initiating a danger control response. A *danger control response* is defined as the cognitive state of mind wherein an individual is aware of a threat and actively attempting to control the source of the threat in an effort to reduce or entirely remove it (Witte *et al.* 1996). A danger control response is initiated when an individual perceives a threat and is able to respond it.

On the other hand, when individuals attempt to control their emotional responses to the danger evoked by the threat, they are initiating a fear control response. A *fear control response* is defined as the state of mind wherein an individual attempts to control the emotional responses to a threat and is no longer thinking about the original threat or danger it evokes (Witte *et al.* 1996). Fear control response is initiated when an individual perceives a threat and feels that he or she is unable to overcome it. This inability to overcome the threat may be due to the perceived size of the threat, the lack of an adequate response to counter the threat, or the perception that the individual would be unable to successfully counter the threat.

Both the fear control response and the danger control response depend on an individual appraisal of the threat and the individual's ability to cope with the threatening situation. The original PRM (Leventhal 1970) and subsequent work (Johnston & Warkentin 2010; Maddux & Rogers 1983; Prentice-Dunn & Rogers 1986; Rogers 1975; Tanner *et al.* 1989; Witte 1992; Witte *et al.* 1996) have shown that threat appraisal occurs and subsequently initiates the coping appraisal. We will discuss each appraisal and its relevant components.

A *threat appraisal* refers to an individual's cognitive calculation of a threat in a given situation, which is determined by both the severity of the threat and his or her susceptibility to it (Maddux & Rogers 1983; Rogers 1975; Witte 1992; Witte *et al.* 1996). *Severity* refers to the individual's perception of the seriousness of the threat, whereas *susceptibility* refers to the individual's perception of the chances of experiencing the threat (Witte 1992). Threat can only be perceived to exist by the individual if both conditions are met. For example, an illness that results in death (high severity) but that has been completely eradicated (no susceptibility) results in no threat, whereas the current threat of H1N1 flu is considered to be high, due to the highly uncomfortable symptoms (severity) and the ease with which it is passed to others (high susceptibility).

When, and only when, an individual perceives a threat, he or she begins the process of appraising whether he or she would be able to cope with it. The *coping*

appraisal refers to the individual's cognitive calculation of whether an action will reduce the threat and whether the individual would be able to perform this action (Witte 1992). *Response-efficacy* refers to the individual's belief regarding the effectiveness of the recommended response to the threat (Witte *et al.* 1996), and *self-efficacy* refers to the individual's belief in his or her ability to successfully perform the recommended response (Witte *et al.* 1996). An individual's ability to cope with a perceived threat is only possible if an individual believes that the response can reduce or remove the threat (*i.e.*, by reducing the severity or susceptibility) and that he or she can execute this response. Continuing the previous example, an individual that perceives H1N1 flu as a threat would appraise their ability to cope as high if he or she believes that the H1N1 vaccine reduces the susceptibility of H1N1 flu, and that the person is able to receive the vaccine. However, if the individual is either unable to obtain the vaccine or does not believe that it reduces possibility of getting H1N1 flu, the coping appraisal would be low.

3.4.1 The EPPM and PMT

Our study relies on the EPPM (Witte 1992; Witte *et al.* 1996), which is an extension of the PRM (Leventhal 1970). The parallel processing model is the theoretical background on which Rogers created PMT (Maddux & Rogers 1983; Rogers 1975). As both EPPM and PMT come from the same theoretical parent, this section will highlight the differences between the two theoretical approaches.

The PRM (Leventhal 1970) was first used to explain the use of fear in communications to motivate individuals to perform some desired behavior. Shortly thereafter, (Rogers 1975) specified PMT to better explain the cognitive response to fear. Rogers, building on (Leventhal 1970), explained that individuals make two different appraisals: threat and efficacy. First, the individual must cognitively appraise the perceived threat in a given situation. For an individual to perceive a threat, he or she must believe that the threat is both harmful and relevant (*i.e.*, it could happen to him or her) (Johnston & Warkentin 2010; Maddux & Rogers 1983; Rogers 1975).

If and only if the individual perceives a threat in a given situation, he or she would proceed to appraising the efficacy of the given response (Maddux & Rogers 1983). The appraisal of the response consists of two parts: response- and self-efficacy. The individual will evaluate whether the indicated behavior can overcome the threat and that he or she is able to execute that response (Johnston

& Warkentin 2010; Maddux & Rogers 1983). The original PMT model did not include self-efficacy, but it was included in the revised model reported in (Maddux & Rogers 1983).

Although PMT has been used in a variety of fields for more than three decades, this theory is the predominant theory in IS for explaining how individuals respond to technological threats, and its use in IS is summarized in Table 5. These findings lend support to the efficacy of PMT in explaining a variety of situations, but all are limited in several areas that can be overcome through EPPM. The additional relationships proposed by EPPM and this study, which have not been studied in prior research, are summarized in Table 6.

Table 5. Summary of PMT Studies in IS.

Study	Core PMT Variables	Other Variables	Findings
(Woon *et al.* 2005)	Susceptibility Severity Self-efficacy Response-efficacy	Response cost	Severity→ behavior Response-efficacy → behavior Self-efficacy → behavior Response cost → behavior
(Pahnila *et al.* 2007)	Threat appraisal Coping appraisal	Sanctions Normative beliefs Information quality Facilitating conditions Habits Rewards	Threat appraisal→ attitude Facilitating conditions → attitude Attitude→ intention Normative beliefs → intention Habits → intention Intention → behavior Information quality→ behavior
(Boss & Galletta 2008)	Threat appraisal Coping appraisal		Threat appraisal→ coping appraisal Coping appraisal → intention Intention → behavior
(Chenoweth *et al.* 2009)	Susceptibility Severity Response-efficacy Self-efficacy	Response cost Maladaptive coping	Susceptibility→ intention Severity → intention Response-efficacy→ intention Response cost → intention Response cost → maladaptive coping Maladaptive coping → intention

Study	Core PMT Variables	Other Variables	Findings
(Herath & Rao 2009)	Susceptibility Severity Response-efficacy Self-efficacy	Response cost Subjective norm Descriptive norm Org. commitment	Severity→ attitude Response-efficacy → attitude Self-efficacy → attitude Self-efficacy → intention Response cost → attitude Attitude → intention Subjective norm→ intention Descriptive norm → intention Organizational commitment → response-efficacy Organizational commitment → intention
(Johnston & Warkentin 2010)	Severity Susceptibility Response-efficacy Self-efficacy	Social influence	Severity→ response-efficacy Severity → self-efficacy Social influence → intention Response-efficacy → intention Self-efficacy → intention
(Liang & Xue 2009)	Severity Susceptibility Threat appraisal Response-efficacy Self-efficacy Coping appraisal	Response cost Social influence	None, theoretical explication of PMT-based Technology Threat Avoidance Theory (TTAT)
(Liang & Xue 2010)	Severity Susceptibility Threat appraisal Self-efficacy Response Efficacy	Response cost	Severity→ Threat appraisal Susceptibility → Threat appraisal Threat appraisal → Intention Response efficacy → Intention Threat appraisal x response efficacy → Intention Self-efficacy → Intention Response cost → Intention Intention → Behavior

Table 6. Comparative Summary of Relationships Studied in EPPM and PMT IS Research.

Relationship	Theory-base	Tested in
Efficacy ⇒ Intention	PMT & EPPM	(Woon *et al.* 2005), (Boss & Galletta 2008), (Herath & Rao 2009), (Johnston & Warkentin 2010), (Liang & Xue 2010)
Efficacy ⇒ Fear	EPPM	No reported tests of this relationship in IS
Severity ⇒ Threat	PMT & EPPM	(Woon *et al.* 2005), (Boss & Galletta 2008), (Chenoweth *et al.* 2009), (Herath & Rao 2009), (Liang & Xue 2010)
Susceptibility ⇒ Threat	PMT & EPPM	(Woon *et al.* 2005), (Boss & Galletta 2008), (Chenoweth *et al.* 2009), (Herath & Rao 2009), (Liang & Xue 2010)
Threat ⇒ Intention	PMT & EPPM	(Pahnila *et al.* 2007), (Herath & Rao 2009), (Liang & Xue 2010)
Threat ⇒ Fear	EPPM	No reported tests of this relationship in IS
Intention ⇒ Behavior	PMT & EPPM	(Pahnila *et al.* 2007), (Boss & Galletta 2008), (Liang & Xue 2010)
Habit ⇒ Behavior	This study	No reported tests of this relationship in IS
Cost ⇒ Behavior	This study	(Chenoweth *et al.* 2009), (Herath & Rao 2009), (Liang & Xue 2010)
Benefit ⇒ Behavior	This study	No reported tests of this relationship in IS
Fear ⇒ Avoidance	EPPM	No reported tests of this relationship in IS
Fear ⇒ Reactance	EPPM	No reported tests of this relationship in IS
Subjective norms ⇒ Social influence	This study	No reported tests of this relationship in IS
Descriptive norms ⇒ Social influence	This study	No reported tests of this relationship in IS
Social influence⇒ Efficacy	This study	No reported tests of this relationship in IS
Social influence⇒ Intention	This study	(Johnston & Warkentin 2010)

PMT expands on only one-half of the original model proposed by (Leventhal 1970); it ignores the emotional response of the individual confronted with a threat. Although the technology threat avoidance theory proposed by (Liang & Xue 2009) does include the emotional coping idea presented in (Leventhal 1970), this theory has yet to be empirically validated and, as with other PMT work in IS, only implements the proposed PMT model without proposing or measuring the emotional responses of the individual. EPPM extends the original PRM (Leventhal 1970) and includes and explains how individuals cope emotionally with threats that they feel they are unable to avoid or effectively respond to.

Second, PMT does not explain what happens to individuals that do not protect themselves and instead behave in a non-prescribed manner. PMT models

focus on individual protection motivation intentions or behavior, and do not measure, propose, or investigate how or why individuals choose to behave contrary to the proposed communication (see (Boss & Galletta 2008; Chenoweth *et al.* 2009; Herath & Rao 2009; Johnston & Warkentin 2010; Pahnila *et al.* 2007; Woon *et al.* 2005). EPPM, however, has two dependent variables: the first variable is intention and behavior involved with protection that the individual uses to reduce or remove the threat by attacking the cause of the threat; the second involves the intention of the individual to ignore or avoid the threat through internal actions that reduce the emotional responses to the threat.

Third, although the expanded PMT (Maddux & Rogers 1983; Prentice-Dunn & Rogers 1986) model includes additional sources of information (*i.e.*, verbal persuasion and observational learning) and how these alter the appraisals of threat and efficacy, work in IS has reviewed these in a piecemeal fashion. In our study, we use EPPM and include most of the previously used additional sources of information to explain behavior. We include subjective norms, descriptive norms, social influence, and cost and benefits.

Further, our study expands upon this theoretical background by considering the habits that individuals form regarding anti-malware applications. Given that the papers in Table 5 focus on the one-time behavior of subjects, it is important to note that such behavior is not truly a one-time episode, but is rather the intention to use the application above and apart from the given, current habit. Thus, we extend EPPM by considering the habitual use of such an application and thereby expand the EPPM to include this construct, as defined by (Verplanken *et al.* 1997).

3.5 Model Development

Having reviewed the underpinnings of EPPM and its differences from PMT, we now turn to the development of our theoretical model, which is depicted in Figure 9. Our model extends beyond the basic EPPM model in several ways. First, the entire EPPM model includes fear as an emotional antecedent to fear control response, and we replicate that here (Witte 1992; Witte *et al.* 1996). Second, we include two forms of social influence (descriptive and subject norms) in our model; these have been considered in other models and are a source of observational learning that can alter the perceptions of efficacy, as proposed in (Maddux & Rogers 1983; Prentice-Dunn & Rogers 1986; Witte 1992). Third, most research using EPPM or PMT is based on a fear appeal, meaning that a threat is communicated to a subject and a proposed solution to the threat is

recommended. Our study divests itself from this methodology and, instead, ascertains the threats perceived by subjects in an area without any experimental manipulation of a threat as evoked by a communication. As such, we are unable to ascertain the recommended response efficacy, and have such have removed it from our model. Fourth, we further extend EPPM by incorporating habit into our model. (Akers & Sellers 2004) and (Thornberry 1989) label such an extension of a theory as "theory integration," which means that at least two existing theories are combined. The aim of theory integration is to offer greater comprehensiveness and increased explanatory value compared to each component theory alone (Farnworth 1989); hence, theory integration can be seen as relevant, if the new integrated model affords increased explanatory power.

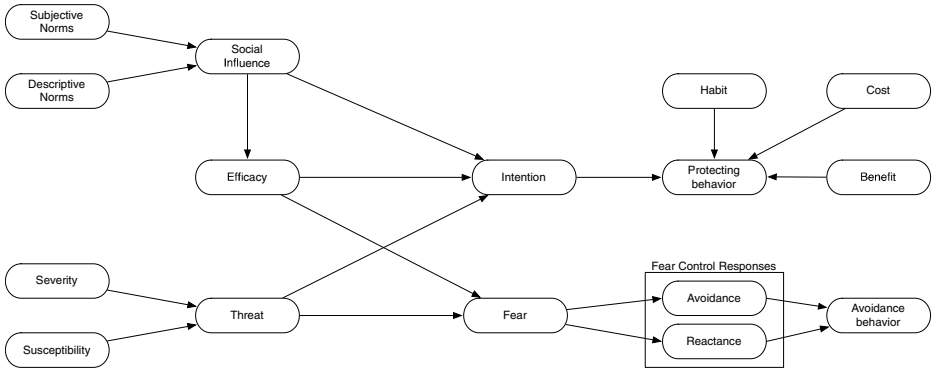

Fig. 9. Theoretical Model.

Akers and Sellers (2004) and Thornberry (1989) provide the following guideline for theory integration. First, scholars should determine if the theories to be merged explain the same or similar phenomena and then review the components of both theories. This process has two goals: 1) To see if the theories to be merged contain the same or similar constructs. If they do, then scholars should explore whether the similar constructs can be integrated within one model. 2) To see if the theories to be integrated have different constructs and theoretical components and whether these theories different components can be used to explain or predict the same or similar phenomena. Considering EPPM and habit in the light of these guidelines, we can easily see that both EPPM and habit can be regarded as behavioral theories; hence, the theories can be seen to explain similar phenomena, and there is no conflict in this respect.

Reviewing these theories for similar components, we conclude there are none. Habit theory focuses on habitual, automatic behavior, and it does not include any other components. EPPM comprises a number of other components, but not habit. As a result, we conclude that that there are no common constructs between EPPM and habit theory. The only difference between these is that habit theory offers an alternative way to explain behavior. Hence, keeping in mind the guidelines by (Akers & Sellers 2004) and (Thornberry 1989), we see that integrating habit theory with EPPM is justified and should increase the explanatory value, compared to either of the models alone.

Last, we include several controls variables that have been included in other IS PMT research to increase the explanatory power of our model and to make our research comparable with other PMT research.

We first elaborate on the sources and effects of threats in our model and then we elaborate on the outcomes of fear and the methods of fear control used in this study. Next, we describe the sources of social influence and the effects of social influence on an individual's efficacy and their intentions to engage in a danger control response.

3.5.1 Threat

As previously described, an individual will not appraise a situation as threatening unless he or she perceives both that the threat is potentially harmful and that there is possibility of experiencing it (Johnston & Warkentin 2010).

The relationships between threat appraisal and its two antecedents have been proposed and supported for many years (Gore & Bracken 2005; Johnston & Warkentin 2010; Liang & Xue 2009; Ng *et al.* 2009; Rogers 1975; Witte 1992; Witte *et al.* 1996). Building on these previous findings, we replicate this portion of the model in accordance with the PRM (Leventhal 1970), PMT (Rogers 1975) and EPPM (Witte 1992). Hence, we hypothesize:

> *H1: The severity of a threat will be positively related to the overall threat appraisal.*
>
> *H2: The susceptibility of a threat will be positively related to the overall threat appraisal.*

Once an individual has appraised a threatening event, this leaves two choices: initiate either a danger control response or a fear control response. As previously

described, a danger control response involves initiating behavior that deals with the source of the threat and has the ultimate goal of reducing or removing it by minimizing or negating either its severity or the individual's susceptibility to it (Johnston & Warkentin 2010; Maddux & Rogers 1983; Rogers 1975; Tanner *et al.* 1989). An individual will have the intention to protect himself or herself from the danger if the individual feels that he or she can successfully execute this behavior.

However, an individual who does not believe in his or her ability to successfully respond in an appropriate manner will feel fear toward the source of the threat (Witte 1992). When an individual forms both a threat appraisal and a coping appraisal, and finds that the threat appraisal is substantially stronger than the coping appraisal, then an emotional response to the threat is initiated (Witte 1992; Witte *et al.* 1996). Either a high level of threat or the inability to successfully engage a response causes the individual to feel a sense of helplessness, and that they lack the ability to avert any potential harm that may occur (Witte 1992). This inability to cope with the threat causes the individual to begin a mental defense against the impending harm that he or she expects to experience, which results in fear (Witte 1992; Witte *et al.* 1996). Unlike PMT, EPPM proposes that, when individuals perceive themselves as helpless victims of circumstances beyond their control, they will respond irrationally and rely on emotional coping mechanisms to reduce the amount of fear they are experiencing.

An inability to significantly reduce the susceptibility or severity of the threat, and a concurrent lack of confidence in the recommended response and the ability to execute the response, results in emotional coping responses, as posited by the PRM (Leventhal 1970) and EPPM (Witte 1992; Witte *et al.* 1996), which has also been supported by previous studies by (Gore & Bracken 2005). We likewise extend these findings to our study and propose the potential dual outcomes of a threat appraisal. Hence, we hypothesize:

H3a: The overall threat appraisal will be positively related to fear.

H3b: The overall threat appraisal will be negatively related to the intention to protect oneself from the threat.

H4: The strength of the relationship between the threat appraisal and fear will be greater than the strength of the relationship between the threat appraisal and the intention to protect oneself from the threat.

3.5.2 Fear

Having shown how the susceptibility and severity of a threat lead to the appraisal of a threat and how the appraisal of a threat can lead an individual to feel fear of the threat, we now explain the effects of fear and the fear control responses used in this study (*i.e.*, avoidance and reactance). *Avoidance* is a fear control response that refers to an individual's resistance to acknowledging a threat in an attempt to deny or minimize its potential impact on the individual (Witte 1992). For example, an individual that feels that she is unable to avoid getting H1N1 flu, and thus experiences fear about the harm that she will feel when she acquires the virus, will attempt to avoid the fear through an attempt at mentally denying the information regarding H1N1 flu and its effects on individuals with the virus. Although she does not alter the threat, she then feels that, at least, it will not be as bad as everyone says. These techniques allow the individual to continue to function and reduce the level of fear, as she believes that she is unable to reduce the imminent threat that it poses to her.

Reactance is a fear control response that refers to the belief of an individual that others are attempting to reduce his or her freedom; thus, the person completely rejects the message. To distinguish this behavior from avoidance, we return to our example. Rather than downplaying the effects of H1N1 on herself, the individual would instead believe that all of the information that she receives regarding the vaccine is instead an attempt by "others" to reduce her ability to function and behave as she desires. Due to this perceived infringement of her rights to believe and behave as she wants, she doubts the motivations behind the source of the information and believes that others are attempting to manipulate her with fear and, thus, believes that the entire situation is overblown or entirely fabricated (Gore & Bracken 2005; Witte *et al.* 1996). Rather than doubting the information itself to minimize its impact, reactance involves doubting the source of the information and the motivation behind its dissemination.

Although other techniques could be used to deal with fear, these are the two proposed and studied by EPPM (Gore & Bracken 2005; Witte 1992; Witte *et al.* 1996). An individual will likely only engage in one of these techniques, as only one is needed to reduce the level of fear felt. Further, given that the context of our study does not specify a source of information concerning malware, we do not anticipate that many subjects will exhibit reactance to an unspecified source. We rather expect the majority of subjects to rely on avoidance to known information concerning malware, as it is difficult to consider the motivations of unknown and

unspecified others (Kelley & Michela 1980). Thus, we propose that subjects in our study will rely on avoidance rather than reactance:

H5a: Fear will be positively related to avoidance

H5b: Fear will not be significantly related to reactance

3.5.3 Social Influence

Social influence refers to an individual's perception that significant and important others support a given behavior (*i.e.*, the use of anti-malware applications in our study) (Johnston & Warkentin 2010; Venkatesh *et al.* 2003). Although there are many different factors that can be used to predict the overall social influence regarding the use of anti-malware applications, our study relies on the use of norms as a common source of social influence (Herath & Rao 2009; Johnston & Warkentin 2010). Specifically, *descriptive norms* refer to the belief that the majority of others behave in a given fashion, whereas *subjective norms* refer to belief that significant others desire the individual to behave in a given fashion (Herath & Rao 2009).

Individuals are able to acquire information by observing others around them and perceiving the norms that exist in a given situation (Maddux & Rogers 1983). One common way to acquire information regarding behavior is to do what an individual believes the majority of others do. This reliance on the perceived normal behavior allows the individual to more readily examine behavior and acquire an intention without having to devote as many cognitive resources as are necessary to examine the behavior itself without any readily accessible information. However, individuals are also often influenced by significant others who provide cues as to how an individual should, or ought, to behave (Leone *et al.* 1999).

Both of these types of norms have been shown to be distinct, yet significant, sources of social influence (Herath & Rao 2009). Thus, an individual can form intentions and attitudes toward a behavior without having to perform the behavior—by observing others and their attitudes toward the given behavior. Thus, we build on this research and propose these two norms as sources of social influence in our study. Hence, we hypothesize:

6a: Subjective norms will be positively related to the social influence.

6b: Descriptive norms will be positively related to the social influence.

The expanded PMT model explains that observational learning serves as a source of additional information that may alter the perceived effectiveness of a response, or the ability to successful execute the recommended response (Maddux & Rogers 1983). Similarly, we expect that individuals observe the actions of others and acquire information regarding the appropriateness and effectiveness of a given behavior in a social setting. Individuals that perceive that others typically behave in a given manner will form beliefs regarding the supposed ease of the behavior and its effectiveness that will affect subsequent intentions regarding this behavior. For example, if an individual believes that most people use an anti-malware application, it is even more likely that the individual will believe that the application must be easy to use because so many people are using it. By learning about the perceived behavior of others, individuals can infer information about engaging in the same behavior. Additionally, the pressure to conform, especially to the behavior of significant others, increases the likelihood that an individual will behave as others do (Martin & Hewstone 2001).

Additionally, social influences should directly affect an individual's intention to engage in a behavior. The main objective of influence is to alter an individual's intended behavior (Bandura 1977; Bandura 1969; Sternthal *et al.* 1978). When an individual believes that others desire for him or her to behave in a given fashion, normative pressure increases the likelihood than an individual will behave in such a fashion. This finding has long been supported in research on influence (Bandura 1977; Bandura 1969), even within the same context of adapting technologies to avoid potential threats (Herath & Rao 2009).

Recent work in IS using PMT has also proposed and found that sources of social influence play a critical role in determining the behavior of individuals in security-related situations, such as in the context of this study (Herath & Rao 2009; Johnston & Warkentin 2010). We build on this work and propose that social influence will affect the perceived efficacy of the individual in executing the recommended response and their intention to behave in the indicated fashion.

H7a: Social influence will be positively related to efficacy.

H7b: Social influence will be positively related to the intention to protect oneself from a threat.

3.5.4 Efficacy

As previously stated, this study does not manipulate the subjects with a fear-inducing message and, thus, cannot specify a recommended response. Instead, we rely on the perceived self-efficacy of our subjects in forming a coping appraisal; therefore, any reference to efficacy is specifically related to self-efficacy, rather than response-efficacy, which was not tested in this study. Additionally, because only self-efficacy was used, the coping appraisal is synonymous with the perception of self-efficacy.

Once an individual has perceived a threat and formed a coping appraisal, he or she is left with two types of responses: control the danger or the fear. Individuals are more likely to enter the fear control process if the threat appraisal is stronger than the coping appraisal, whereas individuals that have stronger coping appraisals than threat appraisals will more likely engage in a danger control response (called protection motivation in PMT) (Witte 1992).

As a higher coping response indicates the belief that the individual is more confident in his or her ability to reduce or minimize the threat, it is more likely that he or she would engage in a danger control response, and thereby alter the source of the threat (Tanner *et al.* 1989; Witte 1992). This type of response allows the individual to avoid the potential for fear and focus instead on reducing the perceived threat.

In accordance with PMT and EPPM, coping appraisals serve as antecedents for either of the two responses (Maddux & Rogers 1983; Rogers 1975; Witte 1992; Witte *et al.* 1996); we build on these previous findings. Additionally, as higher coping appraisals are more likely to result in a danger control response, we propose:

H8a: Efficacy will be positively related to the intention to protect oneself from a threat.

H8b: Efficacy will be negatively related to fear.

H9: The strength of the relationship between efficacy and fear will be less than the strength of the relationship between efficacy and the intention to protect oneself from the threat.

3.5.5 Predicting Behavior

We extend our model to predict behavior, and base this on well-established relationships in prior research. First, we propose that the intention to protect oneself from a threat will be positively related to the actual behavior, as predicted by TRA, TPB, PMT and EPPM. This has been supported in a variety of studies (Ajzen 1985; Boss & Galletta 2008; Dillard 1994; Fishbein & Ajzen 1975; Floyd *et al.* 2000; Maddux & Rogers 1983; Rogers 1975; Tanner *et al.* 1989; Tanner *et al.* 1991; Witte 1992).

Further, building on EPPM (Witte 1992; Witte *et al.* 1996) we propose that the fear-motivated intentions are positively related to behavior that does not protect the individual from the source of the fear. In other words, not using an anti-malware application can be predicted by the individual's avoidance or reactance responses to fear.

H10a: The intention to protect oneself from a threat will be positively related to the related protecting behavior.

H10b: The intention to control fear from a threat will be positively related to the related avoidance behavior.

3.5.6 Habit

Habit is defined as "learned sequences of acts that have become automatic responses to specific cues, and are functional in obtaining certain goals or end-states" (Verplanken & Aarts 1999) p. 104]. Often, habit is assessed with a measurement of past behavior or behavioral frequency (Brug *et al.* 2006; Verplanken & Orbell 2003), such as is the case of the well-known model by (Triandis 1977). However, a number of scholars have criticized the use of measures based on past behavior or behavioral frequency. Brug and his research associates claim that "past behavior only assesses repetition and not the automatic character of habits. If one regards habit strength as a psychological construct, past behavior may not be the best measure" (Brug *et al.* 2006). Verplanken and Orbell concur: "It is unreasonable to accept a measure of past behavior frequency as a measure of habit strength" (Verplanken & Orbell 2003) p. 1315].

The use of an anti-malware application is not, in itself, a one-time behavior that occurs without consideration of past behavior, but is a behavior that is either routine performed or ignored (Verplanken *et al.* 1997). The intention to use or not

use anti-malware software should be also largely predictable by the habit associated with this repetitive behavior (Aarts *et al.* 1998; Cheung & Limayem 2005; Kim & Malhotra 2005; Limayem & Hirt 2003; Verplanken 2006; Verplanken & Orbell 2003); as such, we propose:

> *H11: The habit of using an anti-malware application will be positively related to its usage.*

We include several behavioral controls in our study that have been used in other PMT-based research in IS (Boss & Galletta 2008; Chenoweth *et al.* 2009; Herath & Rao 2009; Johnston & Warkentin 2010; Pahnila *et al.* 2007; Woon *et al.* 2005), and also proposed by the extended PMT model (Maddux & Rogers 1983; Tanner *et al.* 1989). Specifically, we include the cost involved with finding and using such an application and the perceived rewards associated with its use. We anticipate that each will be positively related to the use of an anti-malware application and include them as controls in our model. Hence, we hypothesize:

> *H12a: The perceived costs associated with the behavior will be negatively related to the use of an anti-malware application.*

> *H12b: The perceived benefits associated with the behavior will be positively related to the use of an anti-malware application.*

3.6 Methodology

3.6.1 Pilot Test and Measures

Our study used a survey method to collect data. To maximize the reliability of constructs of our study, we used previously validated and reported instruments (Boudreau *et al.* 2001; Straub 1989), with some minor wording adjustments to fit the context of this study. Appendix 3 provides a detailed list of the scales used for this study. Participants were asked to report their use of anti-malware applications as defined by the survey, and to provide answers for the remaining constructs in the theory. These include: threat, avoidance, reactance, intentions, and behavior (Witte *et al.* 1996); fear (Osman *et al.* 1994); efficacy (Herath & Rao 2009), social influence (Johnston & Warkentin 2010), costs and benefits (Myyry *et al.* 2009); and habit (Verplanken & Orbell 2003).

Given that we slightly modified the previously tested EPPM survey questions and used them in a new context, we performed pre- and pilot tests as follows:

First, our study was pre-tested by 10 faculty members to ensure that the questions matched the EPPM theory and the questions were readable. Then, the survey instrument was pilot tested by students enrolled in a business school course at a public university in China. We obtained 49 usable responses.

Our pilot study used a paper-based questionnaire, which consisted of 67 questions, including an area in which respondents could leave remarks and feedback about the questions asked. We used these responses to ascertain the validity of the questions and to identify any points of confusion within the survey. Based on feedback and initial statistical analysis, several questions were slightly modified prior to the final data collection.

3.6.2 Final Data Collection

The actual data were collected in the fall of 2009 from a public university in China through a paper-based questionnaire. The subjects were undergraduate students participating in a business school course. Before starting the lecture, the lecturer asked the students to fill out the questionnaire. Given that all students filled out the survey in class, the response rate of the survey was 100%. Through this process, we obtained 285 responses by students enrolled in the course. The survey was anonymous; no identifying information of any kind was gathered from the participants. It was also clearly communicated to the respondents that independent university researchers from a different university would analyze the results of their surveys; hence, it was stressed to the students there was no way that their identity could be revealed.

3.7 Data Analysis

3.7.1 Establishing Factorial Validity

Before assessing the hypotheses, several steps were taken to assure the reliability and accuracy of the collected data. First, we ascertained the types of constructs used in this study. Using (Diamantopoulos & Winklhofer 2001) and the sources of the instruments, we ascertained whether constructs were formative or reflective. The remainder of this section will report our procedures for establishing factorial

validity tests for reflective and the formative constructs using their respective tests.

3.7.2 Reflective Constructs

To analyze the factorial validity of the constructs, we used partial least squares (PLS), using SmartPLS version 2.0 (Ringle *et al.* 2005). To establish the validity of our reflective indicators, we followed the procedures outlined by (Gefen & Straub 2005). To establish the convergent validity, we generated a bootstrap with 200 resamples and examined the t-values of the outer model loadings. All retained items were significant at the .05 α level (Table A4.1 in Appendix 4). This demonstrates strong convergent validity for the reflective constructs.

We then used two established methods for establishing discriminant validity: correlating the latent variable scores against the indicators (Table A4.2) and calculating the AVE (Table A4.3). Both of these demonstrated strong convergent validity, excluding indicated items, which were removed from the final data analysis to improve discriminant validity.

Finally, to establish reliability, PLS computes a composite reliability score as part of the model analysis (Table 7). This score is a more accurate assessment of reliability than Cronbach's alpha because it does not assume that the loadings or error terms of the items are equal (Chin *et al.* 2003). Each reflective construct in our research model demonstrates high composite reliability that exceeds standard thresholds.

Table 7. Composite Reliability.

Construct	Composite Reliability
Cost	0.812
Efficacy	0.807
Behavior	0.962
Fear	0.810
Habit	0.909
Intention	0.937
Reactance	0.854
Reward	0.845
Severity	0.885
Social influence	0.838
Susceptibility	0.819

3.7.3 Formative Constructs

Validating formative indicators is more challenging than validating reflective indicators because the established procedures that exist to determine the validity of reflective measures do not apply to formative measures (Petter *et al.* 2007), and the procedures validating formative measures are less known and established (Diamantopoulos & Winklhofer 2001). Researchers have generally used theoretical reasoning to support the validity of formative constructs (Diamantopoulos & Winklhofer 2001), although there are approaches that can be used beyond theoretical reasoning alone (Marakas *et al.* 2007; Petter *et al.* 2007). Though no technique is widely established for validating formative measures, the modified multitrait-multimethod (MTMM) approach, as presented in (Loch *et al.* 2003; Lowry *et al.* 2009; Marakas *et al.* 2007) is a promising solution, and the one we followed.

For each formative item, we created new values that were the product of the original item values by their respective PLS weights (representing each item's weighted score). We then created a composite score for the subjective norm construct (the only formative construct in this study) by summing all the weighted scores for a construct. We then produced correlations of this calculated value with its respective indicators (Table A4.4).

To test convergent validity, we checked whether all the items within the construct highly correlated with each other and whether the items within the construct correlated with the construct value. This was true in all cases, inferring convergent validity. Although we would ideally want inter-item correlations to be higher within a given construct, this cannot be strictly enforced as there are exceptions, depending on the theoretical nature of the formative measure (Diamantopoulos & Winklhofer 2001; Loch *et al.* 2003). Thus, we believe the most meaningful discriminant validity check with formative measures is to look at the degree to which items within a construct correlate to a given construct.

Finally, we used another approach to assess the formative validity, as suggested by (Petter *et al.* 2007), which involves testing the multicollinearity among the indicators. This is particularly important with formative indicators because multicollinearity poses a much greater problem than with reflective indicators. Hence, low levels of multicollinearity are usually indicated with levels of the variance inflation factor (VIF) below 10, but in the case of formative indicators, the VIF levels need to be below 3.3 as a more stringent test (Petter *et*

al. 2007). In our case, the VIF for all indicators were below 3.3; thus, all indicators were used in the final analysis.

In sum, using MTMM analysis and assessing the VIF levels, we conclude that reasonable discriminant validity exists with our formative construct. Finally, because of the nature of formative measures, reliability checks cannot be reasonably made (Diamantopoulos & Winklhofer 2001).

3.7.4 Testing for Common Methods Bias

Given that the data were collected using one method, we used two methods to ascertain the presence of common methods bias. First, we used Harman's single factor (Podsakoff *et al.* 2003). This test required that we run an exploratory unrotated factor analysis on all indicators to see if a single factor emerges that explains the majority of the variance in the model. If so, then common-method bias likely exists at a significant level. The result of our factor analysis for our study produced 45 distinct factors, the largest of which only accounted for 19.63% of the variance of the model.

Second, we examined a correlation matrix of our latent constructs to determine if any of the correlations were above .90, which is strong evidence that common methods bias exists (Pavlou *et al.* 2007). None of the correlations was near this threshold.

Given that our data passed both tests for common methods bias, we conclude that there is little reason to believe that our data exhibit any of the negative effects from common methods bias.

3.7.5 Results of Hypotheses Testing

Given that our data display factorial validity and do not display common methods bias, we tested our theoretical model, which is shown in Figure 10.

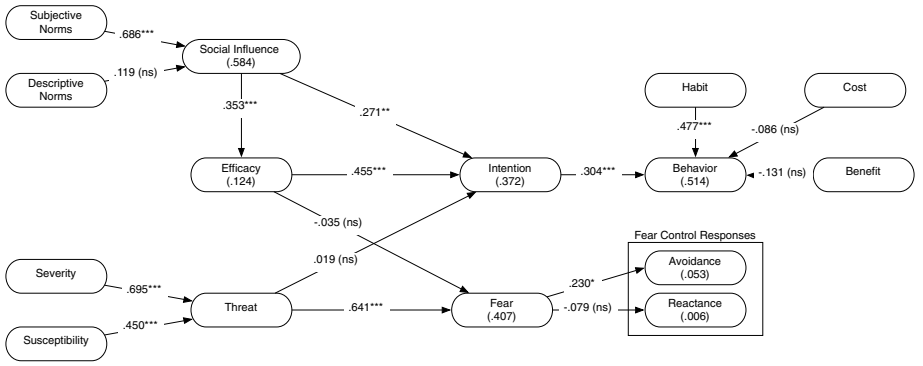

Fig. 10. Model Results.

3.7.6 Ad-hoc Analysis of Users vs. Non-users

Given that the test of our extended EPPM model included both users and non-users, and the dual process nature of EPPM for explaining why individuals either adopt or do not adopt behavior that will protect them from perceived threats, we report the model results based on both users (n = 192) and non-users (n = 92). The same validation procedures were performed for both of these models as were used with the full model.

The model of users (Figure 11) modifies the extended EPPM test depicted in Figure 10. First, given that our extended model shows that efficacy predicts intention, we report the effect of efficacy on fear as well, to compare its effects on the dual processes in EPPM. Second, we explore whether the perceived threat of malware has any relation to efficacy, as reported in other PMT-based IS studies (Boss & Galletta 2008). Third, rather than reporting the relationship of intentions on behavior, we report the predictive power of current behavior on the intention to use the anti-malware application in the near future. Lastly, we report the effects of the two fear control responses (*i.e.*, avoidance and reactance) on the intention to use the anti-malware application in the future.

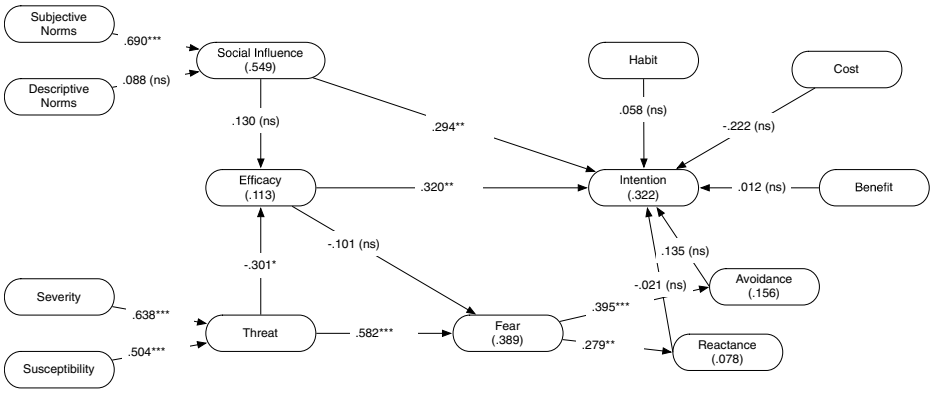

Fig. 11. Model Results for Users of Anti-malware Applications.

The model for non-users (Figure 12) is similarly adopted from the extended model; however, we also include the predictive power of the fear control responses (*i.e.*, avoidance and reactance) on the current non-use of anti-malware applications. The results of these modified, split models and the test of the extended EPPM model are compared in Table 8.

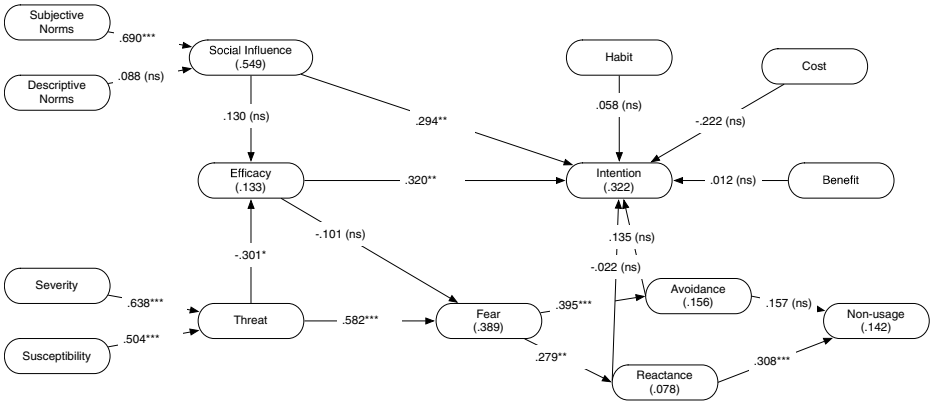

Fig. 12. Model Results for Non-users of Anti-malware Applications.

Table 8. Summary of Results of Comparison Tested Models.

Hypothesis	Full Model		User Model		Non-user Model	
	Coefficient		Coefficient		Coefficient	
Severity → threat	.695	***	.745	***	.638	***
Susceptibility → threat	.450	***	.392	***	.504	***
Threat → fear	.641	***	.629	***	.582	***
Threat → intention	.019	ns	—	—	—	—
Threat → efficacy	—	—	-.114	ns	-.301	*
Fear → avoidance	.230	*	.099	ns	.385	***
Fear → reactance	-.079	ns	.025	ns	.279	**
Avoidance → intention	—	—	.064	ns	.135	ns
Reactance → intention	—	—	-.109	ns	-.022	ns
Avoidance → non-usage	—	—	—	—	.157	ns
Reactance → non-usage	—	—	—	—	.308	***
Subjective norm → social influence	.686	***	.634	***	.690	***
Descriptive norm → social influence	.119	ns	.123	*	.088	ns
Social influence → efficacy	.353	***	.213	**	.130	ns
Social influence → intention	.271	**	.113	ns	.294	**
Efficacy → intention	.455	***	.320	***	.320	**
Efficacy → fear	-.035	ns	-.137	**	-.101	ns
Intention → behavior	.304	***	—	—	—	—
Habit → behavior	.477	***	—	—	—	—
Cost → behavior	-.086	ns	—	—	—	—
Reward → behavior	-.131	ns	—	—	—	—
Behavior → intention	—	—	.091	ns	—	—
Habit → intention	—	—	.001	ns	.058	ns
Cost → intention	—	—	-.001	ns	-.222	ns
Reward → intention	—	—	.097	ns	.012	ns

*** p < .001; ** p < .01; * p < .05; ns – not significant

3.8 Discussion

3.8.1 Summary of Results

The results of our hypotheses, as based on the full model testing, are shown in Table 9 and summarized in this section. First, our model supports the majority of the research that has been performed using PMT in IS—the severity and susceptibility of a threat are important predictors of threat (H1, and H2); the efficacy that one feels in performing the given behavior is a strong indication of

intending to engage in that behavior (H8a); and, the intention to engage in protective behavior is strongly related to the actual behavior (H10a).

Our results also show strong support for EPPM tenets. Namely, that the perceived threat of malware is strongly predictive of the fear that an individual feels due to malware (H3a), which subsequently relates to methods for coping with such fear (H5a and H5b) and their effect on non-usage, which was only supported for reactance (H10b).

Our extensions to PMT and EPPM are also strongly supported. Specifically, the relationships between threat and fear (H3a) would be stronger (H4) than that of threat and the intention to engage in protective behavior (H3b). Likewise, we find that the expected reverse relationship is found with efficacy—the relationship between efficacy and the intention to protect oneself (H8a) is stronger (H9) than the relationship between intentions and fear (H8b). We find further support for the fact that social influences (H6a, H6b, H7a and H7b) are important predictors of efficacy and the intention to engage in protective behavior. Lastly, we find that the actual protective behavior is predicted by habit (H11), but not by cost (H12a) or rewards (H12b) as found in previous studies (Herath & Rao 2009), and (Liang & Xue 2010).

Table 9. Summary of Hypotheses Test Results.

#	Hypothesis	Coefficient	Supported?
1	Severity → threat	.695 ***	Yes
2	Susceptibility → threat	.450 ***	Yes
3a	Threat → fear	.641 ***	Yes
3b	Threat → intention	.019 ns	No
4	Threat → fear > threat → intention	z = 9.32 ***	Yes
5a	Fear → avoidance	.230 *	Yes
5b	Fear → reactance	-.079 ns	Yes
6a	Subjective norm → social influence	.686 ***	Yes
6b	Descriptive norm → social influence	.119 ns	No
7a	Social influence → efficacy	.353 ***	Yes
7b	Social influence → intention	.271 **	Yes
8a	Efficacy → intention	.455 ***	Yes
8b	Efficacy → fear	-.035 ns	No
9	Efficacy → intention > efficacy → fear	z = 6.32 ***	Yes
10a	Intention → behavior	.304 ***	Yes

#	Hypothesis	Coefficient	Supported?
10b	Fear control response (avoidance and reactance) → behavior	.380[3] ***	Partial
11	Habit → behavior	.477 ***	Yes
12a	Cost → behavior	-.086 ns	No
12b	Reward → behavior	-.131 ns	No

*** p < .001; ** p < .01; * p < .05; ns – not significant

3.9 Contributions

This study examined the extent to which home computer users use of anti-malware applications can be explained by EPPM; our extensions to this model are found in related PMT-based research in IS. Our study was the first in IS that empirically tested EPPM. EPPM extends PMT by adding fear, fear control responses, non-usage behavior, and social influence to the nomological network of this research stream. We further extend the original model by including habit and the rewards and costs of using the anti-malware application. In addition, and contrary to PMT, the tested model also included the emotional response of the individual and offered an explanation as to what happened to home users who did not protect themselves and instead behaved in a non-prescribed manner. This study offers new insights regarding home computer users' information security behavior with a new cultural sample—Chinese home computer users.

We have added several new relationships, which have not been examined in the context of IS security, in addition to relationships that were previously examined in IS security, but not in the context of home users. We explored these new relationships and their related contributions.

Our results show that a threat has a significant effect on fear. We found no previous studies in IS security that have examined this relationship. This indicates that emotional responses to threat are important and measurable. Fear is a natural consequence of threat and should be considered when attempting to understand why individuals do or do not adopt technologies that can protect them from technical threats (Liang & Xue 2010).

Second, we found that threat has an insignificant relationship to intention, which is contrary to some reported results based on PMT (Herath & Rao 2009; Liang & Xue 2010; Pahnila *et al.* 2007). We predicted, based on EPPM, that the effects of threat would be more strongly related to the emotional response of fear,

[3] Only reactance was found to be a significant predictor of non-usage by non-users.

which was supported by our results. This is an important finding in that it indicates that threat is more strongly related to the emotional coping process than to the protective coping process. Thus, threat is important in terms of the fear that it ultimately inspires, rather than as a method of influencing individuals to engage in protective behavior. Given that both the present study and study by (Liang & Xue 2010) focused on the use of anti-malware using a student population with similar response rates, we suggest culture differences as a possible explanation for the different results. Our study used students from China, while (Liang & Xue 2010) used US students, which potentially differ in systematic ways in response to threat-related technologies.

Third, our empirical data show that fear has a significant effect on avoidance for both users and non-users, and on reactance for non-users. Further, the results indicate that, in the context of malware and the usage of anti-malware software, that non-usage is best predicted by the individual reaction to the perceived threat and fear of this threat. In other words, individuals are more likely to react to and discount messages related to the threat and emotionally respond to threats. This finding further validates the importance of the emotional coping process in that individuals have an escapist reaction to perceived threats that may preclude them from engaging in behavior that may allow them to completely avoid the threat. We found no previous studies in IS security that have examined this relationship.

Fourth, we found that self-efficacy has insignificant effect on fear alongside a significant relationship with the intention to protect oneself from the threat. The relationship between efficacy and protection intentions has been largely supported in PMT-based IS research (Herath & Rao 2009; Johnston & Warkentin 2010; Liang & Xue 2010), and we extend upon this research by proposing that this construct should have very little effect on the emotional coping process proposed by EPPM, which is supported in this study. This indicates that the most direct method of influencing an individual to engage in protective behavior is to increase their perceived efficacy related to the behavior. We found no previous studies in IS security that reported the singular importance of efficacy on protective intentions and their insignificant link to the emotional coping process.

Fifth, we found that only subjective norms (as opposed to descriptive norms) have a significant effect on social influence and subsequently on an individual's perceptions of efficacy and intentions to engage in protective behavior. This indicates that, despite the individual's level of expertise, based solely on their relationships with others, and how these interactions allow individuals to learn

from relevant others, they can be induced to believe that they are more likely to avoid potential threats (Bandura 1977; Bandura 1969; Bandura 1982). This is an important extension to work on threat avoidance in IS in that it adds methods whereby individuals can be influenced to adopt technologies that would benefit them, which has been mostly overlooked in IS security research to date. We found only one previous study that had included the effects of social influence in their study, but that only in regards to the subjects' intentions (Johnston & Warkentin 2010).

Sixth, intention had a significant effect on behavior. While previous studies in the context of home use have stopped at intention (Anderson & Agarwal, Forthcoming; Johnston & Warkentin 2010), (Pahnila *et al.* 2007) report a strong positive relationship between intention and actual behavior in the context of employee compliance with IS security procedures.

Seventh, habit has a significant effect on behavior. This finding is consistent with the original theory of habit (Verplanken & Orbell 2003). While habit has not been studied in the context of the home user, (Pahnila *et al.* 2007) found that habit explains employee compliance with IS security policies.

Finally, costs and rewards had no significant effect on behavior. This result is not consistent with the extant studies. (Ng & Rahim 2005) reported that cost, namely inconvenience of opening email attachments, has an effect on actual behavior. Similarly, (Woon *et al.* 2005) found that the response cost has an effect on actual behavior. While cultural differences may play a role here, another explanation for this difference is that the study by (Ng & Rahim 2005), (Woon *et al.* 2005) and the present study examined different types of behavior. Employees may apply different reasoning when they violate different types IS security procedures (Siponen *et al.* 2010). A second difference is the response rate. While (Woon *et al.* 2005) do not report the response rate, the response rate in this study is was 100%, and 31% in the study of (Ng & Rahim 2005).

Next, we discuss the implications for practice and research based on our empirical results.

3.9.1 Implications for Practice

Our results suggest that organizations (*e.g.*, schools, departments of education, etc.) should use our results as a basis for developing anti-malware education and campaigning programs for home users. Such an education program should highlight a number of things. First, it should stress the threat of malware for home

users. In particular, an educational program should not only stress that people are at risk of getting malware, but it should also note the malware can be a serious, severe, and significant threat to home users if nothing is done to protect home computers. In this respect, we suggest that communicating fear appeals to home users through education or promotional campaigning. Such fear campaigns should state that, because of malware, a computer may become slower and unusable, and that private information may be sent to unauthorized quarters. Having said that, such fear appeals should be carried out carefully, because users may attempt to avoid the fear by entering into avoidance, in EPPM terms. To avoid this, the campaign should stress that all users can indeed avoid malware with careful Internet surfing and the installation of effective anti-malware tools. It is important to recognize that home users need to believe that they can avoid the threat of malware with proper Internet behavior and appropriate tools.

Also, our results suggest that the use of anti-malware tools can become habitual. This means that organizations aiming to make home users use anti-malware tools should consider ways to get people to try out the anti-malware applications with the hope that home users will routinely use them.

Also, our findings suggest that the influence of family members and friends, as well as others who are important to home users, plays an important role in home use of anti-malware tools. This suggests that education interventions should stress that learners should spread the word on the dangers of malware and the importance of using anti-malware tools, to create "a chain reaction" in anti-malware tool use. Finally, when different education institutions, from comprehensive schools to universities, are offering information technology education, they should also ensure that learners are able to use anti-malware tools.

3.9.2 Implications for Research

We suggest seven areas of future research directions based on our empirical findings.

First, given that the use of anti-malware tools is habitual behavior, future research should study how, or in which way, the use of anti-malware tools becomes habitual. This information would help scholars and practitioners to understand how one creates the habit of using anti-malware tools.

Second, scholars should study effect of the use of campaigning and education interventions on changing Internet user behavior regarding anti-malware tools. In

this respect, we recommend the use of pre- and post-research settings with experimental and control groups. Attempts should be made to understand how social influencers can be better situated to alter behavior to adopt appropriate technologies to reduce the threats posed by technologies such as malware.

Third, also, the effect of e-learning programs vis-à-vis traditional face-to-face learning, programs should be studied using the same setting.

Fourth, in addition to the positive education and campaigning strategies, the use of fear appeals should be studied using pre- and post-research settings with the experimental and control groups (Johnston & Warkentin 2010).

Fifth, future research should examine the development of strategies to avoid avoidance in terms of EPPM, and study the effect of these strategies in the context of home user use of anti-malware tools.

Sixth, future research should test the EPPM model in other countries and examine whether culture plays any role in the use of anti-malware tools. In the same vein, while we regard the business school students as a good and representative of the population of home users, future studies should also examine other types of home users. Finally, as a seventh avenue for future research, while we regard the EPPM model as rather holistic, we challenge scholars to apply other possible theories and models and develop own theories for this important, but less studied, research domain. One other such theory is the theory of moral development. Here the research question is whether Internet users regard actions to prevent malware as a moral responsibility, for example, to protect family members and other Internet users.

3.9.3 Limitations of the study

This study is subject to typical limitations. First, it used respondents only from China. While the findings may not be generalizable to outside of China, the use of data from a single country is typical in top IS journals (Anderson & Agarwal, Forthcoming; Johnston & Warkentin 2010; Siponen & Vance 2010). It is also important to point out that the data from our study comes from the largest country in the world.

Second, a critical reviewer may question if the university students accurately represent home users. While we see that university students are home users, and research papers in top IS journals have used students sample in studying home use (Anderson & Agarwal, Forthcoming; Johnston & Warkentin 2010), it could be that students do not represent all home computer users.

3.10 Conclusion

Malware is an increasing problem for ordinary home Internet users. Previous studies have reported that most home computers are infected by malware—viruses and all unwanted malicious software. And yet, home user information security behavior has received comparatively little empirical research. Previous studies in this area have applied TAM, TRA, TBP, and PMT. To contribute to the current understanding of home user information security behavior, we applied the EPPM, which is a new theory in this research area. We tested this theory in the context of Chinese home users (N = 258).

Our results largely support the model. Our study was the first in IS that empirically tested EPPM. EPPM extends PMT by adding fear, social influence, habit, rewards, and costs. In addition, and contrary to PMT, it also covers the emotional response of the individual and offers an explanation as to what happens to home users who do not protect themselves and instead behave in a non-prescribed manner. In addition, our study offered new insights into a research area, namely home user information security behavior, which has not been widely studied. Finally, our study examined the factors affecting home users' behavior when using anti-malware tools in new context, namely Chinese home computer users and the implications for research and practice were outlined.

4 Control Imbalances: Explaining Why Software Developers Skip Prescribed Testing Procedures

4.1 Abstract

Almost all aspects of our daily lives are supported or augmented through the use of technology and more specifically, through software use. However, due to the complexity of software and the impossibility of bug-free coding, all software contains errors, bugs, or less than desired functionality. The increased focus on agile and other quick-to-market software development practices may be exacerbating this problem. One common way to minimize the likelihood of error-prone software is through testing of the code during the development of the software, prior to release. However, research has shown that developers may omit such tests, which may cost over $60 billion dollars annually in repairs and downtime in the US alone. Despite this, we can locate no studies that focus on the reasons as to why software developers omit these prescribed tests. As a first step in remedying this situation, this study explores why developers omit such tests through the use of Control Balance Theory (Tittle 1995), which is a new theory in IS. Control Balance Theory posits that individuals behave in deviant ways when they feel threatened in regards to their ability to behave as they desire, or when they feel a lack of such control.

We used a scenario-based survey of employees in organizations to test our theoretical model (n = 136). Our results indicate that Control Balance Theory is able to explain several important factors (both situational and personal) that may entice a developer to skip software testing. The most important factors in explaining omitted software tests include: the perception of constraints or controls that require such tests, the self-control and morality of the developer, control imbalances, and violation motivations. Several important contributions for both research and practice are discussed.

4.2 Introduction

Our modern society is based on IT and software. Likewise, it is very common to find errors or bugs in software (Gibson & Senn 1989; Kafura & Reddy 1987). It is widely agreed that there are no silver bullets in software development. There

are and always will be software errors, owing to software complexity (Brooks 1987). While some of the software flaws are blatant and easily fixed, some of them may cause security problems (Siponen *et al.* 2006), or even lead to deaths (Leveson & Turner 1993). To minimize software errors, (Brooks 1987), in his seminal article on software development, suggested the use of incremental development. Nowadays, this approach is taken into practice through such methods as agile (Martin 2003), lnternet-speed, or short cycle time systems development (Baskerville & Pries-Heje 2001; Baskerville & Pries-Heje 2001; Baskerville & Pries-Heje 2002; Baskerville & Pries-Heje 2004; Baskerville *et al.* 2003). Such approaches are seen as important in cutting down the costs of software development, especially in terms of reducing the unnecessary bureaucracy involved in that development (Abrahamsson *et al.* 2003). It is reported that competition to hit the market no later than competitors, tight deadlines, and a tendency to cut "unnecessary" documentation, push software developers toward trading quality for speed (Ahonen & Junttila 2003; Baskerville & Pries-Heje 2001; Baskerville & Pries-Heje 2001; Baskerville & Pries-Heje 2002; Baskerville & Pries-Heje 2004; Baskerville *et al.* 2003). In fact, it is estimated that inadequate testing of software in the USA alone could cost as much as $60 billion yearly in repairs and downtime (Ahonen & Junttila 2003).

And yet, despite of all this hype on the need to have fast release cycles in software development, we find no studies that focus on the reasons as to why software developers omit prescribed tests that could potentially detect and correct errors and bugs (Agrawal & Chari 2007; Anquetil *et al.* 2007). Given that the detection of bugs by software developers can potentially minimize or avoid the negative outcomes from bugs and errors, it is important to determine why developers omit such tests. By elucidating the motivations behind such behaviors serves as the first step for managerial intervention to prevent and or correct such intentions before they occur. Managers could potentially save billions of dollars by improving their ability to monitor, control and ensure that prescribed organizational tests are carried out for all software development projects.

Managers have long attempted to identify ideal portfolios of control or monitoring procedures that would allow them adequate oversight throughout the software development process (Kirsch 1996; Kirsch 1997; Kirsch 2004; Kirsch *et al.* 2002). With the focus of this literature being on the types of controls (*e.g.*, informal, process, or outcome) that would allow managers to increase overall software quality and also completing projects on time, in budget and providing all

desired features, little research has explored how this type of oversight may provide detrimental outcomes to their very endeavor. Other research on trust and control has posited that the use of monitoring or legalistic procedures can lower trust levels, diminish citizenship behaviors (Sitkin & Roth 1993). Related research has also found that the implementation of control and monitoring systems has negative effects on trust and cooperation (Baba 1999; Mulder *et al.* 2006; Piccoli & Ives 2003). This work provides the insight that the use of controls and monitoring in software development may have detrimental outcomes and effects on those being controlled. We seek to better understand how the use of controls may negatively impact software developers and propose the following research question.

RQ1: Does the managerial practice of controlling and managing the software development process produce any negative behaviors or intentions that may bring harm to the organization or those it serves?

As a step in remedying this gap in the literature, we extend the Control Balance Theory (CBT) by (Tittle 1995). CBT is ideally situated to explore the effects of control on software developers as its main tenet is that when individuals feel that they are either more controlling of their environs or are more controlled by others, they seek to balance their control and will engage in acts of defiance. We extend this theory to the software development context and explore whether individuals with control imbalances are more likely to engage in deviance by omitting software development tests proscribed by the organization in an effort to either increase the control they have over others, or in order to retaliate against the sense that the developer feels powerless being overly controlled by others.

This study has several important contributions to both research and practice. For research and theory, this study extends a new theory to information systems and software development, namely Control Balance Theory. This theory expands the current understanding regarding the management and control of deviant behaviors that goes beyond typical formal, informal, and clan controls (Kirsch 1996; Kirsch 1997; Kirsch 2004; Kirsch *et al.* 2002). This theory explains how the individual's perception of control on him or herself can have important implications for their behaviors, beyond the situational factors (*e.g.*, sanctions, incentive structure) that may discourage such practices. Further, this is the first study to empirically validate recent refinements to CBT by Tittle (2004) and test these results in an SEM-based model. The results of this study highlight that managerial practices of control and monitoring of the software development process also has detrimental outcomes that should be considered when developing

and implementing the portfolios of controls used to managed this important process (Kirsch 2002).

For practice, this research shows what factors drive software developers to omit testing during software development. This information will help the management of such behaviors in organizations and companies.

4.3 Previous Research and Background

A number of studies in software engineering have noted the problems concerning software testers omitting planned tests. For example, (Ahonen & Junttila 2003) report, based on their interviews and case studies with software developers, that planned tests are often neglected, ignored, or bypassed by software developers. Developers maintain that oftentimes early phases of software development take more time than estimated; hence, the testing is postponed and eventually, skipped entirely. Finally, when the software is ready for testing prior to its initial launch/release, there is a race to deliver the software to meet tight schedules or deadlines, resulting in the abandonment of the required software tests.

Another area where this issue is recognized is in the literature on Internet-speed or short cycle time systems development (Baskerville & Pries-Heje 2001; Baskerville & Pries-Heje 2001; Baskerville & Pries-Heje 2002; Baskerville & Pries-Heje 2004; Baskerville *et al.* 2003). Based on qualitative interviews in US and Danish companies engaged in such fast-paced development, Baskerville and his colleagues determine that such a development methodology calls for fast, release-oriented, parallel prototyping, where quality is negotiable. This results in some of the tests being omitted in order to release the software more quickly.

This software development methodology is similar to the agile school of thought. The advocates of the agile software methodology believe that traditional software development methods require too much documentation, which may slow down the work. Due to this increase in record keeping and bureaucratic steps, many projects fail to meet their deadlines, scopes, and budgets (Martin 2003). In 2001, a set of developers of light methods (*e.g.*, Extreme Programming, SCRUM, DSDM, Pragmatic Programming) met and put forth the Manifesto for Agile Software Development (Beck *et al.* 2001). This manifesto was further justified later on (Cockburn & Highsmith 2001; Highsmith 2002; Martin 2003). One of the principles of agile software development is to maximize the amount of work not done, and welcome changing requirements, even late on in the development

process (Martin 2003). Such a demand for fast development cycles with late changes increases the overall complexity of the project and increases the likelihood of errors and bugs (Agrawal & Chari 2007; Ahonen & Junttila 2003; Gibson & Senn 1989; Harrison 1992).

Even though all software methodologies differ in terms of oversight and process, all do have a variety of tests that are supposed to be completed by developers. Given that researchers have shown that tests, regardless of the methodology, are still skipped, it is important to determine why individual or even teams of software developers determine why prescribed methodological tests be omitted. This is especially true for methodologies that require more formal testing procedures that are performed by the software developers (*e.g.*, waterfall) as compared to more flexible methodologies (*e.g.*, Agile) that provide more flexibility and focus on product rather than testing.

To summarize, while software engineering and IS literature have recognized the enhanced speed in modern methodologies that increase the complexity of software development and the likelihood for errors and bugs, we find no studies that have specifically examined why employees skip such tests that could reduce errors and bugs and thereby improve the overall quality of the software. Similarly, while the IS security literature is full of cases describing how employees have used computers to perform criminal acts to gain more money, or engage in espionage, the development and spreading of viruses, sabotage, and extortion and superzapping (Parker 1998; Willison 2006), we find no published research focused on explaining why software developers skip prescribed testing procedures. As a step towards overcoming this gap in the research, we next propose a model not yet applied in IS research to examine this phenomenon.

4.4 Theoretical Framework

This study applies Control Balance Theory (CBT), as introduced by (Tittle 1995), originally designed to explain deviant behavior, to the IS context of required software testing during the development of such software by its developers. Deviant behavior is defined by Tittle as "any behavior that the majority of a given group regards as unacceptable or that typically evokes a collective response of a negative type" (Tittle 1995). The deviant acts do not have to be illegal, but merely against some rule, norm, or be perceived as unacceptable by the majority (Piquero & Hickman 2003). For this study, we define deviant behavior as the refusal to or deception regarding the performance of organization mandated software

development tests. While the skipping of such tests may not be illegal in a given situation, it refers to the situations where software developers are expected to perform assigned tests on their code to ensure its quality, prior to endorsing or submitting that code to a client as completed and suited for its intended purpose. As this deviant behavior is against the organization that has mandated such tests, this form of deviance can be an individual acting alone, to entire teams of software developers participating in collective deviance.

The basic premise of CBT is that individuals decide to behave contrary to standard practices and methods when they feel that they are either unable to control their personal lives or that they are largely unfettered from the controlling behaviors of others (Curry 2005; Piquero & Hickman 2003; Tittle 2004). As such, we feel that CBT is well suited to explain the omission of required tests in software development as such behaviors, in the given context, are against the standard behaviors of the organization in this context. Among the criminological theories, CBT is unique, as it posits that provocations reminding people of their control imbalance serves as a key stimulus for the omission of prescribed tests. A typical provocation in these situations is the loss of financial bonuses if the deadline is not met (Baskerville *et al.* 2003).

Beyond the strict focus on deviant behaviors, CBT can also be used to explain both social and situational contexts where the desire for individual autonomy clashes with the organization's desire to control the behavior of the individual (Piquero & Hickman 1999; Tittle 2004). In other words, CBT is useful in explaining when an individual will conform to group/organizational desires or behave in a deviant manner (Piquero & Hickman 2003; Tittle 2004). In the context of software development, CBT is especially useful, as it can explain the performance or lack of required testing in software development as being due to minimal formal control or management oversight (Kirsch 1996; Kirsch 1997; Kirsch 2004; Kirsch *et al.* 2002) that exists in these settings; rather, control is usually in the form of clan control that relies upon the social influence of other experts in the given context. CBT then helps to explain why such informal controls are successful in influencing the developers' testing of software during development.

The two key issues in CBT are control and the related control balance ratio. *Control*, in CBT, refers to the ability of someone to manipulate or block the actions of others or circumstances surrounding the action (Tittle 2004). Thus, control can be thought of as the power or lack of power that an individual

perceives themselves as having in determining how to act in a given situation (Curry 2005). In a given situation there are two types of control perceived by an individual: exerted control and experienced control. *Exerted control* refers to the control that the individual perceives he or she has in relation to controlling others whereas *experienced control* refers to the individual's perception that others are controlling him or her (Tittle 1995; Tittle 2004). In other words, the individual has two perceptions of control; the control that he has on others in getting them to behave as the he desires, and the control that he feels others have on him in getting him to behave as they desire (Piquero & Piquero 2006). The concept of control, and the fact that deviant actions are associated with two types of control (exerted and experienced), is relevant in the context of software development, because software development situations, such as when developers omit tests, can relate to both exerted control and experienced control. An example of an exerted control situation is a manager who is leading a software development team and is able to set her own deadlines and development goals, whereas experienced control is exemplified by a software developer who is ordered to complete a test within a very specific deadline. The comparison of these two types of control (exerted control and experienced control) results in what is termed the control balance ratio.

The *control balance ratio* refers to the total amount of control to which an individual is subject to relative to the total amount of control he or she can exercise (Tittle 1995). The theory holds that when a person exercises control equal to the amount of control the person is subject to; the person's control ratio is balanced (*i.e.*, the ratio score would be close to, or exactly 1). This perceived fit between the exerted and experienced control would increase an individual's likelihood of conforming to expected behaviors rather than to shift toward deviance. CBT posits that only individuals who perceive imbalances in their control ratios feel an internal motivation to modify this imbalance through deviant behavior (Piquero & Hickman 1999; Singer 1997; Tittle 1995; Tittle 2004), such as in omitting software tests.

Tittle proposed control balance as a general all encompassing variable that affects all aspects of the individual's life. For example, if an individual feels more that she is more controlled at the workplace, it is likely that she will endeavor to maintain more control in her home life in order to arrive at a control balance. It is thus important to consider the control levels that an individual feels or perceives in his or her major roles (*i.e.*, employee, home life, recreational affiliations, etc.). Although one study (Hickman *et al.* 2001) has explored the concept of work-

specific control balance, it remains the only such study of its kind. Tittle's refinemement of CBT (2004) continues to propose the importance and eminence of the generalized control balance ratio that encompasses all parts of an individual's life. We build on this work and focus on the general control balances that are felt or perceived by the software developers.

Given that both forms of control are continuous variables (Tittle 1995), it is then possible for the control balance ratio to either fall in excess of, or less than one. Each of these two outcomes is discussed in turn.

A *control surplus* (*i.e.*, when the control balance ratio is greater than one) takes place when the individual exercises greater control than he or she is subjected to (Curry 2005; Tittle 2004). CBT proposes that individuals with control surpluses, having experienced some power over others, have increased motivations to further increase their power over others and further achieve their desires (Piquero & Hickman 1999). Individuals with a control surplus engage in deviant behavior to shift their control imbalances to greater extremes (Curry 2005); although these shifts may only be temporary (Piquero & Hickman 1999). In the context of software development, superiors, such as managers and team leaders, have the potential to generate a control surplus, due to their power over their subordinates. This increased power may incentivize them to omit software tests merely because they can and this further shifts their control surplus.

A *control deficit* (*i.e.*, when the control balance ratio is less than one) occurs if an individual is subject to more control than he or she exercises (Curry 2005; Tittle 2004). A control deficit motivates an individual to escape from the control that he or she is being exposed to from others (Piquero & Hickman 1999). A control deficit may likely create negative emotions for individuals and may thus influence an individual to engage in deviant behavior to control their control ratios (Baron & Forde 2007). Thus, individuals compensate for their lack of control by engaging in deviant behaviors (Piquero & Hickman 1999). In the context of our study, a software developer who is responsible for completing a test within the deadline may feel lack of control, because he is ordered to meet the deadline, but he cannot meet it, nor can he postpone the deadline. Hence, in this case, the developer may compensate for his lack of control by purposefully skipping such a test.

CBT suggests that the greater the control imbalance, the higher the likelihood that an individual would omit prescribed tests (Singer 1997; Tittle 1995). However, a control imbalance by itself only increases the potential for such

behavior (Piquero & Hickman 1999). There must be opportunity for the omission, and the individual needs to be capable of doing it. CBT proposes several constructs that relate with the potential to engage in the omission and the opportunity to do so (Curry 2005; Piquero & Hickman 2003; Piquero & Hickman 1999; Tittle 1995; Tittle 2004). The four additional constructs in CBT are situational provocation, violation motivation, constraints, and self-control.

Situational provocation is defined as experiences that remind an individual of his or her control balance ratio, and how an act of deviance might improve this control balance ratio in the desired direction (Tittle 1995; Tittle 2004). Typical situational provocations in software development are time and budget. There is ongoing demand to develop software faster and cheaper (Baskerville *et al.* 2003). On the other hand, often the software projects fail to meet the deadline and budget (Abrahamsson *et al.* 2003). Keeping this in mind, the typical *situational provocation in this context is* when the software developer is required to increase output without adequate resources (time, budget). Situational provocations are seen as a stimulus or provocation reminding the subject of his or her control ratio imbalance (Curry 2005; Hickman & Piquero 2001; Hickman *et al.* 2001; Tittle 1995; Tittle 2004). This provocation is an intense experience, as most individuals do not consistently think about their control ratios (Tittle 2004). In the case of software testing, typical provocation perceived by the software developers is a lost bonus, because of the profit-based salary system that is associated with keeping to deadlines and within budget. These episodes can be brought about through feelings of debasement and humiliation or from feelings of heightened superiority and entitlement. In summary, CBT proposes that control balances lead to an increased likelihood that a developer may perceive provocations within a situation wherein a control imbalance may be perceived (as tested in this study). Further, when confronted with a provocation in the situation that reminds the individual of his or her control imbalance, it is more likely that the individual will have an increased motivation to omit prescribed tests (*i.e.*, violation motivation).

Violation motivation refers to the degree to which a behavior is seen as advantageous in respect to improving a control imbalance (Tittle 1995). In this study, we define *violation motivation* as the software developer's perception that skipping prescribed tests is advantageous to obtain the desired rewards, such as a bonus, maintaining reputation, or even for keeping one's job by meeting the deadline. Even if a developer experiences a provocation that heightens his or her awareness of his or her control imbalance, the developer will only have an increased motivation to skip tests if the behavior is perceived to improve the

control imbalance in the desired direction (Curry 2005). Even if the developer perceives an opportunity to skip tests, the developer must perceive the utility of doing so. In summary, violation motivation is posited to be high when a developer has a heightened control imbalance, becomes more aware of this imbalance through provocations in the given situation, and the skipping of tests is perceived as a way to increase the control imbalance in the desired direction for the developer. Further, CBT suggests that violation motivation leads to the intention to skip tests (Curry 2005; Tittle 2004).

Constraints refer to both the seriousness of the act and the situational risk of skipping prescribed tests (Tittle 2004). For this study, *seriousness* refers to the potential consequences that the software developer may face if others determine that prescribed tests have not been performed as indicated. In other words, seriousness is focused on how wrong a deviant behavior would be, as perceived by others (Tittle 2004). Seriousness may also be perceived from others' perceptions of how skipped tests may affect interpersonal relationships, opportunities, access to resources, etc. (Tittle 1995).

In turn, for the context of software development in general, and omitting the tests in particular, *situational risk* refers to the probability that other developers, managers, customers, or external auditors would detect that such tests had been skipped (Tittle 2004). Thus, if the developer believes that it is likely or probable that others may be able to detect and control testing procedures, it is likely that he or she will perceive the skipping of such tests as a situational risk, and thus feel constraints in reference to skipping tests. The potential risk of detection is further increased depending on the level of managerial oversight, and types of controls being used to oversee the coding process (Kirsch 1996; 2002). As more intrusive or formal methods of software development (*e.g.*, waterfall) place greater demands for documentation and testing on the developer, it becomes more risky to omit or produce deceptions about the completion of required tests. Deviant behaviors that are perceived as less likely to be detected by others and less likely to be controlled or monitored by others are less risky and are thus more likely to be enacted by the individual (Curry 2005). Likewise, developers that have higher control imbalances, particularly control surpluses, are less likely to feel constraints due to increased tendencies towards omitting prescribed tests.

While Tittle's formulation of constraints resembles the certainty and severity aspects of deterrence theory, (Tittle 2004) notes that constraints in terms of Control Balance Theory focus on the control implications of an act not simply on

the fear of formal and informal sanctions, as suggested by deterrence theory. Constraints are an important factor in CBT as the developer will theoretically weigh the potential gain from skipping tests against the loss of control that such behavior is likely to provoke (Curry 2005). In summary, CBT proposes that developers with control imbalances have lower tendencies to perceive constraints related to omitted tests, and these constraints are subsequently negatively related to the intention to engage in the omissions.

Self-control is defined as the ability of a developer to monitor and master his or her behaviors for the intent of achieving desired long-term goals or objectives (*e.g.*, expertise, mastery, reputation) (Curry 2005; Piquero & Hickman 2003; Piquero & Hickman 1999). Self-control has an important role in CBT as it may influence many of the core constructs. Specifically, the ability of a developer to bypass behaviors that provide benefits for the short-term and rather focus on behaviors that produce long-term benefits is what we term self-control. Specifically, self-control may influence situational provocation, violation motivation, and constraints. Developers who are able to engage in self-control are able to reduce the potential likelihood of impact due to their focus on long-term benefits, goals, and objectives that are outside of the situation wherein the provocations were experienced. This ability to step outside of the situation and think of long-term consequences may allow the individual to defuse situational provocation (Curry 2005). Likewise, beyond reducing the likelihood of situational provocation, self-control can have its own effect on violation motivation. Violation motivation is strongly influenced by the perceived utility of omitting tests. However, if a developer has higher levels of self-control it is likely that the perceived utility of skipping tests is thereby reduced due to the comparison of utilities from short-term omissions and longer-term strategies that revolve around conforming and performing prescribed tests (Tittle 2004). Thus, self-controlled developers are less likely to have motivations to skip prescribed tests.

Similarly, developers with high self-control will be more likely to perceive risks associated with omitting tests. As constraints are partially determined by the risk perceived by the developers who may omit tests, developers that are more focused on long-term goals and benefits may view the potential payoff from such short-term strategies involving omissions as too risky (Piquero & Piquero 2006). As such, these developers will more likely perceive constraints in a given situation that deals with omitted tests. A software developer having a low level of self-control may not be able to see or may not care about the long-term implications of skipping procedures, but rather attempts to satisfy short-term

benefits, such as a financial bonus for meeting a deadline. Long-term implications can be, for example, an increased risk of getting caught, especially if the skipping of tests continues over time. Self-control and its relationship to constraints is interesting in the context of software development (including testing), because the long-term benefits can be difficult to see. Especially, they may be hard to see in companies with a turbulent environment where software testers often change (Baskerville *et al.* 2003). For example, the number of developers depends on the number of contracts gained, or the number of projects completed on time and within the budget. This may also mean that without meeting short-terms goals and benefits (time deadlines and meeting the budget), one cannot obtain long-term benefits, because the developers can be fired if they do not meet deadlines, or team leaders can be fired if they go over the budget too many times.

4.5 Model Development

Prior to developing our theoretical model, we first emphasize the modifications to CBT in this study so as to apply this theory to IS research. First, given the context of this study, we do not distinguish between decadent (*i.e.*, deviance resulting from a control surplus) or submissive deviance (*i.e.*, deviance resulting from a control deficit) (See Tittle 1995). Both types of deviance produce, in fact, the same outcome – a skipping of tests, and thus do not need to be differentiated in this context. This allows a simplification in terms of deviant behavior, being able to lump both types into one form of deviance, the omission of prescribed tests.

Second, as the dependent variable in this study is the omission of prescribed tests, and not conformity, we focus on the control imbalance of the individual as opposed to the control balance (see Appendix 1 for a description of the scenarios used in this study). Thus, in referring to the situation, we are explicitly referring to the crises presented to a software developer that may occur at certain points in his career. This focus on the control imbalances modifies the theory and allows us to look at any imbalance. Again, we simplify the theory by combining both control surpluses and control deficits into the same category, as both are proposed to lead to skipped tests. Such simplification is important as it allows us to test all relationships as linear relationships as opposed to the curvilinear relationships wherein either high or low control imbalance levels are predicted to influence CBT constructs, as proposed in previous work (Curry 2005).

Third, we build upon the original CBT regression-based model proposed by (Tittle 1995), and the only SEM-based study (Curry 2005) by instantiating the importance of self-control in this model. Specifically, we propose that self-control will influence the major intermediate constructs in CBT (*i.e.*, situational provocation, constraints, and violation motivation). The importance of self-control in the original CBT was inferred by (Tittle 1995) and was proposed in later work (Curry 2005; Piquero & Hickman 2003; Piquero & Hickman 1999); although its influence on the CBT process remained untested. We build upon this opportunity and model the influence of self-control on the intermediate CBT constructs.

Fourth, we focus on the omission of prescribed software development tests, which differ from much of the CBT-based research that focused on the performance of a detrimental behavior. Given this difference, our intermediate constructs are more focused on the situation that is resultant from the contextual scenarios that we test in this study. In other words, this application of the theory is heavily based on circumstances and settings within IS/software development and the omission of prescribed tests rather than on the actual production of deviant behaviors that could produce other undesirable outcomes in this context (*e.g.*, substandard code, conflict between developers, industrial sabotage, etc.).

This section will now explain our theoretical-based CBT model about software developers' intentions to omit prescribed tests (see Figure 13). We first explain the effects of the central construct, control imbalance, on situational provocation, violation motivation, and constraints, and their relevance in this context. We then explore the relationships between these four constructs and the intention to omit tests in software development (*i.e.*, procedural violation intention). Subsequently, we explore the effects of self-control on core CBT constructs and propose morality as a counter-explanation to CBT.

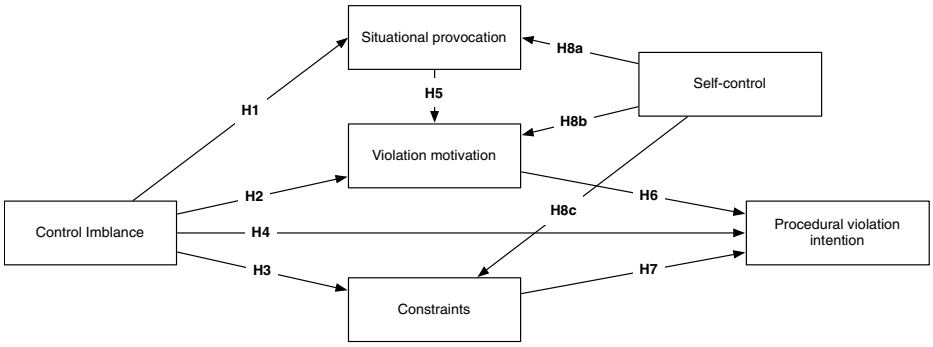

Fig. 13. Theoretical Model.

4.5.1 Control Imbalance

Tittle (1995) notes that a control imbalances may be resultant from a variety of contexts; meaning that one may have a relative balance of control at home but an imbalance at work and in the charitable organization that she volunteers with that results in a general control imbalance for the individual (Hickman & Piquero 2001). More severe control imbalances may increase the likelihood that a developer perceives a provocation in the given situation. Situational provocation is perceived by the developer when he or she becomes aware of some threat to his or her control balance. For example, if a software developer is told that he must complete a deliverable for a client in Fortran, he will sense a threat to his control over his own work processes, especially if he usually prefers to write in modern, object-oriented languages. The salience of a threat to a developer's current control balance will become greater if he already has an imbalance within his control balance ratio. Developers with a control imbalance have already been made aware that they are in an imbalance (Tittle 1995; Tittle 2004) and are attempting to modify their control imbalances to a more favorable position. These developers are thus more sensitive to situations that may alter their control imbalances, and more so if it pushes the imbalance in the incorrect direction.

Given the increased sensitivity that developers with imbalanced control ratios have towards situations that may alter their control imbalances, we expect that situations that threaten one's control will likely result in omitting prescribed software development tests. Previous work has also found that control imbalances often lead to increases in situational provocation (Curry 2005; Piquero &

Hickman 2003; Piquero & Hickman 1999; Tittle 1995; Tittle 2004). We build upon this research and extend these findings to the context of software development.

> *H1: High control imbalances will be positively related to the developer's perceived provocation in the tested scenario.*

CBT proposes that developers with control imbalances have strong motivations to improve these imbalances (Tittle 1995; Tittle 2004). Specifically, developers with control deficits are attempting to achieve a balance between the control they exert on others and the control they feel that is exerted on them, whereas developers with control surpluses, enjoying the surplus and the benefits that they can derive from it, are seeking to further increase the amount of control they exert over others in relation to the control they feel is exerted on them (Curry 2005). This should also hold true for testing procedures in software development. For example, software developers who feel that they have little control over their work environments and over how they perform the work, will attempt to engage in behaviors that allow them to exert more control over their work (*e.g.*, how it is executed, when it is done, where it can be done).

Previous work has also found that control imbalances lead to increased motivations to act deviantly (Baron & Forde 2007; Curry 2005; Piquero & Hickman 1999; Tittle 1995). We extend these findings to the context of testing in software development and propose the following:

> *H2: High control imbalances will be positively related to a developer's motivation to violate company testing procedures.*

Developers with control imbalances are also more sensitive to constraints in the environment that may limit skipping tests when compared to those that are more balanced in their control ratios. As with situational provocation, developers with control imbalances are more sensitive to situational constraints that may impede their abilities to improve their control balances. In order for a developer to skip tests it is necessary that an opportunity be available (*i.e.*, the lack of constraints in the situation) (Singer 1997; Tittle 1995; Tittle 2004). Situational constraints limit the ability of the developer to skip tests due to the potential risks of being caught and the seriousness of perceived punishments (Curry 2005). Thus, if constraints are present in the situation, it is more probable that developers with imbalances are more likely to perceive them due to their motivations to omit tests, which is only possible if constraints can be overcome. Thus, a control imbalance makes the

presence of constraints more salient, if they are present. Further, developers with control deficits will be more sensitive to such constraints given the level of control that others exert over them, and their desire to reduce this level of control relative to the control they are able to exert over others (Tittle 2004).

Previous work has highlighted the relationship between control imbalances and constraints (Curry 2005; Tittle 1995; Tittle 2004). We extend these findings to the context of this study and propose:

> *H3: High control imbalances will be positively related to the developer's perception of constraints in the tested scenario.*

The main tenet of CBT is that control imbalances lead to deviant behaviors (Singer 1997; Tittle 1995; Tittle 2004). Developers omit tests as a means to improve their control imbalances and bypass the control that others have other them (Tittle 1995). Omitting tests allows the developer to increase the amount of control that he or she exerts, and potentially reduces the level of control that he or she is likewise feeling from others. Thus, the greater the level of control imbalance, the greater the intention to omit tests and thereby improve imbalances. This main tenet has been tested and supported in previous literature (Piquero & Hickman 2003; Piquero & Hickman 1999). We extend these findings to the context of our study and propose:

> *H4: High control imbalances will be positively related to the intention to violate company testing procedures.*

4.5.2 Other Control Balance Theory Constructs

Situational provocation serves as a salient reminder of a threat to control that a developer is being confronted with in a situation (Tittle 1995). These situational cues lead to intense feelings that the developer associates with his current control imbalance (Curry 2005). Further, the provocation itself serves as a cue that the developer should omit tests to improve his or her control imbalance (Curry 2005; Tittle 2004). For example, the software developer that is ordered to only use Fortran in his current assignment will become aware that his control ratio is being threatened by further control from his manager and/or client. This threat is perceived as a provocation and is accompanied by strong negative emotions towards both his manager and/or client. This situation now serves as a cue that the developer's control ratio may move in an undesired direction, which can only be

prevented if the developer is able to stop this new controlling directive from coming into full effect or if he is able to engage in his own form of control over this situation. Deviance becomes the method by which the individual is able to either reduce the control that is being exerted over him or to exert his own form of control over others. Thus, the motivation to omit tests is further increased whenever the developer is provoked by the given situation.

Previous work on CBT has found that situational provocation is strongly related to the motivation to engage in deviance (Curry 2005; Piquero & Hickman 2003; Piquero & Hickman 1999; Tittle 2004). We build upon and extend these findings to the context of testing in software development and propose the following hypothesis:

> *H5: High levels of perceived situational provocation will be positively related to the developer's motivation to violate company testing procedures.*

High levels of motivation to skip tests will be strongly related to the intention to skip tests. Building on tenets of CBT and classical motivation theory (Cofer and Appley 1967), we propose that software developers with a motivation to engage in deviance by not performing prescribed tests will be more likely to intend to do so rather than those with less motivation. Developers that are more motivated to omit tests have more reasons and emotions that would result in greater benefits to the developer if they did so. Specifically, the threat to the control imbalance and negative emotions associated with the threat to this imbalance will be reduced by omitting tests, and thus the intention to omit them will increase.

The link between motivation, intention, and eventual behavior has been well studied and validated in research (Appley 1991) and within the theoretical context of CBT (Curry 2005; Piquero & Hickman 2003). We thus extend these findings to the context of this study and propose the following:

> *H6: High levels of violation motivation will be positively related to the intention to violate company testing procedures.*

As explained by CBT (Tittle 1995; Tittle 2004), constraints impinge upon the ability of the developer to omit tests. Constraints make the omission of tests more risky and minimize the payoff that the developer could reasonably expect by skipping tests. For example, if the software developer being forced to use Fortran also has coworkers that feel that this request is reasonable; it would be likely that the coworkers engage in informal sanctioning of any deviant behavior by the individual. These sanctions could include excluding the developer from social

gatherings or even a weakening of relationships. Thus, the intention to omit tests would be strongly influenced as the potential incentives of omissions by the developer would be minimized or even potentially reversed due to the risks and negative consequences that may occur for the developer.

The negative relationship between constraints and deviance has been strongly supported in the CBT literature (Curry 2005; Piquero & Hickman 2003; Piquero & Hickman 1999; Piquero & Piquero 2006). We extend these findings to the constraints in software development and propose:

H7: High levels of perceived constraints will be negatively related to the intention to violate company testing procedures.

4.5.3 Self-control and CBT

Omission of tests can also be viewed as a short-term approach to responding to threats to one's control imbalance in an attempt to improve the control ratio of the developer (Tittle 2004). The response to a situation is focused on the immediate threat provided and how the developer can respond to that threat at that point in time; little thought is given to the future and how such behavior may or may not lead to the fulfillment of long-range goals (Curry 2005). In other words, omitted tests that are motivated by an opportunity in a specific situation are a form of low self-control (Curry 2005). Developers with higher levels of self-control are more likely to focus on long-term objectives and goals, and are thus more insensitive to situational provocations and motivations that may increase the likelihood of omitting tests. Further, their insensitivity to perceived factors that lead to skipped tests also leads them to be more aware of constraints in the situations that may affect long-term objectives and goals. Thus, the constraints on skipped tests are also heightened. This focus on the long-term makes it less likely that a developer will skip tests by negatively impacting its positive predictors and by increasing the constraints on deviance.

Previous work in CBT has found that low self-control is more likely to result in deviance (Baron & Forde 2007; Curry 2005; Piquero & Piquero 2006) and we build upon and extend this work to the context of our study. Specifically, we hypothesize the following:

H8: Developers with high levels of self-control will be negatively related to the developer's perceptions of the opportunities and incentives to skip software tests. Specifically:

H8a: Developers with high levels of self-control will be negatively related to the developer's perceived provocation in the tested scenario.

H8b: Developers with high levels of self-control will be negatively related to the developer's motivation to violate company testing procedures.

H8c: Developers with high levels of self-control will be positively related to the developer's perception of constraints in the tested scenario.

4.5.4 Morality

Previous work in general criminology and CBT has proposed that developers may also be less prone to omit tests simply due to the fact that he or she defines the act as wrong and immoral (Hickman & Piquero 2001; Hickman *et al.* 2001; Piquero & Hickman 1999; Piquero & Piquero 2006). *Morality* refers to the belief that certain behaviors are wrong, and hence should be prohibited (Piquero & Hickman 1999). Developer morality is a relevant and interesting factor in the area of software development for a number of reasons. First, laws in this area tend to lag behind the technical development, which calls for moral decision making by developers. Second, laws vary in different countries regarding IT, also leaving room for developer moral decision making. Third, potential customers may not be familiar with the actual context of software development with the result that they may not demand certain tests. Even if they were to demand certain tests, it is difficult for clients to ascertain if tests were really carried out or not. This may increase the likelihood that software developers omit tests or leave errors in the system, because they calculate that, due to the complexity of software or other related factors, it might be difficult to pinpoint the individual developer who caused the error. Because the regulations or laws are not there, or they are unclear, and the risk of getting caught could be low, it is relevant to examine the role of moral decision making. Finally, professional codes and computer ethics courses required by ACM curriculum can be seen to teach software developers the value in prescribed tests being followed. Given such a specific relevance of a developer's moral decision making in this area and the results from other areas suggesting that a developer will not omit tests if they have high moral beliefs,

despite any imbalances, provocations, constraints, or motivation to engage in deviance, we control for the perceived morality of omitting tests as perceived by developers in this study and propose:

> *H9: Developers that perceive the omission of software tests as wrong (i.e., high levels of morality) will be negatively related to the intention to violate company testing procedures.*

4.6 Methodology and Study Design

To test the control balance theory, we used a scenario-based survey design, which is a common method for testing CBT (Curry 2005; Piquero & Piquero 2006) and is also an accepted method in information systems analysis (Siponen & Vance 2010). The strength of the scenario-based approach is that it allows for the addition of contextual details in a survey-based situation. Also, scenarios describe the situation in third-person terms.

In the scenarios, respondents are asked to think as if they were in the same situation as the person in the scenario (Piquero & Piquero 2006). To ensure that the gender of the third-person scenario does not influence respondents' answers, we used a common last name in the scenario instead of a first name (as that would reveal the gender of the person acting in the scenario). It is also important that scenarios describe common and realistic situations (Siponen & Vance 2010).

To ensure that the scenarios describe realistic and common situations, we followed the belief elicitation process (Limayem & Hirt 2003; Siponen & Vance 2010) and interviewed 10 experienced software developers individually, asking them to list common situations where software developers (and also testers) may omit key tests. From these situations we derived four scenarios, which were perceived as realistic by these experts.

In addition, when designing the scenarios in terms of the control balance theory, three issues were kept in mind. The first was that there needed to be an opportunity for action and the second was related to situational provocation (Piquero & Piquero 2006; Tittle 2004). Provocations are "contextual features that cause people to become more keenly cognizant of their control ratios and the possibilities of altering them through deviant behavior" (Tittle 1995). In our scenarios, the situational provocation was the lack of a bonus and the possibility for the software developers to obtain a bonus through omitting tests. This

provocation was suggested by the software developers and it is also noted in the literature (Ahonen & Junttila 2003).

Third, due to the two types of control imbalances, we included scenarios that involved both types of imbalances. For an excess of control imbalance, we relied upon a software development project lead/manager, which had the ability to exert control on his/her project team. On the other hand, we also included scenarios that used individuals that were being more controlled than they were controlling others. The use of lower-level, or lower power software developers was meant to exude the control imbalance brought about by an increased perception of being controlled by others. By including scenarios with excesses and lack of control, we attempted to match scenarios to the theoretical underpinnings of CBT.

The realism of this provocation, as presented in the scenario, was further validated by 10 experienced software developers. The scenarios are described in Appendix 1. Of the software development phases, we select testing, because it is the key means for assuring the quality of software produced (Ahonen & Junttila 2003).

4.6.1 Pilot Test and Measures

Our study used a survey method to collect data. To maximize the reliability of the constructs in our study, we used previously validated and reported instruments (Boudreau *et al.* 2001; Straub 1989) with some minor wording adjustments to fit the context of this study. Appendix 5 provides a detailed list of the scales that were used for this study. Participants were asked to report their responses to a scenario based on their own beliefs, as if they were the individual in the scenario. In the survey, participants were asked to provide answers for the constructs in the theory. These included control (Curry 2005; Piquero & Piquero 2006), situational provocation (Curry 2005), violation motivation (Curry 2005), constraints (Piquero & Piquero 2006), violation intention (Johnston & Warkentin 2010), self-control (Curry 2005), and morality (Paternoster & Simpson 1996).

Given that we slightly modified the previously tested CBT survey questions and used them in a new context, we performed two pilot tests as follows.

Our pilot studies used a paper-based questionnaire, which consisted of roughly 60 questions, including an area in which respondents could leave remarks and feedback about the questions asked. We used these responses to ascertain the validity of the questions and to identify any points of confusion within the survey.

The first pilot study used 38 students enrolled in a course on introductory information systems in a large public university in Finland. Participants read one scenario and responded to the questions. Participants were asked to identify any wording or questions that were confusing. Based on these remarks and the results of the initial pilot study, we modified several of the questions.

The second pilot study also used 38 students from another course on introductory information systems at the same university. The same procedures were used with all four scenarios, which resulted in minimal changes to the CBT instruments and the scenarios. We thus determined that the instrument and the scenarios were ready for final data collection.

4.6.2 Actual Data Collection

The actual data were collected from IT graduates at a large public university in Finland. Graduates were contacted via email to participate in the study and be entered into a draw for an iPod Nano. We obtained 136 usable responses (total sample size of 692; response rate = 19.5%) from this list.

4.7 Data Analysis and Results

4.7.1 Coding Control Balance

We followed the procedures set forth by (Piquero & Hickman 1999; Piquero & Piquero 2006) to calculate the control balance from the established control scales. The total control that the participant exerted was calculated by summing the items related to exerted control and this sum was then divided by the sum total of the control that the participant felt was exerted upon him or her. Thus, a score of one represents a person that is completely balanced and a score larger or less than one represents an imbalanced control ratio. This raw control balance ratio was then transformed so that, if the control balance ratio was less than one, it was inverted so that all control imbalances were greater than one. This single measure was then used as the manifest item for control imbalances in our structural equation model test.

4.7.2 Establishing Factorial Validity

Before assessing the hypotheses, several steps were taken to assure the reliability and accuracy of the collected data. First, we ascertained the types of constructs used in this study. Using (Diamantopoulos & Winklhofer 2001) as the sources of the instruments, we ascertained whether constructs were formative or reflective. All constructs in this study we ascertained to be reflective (excepting control, which is a manifest construct), based on the instructions in (Diamantopoulos & Winklhofer 2001). The remainder of this section will report our procedures for establishing factorial validity tests for our reflective constructs using their respective tests.

To analyze the factorial validity of the constructs, we used partial least squares (PLS) with SmartPLS version 2.0 (Ringle *et al.* 2005). To establish the validity of our reflective indicators, we followed the procedures outlined by Gefen and Straub (2005). To establish convergent validity, we generated a bootstrap with 200 resamples and examined the t-values of the outer model loadings. All retained items were significant at the 0.05 α level (Table A6.1 in Appendix 6). This demonstrates strong convergent validity for the reflective constructs.

We then used two established methods for determining the discriminant validity: correlating the latent variable scores against the indicators (Table A6.2) and calculating the AVE (Table A6.3). Both of these demonstrated strong convergent validity, excluding the indicated items, which were removed from the final data analysis to improve discriminant validity.

Finally, to establish reliability, PLS computes a composite reliability score as part of the model analysis (Table 10). This score is a more accurate assessment of reliability than Cronbach's alpha because it does not assume the loadings or error terms of the items to be equal (Chin *et al.* 2003). Each reflective construct in our research model demonstrates high composite reliability that exceeds standard thresholds.

Table 10. Composite Reliability.

Construct	Composite Reliability
Constraints	0.8502
Intentions	0.9701
Morality	0.8746
Self-control	0.8596
Situational provocation	0.8921
Violation motivation	0.9273

4.7.3 Testing for Common Method Bias

Given that data were collected using one method, we used three methods to establish the presence of a common-method bias. First, we used Harman's single factor (Podsakoff *et al.* 2003). This test required that we run an exploratory unrotated factor analysis on all of the indicators. The aim of the test is to see if a single factor emerges that explains the majority of the variance in the model. If so, then common-method bias likely exists at a significant level. The result of our factor analysis for our study produced 21 distinct factors, the largest of which only accounted for 42.58% of the variance of the model.

Second, we examined a correlation matrix of our latent constructs to determine whether any of the correlations were above 0.90, which is strong evidence that a common-method bias exists (Pavlou *et al.* 2007). None of the correlations were near this threshold.

The third, and most recent and accepted test for common methods bias (Liang *et al.* 2007) is to compare the substantively explained variance of the items against average methods based variance. To do this, all items were loaded onto a reflective first-order construct to represent the methods variance and it was related to all items in the model. All items were loaded onto their own, single-item indicator constructs, which were also predicted by the original construct with its multiple items. A bootstrap of this entire model was performed to extract the significance of all relationships in the model, and the loadings of all relationships. Based on this analysis the average substantively explained variance of the items is .861, while the average method-based variance is .000. This makes a ratio of 15,307:1. In addition, all of the relationships between the items and the method-based construct were insignificant.

Given that our data passed both tests for common-method bias, we conclude that there is little reason to believe that our data exhibit any of the negative effects from common-method bias.

4.7.4 Pre-SEM Model Testing of Control Balance Testing

Tittle (2004) proposed and refined Control Balance Theory in this later work, and set forth a four-step process to verify the integrity of the theory based on regression models. We perform these tests, prior to testing the SEM-based model used in this study, in order to more fully test the correctness and appropriateness of CBT in this new context. These tests were set forth in order to ascertain whether control was having an influence on deviant behavior, prior to the testing of any model using CBT and are ancillary to our theoretical model. We thus set forth these tests, prior to testing our CBT-based model. We are the first to report the results of these tests.

We test the modified version of CBT as dictated in (Tittle 2004) as an additional test of the theory. Although such tests and the refined model from (Tittle 2004) are based on both regression, and submissive and decadent forms of deviance, we provide these results to further validate CBT and its refinements, as proposed in (Tittle 2004).

Prescribed CBT Tests from (Tittle 2004)

Step 1 (Control balance on submission). Tittle (2004) reports that the first test of the CBT should show that the control ratio does predict submission, measured as a binary variable. To test this, we used the control balance ratio (without inversions, as described in section 6.1) and performed a logistic regression on the binary variable submission. *Submission* is scored as 1 if the intention to skip prescribed software development tests was less than 3.5 (*i.e.*, the median on the scale of 1, no intention to skip tests, to 7, complete intention to skip tests), or 0 if the intention score was greater than 3.5. The results of this logistic regression are shown in Table 11. As can be seen, this first step is significant, and in the expected direction ($\beta = -1.573$, $p = 0.05$), thus supporting the first test that individuals who experience balanced control ratios are less likely to engage in submissive types of deviance (*i.e.*, subjugation to others that exert control over the individual).

Table 11. Logistic Regression of Control Balance on Submissive Intentions.

Variable	Coefficient	p
Control balance	−1.573	0.05
Constant	0.835	0.38

Step 2 (Control balance on conformity). The second test involves showing the predictive power of a dichotomous control balance ratio (again, without inversions) on a dichotomous variable representing the conformity intentions of the subject. *Conformity* is when the intention to skip software testing is neither likely nor unlikely. To represent this, we scored conformity as a 1 if the intention score was ±0.1 from 3.5, or a 0 for all other scores. The logistic regression of the control balance ratio on the binary conformity variable is summarized in Table 12. Again, the results indicate that individuals who are relatively balanced in terms of control ratios are more likely to conform to the behaviors of others ($\beta = -1.212$, $p = 0.046$).

Table 12. Logistic Regression of Control Balance on Conformity Intention.

Variable	Coefficient	p
Control balance (binary)	1.212	0.046
Constant	-0.835	0.38

Step 3 (Control imbalances on deviance). The third test involves testing whether a dichotomous control imbalance ratio (without inversions) is able to predict deviant intentions. Control imbalances were scored as 1 if the control balance ratio was above 1.1 or below 0.9, and as 0 if it was between these two scores. The logistic regression of the dichotomous control imbalance ratio on intentions is reported in Table 13. Despite the support in the previous two tests, this test is not supported, contrary to our expectations. Although the results are in the right direction, the lack of significance may be due to a lack of power in this study, or due to a smaller than expected effect size.

Table 13. Logistic Regression of Control Balance on Deviant Intentions.

Variable	Coefficient	p
Control balance (binary)	0.402	0.195
Constant	3.016	0.000

Step 4 (Control balance on deviance). The final test involves testing the effects of the control balance ratio (without inversions) on the deviant intentions. This regression is summarized in Table 14. This main tenet of CBT is supported in this model, indicating that an individual who is more balanced in terms of their control ratios is less likely to skip software testing.

Table 14. Logistic Regression of Control Balance on Deviant Intentions.

Variable	Coefficient	p
Control balance	-0.747	0.040
Constant	3.648	0.000

With three of the four tests prescribed by (Tittle 2004) being supported, we argue that CBT is supported with our data and continue with the suggested interactions proposed in (Tittle 2004).

Predicted Interaction Tests Theorized by (Tittle 2004)

We additionally test and report the theorized 4-way interaction proposed by (Tittle 2004). (Tittle 2004) simplified his theory into the basic idea that provocation of an individual, reminding him of his control ratio, leads to the motivation to engage in deviance. The motivation for deviance is defined by the interaction of the control ratio, opportunity for deviance, the constraints in the given situation, and the individual's self-control. In other words, an individual will be more likely to engage in deviance if he has a control imbalance, perceives an opportunity to engage in deviance, perceives few constraints, and has low levels of self-control. As our model incorporates these ideas, we merely explore these interactions as a complementary analysis to our theoretical model. (Tittle 2004) does not propose actual interactions within his model, but proposes that the motivation to engage in deviance is increased when these variables that contribute to motivation are high.

Given the nature of a 4-way interaction, it is important to show all 2-way, 3-way, and main effects in order to understand what is being proposed by (Tittle 2004). Thus, we report several models that build up to the complete model proposed by (Tittle 2004), as shown in Table 15.

Table 15. Summary of Interactive Model Tests Theorized by Tittle (2004).

Variable	Base Model		Interaction Model		3-way Interaction Model		Full Model	
	Coef.		Coef.		Coef.		Coef.	
Constraints	−0.526	***	−0.093	ns	−0.150	ns	6.366	ns
Control imbalance	0.693	*	2.596	ns	8.034	ns	28.810	ns
Self-control	−0.209	+	−0.213	ns	−3.645	ns	14.998	ns
Violation motivation	0.179	*	0.724	ns	0.502	ns	13.240	+
Con. imbal. x constraints	—	—	0.139	ns	0.267	ns	−5.539	ns
Con. imbal. x self-control	—	—	0.669	ns	3.683	ns	−13.082	ns
Con. imbal. x vio. mot.	—	—	−0.172	ns	0.104	ns	−11.081	+
Constrains x self-control	—	—	−0.094	ns	0.113	ns	−2.869	ns
Constraints x vio. mot.	—	—	−0.063	ns	−0.315	ns	−2.330	+
Self-control x vio. mot.	—	—	0.008	ns	0.575	ns	−4.778	ns
Con. imbal. x constraints x self-control	—	—	—	—	−0.191	ns	2.488	ns
Con. imbal. x constraints x vio. mot.	—	—	—	—	0.191	ns	1.952	+
Con. imbal. x self-control x vio. mot.	—	—	—	—	−0.492	+	4.271	ns
Constraints x self-control x vio. mot.	—	—	—	—	0.003	ns	0.853	+
Con. imbl. x constraints x self-control x vio. mot.	—	—	—	—	—	—	0.754	+
Constant	5.476	***	7.039	*	13.248	ns	−28.243	ns
Adj. R^2	0.276		0.325		0.324		0.335	
F	13.87	***	6.42	***	5.04	***	4.99	***

*** p < .001; ** p < .01; * p < .05; + p < .10; ns — not significant

The results of the full model are problematic, but do indicate partial support for the interactive effects of the four main constraints on the motivation to engage in deviant behavior, as refined by (Tittle 2004). First, we note that the majority of the reported results are non-significant, which can be blamed on the highly

collinear results inherent in models built upon interactive effects. Given that the purpose of these tests is to determine the potential significance of such large-order interactive effects, it would be very difficult to test such terms without high levels of collinearity between the variables entered in the model. As a result, only the baseline model can be accurately relied upon for statistically valid results and the inferences derived from the full model are problematic given the extremely high collinearity of the model.

Regardless of the concerns with collinearity, the full model does show that the higher order interactive terms do, in fact, display near significance in reporting deviant intentions. Specifically, it appears that higher levels of control imbalance, constraints, self-control, and violation motivation generally lead to increased intentions to engage in deviance, as shown in the gray portion of Table 15. This leads us to expect that our theoretical model should also show that these same constructs should be powerful indicators of the intention to engage in deviance by omitting prescribed software tests.

4.7.5 Results of Hypotheses Testing

Given that our data display factorial validity, do not display common-method bias, and that they pass the majority of the supplemental CBT-confirming tests proposed by (Tittle 2004), we test our theoretical model, which is displayed in Figure 14. The results of our hypotheses, as based on the model testing, are shown in Table 16.

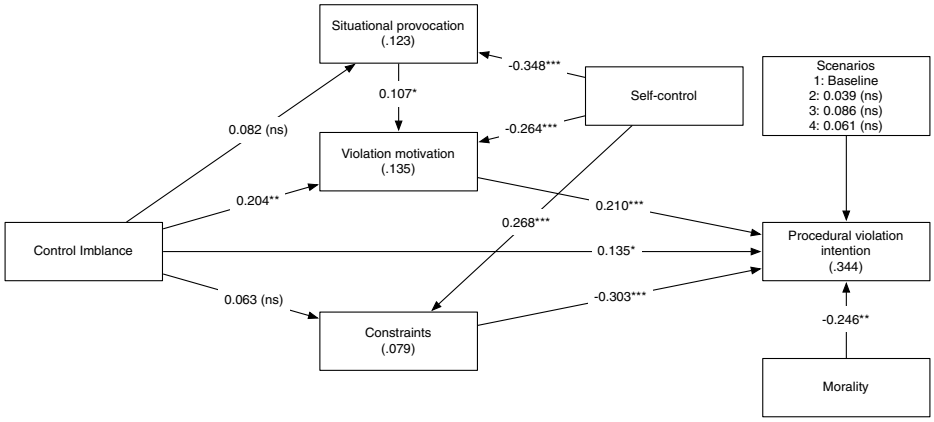

Fig. 14. Model Results.

Table 16. Summary of Hypotheses Tests Based on Theoretical Model Results.

#	Hypothesis	Coefficient	Supported?
1	Control imbalance → Situational provocation	0.082 ns	No
2	Control imbalance → Violation motivation	0.204 **	Yes
3	Control imbalance → Constraints	0.063 ns	No
4	Control imbalance → Intention	0.135 *	Yes
5	Situational provocation → Violation motivation	0.107 *	Yes
6	Violation motivation → Intention	0.210 ***	Yes
7	Constraints → Intention	−0.303 ***	Yes
8a	Self-control → Situational provocation	−0.348 ***	Yes
8b	Self-control → Violation motivation	−0.264 ***	Yes
8c	Self-control → Constraints	0.268 ***	Yes
9	Morality → Intention	−0.246 **	Yes

*** p < .001; ** p < .01; * p < .05; ns — not significant

4.8 Discussion

This study provides two important general contributions to research. First, this study is the first to empirically examine the omission of tests in software development, to the best of our knowledge, from the perspective of internal perceptions and situational factors. As a second contribution, this study utilizes control balance theory, which has not been used or empirically tested in IS. The remainder of this section will first summarize the results and then expound upon the contributions of this study for both research and practice.

4.8.1 Summary of Results

Our results largely support the theoretical model, with two exceptions. Both of the insignificant relationships were with control balance: the first being the relationship between control and situational provocation (H1) and the second the relationship of control and constraints (H3). It is possible that these relationships were insignificant due to the nature of the scenarios. As discussed in the model development section, it is possible for these constructs to exist, but to show no relationship given the situation that is being experienced. Although an individual may have a control imbalance, it is possible that the perceived provocation is not influenced by the control imbalance as the threats are perceived more as job

requirements or requests rather than events that evoke strongly negative, emotional reactions that are indicative of control imbalances.

Likewise, even if an individual has a control imbalance and perceives a provocation and motivation to skip software testing, it is possible that he or she also failed to perceive any constraints in the given scenario. It is possible that the individual perceived the potential risks of being discovered as low, or minimal, or focused on the unlikelihood of others sanctioning the individual for acting as they did, especially since the scenario highlighted that the behavior already did occur and a bonus was assigned. Thus, the assigning of a bonus and the fact that no one suspected the individual in the scenario of any deviance may have artificially minimized the relationship between control balance and constraints.

The remainder of our model reports significant relationships, which will be discussed in turn. First, our results suggest that a control imbalance leads to an increased intention to skip software development tests (H4), as suggested by the main tenet of CBT (Tittle 1995; Tittle 2004). While our study is the first application of CBT to software development, and hence this is a new finding in the areas of information systems and software development, studies in other fields have found that control imbalance leads to deviant action. For example, (Baron & Forde 2007) studied control balance theory by using the homeless as a sample (n = 400). Their findings suggest that both control deficits and control surpluses were related to assault and serious theft, but not minor theft. Similarly, (Piquero & Hickman 1999) found that control ratio deficits and surpluses predict the intention to engage in fist-fighting and deviant sexual practices among college students.

Second, our results suggest that control imbalance leads to an increased motivation to omit software development testing (H2). While this is a new finding in the area of information systems, the results are consistent with other related work using CBT (Curry 2005). While this study finds a direct, and significant relationship with the motivation to engage in deviance, Curry (2005) found that this effect was curvilinear in his sample, and very weak. Thus, this study is the first, by focusing on the control imbalances of its subjects, to show that control imbalances are an important indicator of the motivation to engage in deviance. In other words, if software developers feel a lack of power to decide how they will code, or the outcomes of such coding efforts, they may engage in deviance forms of behavior in an attempt to arrive at some level of control balance.

Third, our results indicate that motivation to omit tests leads to an increased intention to omit software development tests (H6). Given that motivations are

strong indicators of behaviors, it is no surprise that this relationship is significant (Cofer & Appley 1967). This finding is consistent with CBT (Tittle 1995) and previous research (Curry 2005).

Fourth, our results suggest that constraints significantly decrease software developers' intention to omit tests in software development (H7). Consistent with our results, (Tittle 1995), in his original theory, suggested that constraints have a strong negative relationship with deviant behavior/intention to engage in deviant behavior. Further, this was the strongest predictor of violation intention ($\beta = -0.408$). This indicates that the risks and seriousness of such constraints are important indicators and managerial levers that can be used to dissuade software developers from omitting required tests in software development. In alignment with classic deterrence theory (Gibbs 1975), this study finds support for the relationship between risks and the intention to avoid such risks by not engaging in the behavior.

Fifth, our model shows that both high levels of self-control (H8) and morality (H9) diminish the likelihood of an individual omitting to perform software development tests. Self-control was found to decrease both the likelihood of perceiving provocation within the situation and the motivation involved in skipping software tests. Additionally, self-control was found to increase the perceived constraints in the tested scenarios regarding omitted software development tests. Thus, individuals with higher levels of self-control are less likely to engage in deviant behavior.

In a related fashion, individuals with high levels of morality or moral reasoning were also less inclined to engage in deviant behavior. Thus, these two personality traits are important factors in determining the eventual intention to engage in deviant behavior.

Lastly, our study is the first to include, test and report the refinements and simplifications to CBT, as proposed in (Tittle 2004). Although some researchers have explored the basic CBT model proposed by Tittle (1995), and test the CBT process (Curry 2005), there has been no research to empirically validate the simplifications and tests for control balance as set forth in Tittle (2004). We provide these tests of control balance on deviance in Section 6.4.1 as preliminary tests to our theoretical model, and rely upon these tests to show that control imbalances are important indicators of deviant behavior and its related antecedents.

4.8.2 Implications for Research

We would like to highlight a number of implications for research based on our study. First, this is the first study to adopt CBT in an IS context, specifically to software development. Software development is an important and central process in information systems, however, there is a paucity of research that explains how this process may be improved outside of the control literature. This work provides a novel view of this process that is supplemental to that of control, and may provide additional insights to direct future research.

This study also has important implications for IS control research. This study can be used by IS researchers examining other control-related phenomena in an effort to explore why individuals often engage in behaviors that are seen as anti-social, illegal, or immoral. Control-based literature has an underlying assumption that controlled individuals are rational and will behave in rational manners in order to avoid sanctions and receive incentives awarded by the control system in place. However, CBT highlights that individuals often act in non-rational ways in order to increase their control over others or strike back at those that they feel are overly controlling their work process and/or outcomes. Further, this study highlights that the use of control has detrimental impacts on those being controlled that is generally ignored or not considered. These areas tend to be understudied in control research, and this theory is ideally situated to study such contexts. This study adds additional insights that go beyond the suggestions offered by traditional control techniques (Kirsch 1996; Kirsch 1997; Kirsch 2004; Kirsch *et al.* 2002).

The use of CBT provides a broader range of motivations and factors than can encourage an individual to engage in deviance, understand the motivations, and thereby prevent them. Specifically, this study shows that the risk of such deviant behaviors has a strong impact on whether individuals intend to engage in deviance. Thus, further research is needed that can explore how the risk of engaging in such deviance can be altered in order to minimize potential deviance. Perhaps the inclusion of more clan-based controls would be able to highlight such risks and thereby minimize deviant behaviors.

This study also has important implications for the IS group and trust–based research streams. Control balance theory shows how the use of controls produces detrimental impacts on teams and can undermine trust of management at the same time. Although similar research has been done in other fields that links the usage of controls to lower trust levels, less cooperation ad higher levels of distrust

(Baba 1999; Mulder *et al.* 2006; Piccoli & Ives 2003), these literature streams in IS have yet to explore how control relates to and affects their central constructs. CBT provides the theoretical bridge between these disparate research streams and provides many insights that can be used for future research.

This study also highlights the potential to develop context-specific items for control balance that may provide additional insights into other IS-related areas. Earlier research on control balance theory has mainly used generic items to measure control balance in general. (Tittle 1995) has suggested that people may have different control ratios in different areas of their life, such as in the workplace, in a family setting, and in other organizations to which an individual belongs. The only way to know if CBT is appropriate for the context of software development, or other IS contexts, is to develop such specific items. As mentioned, we believe that context-specific items and scenarios could lead to an increased significant relationship between control imbalance and situational provocation and constraints. This increased understanding could provide much needed insight as to how control imabalances in the workplace are created, and which factors or behaviors will most likely lead to imbalances in controlees.

Tittle notes that the constraints, in terms of control balance theory, focus on the counter-control provided by others. While (Tittle 2004) recognizes the use of formal and informal sanctions as a set of measures for constraints, he sees that constraints in CBT are wider in scope than formal and informal sanctions in terms of deterrence or control theories. Current research lacks such a set of constraints (Curry 2005). Hence, future research is needed to develop constraints in terms of control balance theory in the context of this study or other IS-related contexts. Such constraints can be developed by examining what actions work as counter-controls; that is, have the potential to alter people's feeling of control in a given act. In order to do this, we suggest the use of two approaches. The first one is inductive, where scholars ask developers to report through interviews which things function as constraints that influence their control balance with respect to omitting tests in the development of software. With the other approach, scholars should come up with a list of potential actions generating counter-control (and hence affecting control balance) and then ask software developers to rank these. The two approaches could also be combined in a larger effort to explore constraints in an IS context.

Control balance theory suggests that deviant or anti-social acts are mainly – but not fully – based on rational decision making. These deviant acts may also

not be fully rational; for example, impulsive behaviors or extreme self-control related to non-rational goals or objectives that may influence the control balance process (Tittle 2004). Future research should study whether the other factors, such as habit, influence the control balance process or have direct links to behavior. For example, it could be postulated that deviant actions become habitual after a certain number of repetitions and, after that, the control imbalance or situational provocation no longer explains the deviant act in question. Following this line of thinking, it can be seen in the context of software development that the omitting of tests is so common that it may become a habit.

Research opportunities from a corporate crime perspective, which are widely studied in criminology, have received less attention in IS in general, and in this context in particular. According to this perspective, employees commit deviant actions on the behalf of the company (Paternoster & Simpson 1996). Applying this idea to software development, the scenarios could be designed in a way that the scenario character is helping the company. That is, the employees do not skip tests to help themselves or to improve their control balance, but rather to maximize the interests of their company. Further, future research could explore whether individuals that are balanced in terms of control engage in more citizenship behaviors and are thereby more cooperative and better resources for their organizations.

We also call for future research on this topic using other theories that might explain the behavior used in this study. For example, one potential theory that could explain this behavior is neutralization techniques (Siponen & Vance 2010). For instance, using a metaphor of the ledger, software developers may neutralize their actions by claiming that, because their overall software development performance is good, they can occasionally omit tests.

While theory verification has played a part in IS behavioral research, sometimes it is fruitful not only to apply generic theories from other disciplines, but also to ponder what are ultimately the context-specific issues that lead employees or companies to omit tests. To this extent, as another research avenue, we suggest the use of an inductive approach to study this, where scholars ask developers to report through interviews which things may influence omitting tests in the development of software. Possible reasons that may pave the way towards a situation where employees omit prescribed tests in software development could be (i) strong demand for agile and lean development, (ii) tight deadlines, (iii) release-based development, (iv) bonus-based salaries, and (v) customers possible lack of technical knowledge. A related, yet interesting research topic, would be to

examine whether the complexity of software and the tendency to de-humanize man-made errors as "computer errors" (Moor 1985; Siponen 2004) help software developers to neutralize their deviant behaviors. Or do the software complexity and the tendency to de-humanize man-made errors play a role in software developers' rational choice calculations? In other words, do software developers omit tests or leave errors in the system because they calculate that, due to the complexity of software or other related factors, it might be difficult to pinpoint the individual developer who has caused the error or who omitted tests that may have uncovered such errors?

Finally, keep in mind that the increased tendency of agile or fast release-oriented IS development increases the likelihood that developers skip planned tests, compared with the more traditional development approach. Here the assumption is that in agile development, omitting planned testing may be more socially acceptable or easily neutralizable (*i.e.*, neutralization techniques) using fast release and minimized development costs as an excuse to skip tests.

4.8.3 Implications for Practice

Our findings have implications for software development organizations, customer organizations that order and use software, and the general public (who also pay for or use the software). Customers and the general public need to understand that tight deadlines with high bonus systems might further motivate developers to omit tests that could reduce the numbers of errors and thereby improve the overall quality of the software. In fact, when the competition is tight, in the sense that there is a need to quickly get the product to market, even the software development company may not care if some features of the software are not working (Baskerville & Pries-Heje 2001). Customer organizations ordering the software and the software users need to understand this and also realize that one key way to change this is by demanding both high quality and high functionality (Baskerville & Pries-Heje 2001).

For the organizations developing software, we would like to highlight three findings. First, given that control imbalance leads to the intention to omit software development tests, and that control imbalance increases the motivation to omit such testing, we suggest that the level of control balance can be measured during recruitment or when interviewing potential employees. This is especially important to consider, as the global control ratio of an individual, which

influences CBT-related deviant behaviors, is largely outside of the control or influence of management. Further, management should be aware of the effects that demands and other work situations may make on their employees' control balance ratios. If situations could be identified in advance that may threaten control balance ratios, managers may be better equipped to defuse situations in advance and thereby avoid potential deviant behaviors that these situations may motivate.

Second, given that situational provocation leads to the motivation to omit tests, we suggest a number of practices to avoid this outcome. In our study, situational provocations manifested themselves through bonuses associated with a deadline. The first practice is to set realistic deadlines. The second approach is to associate quality indicators with bonuses, or to introduce peer-review systems in order to make sure that important tests are not omitted. Other such approaches can be identified and tested in future research.

Third, given that our results suggest that properly designed constraints significantly decrease software developers' intentions to engage in the behavior of omitting tests, we suggest that software companies adopt a number of formal and informal controls in order to minimize this practice. These constraints can be based on both formal, informal, and clan methods of control (Kirsch 1996; Kirsch 1997; Kirsch 2004; Kirsch *et al.* 2002). Being that constraints are the most easily implemented, managed, and influenced area in the CBT model, it is likely the most profitable method that a company could employ to encourage software testing.

4.9 Conclusion

Software quality is recognized as a key concern in software development. Previous research shows that software quality issues are rather related to the management of people issues, such as when software developers neglect proper testing practices, than to technical issues. And yet, we find no studies that have explored which factors make software developers omit designed and agreed-upon tests. In other words, what makes software developers cheat when doing tests? Further, this study expands upon our understanding of this process by exploring how control methods also produce detrimental effects on those being controlled that may harm the controlling organization. We suggested that control balance theory, which has never been applied in the field of IS, explains why software

developers omit tests in an attempt to feel a sense of balance in terms of how they control others and how they are controlled by others.

Our empirical results support the theory (n = 136). Based on our findings, we suggest a number of practices to ensure that software developers do not omit tests. First, managers can attempt to balance the control levels that individuals feel they are able to exert over themselves, their environments, and how they work, and the control they feel is exerted over them in these same areas. Second, managers could become more aware of how the situational factors and the individual's own self-control may alter the perception that such a behavior would be possible and beneficial for the individual. This information, in turn, would help software companies take preventative actions aimed at minimizing such behaviors before they occur.

5 Blowing the Whistle on Computer Abuse: Extending Whistle-Blowing Theory Using Anonymity, Trust, and Perceived Risk with Whistle-blowing Systems

5.1 Abstract

Online whistle-blowing systems are becoming increasingly prevalent channels for reporting organizational abuses. Given that the Sarbanes-Oxley Act and similar laws throughout the world require firms to establish whistle-blowing procedures and systems, whistle-blowing research and applications should only increase in importance. Although an established stream of research has developed whistle-blowing theory to explain conventional whistle-blowing behavior, this theory is not designed to explain use of anonymous, online whistle-blowing systems—a unique phenomenon that introduces a unique set of factors.

This study extends whistle-blowing theory to include three factors especially salient in the context of online whistle-blowing systems: anonymity, trust, and perceived risk. We empirically test our model within the context of reporting computer abuse using student and professional samples. Our findings showed that trust in both the report-receiving authority and the whistle-blowing tool itself strongly impacted willingness to report computer abuse. Moreover, perceptions of anonymity strongly increased trust in both the report-receiving authority and the whistle-blowing tool. Additionally, the perceived risk of the computer abuse indirectly affected willingness to report. Our findings result in an extended whistle-blowing model (adding trust, risk, and anonymity) that has strongly increased explanatory power over traditional whistle-blowing theory.

5.2 Introduction

A persistent global problem receiving increasing attention is organizational fraud and abuse. A key means of uncovering such fraud and abuse is through whistle-blowing, which is "the disclosure by organization members (former or current) of illegal, immoral, or illegitimate practices under the control of their employers, to persons or organizations that may be able to effect action" (Near & Miceli 1995). In recent years, legislation such as the Sarbanes-Oxley Act in the United States and similar legislation in other countries have required public companies to

establish channels through which whistle-blowers can anonymously report abuses[4].

In order to better understand whistle-blowing behavior, researchers have developed whistle-blowing theory (Near & Miceli 1995). A key distinction of this theory is that it explains that an individual does not choose to whistle-blow based on a traditional cost-benefit calculus (as widely seen in risk-related IS literature) because there are few, if any, personal benefits of whistle-blowing. The theory thus focuses on whether someone determines something to be worthy of reporting (*e.g.*, bad enough to report) and whether or not that person believes he or she has a personal responsibility to whistle-blow following an incident (Near & Miceli 1995; Near & Miceli 1996; Park *et al.* 2008; Smith & Keil 2003).

Although whistle-blowing theory has been shown to be robust across a variety of settings, the theory has not been applied to the phenomenon of online whistle-blowing report systems[5], which are an increasingly prevalent and important means of receiving whistle-blowing reports (Young 2009). These systems allow users to submit whistle-blowing reports anonymously from any place that has Internet connectivity. Whistle-blowing systems are differentiated from traditional means of whistle-blowing—such as telephone hotlines and post office boxes—because they require interaction with a system, which introduces a unique set of user perceptions (Moore & Benbasat 1991). Further, research on mediation communications has found that increased distance and technology mediation between the communicators makes it more difficult to communicate. Specifically, communicators have more difficulty in creating a shared context and transferring information, and are prone to experience more conflict within their relationship (Hinds & Bailey 2003; Hinds & Mortensen 2005). The increased difficulty in creating a shared context and transferring information increases the likelihood of miscommunication (Rogers & Lea 2005), thus undermining the effectiveness of such systems. Given the even sharing of information, increased likelihood of conflict, and a lack of a shared context, online whistle blowing systems have additional hurdles to overcome than the traditional means for whistle blowing.

---

[4] For the U.S., see the Sarbanes-Oxley Act, Section 301; in Canada, see Multilateral Instrument 52-110 section 2.3; in the U.K., see the Combined Code for Corporate Governance C.3.4.

[5] For examples of whistle-blowing systems, see http://silentwhistle.com or http://clearviewconnects.com.

We expect three factors in particular—namely anonymity, trust, and risk—to be salient in usage of an online whistle-blowing system because of their heightened effects in other online systems as compared to traditional whistle blowing mechanisms (Gefen *et al.* 2003; Jarvenpaa & Tractinsky 1999; Pinsonneault & Heppel 1998). This paper extends whistle-blowing theory to include these three factors in order to better explain users' intentions to whistle-blow using the system. These three factors are briefly described as follows.

First, *anonymity* is widely assumed and accepted to be a critical factor in individuals' decisions to use whistle-blowing systems (Young 2009). We were thus surprised to learn that although previous treatments of whistle-blowing theory tacitly acknowledge the importance of anonymity (Near & Miceli 1995), its effects on whistle-blowing behavior have neither been directly theorized nor examined empirically in the literature. The importance of anonymity is even more crucial in an online setting, in which several components influence perceptions of anonymity, beyond simply lack of identification. Specifically, (Pinsonneault & Heppel 1998) identified five dimensions of anonymity in online settings: lack of identification, diffused responsibility, lack of proximity, lack of knowledge of others, and confidence in the system. Our theoretical extensions incorporate each of these dimensions in order to show how perceptions of anonymity influence individuals' willingness to whistle-blow.

Second, another implicit factor in many whistle-blowing studies is *trust*: people are believed to be more likely to whistle-blow if they feel they can trust the authority to which they report (Smith & Keil 2003). Again we were surprised to learn that trust has not been explicitly theorized or tested in the context of whistle-blowing. Further, the criticality of trust may be even more salient in online settings, given research findings showing the importance of trust in users' interaction with e-commerce systems (Gefen *et al.* 2003). Trust may be especially important for users with no prior experience with the online system (McKnight *et al.* 2002).We thus incorporate trust in the report-receiving authoring into our expanded model of whistle-blowing—contributing to both the trust and whistle-blowing literature. Additionally, recent research has shown that trust can also be placed in IT artifacts (Vance *et al.* 2008; Wang & Benbasat 2005), especially in situations involving high personal risk (McKnight 2005). For this reason, our extension of whistle-blowing theory also incorporates trust in the whistle-blowing tool.

Third, perceived risk is central to whistle-blowing because of the high-risk nature of whistle-blowing (Miceli & Near 1984)—with retaliation being the

foremost risk (Miceli & Near 1985). Research in IS has consistently shown the substantial effects of perceived risk (Dinev & Hart 2006; Grazioli & Jarvenpaa 2000; Malhotra *et al.* 2004), and yet, despite the central role of risk, whistle-blowing theory literature does not explicitly describe the effects of perceived risk. Because prior research has established that many users perceive risk in online transactions (Jarvenpaa & Tractinsky 1999) we can reasonably theorize that users will likewise perceive heightened risk in making whistle-blowing reports using an online tool Thus we extend whistle-blowing theory to explicitly describe the effects of perceived risk.

Because traditional whistle-blowing theory was not designed to explain these above factors, a gap exists in our theoretical and empirical understanding of users' whistle-blowing behavior using online systems. To address this research gap, we develop a model that significantly extends traditional whistle-blowing theory to answer three research questions:

- What is the role of perceived anonymity in users' use of online whistle-blowing systems?
- How does trust affect users' intentions to whistle-blow using online whistle-blowing systems?
- What is the effect of perceived risk of whistle-blowing on users' intentions to whistle-blow using online whistle-blowing systems?

To answer these questions, we ground our examination of whistle-blowing behavior within the highly salient IT context of *computer abuse*, which is defined as "the unauthorized and deliberate misuse of assets of the local organizational information system by individuals" (Straub 1990). Extending the reporting of computer abuse in an organization is a natural and highly relevant IT extension of whistle-blowing theory, because this domain encompasses the three salient elements of whistle-blowing outlined by (Near & Miceli 1996), namely: (1) a wrongdoer commits an act believed to be improper; (2) a whistle-blower observes the wrongdoing and reports it to an authority; (3) the authority receives the report of wrongdoing. To empirically test our model, we performed a cross-sectional survey using student and professional samples. Our findings strongly supported our innovative model, and showed that trust in both the report-receiving authority and the whistle-blowing tool itself strongly impacted willingness to report computer abuse. Moreover, perceptions of anonymity strongly increased trust in

both the report-receiving authority and the whistle-blowing tool. Additionally, the perceived risk of the computer abuse indirectly affected willingness to report.

The remainder of this paper is organized as follows. First, we review whistle-blowing theory and propose our model extension. Second, we discuss the methodology for testing our model. Third, we discuss the results of our data analysis, followed by a discussion of the contributions made by these results. Fourth, we discuss the implications of the contributions for research and practice, along with limitations of the study and future research opportunities. Finally, we conclude with our observations behind the contributions of the study.

5.3 Theoretical Model

Our theoretical model builds on whistle-blowing theory and a recent whistle-blowing model by (Park *et al.* 2008) in the IS literature. Whistle-blowing theory posits that: (1) a problem must be perceived as major before an individual will consider reporting it; (2) the greater the problem (as perceived by the individual), the greater the individual's sense of personal responsibility to report it; and (3) the stronger the individual's sense of personal responsibility for reporting a problem, the more likely it is that he or she will actually follow through and report the problem. From this theory, the assessment that a *problem ought to be reported* is defined as the perception that a known problem should be brought to the attention of someone who can rectify the problem or prevent it from recurring (Near & Miceli 1996). A person's assessment that he or she has a *personal responsibility to report* is defined as the felt individual obligation that the individual should be the one to notify someone who can correct the given problem (Near & Miceli 1996). Again, cost-benefit is not part of the model due to the lack of benefits in reporting.

Little literature in IS has considered whistle-blowing theory (or related theories), and the studies that have considered it have generally focused on reporting bad news in problematic software projects and reluctance around software project problem escalation (Keil 1995; Keil *et al.* 2007; Keil *et al.* 2000; Keil & Robey 1999; Park *et al.* 2008; Smith & Keil 2003). Key to our theoretical model, (Park *et al.* 2008) built on (Dozier & Miceli 1985) basic whistle-blowing model to predict willingness to report bad news in software projects. In this context, they supported the fundamental propositions depicted in Figure 15. As a further extension to this model, they considered the impacts of perceived time urgency (*e.g.*, how not reporting problems may negatively impact the project schedule) and whether an external vendor could be blamed for the project's issues

(perceived fault responsibility). These two factors are not included in our model as they are specific to reporting bad news in software projects.

Fig. 15. Basic Whistle-blowing Model.

For purposes of nomological validity, we replicate the following hypotheses from the basic whistle-blowing model:

> *H1. A person's increased assessment of personal responsibility to report computer abuse increases his or her willingness to report computer abuse.*
>
> *H2. A person's increased assessment that a computer abuse scenario ought to be reported increases his or her assessment of personal responsibility to report computer abuse.*

5.3.1 Core Theoretical Extensions

We add five primary theoretical extensions to the basic whistle-blowing model depicted in Figure 16, which are further developed in this section. Based on the extent literature and theory, we propose that a whistle-blowing model that is enhanced for more explanatory power will also take into account (1) perceptions of anonymity, (2) trust in the reporting tool, (3) trust in the report-receiving authority, (4) the perceived risk of reporting, and (5) public self-awareness. Our extension of whistle-blowing theory moves from a traditional model that focuses primarily on responsibility to a holistic model that includes trust, risk, and personal responsibility. Our extended model is depicted in Figure 16, and further explained in the following discussion.

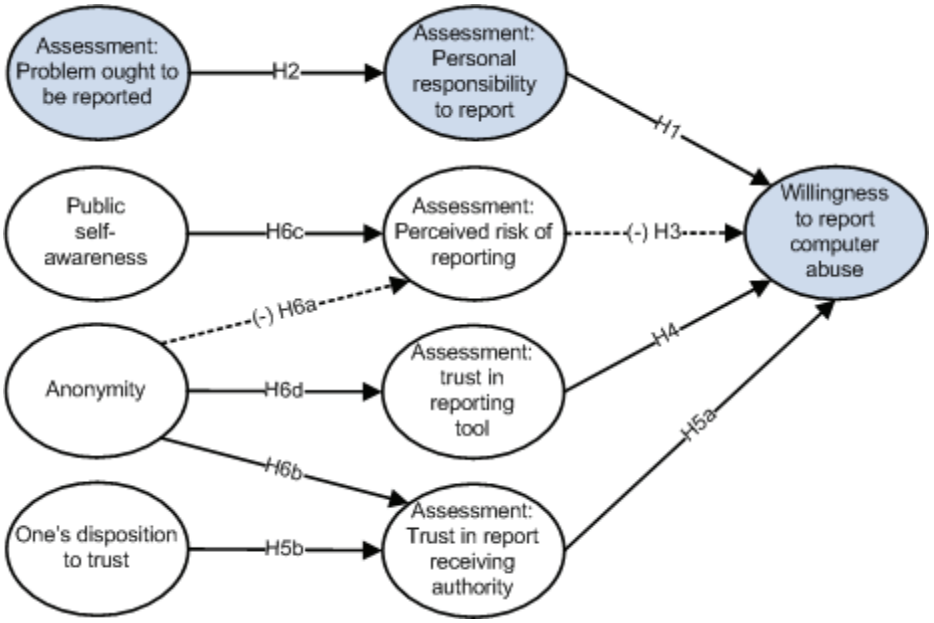

Fig. 16. Theoretical Extensions to Whistle-blowing Theory.

Adding Risk of Reporting to the Model (H3)

The omission of risk from extant whistle-blowing models is a surprising oversight, which if addressed can greatly add to explanatory power of whistle-blowing theory. First, risk is endemic in virtually all decision making where outcomes are uncertain (Pablo *et al.* 1996; Williams & Noyes 2007). This uncertainly is clearly exists in all whistle-blowing cases, which are naturally fraught with high risk and uncertain outcomes. For example, research has stated that the most important overall consideration in the risk of whistle-blowing is whether or not one is protected from retaliation (Miceli & Near 1985). Higher risk situations could engender higher costs because of the underlying stakes involved (Miceli & Near 1984), and in turn can result in social embarrassment and retaliation. As an example, accusing a boss of committing fraud through email would have more potential for personal risk than accusing a colleague of playing computer games during work hours.

Risk beliefs are defined as "the trustor's belief about likelihoods of gains or losses outside of considerations that involve the relationship with the particular trustee" (Mayer *et al.* 1995). Importantly, risk beliefs are independent of the

characteristics of the trustee. If risk beliefs are high, the trusting intentions of the trustor will be reduced. Previous research has shown that decision-makers' perception of risk is composed of the probability of negative outcomes and the magnitude of likely loss from those negative outcomes, which (Smith & Keil 2003) define as an "expected value of the loss" (p. 75). Thus, for our study we define the *perceived risk of reporting* as an individual's assessment of both the likelihood and magnitude of potential losses that may result from reporting an incident of computer abuse.

Previous research has often found that trust and risk are negatively related to each other. In a study of the disclosure of information in a risky situation, a context that easily extends to whistle-blowing, (Metzger 2006) explained that consumers do a cost-benefit analysis in which risk, trust, and benefits are compared before deciding to disclose information. They support the notion that trust is an antidote to risk. Other studies, using various theories, empirically support the notion of balancing trust against risk in making disclosures and other related trusting-intentions decisions (Dinev & Hart 2006; Grazioli & Jarvenpaa 2000; Malhotra *et al.* 2004; Mayer *et al.* 1995; McKnight *et al.* 1998).

These concepts, findings, and explanations naturally extend to a whistle-blowing context because a whistle-blower needs to weigh risk and trust in a given scenario before disclosing potentially damaging information. The key caveat is that an individual's whistle-blowing calculus is focused on risk, not benefit because again, benefits are hard to find in whistle-blowing. For example, in a difficult economic climate, a whistle-blower's dependence on the job, both economically and emotionally, will provide additional perceived risk in "mounting a challenge to organizational authority" (Miceli & Near 1984). First, the individual must assess the likelihood of succeeding in this challenge. Next, the magnitude of loss would be determined for such a failure, which can be everything from shame and embarrassment to job loss, lawsuits, and even jail time (for alleged false accusations). By combining these two assessments, an individual internally calculates the risk involved with reporting an incident to some other party. We thus posit that the greater the personally perceived risk is in a potential whistle-blowing incident, the decreased likelihood one will feel trust and/or believe that the potential loss is worth engaging in whistle-blowing Thus, the less personal risk people perceive in reporting an incident, the more likely they will be willing to report, aside from their internal calculus of their responsibility to report:

H3. A person's increased perceived risk of reporting computer abuse decreases his or her willingness to report computer abuse.

Adding Trust to the Model

As noted in the previous section, risk and trust are often considered together. Research on risk and trust has defined trust as a "willingness to take risk" and the level of trust can be an indication of the amount of risk one is willing to assume (Schoorman *et al.* 2007). Likewise, trust is often conceptualized as a means of coping with perceived risks (Gefen *et al.* 2003); thus, the greater the risk perceived in a given situation, the greater the amount of trust required to cope with the risk (Schoorman *et al.* 2007; Williams & Noyes 2007). When an individual blows the whistle on computer abuse in an organization, he or she is displaying trust toward the organization and is willing to accept potentially negative outcomes resulting from his or her accusation. In our model, we consider two salient sources of trust: the IT artifact itself (reporting tool) and the report-receiving authority.

Trust in the Reporting Tool (H4)

Research has shown that people form trusting beliefs not only in people, but also in the IT artifacts with which they interact (Komiak & Benbasat 2006; Vance *et al.* 2008; Wang & Benbasat 2005). Although the concept of trust involves important differences, depending on whether the object of trust is a person or a technology, trust in IT and trust in people are similar in that they both require the trustor to rely or depend on the object of trust (McKnight 2005).This trust in IT is manifested when people rely on the IT artifact (McKnight 2005). A body of research has found that people consciously and unconsciously place trust in technology through anthropomorphism, attributing to technology human characteristics such as agency (Friedman & Millett 2007); personality, friendliness, and helpfulness (Reeves & Nass 1996); morality or responsibility (Muir 1987); and benevolence and credibility (Cassell & Bickmore 2000); and by considering computers—through their interfaces—as social actors (Nass *et al.* 2006). Recent research has extended these findings and found evidence that the IT trust formation process occurs when an IT artifact—rather than a business or organization—is the object of trust (*i.e.*, whether or not people perceived the IT

artifact to possess dependable/useful characteristics) (Komiak & Benbasat 2006; Vance *et al.* 2008; Wang & Benbasat 2005).

As with trust placed in people, trust in IT artifacts has been found to lead to increased adoption and use of those artifacts (Qiu & Benbasat 2006; Vance *et al.* 2008; Wang & Benbasat 2008). In the context of this study, we conceptualize trust in the IT artifact as trust in an anonymous reporting tool. In summary, we predict:

> *H4. A person's increased trust in the reporting tool increases his or her willingness to report computer abuse.*

Trust in Report Report-Receiving Authority (H5)

Third-party trust—specifically in the report-receiving authority—is a potentially critical element that we consider in respect to whistle-blowing. The literature shows that people are more likely to whistle-blow if they feel they can trust the *authority* (the party to whom they are reporting), which is counterbalanced by how risky and costly they perceive an incident to be (Smith & Keil 2003). The potential of trust to override fear of retaliation is driven by a broader knowledge of the importance of trust and risk in online settings. Trust in people has typically been measured in terms of benevolence, competence, and integrity (Mayer *et al.* 1995), and a very strong predictive connection exists between trusting beliefs and trusting intentions (McKnight *et al.* 2002). Hence, if the authority is perceived as trustworthy—whether or not the party provides assurances of protection—a potential whistle-blowing party is much more likely to feel safe, and thus be willing to whistle-blow, if they feel that the authority generally acts with benevolence, competence, and integrity.

Meanwhile, seminal trust literature (McKnight *et al.* 2002; McKnight *et al.* 1998) indicates that trusting beliefs are created toward a target based on a given context. In our case, the most salient target of trust—outside of the reporting tool—is the authority in the organization that receives the whistle-blowing report (Smith & Keil 2003) Because our context of trusting beliefs deals directly with representatives of the organization or institution, we omit institution-based trust because it is essentially the same concept in our context. Furthermore, trusting beliefs have consistently been shown to influence trusting intentions (McKnight *et al.* 2002; McKnight *et al.* 1998) ; thus, we omit this relationship from our model. In summary, we predict that a person's assessment of trust in the report-receiving authority increases an individual's willingness to report:

H5a. A person's increased trusting beliefs in the report-receiving authority increases his or her willingness to report computer abuse.

Further building on H5a, substantial literature shows that trust can be highly influenced with the degree to which one has a disposition to trust others (McKnight *et al.* 2002; McKnight *et al.* 1998). Thus, for purposes of nomological validity, we replicate the following:

H5b. A person's increased disposition to trust increases his or her trusting beliefs.

Adding Anonymity and Public Self-Awareness to the Model (H6)

As our final major extension, seminal theory on whistle-blowing points to anonymity as a highly promising factor that should affect an individual's an individual's calculation of risk (and trust) of whistle-blowing for a particular incident (Near & Miceli 1995). However, the concept of anonymity is addressed only superficially and is neither explicitly theorized nor adequately tested empirically in the whistle-blowing literature. Meanwhile, anonymity researchers have shown that in a social context there is a lot more to anonymity than simple lack of identification (Pinsonneault & Heppel 1998). For our conceptualization of anonymity, we rely on (Pinsonneault & Heppel 1998), who arguably provided the most robust conceptualization and measurement of anonymity in a system and social setting. We therefore define *anonymity* as the degree to which an individual feels free from social evaluation and from retaliation threats from the organization. Importantly, "anonymity can only significantly affect disinhibition, and other behaviors in general, when social evaluation is an important source of inhibition" (Pinsonneault & Heppel 1998). This conceptualization is particularly salient in a whistle-blowing context because of the potential for social impact and retaliation. Namely, anonymity is recognized as pivotal to whistleblowers' willingness to divulge information (Rains & Scott 2007).

(Pinsonneault & Heppel 1998) notion of anonymity is broken into five factors that we manipulate in our study: lack of identification, diffused responsibility, lack of proximity, lack of knowledge of others, and confidence in the system[6].

[6] *Lack of identification* refers to the inability of others to identify the individual based on his or her actions, comments, or ideas. *Diffused responsibility* refers to individual's perception that he or she is not more responsible for reporting the computer abuse, but rather that all members within a group are equally responsible. *Proximity* refers to the degree to which the individual feels that he or she is being

The socially grounded factors of anonymity are theorized to be highly effective because they promote disinhibition. *Disinhibition* occurs when one feels free to perform public behaviors, and it is predicted by the degree to which one experiences public and private self-awareness (Pinsonneault & Heppel 1998).

Private self-awareness refers to an individual's focus on the internal aspects of his or her self (Pinsonneault & Heppel 1998). These internal aspects may include perceptions, thoughts, feelings, standards, or values (Diener *et al.* 1976; Pinsonneault & Heppel 1998; Prentice-Dunn & Rogers 1982). If individuals feel low levels of private self-awareness, they are likely to experience *deindividuation*, which refers to the transformation of a group of individuals into a united entity that seems to respond as one collective mind. When individuals are deindividuated they become immersed in the group and are less able to regulate their own behaviors based on their own internal processes, standards, and values, but instead rely upon the decisions of the collective group (Diener *et al.* 1976; Prentice-Dunn & Rogers 1982). Group member behaviors are thus regulated based on group, rather than individual, internal norms and standards.

Public self-awareness refers to an individual's focus on himself or herself as a social object and the individual's concern with the individual's appearance and impression in the social situation of the group (Prentice-Dunn & Rogers 1982). An individual who is publicly self-aware places greater importance on being positively evaluated and judged by others within the given group (Abrams & Brown 1989). Individuals experiencing low public self-awareness will be less concerned with the group's social standards and less susceptible to pressures resulting from conformity and social evaluations (Pinsonneault & Heppel 1998). This decrease in social pressure causes the individual not to expect retaliation, censure, or other negative outcomes and thus he or she will behave in a disinhibited manner (Diener 1977; Diener *et al.* 1976).

Given this background, it is important to emphasize that the less people feel their comments can be identified, the more they feel a lack of direct responsibility for their comments (Diener 1977; Diener *et al.* 1976), the further away they are from other socially relevant people , the less that others know personally relevant

---

observed by others (*e.g.*, peers, supervisors, external agents). *Knowledge of other Group members* refers to the idea that others within the group could more easily identify the individual due to their deep interaction history and thus, individuals have a perception that others can more readily identify him or her based on small nuanced characteristics that are difficult to occlude. *Confidence in the system* refers to the individual's relative experience with the reporting tool and thus reflects the individual's perception that he or she can successfully use the tool for its intended purpose.

identifying information about them (Postmes & Spears 1998), and the more confidence they feel that a system will not reveal their identity, the more they will experience disinhibition through decreased public and private self-awareness (Postmes & Spears 1998). This disinhibition should decrease perceptions of risk of reporting computer abuse, especially as they relate to social risks and retaliation.

As individuals feel less private and public self-awareness, they have smaller expectations regarding potential negative outcomes of whistle-blowing—resulting in less overall perceived risk in whistle-blowing because there are smaller chances for retaliation and censure (Pinsonneault & Heppel 1998; Postmes & Spears 1998). We also posit that because of the negative relationship between trust and risk (Komiak & Benbasat 2006; Mayer *et al.* 1995; Nicolaou & McKnight 2006; Pavlou & Gefen 2005), anonymity will increase trust while decreasing risk. Conversely, an increased sense of public self-awareness increases perceived risks.

H6a. A person's increased perception of anonymity decreases his or her perceived risk of reporting computer abuse.

H6b. A person's increased perception of anonymity increases his or her trusting beliefs in the report-receiving authority.

H6c. A person's increased perception of public self-awareness increases his or her perceived risk of reporting computer abuse.

A highly related aspect of anonymity and trust in online environments that is coming to light in research is trust in the IT artifact used to share sensitive information and how beliefs regarding anonymity relate to this form of trust (*e.g.*, Vance 2008). Trust in the IT artifact means that "one securely depends or relies on the technology instead of trying to control the technology" (McKnight 2005).

Trust in the IT artifact is formed in a variety of ways. User perceptions of system quality increase trust in the IT artifact (Vance *et al.* 2008), as well as increase perceived ease of use (Gefen *et al.* 2003; Vance *et al.* 2008). Further, trust increases when the user believes the system "to have the functionality or functional capability to do some task the trustor wants done," and consistently and reliably performs "what it is designed to do without frequent 'crashing,' delays, or unexpected results" (McKnight 2005).

In our context, anonymity is a crucial capability for whistle-blowing systems because anonymity is pivotal to whistle-blower's willingness to divulge

information (Rains & Scott 2007). With the risks of identification being so high—including job loss, ostracism, and threats (Gundlach *et al.* 2003; Miceli & Near 1985; Miceli & Near 1984)—users must substantially trust or securely depend on the whistle-blowing system before they will use the system.

Given this theoretical support, we hypothesize that users' perceptions of the degree or quality of anonymity provided by the whistle-blowing system will increase their trust in the system. A perception that the whistle-blowing process is anonymous will necessarily include the belief that the reporting tool used to anonymize the reported information is trustworthy, that is, reliable and dependable in its functionality (McKnight 2005). Accordingly, we hypothesize:

H6d. Anonymity increases trust in the reporting tool.

5.3.2 Covariates for Whether a Problem Ought to Be Reported

As a final extension of our model, we further describe covariates that are most likely to predict a person's assessment that computer abuse ought to be reported. Because of the critical connection in the literature between a user feeling a problem ought to be reported and feeling responsibility to report, we carefully reviewed the literature for factors that would further encourage someone to feel that a problem ought to be reported, and thus have an increased sense of responsibility to report the problem. One general factor reported throughout the literature relates to an individual's general experience. The more experience a person has, as manifested by age and educational level (Smith & Keil 2003) or organization tenure or work experience (Near & Miceli 1995; Rothwell & Baldwin 2006), the more that person feels a problem should be reported and will feel responsible for whistle-blowing. Potential reasons for this connection with experience are increased organizational loyalty, more knowledge or awareness of what happens when problems are not reported, and generally increased maturity associated with increased felt responsibility. Further, these types of employees tend to have more power, resources, and status, all of which enable them to believe that they could withstand any potential retaliation from the organization (Smith & Keil 2003). Hence, we predict the following:

H7. Age (a), education (b), and work experience (c) increase a person's assessment that a computer abuse scenario ought to be reported.

Another key factor suggested in the literature is that of a person's ethical viewpoints. Some researchers have investigated the influence of an organization's ethical climate, but it was not found to be a reliable determinant of reporting behavior (Rothwell & Baldwin 2006). However, ethics-based research has found that an individual's ethical disposition is a strong determinant of behavior. Likewise, whistle-blowing literature witnessed similar findings in that those with a propensity for deontological reasoning (*e.g.*, formalism) would be more ethically sensitive to what ought to be reported and thus more willing to report an incident (Arnold & Ponemon 1991; Smith & Keil 2003). Likewise, religious views are likely to influence these ethical viewpoints (Smith & Keil 2003), but we believe consideration of ethics itself is more than sufficient, as we are not concerned with the source of these ethical viewpoints. Because formalism is the most dominant operationalization of deontological reasoning in the literature, we predict the following:

> *H7d. A disposition toward ethical formalism increases a person's assessment that a computer abuse scenario ought to be reported.*

A final, and perhaps most important, factor that we include is the impact of the risk of the potential computer abuse to the organization itself (Miceli & Near 1985; Near & Miceli 1995). In our model, the more risky the computer abuse is to an organization (in terms of potential loss), the more likely it is that the organization will emphasize computer abuse prevention and will encourage members of the organization to want to prevent it (Miceli & Near 1985; Near & Miceli 1995). For example, an employee hacking into a computer to steal trade secrets is immensely more risky (in terms of costs to an organization) than an employee using the Internet during work hours to check his or her investment portfolio. Clearly, an organization would find it much more important to prevent the former than the latter.

Recent research has shown that the type of wrongdoing that occurs in an organization does differentially affect whether someone is willing to whistle-blow (Near *et al.* 2004). Preliminary evidence has provided some support for the idea that unethical behavior that is perceived to be more damaging to a group or organization is more likely to be reported than less damaging behavior (Trevino & Victor 1992). However, a key caveat in reporting wrongdoing is that, even if perceived wrongdoing has high potential cost to an organization, a person will not want to whistle-blow if he or she feels that the organization will not do anything about it (Near *et al.* 2004). Hence, a high-organizational-risk scenario may cause

a person to feel that a problem ought to be reported but *not* feel a personal responsibility to report if he or she works in an organizational climate where there is doubt that positive action will follow from whistle-blowing. In summary,

> *H7e. The riskiness of a computer abuse scenario increases a person's assessment that a computer abuse scenario ought to be reported.*

Figure 17 summaries our extended operational model with all proposed hypotheses.

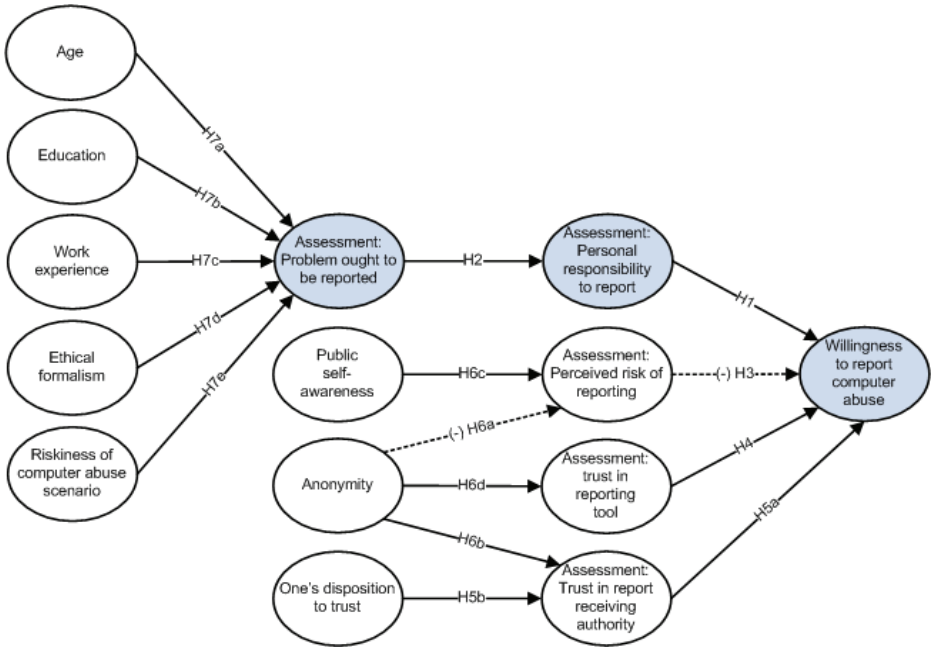

Fig. 17. Extended Operational Model of Whistle-blowing Computer Abuse.

5.4 Methodology

Our studies (one using university students and the other using full-time professionals) used a hypothetical scenario method (*i.e.*, vignette method), which is well established and accepted in studies involving questions of unethical, antisocial, and criminal behavior (Siponen & Vance 2010). This method is likewise well established in the IS field in studies of computer-related abuse and ethics issues (D'Arcy *et al.* 2009; Malhotra *et al.* 2004; Siponen & Vance 2010). A

thorough review by (Siponen & Vance 2010) established several strengths and advantages of the scenario method over tracking disclosures or actual behavior, including greater accuracy and validity.

A key methodological advantage of the scenario method for our study is its ability to indirectly measure intention. This is important in contexts of ethical behavior (such as whistle-blowing) in which participants are prone to respond in socially desirable ways or conceal their true tendencies (Trevino & Victor 1992). The scenarios describe the behavior of another person in hypothetical terms, thus making the reporting of intention less intimidating (Harrington 1996).

5.4.1 Scenario Design

To increase the generalizability of our research, we created two different sets of scenarios that were applied in two different studies: one for students in a hypothetical scenario of disclosing computer abuse through a specialized reporting system in a university setting, and another for professionals in a hypothetical scenario of disclosing computer abuse through a specialized reporting system in a professional setting. Our vignettes were carefully created to manipulate six independent variables with two conditions each (riskiness of scenario, privacy/identification, diffused responsibility, proximity, knowledge of others, and confidence in the reporting system) to represent a range of risk and various circumstances under which the reporting would occur. As a result, our manipulations represented a $2 \times 2 \times 2 \times 2 \times 2 \times 2$ design that generated 64 distinct vignettes. Every manipulation was truly randomized by our software to create one of 64 distinct vignettes for each participant. Table 17 describes the operationalization of each manipulation. Online Appendix 9 provides the full text for the scenarios.

Table 17. Operationalization of Each Manipulation.

Manipulation	Level Attenuating Reporting	Level Facilitating Reporting
Riskiness of the computer abuse scenario	High	Low
Privacy	Low (personal ID publicly revealed)	High (personal ID not revealed)
Diffusion of responsibility	High (low conveyed responsibility to report)	Low (high conveyed responsibility to report)
Proximity	Low (close proximity to participant's location)	High (distant from participant's location)
Knowledge of others	Study 1: High (small class) Study 2: High (portion of a department)	Study 1: Low (entire university) Study 2: Low (entire organization)
Confidence in reporting system	Low quality/confidence in the system	High quality/confidence in the system

5.4.2 Scenario Testing and Pilot Test

Two rounds of data collection and expert analysis were conducted to create appropriate scenarios that could be used to realistically manipulate our IVs. We first adapted scenarios from (Siponen & Vance 2010) to create a list of risky computer abuse scenarios. We then had 15 graduate students use the risk scale from our study to rate the degree to which they believed each scenario was risky. We chose the two scenarios that were deemed to be the statistically least and /most risky from this study. We also created wording to represent the five levels of anonymity that we manipulated, according to the theory and instrumentation set forth by (Pinsonneault & Heppel 1998). We had five experts review these manipulations to ensure that the manipulations were true to the underlying theoretical meaning of the anonymity subconstructs. We also adopted several of the experts' helpful wording suggestions.

Once we believed that we had the appropriate manipulations, we conducted a pre-pilot test with 69 graduate students. The test included all the manipulations and instrumentation for each pilot tester. We specifically asked for any wording issues or points of confusion that needed to be rectified. We further tested the manipulations to make sure they were effective. All manipulations exhibited the predicted directionalities.

Once our final improvements were made, we pilot-tested the study using 148 graduate students at a large public university in the eastern United States. We

used this final pilot to validate the manipulations and to test factorial validity of the instrumentation (see next section).

5.4.3 Participants

After completing our full pilot test, we conducted two studies. The first involved 569 student volunteers at a large public university in the southwest United States. The students were enrolled in an introductory-level information systems course that was open to all students at the campus. All students volunteered to participate for minimal extra credit and for the chance to receive one of several gift cards. The second study involved a carefully selected, paid panel of online participants, who were selected by a professional market research and survey research firm. Using this firm, we were able to target 202 participants over age 24 who worked full-time in computer-based jobs (we commissioned 200 respondents, but two extra responses were received). Human-subjects approval was granted for the studies, and all protocols were carefully followed.

Online panels are used frequently, and are firmly established in behavioral research (Barchard & WIlliams 2008; Bennett & Robinson 2000; Birnbaum 2004). Collecting data through a paid market research firm offers several advantages for gaining high quality data from working professionals (Bennett & Robinson 2000). In the context of our study, complete anonymity was guaranteed, since we were never given the participants' names. According to (Bennett & Robinson 2000), anonymity is particularly useful because it is one of the requirements for obtaining honest, self-report responses to questions regarding sensitive subjects like internal computer abuse in the workplace (Bennett & Robinson 2000). Moreover, the Internet panel allows researchers examining topics of a sensitive nature (*e.g.*, internal computer abuse) to receive responses less inhibited by social desirability effects because anonymity is ensured (Bennett & Robinson 2000). Another advantage is that data collected over the Internet via a panel of respondents is more reflective of the broader population than is data collected in more restricted settings (*e.g.*, a college classroom, college alumni, one organization) (Barchard & WIlliams 2008; Birnbaum 2004).

Table 18 summarizes the descriptive statistics for the participants of the two studies.

Table 18. Descriptive Statistics of Participants in Study 1 and Study 2.

Sample	Average age (SD)	Average years work experience	Employment status	Male/Female %	Education level %
Study 1: 569 students	20.03 (2.67)	n/a	51.7% not employed 38.9% part-time 5.4% full-time	47.1%/48.7%	89.9% some college 5.4% undergraduate
Study 2: 202 working professionals	41.27 (13.43)	19.96 (13.47)	100% full-time	47.5%/52.0%	14.4% high school 37.8% some college 37.3% undergraduate 9.5% masters 1% Ph.D. / professional

5.4.4 Measures

Online Appendix 1 provides detail on the major scales we used in our study, all of which were taken from previously validated instruments (some with minor wording adjustments for context). In the pre-experiment data, we gathered background data on an individual's disposition to trust (McKnight *et al.* 2002), his or her propensity toward ethical and social risk-taking (Weber *et al.* 2002), and the degree to which he or she has tendencies toward ethical formalism (Schminke & Wells 1999). After the randomized scenarios were given to and processed by the participants, they filled out the post-experiment scales. These included risk beliefs of the scenario and risk beliefs of reporting the incident (Jarvenpaa & Tractinsky 1999; Malhotra *et al.* 2004), public self-awareness (Pinsonneault & Heppel 1998), the five anonymity subconstructs (Pinsonneault & Heppel 1998), belief that the problem ought to be reported (Park *et al.* 2008), perceived responsibility to report the incident (Park *et al.* 2008), willingness to report the incident (Park *et al.* 2008), trusting beliefs (McKnight *et al.* 2002), and trust in the computer-abuse reporting tool (Grazioli & Jarvenpaa 2000), which was gathered in the second study only.

5.5 Data Analysis

Online Appendix 2 documents the analyses we performed to test common methods bias, mediation, moderation, and other validation criteria. The results of these tests demonstrate that our model meets or exceeds the rigorous standards expected for positivist IS research (Straub *et al.* 2004).

Partial Least Squares (PLS) was used to analyze our model using PLS-Graph 3.0. PLS was chosen because of its ability to analyze second-order formative constructs (our model included two: *anonymity* and *trusting beliefs*). In contrast, this form of construct is problematic for covariance-based SEM techniques (Chin 1998). Table 19 summarizes the hypotheses, path coefficients, and *t*-values for both studies. Figure 18 and Figure 19 depict the results of both studies (again, trust in the reporting tool was collected in the professional study only). Tables A8.5A and A8.5B summarize the measurement model statistics for both studies. Finally, to demonstrate the increase in R^2 in willingness to report provided by our newly proposed model, as compared to the traditional whistle-blowing model seen in Figure 1, we also ran both sets of data with the traditional model; the results are summarized in Figure 20 and Figure 21.

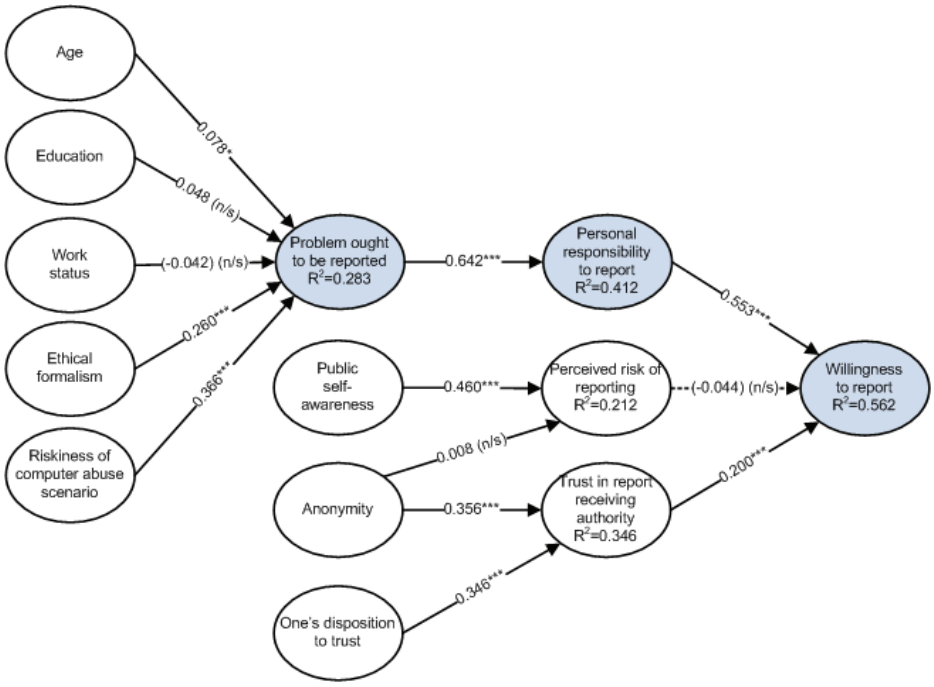

Fig. 18. Study 1 Student Model Results.

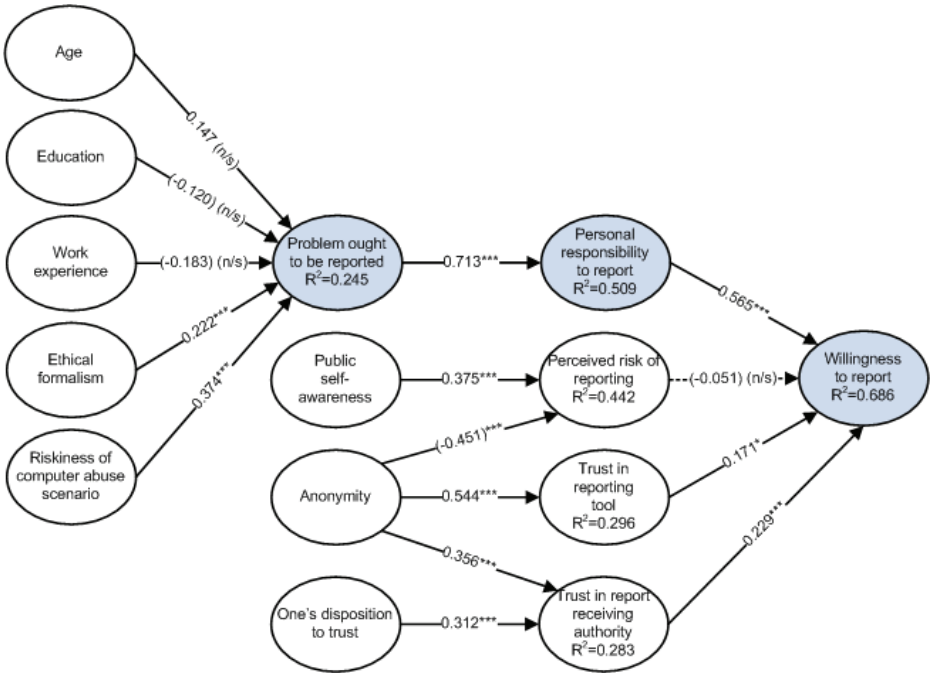

Fig. 19. Study 2 Professional Model Results.

Fig. 20. Study 1 Students with Traditional Whistle-blowing Model.

Fig. 21. Study 2 Professionals with Traditional Whistle-blowing Model.

5.6 Discussion

5.6.1 Summary of Results

Our theoretical model, which extends whistle-blowing theory with concepts of anonymity, risk, and trust, was tested in two studies—one involving student participants and the other involving professional participants—that provided highly consistent results. We showed that increased felt responsibility increased willingness to whistle-blow (H1); increased feelings that an incident ought to be reported increased felt responsibility to whistle-blow (H2); increased trust toward the tool used for whistle-blowing increased willingness to whistle-blow (H4); increased trust in the report-receiving authority increased willingness to whistle-blow (H5a); increased disposition to trust increased trust in the report-receiving authority (H5b); increased perceptions of anonymity increased trust in the report-receiving authority (H6b) and trust in the reporting tool (h6d); increased public self-awareness increased perceived risk of reporting (H6c); increased disposition toward formalism increased the feelings that an incident ought to be reported (H7d); and increased perceived riskiness of the violation scenario increased the feelings that an incident ought to be reported (H7e).

In terms of mixed results, anonymity did not decrease the perceived risk of reporting in the student study (H6a); in contrast, anonymity dramatically decreased the perceived risk of reporting in the professional study (H6a). Only in Study 1 was age shown to be a factor that increased an individual's feelings that an incident ought to be reported; however, the β of this relationship was only 0.078, which calls into question how meaningful this finding is, per (Chin 1998). Finally, while in both studies the perceived riskiness of the scenario increased participants' feelings that an incident ought to be reported (H7e), in both cases, perceived personal risk of reporting did not decrease an individual's willingness to whistle-blow (H3).

Table 19. Summary of Hypotheses, Path Coefficients, and Significance Levels.

Tested paths	Study 1 (Students)			Study 2 (Professionals)		
	Path coef.	t-value	Support?	Path coef.	t-value	Support?
Hypotheses						
H1. Responsibility → Willingness	0.553	16.43***	Yes	0.565	9.95***	Yes
H2. Ought → Responsibility	0.642	20.60***	Yes	0.713	18.47***	Yes
H3. Perceived risk of reporting (-) → Willingness	(-0.044)	1.33(n/s)	No	(-0.051)	1.09(n/s)	No
H4. Trust in reporting tool → Willingness	n/a	n/a	n/a	0.171	2.47*	Yes
H5a. Trust in report-receiving authority → Willingness	0.200	4.64***	Yes	0.229	4.63***	Yes
H5b. Disposition to trust → Trust in report-receiving authority	0.346	8.39***	Yes	0.312	6.06***	Yes
H6a. Anonymity (-) → Perceived risk of reporting	0.008	0.10(n/s)	No	(-0.451)	5.83***	Yes
H6b. Anonymity → Trust in report-receiving authority	0.356	7.89***	Yes	0.356	5.92***	Yes
H6c. Public self-awareness → Perceived risk of reporting	0.460	12.29***	Yes	0.375	4.81***	Yes
H6d. Anonymity → Trust in reporting tool	n/a	n/a	n/a	0.544	10.71***	Yes
Exploratory Covariates						
H7a. Age → Ought	0.078	2.28*	Yes	0.147	1.45(n/s)	No
H7b. Education →Ought	0.048	1.02(n/s)	No	(-0.120)	1.90(n/s)	No
H7c. Work years → Ought	(-0.042)	0.94(n/s)	No	(-0.183)	1.72(n/s)	No
H7d. Formalism → Ought	0.260	6.03***	Yes	0.222	3.65***	Yes
H7de. Riskiness of scenario → Ought	0.366	9.39***	Yes	0.374	7.10***	Yes

*** p < .001; ** p < .01; * p < .05; ns — not significant

5.6.2 Contributions to Research

A key contribution of this study is our extension of the traditional whistle-blowing model in a computer-abuse context that provides a better overall explanation for why someone would be willing to whistle-blow computer-abuse incidents. We also do so in the context of anonymous, whistle blowing tools, which are increasingly used because of the Sarbanes-Oxley Act and other similar international acts that require whistle-blowing mechanisms in the workplace. Specifically, we tested our data using the traditional whistle-blowing model depicted in Figure 15 and with our extended model, so that we could compare the increase in R^2 resulting from our improved model, which clearly demonstrated highly meaningful increases in explanatory power: The R^2 for willingness to report in the basic student model was 0.481 and the R^2 for the final student model was 0.562; resulting in a 17% increase in explanatory power and a medium-to-large effect size ($f^2 = 0.19$) that was highly significant at $F_{(1,556)} = 105.45$, $p < 0.001$[7]. The R^2 for the basic professional model was 0.580 and the final R^2 was 0.686, resulting in an 18% increase in explanatory power and a large effect size ($f^2 = 0.35$) that was highly significant at $F_{(1,188)} = 65.80$, $p < 0.001$.

The addition of the anonymity construct was a factor that was widely acknowledged as important but never explicitly theorized and tested for whistle-blowing. We went far beyond the traditional conceptualization of anonymity as a dichotomous construct to a rich, social second-order construct that includes lack of identification, diffused responsibility, lack of proximity, lack of knowledge of others, and confidence in the system (Pinsonneault & Heppel 1998). This conceptualization of anonymity is particularly useful in our context because the decision of whether to whistle-blow or not requires substantial trust in and becoming vulnerable to another party. Thus, a major contribution of this study is theorizing and providing empirical support for the influence of perceived anonymity on trusting beliefs in this context.

A further contribution of our model is its demonstrated effect of trust on users' willingness to blow the whistle. We conceptualized trust as two distinct constructs: (1) trust in the report-receiving authority and (2) trust in the IT artifact used to make the whistle-blowing report. Our results showed that not only are these two

[7] Significance was calculated using a pseudo F test as demonstrated by \citet{Mathieson:2001fv}; where F is calculated as follows: $F = f^2*(n-k-1)$ where k is number of independent constructs, n is sample size; at 1 and n-k degrees of freedom.

forms of trust empirically distinct, but they also each contribute significantly to willingness to report. Both forms of trust thus meaningfully extend the whistle-blowing model in explaining users' willingness to report.

The impact of trust in the IT artifact is particularly interesting given that it is under the full control of designers and can perhaps be most easily improved. In order to increase trust in the IT artifact, reliability, dependability, and quality in the user interface are integral—"the entire system infrastructure should demonstrate quality, for deficient software at one level may hurt perceptions at several levels" (McKnight 2005).

Finally, because virtually all social decisions involve elements of risk, we expanded traditional whistle-blowing theory to include factors related to risk. First, we considered a person's perceptions of personal risk in willingness to whistle-blow and found that it was not a significant factor. However, the degree to which an incident was seen as risky in general, had a powerful effect on an individual's feelings that an incident ought to be reported. In this manner, we were able to tease out the differential effects of risk to oneself and risk to an individual's organization, and found that perceived risk to an individual's organization was the more important factor. We also found that the social construct of public self-awareness, grounded in (Pinsonneault & Heppel 1998), directly increased an individual's perceived risk of whistle-blowing.

We summarize the positive and negative factors that were supported in both of our studies in Table 20. Figure 22 summarizes our modified, proposed model that is based on the supported results.

Table 20. Factors that Affect an Individual's Willingness to Whistle-blow Computer Abuse.

Major factor/relationship that affects the model	Supported in Study 1 (students)?	Supported in Study 2 (professionals)?
Positive Factors		
Felt responsibility to report	Yes	Yes
Feeling the computer-abuse incident is serious enough that someone ought to report it	Yes	Yes
A propensity toward ethic formalism	Yes	Yes
Perceived riskiness of the computer abuse scenario	Yes	Yes
Trust in the authority that will receive the computer-abuse report	Yes	Yes
A trusting disposition	Yes	Yes
Anonymity increases trust in report-receiving authority	Yes	Yes

Major factor/relationship that affects the model	Supported in Study 1 (students)?	Supported in Study 2 (professionals)?
Age	Yes (but weak β)	No
Anonymity decreases perceived risk of reporting	No	Yes
Trust in the reporting system/tool	Not collected	Yes
Negative Factors		
Public self-awareness increases perceived risk of reporting	Yes	Yes

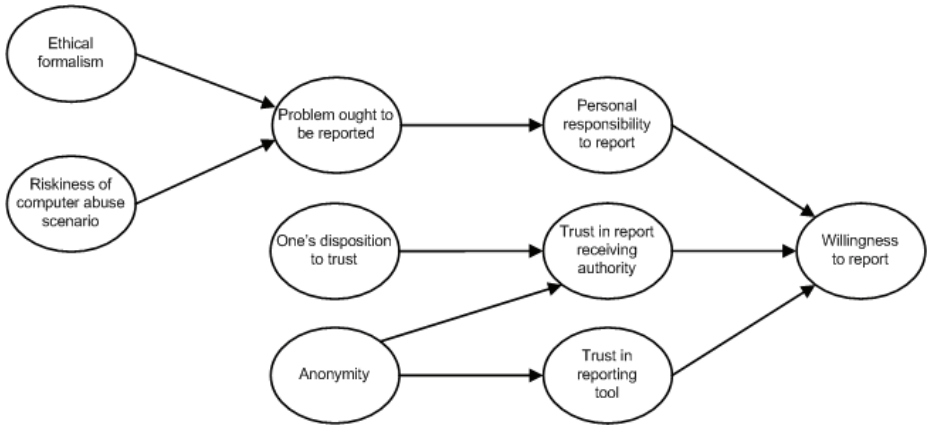

Fig. 22. Suggested Computer-abuse Whistle-blowing Model.

5.6.3 Implications for Practice

Our empirical results hold several implications for practice, beyond what was established in previous whistle-blowing research. First, the strong effect of perceived anonymity on users' willingness to report clearly highlights the importance of fostering ethically valid impressions of the anonymity of the whistle-blowing submission process and reporting tool among users (*e.g.*, incorporating a third-party reporting tool that in no way captures IP addresses or any unique user information). Because we demonstrate that anonymity comprises several facets, there are therefore several approaches to enhance the perceived anonymity beyond simply removing names or other basic identifiers from a report.

For example, the "proximity" component of anonymity suggests that practitioners can increase perceived anonymity by allowing individuals to access and file reports from the convenience of private locations (*e.g.*, from home, via

Internet). Similarly, the "knowledge of other group members" component suggests that practitioners should prevent peers of whistle-blowers from accessing reports, thereby precluding them from identifying whistle-blowers based on their knowledge of group members or familiarity with the situation. The subcomponent "diffused responsibility" indicates that practitioners should charge all members of organizations equally with the responsibility of reporting abuse, not just obvious organizational positions such as internal audit and middle management. In this way, the responsibility to whistle-blow will be diffused throughout the organization, further adding to users' perception of anonymity. The "confidence in the system" component suggests that practitioners should work to train users in the whistle-blowing tool, providing workshops and tutorials on how to submit or complete reports. Moreover, it is likely highly beneficial to use a proven, third-party vendor to provide a tool that is certified as never capturing user-related information (including IP addresses, work location, and to explicitly communicate this to end-users. This will help assure users of the anonymity provided by the whistle-blowing tool.

A second major set of implications for practitioners is the importance of trust in fostering willingness to blow the whistle, both in the report-receiving authority representing the organization and in the IT artifact used to whistle-blow. Because trust is built slowly over time (Lewicki & Wiethoff 2000), a trustor will rely on the reputation of the trustee. Thus, it is important to develop a reputation for being trustworthy. This trustworthiness is built through successive positive interactions with the report-receiving authority. For example, whistle-blowing reports should be handled in a predictable, reliable, fair, and consistent manner by the report-receiving authority. Thus, practitioners can increase trust in those receiving the reports by treating each reported incident equally, thoroughly investigating the report, and consistently applying sanctions to parties who are found to abuse the computer systems of the organization.

As a further implication for practice, the trust in the whistle-blowing tool can be developed through consistent and reliable availability to those who may report such incidents. If employees are unable to reliably access or use the tool, it is unlikely that they would trust such a tool to report incidents. Thus, all aspects of the reporting tool, including the user interface, should demonstrate high system quality to the user, as this will increase trust in the IT artifact (McKnight 2005). Again, this points to using a certified third party that specializes in hosting, securing, and delivering such tools, rather than building such a tool in-house.

Our empirical results additionally demonstrated that increased perceptions of anonymity substantially increased levels of trust in the report-receiving authority and the tool, suggesting that a promising way to increase trust in both the report-receiving authority and the whistle-blowing tool is through techniques that ensure anonymity. As practitioners work to improve perceptions of the various facets of anonymity, trust in the report-receiving authority and the reporting tool should increase. We suggest that such reporting tools could be perceived as even more reliable if their degree of anonymity and the security of their data-storage procedures can be verified and certified by an independent authority, which could be delivered through a formal IT risk assessment process and even a new third-party certification process similar to TRUSTe or Verisign.

Our results further corroborate those of previous research to indicate that one important way practitioners can encourage employees to blow the whistle is by reinforcing the notion of their ethical responsibility to report an incident. There are three ways to accomplish this. First, training employees regarding deontological reasoning (*i.e.*, formalism) to increase their sensitivity to ethical reasoning. This training can center specifically on the employees' personal responsibility to blow the whistle when they know about computer-abuse incidents. By personalizing internal messages about employee obligations to report misconduct, employees may have an increased perception that they should report incidents that they know about. Second, training employees regarding the impact of computer abuse on the organization and what constitutes computer abuse. By educating the employees about the riskiness of computer abuse, the perceived impact and risk for the organization would increase, and thereby increase the sense that if such an event were witnessed, the employee would see greater value in reporting it. Third, treating employees as valued, respected stakeholders who share in the successes and failures of an organization (*e.g.*, bonuses, equity ownership opportunities). That way, they are more likely to understand and care about the potential financial harm that can occur from various computer abuses.

5.6.4 Limitations and Future Research

There are several limitations in our study that give rise to future research possibilities. First and most challenging is that we did not examine actual computer-abuse incidents and reporting. Since data on actual whistle-blowing,

like other unethical behaviors, is difficult to collect using traditional techniques (Trevino & Victor 1992), such a study would most likely need to be conducted using secondary organizational data. Instead, we followed the standard practice of using hypothetical scenarios to measure ethical behavior (O' Fallon & Butterfield 2005).

As another limitation, an individual's personal perceptions of risk may play a bigger role in the overall model when it involves a real-life situation as opposed to a hypothetical scenario. Thus, we are hesitant to remove risk from our model, but do so given the current lack of empirical support for its inclusion. For example, if we were to simplify the professional model (removing trust and responsibility as predictors of willingness to whistle-blow), we would find that the β between perceived risk and the willingness to report would be highly significant at ($\beta = -0.419$, $t = 6.97$). However, the R^2 for willingness would only be 0.175. By adding the responsibility and trust factors, the R^2 dramatically increases for the overall model to 0.686 and the β for perceived risk become insignificant. Another possibility for this finding is that trust in the trust-receiving authority, trust in the reporting tool, and strong personal responsibility mitigate perceptions of risk. Experimental designs would be helpful in explicitly examining the effect of perceived risk under varying levels of trust and personal responsibility.

Likewise, moving beyond individual calculus and assessments, some people are more willing to take risks than others. Previous literature has stated that a person's propensity for taking risks can have a large impact on whether or not someone is willing to whistle-blow (Smith & Keil 2003). Thus, an individual's propensity toward risk taking would likely be a useful consideration for a future study.

An emerging literature further shows that trust and distrust are related, but separate constructs that are often important to consider together. Certainly, the possibility exists that organizational distrust could be a very strong, negative factor that prevents reporting of whistle-blowing, and thus should be considered in future research.

A further limitation of our research, based on (Near & Miceli 1995), is that while anonymity increases the likelihood that someone will want to whistle-blow, it can decrease the organizational effectiveness of whistle-blowing because anonymous complaints are not always taken seriously. However, with computer abuse, the accusations can typically be quickly and easily verified so anonymity

may not decrease the effectiveness of computer-abuse reporting, but this can only be verified in another study.

Aside from the factors we mentioned, there are several more possibilities in the literature that we did not consider, either because they were highly context-specific or because they involved atheoretical or exploratory demographic considerations. These potential factors could include organizational position (Near & Miceli 1996), job satisfaction (Smith & Keil 2003), organization climate (Smith & Keil 2003), and financial incentives.

5.7 Conclusion

Computer abuse is costly for organizations and a threat to their success (Straub 1990; Theoharidou *et al.* 2005; Vardi & Wiener 1996). Companies can reduce these losses through costly monitoring processes (Straub 1990), or they can train and rely on their employees to report incidents of misconduct through whistle-blowing (Miceli & Near 1984; Near & Miceli 1995). Although whistle-blowers can put themselves at risk by challenging the organization (Miceli & Near 1984), whistle-blowing continues to this day and is often reported in the modern press as firms struggle to achieve compliance with laws such as the Sarbanes-Oxley Act.

Thus study extends whistle-blowing theory to IS and expands the underlying model to include several other important variables. We show that individual perception that an incident should be reported is increased when individuals have increased levels of formalism and perceive that the incident is of high risk to the organization. Further, once an individual feels that an incident ought to be reported, we show that the likelihood to report is influenced by the individual's perception that the incident should be reported. Our study extends this model, and further shows that trust in the reporting tool and trust in those receiving the reported incidents are also powerful predictors of an individual's willingness to report a computer-abuse incident. Lastly, we show that by increasing the level of felt anonymity, individuals have increased levels of trust with both the reporting mechanisms and those receiving the report and thus are more likely to report, despite the level of personal risk that the individual feels by reporting the incident. Although we have explained a large amount of variance, there is room for future studies to consider other antecedents and consequences of whistle-blowing.

6 Conclusion

This dissertation examined deliberate behaviors that individuals knowingly perform that result in increased vulnerability towards IS-related threats. As security related behaviors can result in major problems for individuals and organizations (Curry 2005; Liang & Xue 2009; Theoharidou *et al.* 2005), understanding the motivations behind purposeful behaviors that increase these risks is an important endeavor for security research. However, little research has been reported on these security-related behaviors.

To address this gap in the literature these studies investigate different behaviors that have been under-investigated in IS security research using novel theories that provide distinct and important insights not offered by extant theories in the IS security research stream. Four separate studies are reported to better investigate these security-related behaviors that increase the individual's or the organization's vulnerability to technological threats. The four studies involve 1,430 total subjects, which represents one of the largest IS security-related studies to date.

6.1 Comparison of Studies

Each of the four studies, involving unique behaviors (*i.e.*, cyberloafing, anti-malware usage, omission of software development tests, and whistle-blowing) and theoretical perspectives (*i.e.*, the theory of interpersonal behavior, the extended parallel processing model, control balance theory, and whistle-blowing theory augmented with trust and anonymity research), offers distinct and novel contributions to the IS security research stream. Despite the different behaviors and theoretical perspectives, several similarities emerge from these studies.

6.1.1 Importance of Habit

Two of the reported studies signal that habit tends to be one of, if not the strongest predictor, of the indicated behavior. The study on cyberloafing reveals that habit is the strongest predictor of current cyberloafing behaviors, a finding that is sustained in the anti-malware application study. Given the relative ease of habit creation for these types of behaviors, this finding is important for research attempting to form methods to reduce the occurrence of such behaviors, as the habits must be addressed and reversed. Habits do not easily reverse and

interventions meant to reverse such behaviors need to carefully consider the motivations behind such habits.

6.1.2 Tenuous Effect of Controls and Constraints on Security-related Behaviors

Three of the studies include constructs that indicate that classical approaches to deterrence offer little to no effect on desired behaviors. The study on cyberloafing shows non-significant effects on the attitudes towards cyberloafing, while the study on anti-malware usage reveals that security-increasing behaviors are also not predicted by the costs or rewards associated with such behaviors. Lastly, the study on the omission of software development tests reveals that constraints associated with the desired behavior also have no effect on reducing the behavior. All three of these studies show that the classical approach, or the control approach to managing security-related behaviors has little influence on the behaviors studied in this dissertation.

6.1.3 Importance of Emotion

All of the studies greatly expand the IS security research by incorporating aspects of emotion into their models, and revealing that emotions are important concepts that should be considered when researching threat-related behaviors. Given that the concept of threat is closely related to fear, as supported by the EPPM (Witte 1992; Witte *et al.* 1996), security research should also be considering theories that integrate emotion into their models. Of importance, this dissertation highlights the relevancy of fear and trust for future security research. The EPPM study shows that fear is significantly predicted by threat, and as security-related behaviors are heavily influenced by threat, it is important to consider whether individuals engage in emotion-focused coping and experience fear.

Second, the study in whistle-blowing shows how trust may also have important implications for future security research. Both affective and cognitive trust exist (McKnight *et al.* 2002), and the importance of affective trust in security research is understudied. The whistle-blowing study, and the control balance study each highlight that trust in those controlling the individual is able to reduce if not remove all detrimental impacts of monitoring and controlling the individual.

Thus, future research should further explore how useful affective, and cognitive trusts have on predicting and motivating security-increasing behaviors.

6.2 Contributions

This dissertation makes several important general contributions to IS security research. First, this study makes an important contribution to this research stream by focusing on behaviors that intentionally increase the vulnerability to technology-related threats. As the majority of this research stream has focused on behaviors that protect the individual, this perspective is novel, and offers distinct insights that are not being discussed in extant literature. By focusing on these types of behaviors, this dissertation establishes the relevancy of this approach and how such behaviors are not easily deterred, are emotional, and ruled by habit.

Second, this dissertation indicates that the usage of novel theories in IS security research is an important contribution due to the novel insights that these theories provide to extant literature, and by expanding the nomological network of this research stream. The theories used in this dissertation highlight the importance of many constructs that have not been addressed in extant literature, namely: affect, social influence, control imbalance, fear, emotion-focused coping, trust, and anonymity. The introduction of these constructs and theories into IS security research advances our understanding of these behaviors, and introduces many important avenues for future research. Second, these theories produce novel insights into this research stream that were lacking, given the focus on classic deterrence theory (Gibbs 1975) and the protection motivation theory (Maddux & Rogers 1983; Rogers 1975).

TIB expands the current research stream by showing how habits, affect, attitudes and social influence are all important antecedents to security-relayed behaviors. All of these antecedent conditions are not present in extant security research and show how such constructs can be important for future research in this area. Further, interactive effect between intentions, facilitating conditions and habit is an entirely novel concept that shows how such antecedents may interact and produce nonlinear effects.

EPPM advances IS security research by introducing the concept of emotion-focused coping, an ancillary coping mechanism to the widely used protection-focused coping in PMT-based studies (Maddux & Rogers 1983; Rogers 1975). This theory calls attention to the emotional effects that may be induced by

perceived threats, and how individuals may focus entirely on the emotions, rather than protecting themselves from perceived threats.

CBT extends IS security research by presenting how control theory may have detrimental impacts on those being controlled, a concept that has been largely overlooked in IS research. Further, these detrimental effects show how such control imbalances may also result in increased likelihoods to engage in behaviors that result in more vulnerability from future threats. These behaviors are then not enacted to avoid emotions, or reactions to other antecedents, but as rational acts meant to achieve what is perceived as a more equitable environment for the individual.

The whistle-blowing theory, extended by trust, risk and anonymity research, highlights how security-related behaviors should also consider how trust and anonymity may also be important antecedents of such behaviors. Given that extant research has not incorporated the use of trust, risk or anonymity into their models, this research introduces how these constructs may further expand our understanding of why individuals engage in behaviors that ultimately create more risk in their lives.

6.3 Conclusion

This dissertation examines the intentional behaviors that increase the vulnerability that individuals and organizations experience when given security-related behaviors are performed. Extant research has generally ignored these types of behaviors.

To address this research gap, this dissertation specifically focuses on these vulnerability-increasing behaviors, and incorporates theoretical perspectives that have yet to be used in IS security research. Four studies are performed, which use a total of 1,430 subjects to test their respective models.

The four theoretical models were largely supported, which provides several important contributions for IS security research and practice. The results of this dissertation provide important contributions for security research and enhance our understanding of the deliberate behaviors that increase security-related vulnerabilities. Additionally, the usage of novel theoretical perspectives further enhances our understanding of these types of behaviors and provides unique perspectives that have been missing in extant security research. These findings have important implications for both IS security research and practice.

References

Aarts H, Paulussen T & Schaalma H (1997) Physical Exercise Habit: On the Conceptualization and Formation of Habitual Health Behaviours. Health Education Research 12(3): 363–374.

Aarts H, Verplanken B & van Knienberg A (1998) Predicting Behavior From Actions in the Past: Repeated Decision Making or a Matter of Habit? Journal of Applied Psychology 28(15): 1355–1374.

Abrahamsson P, Warsta J, Siponen M & Ronkainen J (2003) New Directions on Agile Methods: A Comparative Analisys. Proceedings of the IEEE International Conference on Software Engineering.

Abrams D & Brown R (1989) Self-consciousness and Social Identity: Self-regulation as a Group Member. Social Psychology Quarterly 52(4): 311–318.

Agrawal M & Chari K (2007) Software Effort Quality and Cycle Time: A Study of CMM Level 5 Projects. IEEE Transactions on Software Engineering 33(3): 145–156.

Ahonen JJ & Junttila T (2003) A Case Study on Quality-Affecting Problems in Software Engineering Projects. Proceedings of IEEE International Conference on Software–Science Technology & Engineering.

Ajzen I (1985) From Intentions to Actions: A Theory of Planned Behavior Action-control. From Cognitions to Behavior 11: 11–39.

Ajzen I & Fishbein M (1977) Attitude-behavior Relations: A Theoretical Analysis and Review of Empirical Research. Psychological Bulletin 84(5): 888–918.

Akers RL & Sellers CS (2004) Criminological Theories: Introduction Evaluation and Application. Los Angeles CA, Los Angeles Roxbury Publishing.

Anandarajan M (2002) Profiling Web Usage in the Workplace: A Behavior-Based Artificial Intelligence Approach. Journal of Management Information Systems 19(1): 243–266.

Anderson CL & Agarwal R (in press) Practicing Safe Computing: A Multi-method Empirical Examination of Home Computer Use Security Intentions. MIS Quarterly.

Anquetil N, de Oliveira KM, de Sousa KD & Dias MGB (2007) Software Maintenance Seen as a Knowledge Management Issue. Information and Software Technology 49(5): 515–529.

Appley MH (1991) Motivation Equilibration and Stress. Lincoln, NE: ,University of Nebraska Press.

Arnold DFS & Ponemon LA (1991) Internal Auditors' Perceptions of Whistle-Blowing and the Influence of Moral Reasoning: An Experiment Auditing. A Journal of Practice & Theory 10(2): 1–15.

Ashforth BE & Mael F (1989) Social Identity Theory and the Organization. Academy of Management Review 14(1): 20–39.

Aytes K & Connolly T (2004) Computer and Risky Computing Practices: A Rational Choice Perspective. Journal of Organizational and End User Computing 16(2): 22–40.

Baba ML (1999) Dangerous Liaisons: Trust Distrust and Information Technology in American Work Organizations. Human Organization 58(3): 331–346.

Bamberg S, Ajzen I & Schmidt P (2003) Choice of Travel Mode in the Theory of Planned Behavior: The Roles of Past Behavior Habit and Reasoned Action. Basic and Applied Social Psychology 25(3): 175–187.

Bamberg S & Schmidt P (2003) Incentives Morality or Habit? Predicting Students' Car Use for University Routes with the Models of Ajzen, Schwartz and Triandis. Environment and Behavior 35(2): 264–285.

Bandura A (1977) Self-Efficacy: Toward a Unifying Theory of Behavioral Change. Psychological Review 84(2): 191–215.

Bandura A (1969) Social-Learning Theory of Identificatory Processes. In: Goslin DA (ed) Handbook of socialization theory and research. Rand McNally & Company: 213–262.

Bandura A (1982) Self-Efficacy Mechanism in Human Agency. American Psychologist 37(2): 122–147.

Barchard KA & WIlliams J (2008) Practical Advice for Conducting Ethical Online Experiments and Questionnaires for United States. Psychologists Behavior Research Methods 40(3): 1111–1128.

Baron SW & Forde DR (2007) Street Youth Crime: A Test of Control Balance Theory. Justice Quarterly 24(2): 335–355.

Baskerville RL & Pries-Heje J (2001) A Multiple-theory Analysis of a Diffusion of Information Technology Case. Information Systems Journal 11(3): 181–212.

Baskerville RL & Pries-Heje J (2001) Racing the E-bomb: How the Internet is Redefining Information Systems Development Methodology Proceedings of the IFIP TC8/WG8 2 Working Conference on Realigning Research and Practice in Information Systems Development: The Social and Organizational Perspective: 49–68.

Baskerville RL & Pries-Heje J (2002) Information Systems development @ Internet Speed: A New Paradigm in the Making. Proceedings of ECIS: 6–8.

Baskerville RL & Pries-Heje J (2004) Short Cycle Time Systems Development. Information Systems Journal 14(3): 237–264.

Baskerville RL, Ramesh B, Levine L, Pries-Heje J & Slaughter SA (2003) Is internet-speed Software Development Different? IEEE Software 20(6): 70–77.

Beck K, Beedle M, van Bennekum A, Cockburn A, Fowler WCM, Grenning J, Highsmith J, Hunt A, Jeffries R, Kern J & others (2001) Manifesto for Agile Software Development. Agile Workgroup Cited 2011/5/5. URI: http://johnlevyconsultingcom /pdf/SB6–4_Agile_Manifestopdf/.

Bennett RJ & Robinson SL (2000) Development of a Measure of Workplace Deviance. Journal of Applied and Social Psychology 85(3): 349–360.

Bergeron F, Raymond L, Rivard S & Gara M-F (1995) Determinants of EIS Use: Testing a Behavioral Model. Decision Support Systems 14(2): 131–146.

Birnbaum MH (2004) Human Research and Data Collection via the Internet. Annual Review of Pscyhology 55(1): 803–822.

Blanchard AL & Henle CA (2008) Correlates of Different Forms of Cyberloafing: The Role of Norms and External Locus of Control. Computers in Human Behavior 24(3): 1067–1084.

Boss S & Galletta DF (2008) Scared Straight: An Empirical Comparison of Two Major Theoretical Models Explaining User Backups. Proceedings of ICIS.
Boudreau M-C, Gefen D & Straub DW (2001) Validation in Information Systems Research: A State-of-the-art Assessment. MIS Quarterly 25(1): 1–17.
Brooks FP (1987) No Silver Bullet: Essence and Accidents of Software Engineering. Computer 20(4): 10–19.
Brug J, de Vet E, de Nooijer J & Verplanken B (2006) Predicting Fruit Consumption: Cognitions Intention and Habits. Journal of Nutrition Education and Behavior 38(2): 73–81.
Bryant K & Campbell J (2005) An Empirical Study of User Practice in Password Security and Management. Proceedings of the ACIS.
Bunnell J, Podd J, Henderson R, Napler R & James M-K (1997) Cognitive Associative and Conventional Passwords: Recall and Guessing Rates. Computers & Security 16(7): 629–641.
Cassell J & Bickmore T (2000) External Manifestation of Trustworthiness in the Interface. Communications of the ACM 43(12): 50–56.
Chan M, Woon IMY & Kankanhalli A (2005) Perceptions of Information Security at the Workplace: Linking Information Security Climate to Compliant Behavior. Journal of Information Privacy and Security 1(3): 18–41.
Chang MK & Cheung W (2001) Determinants of the Intention to use Internet/WWW at Work: A Confirmatory Study. Information & Management 39(1): 1–14.
Chenoweth T, Minch R & Gattiker T (2009) Application of Protection Motivation Theory to Adoption of Protective Technologies. Proceedings of HICSS: 1–10.
Cheung MKC & Limayem M (2005) The Role of Habit in Information Systems Continuance: Examining the Evolving Relationship Between Intention and Usage. Proceedings of ICIS.
Cheung W, Chang MK & Lai VS (2000) Prediction of Internet and World Wide Web Usage at Work: A Test of an Extended Triandis Model. Decision Support Systems 30(1): 83–100.
Chin WW (1998) Commentary: Issues and Opinion on Structural Equation Modeling. MIS Quarterly 22(1): vii-xvi.
Chin WW, Marcolin BL & Newsted PR (2003) A Partial Least Squares Latent Variable Modeling Approach for Measuring Interaction Effects: Results from a Monte Carlo Simulation Study and an Electronic-Mail Emotion/Adoption Study. Information Systems Research 14(2): 189–217.
Cockburn A & Highsmith J (2001) Agile Software Development the People Factor. Computer 34(11): 131–133.
Cofer CN & Aley MH (1967) Motivation: Theory and Research. John Wiley.
Culnan MJ & Williams CC (2009) How Ethics Can Enhance Organizational Privacy: Lessons from the ChoicePoint and TJX Data Breaches. MIS Quarterly 33(4): 673–687.
Curry TR (2005) Integrating Motivating and Constraining Forces in Deviance Causation: A Test of Causal Chain Hypotheses in Control Balance Theory. Deviant Behavior 26(6): 571–599.

D'Arcy J & Hovav A (2007) Deterring Internal Information Systems Misuse. Communications of the ACM 50(10): 113–117.

D'Arcy J, Hovav A & Galletta DF (2009) User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. Information Systems Research 23(1): 79–98.

Diamantopoulos A & Winklhofer HM (2001) Index Construction with Formative Indicators: An Alternative to Scale Development. Journal of Marketing Research 38(2): 269–277.

Diener E (1977) Deindividuation: Causes and Consequences. Social Behavior and Personality 5(1): 143–155.

Diener E, Fraser S, Beaman A & Kelem R (1976) Effects of deindividuation variables on stealing among Halloween trick-or-treaters. Journal of Personality and Social Psychology 33(2): 178–183.

Dillard JP (1994) Rethinking the Study of Fear Aeals: An Emotional Perspective. Communication Theory 4(4): 295–321.

Dinev T & Hart P (2006) An Extended Privacy Calculus Model for E-Commerce Transactions. Information Systems Research 17(1): 61–80.

Dozier JB & Miceli MP (1985) Potential Predictors of Whistle-blowing: A Prosocial Behavior Perspective. Academy of Management Review 10(4): 823–836.

Ernst & Young (2009 European Fraud Survey 2009: Is Integrity a Causalty of the Downtown. Ernst & Young Report. Cited 2011/5/5. URI: http://wwweycom/UK/en/Services/Assurance/Fraud-Investigation---Dispute-Services/European-fraud-survey-2009/.

Farnworth M (1989) Theory Integration Versus Model Building. In: Messner SF, Krohn MD & Liska AE (eds) Theoretical integration in the study of deviance and crime. Albany, NY, State Univ of New York Press: 93–100.

Fishbein M & Ajzen I (1975) Belief Attitude Intention and Behavior: An Introduction to Theory and Research. Reading, MA, Addison-Wesley

Floyd DL, Prentice-Dunn S & Rogers RW (2000) A Meta-Analysis of Research on Protection Motivation Theory. Journal of Applied Social Psychology 30(2): 407–429.

Friedman B & Millett LI (2007) Reasoning about Computers as Moral Agents: A Research Note. Human Values and the Design of Computer Technology: 130–148.

Gagnon M-P, Godin G, Gane C, Fortin J-P, Lamothe L, Reinharz D & Cloutier A (2003) An Adaptation of the Theory of Interpersonal Behavior to the Study of Telemedicine Adoption by Physicians. International Journal of Medical Informatics 71(2–3): 103–115.

Galletta DF & Polak P (2003) An Empirical Investigation of Antecedents of Internet Abuse in the Workplace. SIG Workshop on HCI at ICIS: 47–51.

Gefen D, Karahanna E & Straub DW (2003) Trust and TAM in Online Shoing: An Integrated Model. MIS Quarterly 27(1): 51–90.

Gefen D & Straub DW (2005) A Practical Guide to Factorial Validity Using PLS-Graph: Tutorial and Annotated Example. Communications of the AIS 16(5): 91–109.

Gibbs JP (1975) Crime Punishment and Deterrence. Elsevier
Gibson VR & Senn JA (1989) System Structure and Software Maintenance Performance. Communications of the ACM 32(3): 347–358.
Gore TD & Bracken CC (2005) Testing the Theoretical Design of a Health Risk Message: Reexamining the Major Tenets of the Extended Parallel Process Model. Health Education & Behavior 21(1): 27–41.
Grazioli S & Jarvenpaa SL (2000) Perils of Internet Fraud: An Empirical Investigation of Deception and Trust with Experienced Internet Consumers. IEEE Transactions on Systems Man and Cybernetics-Part A: Systems and Humans 30(4): 395–410.
Gundlach MJ, Douglas SC & Martinko MJ (2003) The Decision to Blow the Whistle: A Social Information Processing Framework. Academy of Management Review 28(1): 107–123.
Harrington SJ (1996) The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions. MIS Quarterly 20(3): 257–278.
Harrison W (1992) An Entropy-Based Measure of Software Complexity. IEEE Transactions on Software Engineering 18(11): 1025–1029.
Herath T & Rao HR (2009) Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations. European Journal of Information Systems 18(1): 106–125.
Herath T & Rao HR (2009 Encouraging Information Security Behaviors in Organizations: Role of Penalties Pressures and Perceived Effectiveness. Decision Support Systems 47(1): 154–165.
Hickman M & Piquero AR (2001) Exploring the Relationships Between Gender Control Balance and Deviance. Deviant Behavior 22(4): 323–351.
Hickman M, Piquero AR, Lawton BA & Greene JR (2001) Applying Tittle's Control Balance Theory to Police Deviance Policing. An International Journal of Police Strategies and Management 84(4): 497–519.
Highsmith J (2002) Agile Software Development Ecosystems. Addison-Wesley.
Hinds PJ & Bailey DE (2003) Out of Sight Out of Sync: Understanding Conflict in Distributed Teams. Organization Science 14(6): 615–632.
Hinds PJ & Mortensen M (2005) Understanding Conflict in Geographically Distributed Teams: The Moderating Effects of Shared Context and Spontaneous Communication. Organization Science 16(3): 290–307.
Jarvenpaa SL & Tractinsky N (1999) Consumer Trust in an Internet Store: A Cross-Cultural Validation. Journal of Computer-Mediated Communication 5(2): 1–32.
Johnston AC & Warkentin M (2010) Fear Aeals and Information Security Behaviors: An Empirical Study. MIS Quarterly 34(3): 549–566.
Kafura D & Reddy GR (1987) The Use of Software Complexity Metrics in Software Maintenance. IEEE Transactions on Software Engineering 13(3): 335–343.
Kahneman D & Tversky A (1979) Prospect Theory: An Analysis of Decision Under Risk. Econometrica 47(2): 263–291.
Keil M (1995) Pulling the Plug: Software Project Management and the Problem of Project Escalation. MIS Quarterly 19(4): 421–447.

Keil M, Im GP & Mahring M (2007) Reporting Bad News on Software Projects: The Effects of Culturally Constituted Views of Face-saving. Information Systems Journal 17(1): 59–87.
Keil M, Mann J & Rai A (2000) Why Software Projects Escalate: An Empirical Analysis and Test of Four Theoretical Models. MIS Quarterly 24(4): 631–664.
Keil M & Robey D (1999) Turning Around Troubled Software Projects: An Exploratory Study of the Deescalation of Commitment to Failing Courses of Action. Journal of Management Information Systems 15(4): 63–87.
Kelley HH & Michela JL (1980) Attribution Theory and Research. Annual Review of Psychology 31(1): 457–501.
Kim SS & Malhotra NK (2005) A Longitudinal Model of Continued IS Use: An Integrative View of Four Mechanisms Underlying Postadoption Phenomena. Management Science 51(5): 741–755.
Kirsch LJ (1996) The Management of Complex Tasks in Organizations: Controlling the Systems Development Process. Organization Science 7(1): 1–21.
Kirsch LJ (1997) Portfolios of Control Modes and IS Project Management. Information Systems Research 8(3): 215–239.
Kirsch LJ (2004) Deploying Common Systems Globally: The Dynamics of Control. Information Systems Research 15(4): 374–395.
Kirsch LJ, Sambamurthy V, Ko D-G & Purvis RL (2002) Controlling Information Systems Development Projects: The View from the Client. Management Science 48(4): 484–498.
Kohlberg L (1984) The Psychology of Moral Development. New York, NY, Harper & Row.
Komiak SYX & Benbasat I (2006) The Effects of Personalization and Familiarity on Trust and Adoption of Recommendation Agents. MIS Quarterly 30(4): 941–960.
Lee SM, Lee S-G & Yoo S (2004) An Integrative Model of Computer Abuse Based on Social Control and General Deterrence Theories. Information & Management 41(6): 707–718.
Leone L, Perugini M & Ercolani AP (1999) A Comparison of Three Models of Attitude-behavior Relationships in the Studying Behavior Domain. European Journal of Social Psychology 29(2–3): 161–189.
Leventhal H (1970) Findings and Theory in the Study of Fear Communications. In: Berkowitz L (ed) Advances in experimental social psychology (volume 5). New York, NY, Academic Press: 119–186.
Leveson NG & Turner CS (1993) An Investigation of the Therac-25 Accidents. Computer 26(7): 18–41.
Lewicki RJ & Wiethoff C (2000) Trust Trust Development and Trust Repair. In: Deutsch M & Coleman PT (eds) Handbook of conflict resolution: theory and practice. San Fransisco, CA, Jossey-Bass: 92–119.
Liang H & Xue Y (2009) Avoidance of Information Technology Threats: A Theoretical Perspective. MIS Quarterly 33(1): 71–90.

Liang H & Xue Y (2010) Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. Journal of the Association for Information Systems 11(7): 394–413.

Lim VKG (2002) The IT Way of Loafing on the Job: Cyberloafing Neutralizing and Organizational Justice. Journal of Organizational Behavior 23(5): 675–694.

Lim VKG & Teo TSH (2005) Prevalence Perceived Seriousness Justification and Regulation of Cyberloafing in Singapore: An Exploratory Study. Information & Management 42(8): 1081–1093.

Lim VKG, Teo TSH & Loo GL (2002) How do I Loaf Here? Let me Count the Ways. Communications of the ACM 45(1): 66–70.

Limayem M & Hirt SG (2003) Force of Habit and Information Systems Usage: Theory and Initial Validation. Journal of the Association for Information Systems 4(1): 65–97.

Litvinoff J (2008) Most Computers Are Infected By Some Form of Virus or Spyware. Midweek May(7).

Loch K, Straub DW & Kamel S (2003) Diffusing the Internet in the Arab World: The Role of Social Norms and Technological Culturation. IEEE Transactions on Engineering Management 50(1): 45–63.

Lowry PB, Romano NCJ, Jenkins JL & Guthrie RW (2009) The CMC Interactivity Model: How Interactivity Enhances Communication Quality and Process Satisfaction in Lean-Media Groups. Journal of Management Information Systems 26(1): 155–195.

Madden TJ, Ellen PS & Ajzen I (1992) A Comparison of the Theory of Planned Behavior and the Theory of Reasoned Action. Personality and Social Psychology Bulletin 18(3): 3–9.

Maddux JE & Rogers RW (1983) Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change. Journal of Experimental Social Psychology 19(5): 469–479.

Malhotra NK, Kim SS & Agarwal J (2004) Internet Users' Information Privacy Concerns (IUIPC): The Construct the Scale and a Causal Model. Information Systems Research 15(4): 336–355.

Malle BF (1999) How People Explain Behavior: A New Theoretical Framework. Personality and Social Psychology Review 3(1): 23–48.

Manrique de Lara PZ (2007) Relationship between Organizational Justice and Cyberloafing in the Workplace: Has "Anomia" a Say in the Matter? CyberPsychology & Behavior 10(3): 464–470.

Marakas GM, Johnson RD & Clay PF (2007) The Evolving Nature of the Computer Self-efficacy Construct: An Empirical Investigation of Measurement Construction Validity Reliability and Stability Over Time. Journal of the Association for Information Systems 8(1): 16–46.

Martin R & Hewstone M (2001) Conformity and Independence in Groups: Majorities and Minorities. In: Hogg MA & Tindale RS (eds) Handbook of social psychology: group processes (chapter 9). Wiley Online Library: 209–234.

Martin RC (2003) Agile Software Development: Principles Patterns and Practices. Saddle River, NJ, Prentice Hall.

Mayer RC, Davis JH & Schoorman FD (1995) An Integrative Model of Organizational Trust. Academy of Management Review 20(3): 709–734.
McKnight DH (2005) Trust in Information Technology. In: Davis GB (ed) Encyclopedia of management. Malden, MA, Blackwell: 329–331.
McKnight DH, Choudhury V & Kacmar C (2002) Developing and Validating Trust Measures for e-Commerce: An Integrative Typology. Information Systems Research 13(3): 334–359.
McKnight DH, Cummings LL & Chervany NL (1998) Initial Trust Formation in New Organizational Relationships. Academy of Management Review 23(3): 473–490.
Mesa C (1999) The High Cost of Cyberslacking. Newsweek 134(48): 62–65.
Metzger MJ (2006) Effects of Site Vendor and Consumer Characteristics on Web Site Trust and Disclosure. Communications Research 33(1): 155–179.
Miceli MP & Near JP (1984) The Relationships Among Beliefs Organizational Position and Whistle-Blowing Status: A Discriminant Analysis. Academy of Management Journal 27(4): 687–705.
Miceli MP & Near JP (1985) Characteristics of Organizational Climate and Perceived Wrongdoing Associated with Whistle-Blowing Decisions. Personnel Psychology 38(3): 525–544.
Miceli MP & Near JP (1988) Individual and Situational Correlates of Whistle-Blowing. Personnel Psychology 41(2): 267–281.
Miller LL (2008) The Perils of Federalism: Race Poverty and the Politics of Crime Control. Oxford University Press.
Moor JH (1985) What is Computer Ethics. Metaphilosophy 16(4): 266–275.
Moore GC & Benbasat I (1991) Developing of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation. Information Systems Research 2(3): 192–222.
Muir BM (1987) Trust between Humans and Machines and the Design of Decision Aids. International Journal of Man Machine Studies 27(5–6): 527–539.
Mulder LB, van Dijk E, Cremer DD & Wilke HAM (2006) Undermining Trust and Cooperation: The Paradox of Sanctioning Systems in Social Dilemmas. Journal of Experimental Social Psychology 42(2): 147–162.
Myers MD & Newman M (2007) The Qualitative Interview in IS Research: Examining the Craft. Information & Organization 17(1): 2–26.
Myyry L, Siponen M, Pahnila S, Vartiainen T & Vance A (2009) What Levels of Moral Reasoning and Values Explain Adherence to Information Security Rules? An Empirical Study. European Journal of Information Systems 18(1): 126–139.
Nass C, Takayama L & Brave S (2006) Socializing Consistency: From Technical Homogeneity to Human Epitome. In: Zhang P, Schneiderman B & Galletta DF (eds) Human-computer interaction and management information systems—foundations advances in management information systems (chapter 17). ME Sharpe Inc: 373–392.

Near JP, Dworkin TM & Miceli MP (1993) Explaining the Whistle-Blowing Process: Suggestions from Power Theory and Justice Theory. Organization Science 4(3): 393–411.

Near JP & Miceli MP (1995) Effective Whistle-Blowing. Academy of Management Review 20(3): 679–708.

Near JP & Miceli MP (1996) Whistle-Blowing: Myth and Reality. Journal of Management 22(3): 507–526.

Near JP, Rehg MT, van Scotter JR & Miceli MP (2004 Does Type of Wrongdoing Affect the Whistle-Blowing Process? Business Ethics Quarterly 14(2): 219–242.

Ng B-Y, Kankanhalli A & Xu Y (2009) Studying Users' Computer Security Behavior: A Health Belief Perspective. Decision Support Systems 46(4): 815–825.

Ng B-Y & Rahim MA (2005) A Socio-Behavioral Study of Home Computer Users Intention to Practice Security. Proceedings of PACIS: 234–247.

Nicolaou AI & McKnight DH (2006) Perceived Information Quality in Data Exchanges: Effects on Risk Trust and Intention to Use. Information Systems Research 17(4): 332–351.

O' Fallon M & Butterfield K (2005) A Review of the Empirical Ethical Decision-making Literature: 1996–2003. Journal of Business Ethics 59(4): 375–413.

Osman A, Barrious FX, Osman JR, Schneekloth R & Troutman JA (1994) The Pain Anxiety Symptoms Scale: Psychometric Properties in a Community Sample. Journal of Behavioral Medicine 17(5): 511–522.

Ouchi WG & Maguire MA (1975) Organizational Control: Two Functions. Administrative Science Quarterly 20(4): 559–569.

Pablo AL, Sitkin SB & Jemison DB (1996) Acquisition Decision-making Processes: The Central Role of Risk. Journal of Management 22(5): 723–746.

Pahnila S, Siponen M & Mahmood A (2007) Employees' Behavior towards IS Security Policy Compliance. Proceedings of HICSS.

Panko RR & Beh HG (2002) Monitoring for Pornography and Sexual Harassment. Communications of the ACM 45(1): 84–87.

Park C, Im G & Keil M (2008) Overcoming the Mum Effect in IT Project Reporting: Impacts of Fault Responsibility and Time Urgency. Journal of the Association for Information Systems 9(7): 409–431.

Parker DB (1998) Fighting Computer Crime: A New Framework for Protecting Information. Wiley Inc.

Passos AM & Caetano A (2005 Exploring the Effects of Intragroup Conflict and Past Performance Feedback on Team Effectiveness. Journal of Managerial Psychology 30(3/4): 231–244.

Paternoster R & Simpson S (1996) Sanction Threats and Appeals to Morality: Testing a Rational Choice Model of Corporate Crime. Law & Society Review 30(3): 549–584.

Pavlou PA & Gefen D (2005) Psychological Contract Violation in Online Marketplaces: Antecedents Consequences and Moderating Role. Information Systems Research 16(4): 372–399.

Pavlou PA, Liang H & Xue Y (2007) Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-agent Perspective. MIS Quarterly 31(1): 105–136.

Pee LG, Woon IMY & Kankanhalli A (2008) Explaining Non-work-related Computing in the Workplace: A Comparison of Alternative Models. Information & Management 45(2): 120–130.

Pennington R, Wilcox HD & Grover V (2004) The Role of System Trust in Business-to-Consumer Transactions. Journal of Management Information Systems 20(3): 197–226.

Petter S, Straub DW & Rai A (2007) Specifying Formative Constructs in Information Systems Research. MIS Quarterly 31(4): 623–656.

Petty RE & Wegener DT (1998) Attitude Change: Multiple Roles for Persuasion Variables. The Handbook of Social Psychology 1(2): 323–390.

Piccoli G & Ives B (2003) Trust and the Unintended Effects of Behavioral Control in Virtual Teams. MIS Quarterly 27(3): 365–395.

Pinsonneault A & Heel N (1998) Anonymity in Group Suort Systems Research: A New Conceptualization Measure and Contingency Framework. Journal of Management Information Systems 14(3): 89–108.

Piquero AR & Hickman M (2003) Extending Tittle's Control Balance Theory to Account for Victimization. Criminal Justice and Behavior 30(3): 282–301.

Piquero AR & Hickman M (1999) An Empirical Test of Tittle's Control Balance Theory. Criminology 37(2): 319–342.

Piquero NL & Piquero AR (2006) Control Balance and Exploitative Corporate Crime. Criminology 44(2): 397–430.

Podsakoff PM, MacKenzie SB, Lee J-Y & Podsakoff NP (2003) Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies. Journal of Applied Psychology 88(5): 879–903.

Postmes T & Spears R (1998) Deindividuation and Antinormative Behavior: A Meta-Analysis. Psychological Bulletin 123(3): 238–259.

Prentice-Dunn S & Rogers RW (1986) Protection Motivation Theory and Preventive Health: Beyond the Health Belief Model. Health Education Research 1(3): 153–161.

Prentice-Dunn S & Rogers RW (1982) Effects of Public and Private Self-Awareness on Deindividuation and Aggression. Journal of Personality and Social Psychology 43(3): 503–513.

Qiu L & Benbasat I (2006) An Investigation in the Effects of Text-to-Speech Voice and 3D Avatars on the Quality of Live Help in Electronic Commerce. ACM Transactions on Computer-Human Interaction 12(4): 329–355.

Rains SA & Scott CR (2007) To Identify or not to Identify: A Theoretical Model of Receiver Responses to Anonymous Communication. Communication Theory 17(1): 61–91.

Reeves B & Nass C (1996) The Media Equation: How People Treat Computers, Television and New Media Like Real People and Places. CSLI Publications and Cambridge university Press.

Rhee H-S, Ryu Y & Kim C-T (2005) I Am Fine but You Are Not: Optimistic Bias and Illusion of Control on Information Security. Proceedings of ICIS: 381–394.
Ringle CM, Wende S & Will S (2005) SmartPLS (20 (M3) Beta.
Robinson SL & Weldon E (1993) Feedback Seeking in Groups: A Theoretical Perspective. British Journal of Social Psychology 32(1): 71–86.
Rogers P & Lea M (2005) Social Presence in Distributed Group Environments: The Role of Social Identity. Behaviour & Information Technology 24(2): 151–158.
Rogers RW (1975) A Protection Motivation Theory of Fear Appeals and Attitude Change. The Journal of Psychology 91(1): 93–114.
Roshier B (1989) Controlling Crime. Open University Press.
Rothwell GR & Baldwin JN (2006) Ethical Climates and Contextual Predictors of Whistle-Blowing. Review of Public Personnel and Administration 26(3): 216–244.
Schminke M & Wells D (1999) Group Processes and Performance and their Effects on Individuals' Ethical Frameworks. Journal of Business Ethics 18(4): 367–381.
Schoorman FD, Mayer RC & Davis JH (2007) An Integrative Model of Organizational Trust: Past Present And Future. Academy of Management Review 32(2): 344–354.
Seymour L & Nadasen K (2007) Web Access for IT Staff: A Developing World Perspective on Web Abuse. The Electronic Library 25(5): 543–557.
Sheard BH, Hartwick J & Warshaw PR (1988) The Theory of Reasoned Action: A Meta-Analysis of Past Research with Recommendations for Modifications and Future Research. Journal of Consumer Research 15(12): 325–343.
Siau K, Fui-Hoon F & Teng L (2002) Acceptable Internet Use Policy. Communications of the ACM 45(1): 75–79.
Simmers CA (2002) Aligning Internet Usage with Business Priorities. Communications of the ACM 45(1): 71–74.
Singer SI (1997) Review of Control Balance: Toward a General Theory of Deviance. American Sociological Review 26(4): 492–493.
Siponen M (2004) A Pragmatic Evaluation of the Theory of Information Ethics. Ethics and Information Technology 6(4): 279–290.
Siponen M, Baskerville RL & Heikka J (2006) A Design Theory for Secure Information Systems Design Methods. Journal of the Association for Information Systems 7(11): 725–770.
Siponen M, Karjalainen M & Sarker S (2010) Unearthing Social Mechanisms that Lead Employees to Violate IS Security Procedures: An Inductive Study. IFIP TC8/11 Security Conference.
Siponen M & Livari J (2006) Six Design Theories for IS Security Policies and Guidelines. Journal of the Association for Information Systems 7(7): 445–472.
Siponen M & Vance A (2010) Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. MIS Quarterly 34(1): 487–502.
Siponen M & Vartiainen T (2004) Unauthorized Copying of Software and Levels of Moral Development: A Literature Analysis and its Implications for Research and Practice. Information Systems Journal 14(4): 387–407.

Sitkin SB & Roth NL (1993) Explaining the Limited Effectiveness of Legalistic "Remedies" for Trust/Distrust. Organization Science 4(3): 367–392.
Smith HJ & Keil M (2003) The Reluctance to Report Bad News on Troubled Software Projects: A Theoretical Model. Information Systems Journal 13(1): 69–95.
Stanton J M (2002) Company Profile of the Frequent Internet User. Communications of the ACM 45(1): 55–59.
Staw BM, Sutton RI & Pelled LH (1994) Employee Positive Emotion and Favorable Outcomes at the Workplace. Organization Science 5(3): 51–71.
Sternthal B, Dholakia R & Leavitt C (1978) The Persuasive Effect of Source Credibility: Tests of Cognitive Response. The Journal of Consumer Research 4(4): 252–260.
Straub DW (1990) Effective IS Security. Information Systems Research 1(3): 255–276.
Straub DW (1989) Validating Instruments in MIS Research. MIS Quarterly 13(2): 147–169.
Straub DW, Boudreau M-C & Gefen D (2004) Validation Guidelines for IS Positivist Research. Communications of the AIS 13(24): 380–426.
Straub DW & Goodhue DL (1991) Security Concerns of Systems Users: A Study of Perceptions of the Adequacy of Security. Information & Management 20(1): 13–27.
Tanner JFJ, Day E & Crask MR (1989) Protection Motivation Theory: An Extension of Fear Appeals Theory in Communication. Journal of Business Research 19(4): 267–276.
Tanner JFJ, Hunt JB & Eright DR (1991) The Protection Motivation Model: A Normative Model of Fear Appeals. Journal of Marketing 55(3): 35–45.
Theoharidou M, Kokolakis S, Karyda M & Kiountouzis E (2005) The Insider Threat to Information Systems and the Effectiveness of ISO 17799. Computers & Security 24(6): 472–484.
Thornberry TP (1989) Reflections on the Advantages and Disadvantages of Theoretical Integration. In: Messner SF, Krohn MD & Liksa AE (eds) Theoretical integration in the study of deviance and crime. Albany, NY, State University Press of New York.
Tittle CR (1995) Control Balance: Toward a General Theory of Deviance. Westview Press.
Tittle CR (2004) Refining Control Balance Theory Theoretical. Criminology 8(4): 395–428.
Trevino LK & Victor B (1992) Peer Reporting of Unethical Behavior: A Social Context Perspective. Academy of Management Journal 35(1): 38–64.
Triandis H (1977) Interpersonal Behavior. Brooks/Cole Pub Co.
Turner JC (1985) Social Categorization and the Self-concept: A Social Cognitive. Theory of Group Advances in Group Processes 2: 77–121.
Urbaczewski A & Jessup LM (2002) Does Electronic Monitoring of Employee Internet Usage Work? Communications of the ACM 45(1): 80–83.
Valois P, Desharnais R & Godin G (1988) A Comparison of the Fishbein and Ajzen and Triandis Attiudinal Model for the Prediction of Exercise Intention and Behavior. Journal of Behavioral Medicine 11(5): 459–472.

Vance A, Elie-dit-cosaque C & Straub DW (2008) Examining Trust in IT Artifacts: The Effects of System Quality and Culture on Trust. Journal of Management Information Systems 24(4): 73–100.

Vardi Y & Wiener Y (1996) Misbehavior in Organizations: A Motivational Framework. Organization Science 7(2): 151–165.

Venkatesh V, Morris MG, Davis GB & Davis FD (2003) User Acceptance of Information Technology: Toward a Unified View. MIS Quarterly 27(3): 425–478.

Verplanken B (2006) Beyond Frequency: Habit as Mental Construct. British Journal of Social Psychology 45(3): 639–656.

Verplanken B & Aarts H (1999) Habit Attitude and Planned Behaviour: Is Habit an Empty Construct or an Interesting Case of Goal-Directed Automaticity? European Review of Social Psychology 10(1): 101–134.

Verplanken B, Aarts H & van Knienberg A (1997) Habit Information Acquisition and the Process of Making Travel Mode Choices. European Journal of Social Psychology 27(5): 539–560.

Verplanken B & Orbell S (2003) Reflections on Past Behavior: A Self-Report Index of Habit Strength. Journal of Applied Social Psychology 33(6): 1313–1330.

Wang W & Benbasat I (2005) Trust in and Adoption of Online Recommendation Agents. Journal of the Association for Information Systems 6(3): 72–101.

Wang W & Benbasat I (2008) Attributions of Trust in Decision Support Technologies: A Study of Recommendation Agents for E-Commerce. Journal of Management Information Systems 24(4): 249–273.

Weber EU, Blais A-R & Betz NE (2002) A Domain-specific Risk-attitude Scale: Measuring Risk Perceptions and Risk Behaviours. Journal of Behavioral Decision Making 15(4): 263–290.

Williams DJ & Noyes JM (2007) How Does our Perception of Risk Influence Decision-making? Implications for the Design of Risk Information. Theoretical Issues in Ergonomics Science 8(1): 1–35.

Willison R (2006) Understanding the Perpetration of Employee Computer Crime in the Organisational Context. Information and Organization 16(4): 304–324.

Willison R & Siponen M (2009) Overcoming the Insider: Reducing Employee Computer Crime through Situational Crime Prevention. Communications of the ACM 52(9): 133–137.

Witte K (1992) Putting the Fear Back into Fear Appeals: The Extended Parallel Process Model. Communication Monographs 59(4): 329–349.

Witte K, Cameron KA, McKeon JK & Berkowitz JM (1996) Predicting Risk Behaviors: Development and Validation of a Diagnostic Scale. Journal of Health Communications 1(4): 317–341.

Woon IMY & Pee LG (2004) Behavioral Factors Affecting Internet Abuse in the Workplace—An Empirical Investigation. Proceedings of SIGHCI Workshop at ICIS: 80–84.

Woon IMY, Tan G-W & Low R (2005) A Protection Motivation Theory Approach to Home Wireless Security. Proceedings of ICIS: 367–380.

Yasin R (2000) Web Slackers. Internet Week March(3). Cited 2011/5/5. URI: http://wwwinternetweekcom/lead/lead101599htm/.

Appendix 1 Instruments (Study 1)

All items are measured on a standard 7-point Likert scale (Strongly disagree to strongly agree), unless otherwise indicated.

Attitude (Pennington et al. *2004)*

1. Using the Internet at work for non-work reasons is a bad idea
2. Using the Internet at work for non-work reasons is a good idea
3. Using the Internet at work for non-work reasons is a ___ idea (Foolish idea to Wise idea)*[8]

Beliefs about Outcomes (Pee et al. *2008)*

Using Internet at work for non-work-related purposes will result in . . . (7-point scale: very unlikely–50% chance–very likely)

Penalties

1. Warnings
2. Reprimands
3. My Internet access privileges being restricted by the organization

Benefits

1. Saving my personal time using private Internet access
2. Saving my personal expense for using private Internet access
3. Convenience
4. More interesting work life
5. Increase in my work productivity

Evaluation of Outcomes (Pee et al. *2008)*

Evaluate each of the items in the list below as a penalty for using the Internet at work for non-work purposes: (7-point scale: very lenient–just right–very harsh)

[8] An '*' indicates that the item was reverse coded

Penalties

1. Warnings
2. Reprimands
3. My Internet access privileges being restricted by the organization

Benefits

1. Saving my personal time using private Internet access
2. Saving my personal expense for using private Internet access
3. Convenience
4. More interesting work life
5. Increase in my work productivity

Social Factors (Pee et al. *2008)*

Evaluate each item in the list below as pertaining to his/her/their approval of you using the Internet at work for non-work-related purposes: (7-point scale: very low–moderate–very high)

1. My family's
2. My friends' (outside of work)
3. My co-workers'
4. My immediate supervisor's
5. My IT department's
6. My top management's

Norms (Gagnon et al. *2003)*

1. My family would expect that I use the Internet at work for non-work purposes
2. My friends outside of work would expect that I use the Internet at work for non-work purposes
3. My clients would expect that I use the Internet at work for non-work purposes
4. My co-workers would expect that I use the Internet at work for non-work purposes

5. The IT department at work would expect that I use the Internet at work for non-work purposes
6. Top-level management would expect me to use the Internet at work for non-work purposes

Roles (Bamberg & Schmidt 2003)

1. For me as a employee of X it is (appropriate/not appropriate) to use the Internet at work for non-work purposes
2. Using the Internet at work for non-work purposes is (fitting/not fitting) my position as an employee of X
3. Due to my role at work it is (justified/not justified) to use the Internet for non-work related purposes

Self Concept (Gagnon et al. *2003)*

1. I would feel bad if I was not using the Internet at work for non-work purposes
2. Using the Internet at work for non-work purposes would be in my principles
3. It would be unacceptable to not use the Internet at work for non-work purposes

Affect (Pee et al. *2008)*

I feel that using Internet provided by the organization for non-work related purposes is…

1. Pleasant–unpleasant
2. Boring–interesting*
3. Gratifying-displeasing

Habit (Verplanken & Orbell 2003)

In regards to using the Internet at work for non-work related reasons, answer the following questions.

1. I do it frequently
2. I do it automatically.
3. I do it without having to consciously remember.

4. It makes me feel weird if I do not do it.
5. I do it without thinking.
6. It would require effort not to do it.
7. It belongs to my (daily, weekly, monthly) routine.
8. I start doing it before I realize I'm doing it.
9. I would find it hard not to do.
10. I have no need to think about doing it.
11. It's typically for "me."
12. I have been doing it for a long time.

Facilitating Conditions (Pee et al. *2008)*

In my organization (7-point scale: never–sometimes–very often)

1. My ability to use the Internet at work is high
2. My access to the Internet at work is high
3. The Internet connection at work is fast

Intention (Pee et al. *2008)*

1. I intend to use the Internet at work for non-work-related purposes in the future (strongly disagree–neutral–strongly agree)
2. I will use the Internet at work for non-work-related purposes in the future (7-point scale: very unlikely–50% chance–very likely)
3. I expect to use the Internet at work for non-work-related purposes in the future (strongly disagree–neutral–strongly agree)

Behavior (Pee et al. *2008)*

1. In general, I use the Internet at work for non-work-related purposes
2. I access the Internet at work for non-work-related purposes several times each day (7-point scale: very unlikely–50% chance–very likely)
3. I do not spend a significant amount of time on the Internet at work for non-work-related purposes*

Appendix 2 Supplementary Data Validation Procedures (Study 1)

This is not meant for publication in the journal, but can be included as an online appendix if desired. It is meant to aid the reviewers in the examination of this study.

Table A2.1. T-statistics for Convergent Validity of Reflective Constructs.

Latent Construct	Indicator	t-statistic	
Affect	affect1	69.326924	***
	affect2	57.225211	***
	affect3	48.335812	***
Attitude	att1	42.814446	***
	att2	68.042931	***
	att3	9.144617	***
Behavior	beh1	22.295051	***
	beh2	124.342415	***
	beh3	77.634387	***
Habit	habit1	20.214993	***
	habit2	17.57084	***
	habit3	16.133887	***
	habit4	13.346024	***
	habit5	13.407935	***
	habit6	14.014781	***
	habit7	36.226714	***
	habit8	9.266335	***
	habit9	13.768453	***
	habit10	0.411227	(d)
	habit11	36.262622	***
	habit12	22.293884	***
Intention	int1	45.749226	***
	int2	58.192053	***
	int3	103.147881	***
Roles	roles1	32.306926	***
	roles2	39.560337	***
	roles3	20.733938	***
Self-concept	sc1	13.415741	***
	sc2	29.835133	***
	sc3	54.090799	***

*** $p < .001$; (d) dropped item

Table A2.2 Discriminant Validity with Latent Scores of Reflective Indicators.

Indicator	Affect	Attitude	Behavior	Habit	Intention	Roles	Self Concept
affect1	0.948	0.568	0.682	0.651	0.643	0.640	0.745
affect2	0.944	0.512	0.613	0.581	0.560	0.606	0.676
affect3	0.946	0.510	0.611	0.595	0.562	0.606	0.720
att1	0.573	0.923	0.540	0.636	0.582	0.628	0.624
att2	0.506	0.936	0.523	0.586	0.613	0.679	0.631
att3	0.378	0.769	0.384	0.365	0.361	0.487	0.446
beh1	0.592	0.509	0.887	0.686	0.590	0.481	0.527
beh2	0.666	0.555	0.961	0.735	0.704	0.568	0.612
beh3	0.625	0.493	0.948	0.688	0.710	0.549	0.597
habit1	0.520	0.495	0.696	0.792	0.605	0.513	0.547
habit2	0.447	0.465	0.595	0.797	0.531	0.435	0.445
habit3	0.495	0.482	0.536	0.815	0.553	0.452	0.492
habit4	0.516	0.528	0.480	0.775	0.548	0.555	0.579
habit5	0.456	0.461	0.480	0.771	0.537	0.463	0.472
habit6	0.460	0.421	0.461	0.746	0.478	0.455	0.515
habit7	0.603	0.538	0.752	0.866	0.655	0.493	0.606
habit8	0.393	0.346	0.377	0.664	0.390	0.319	0.410
habit9	0.525	0.517	0.494	0.772	0.529	0.492	0.553
habit10	0.027	0.055	-0.062	0.050*	-0.012	0.064	0.047
habit11	0.588	0.549	0.721	0.879	0.674	0.516	0.574
habit12	0.566	0.548	0.742	0.823	0.805	0.546	0.593
int1	0.604	0.553	0.680	0.735	0.948	0.592	0.621
int2	0.581	0.566	0.662	0.684	0.960	0.630	0.617
int3	0.608	0.618	0.718	0.710	0.963	0.645	0.666
roles1	0.578	0.668	0.505	0.544	0.594	0.883	0.715
roles2	0.628	0.617	0.533	0.593	0.612	0.907	0.730
roles3	0.512	0.512	0.471	0.446	0.501	0.847	0.656
sc1	0.634	0.503	0.537	0.599	0.510	0.578	0.781
sc2	0.650	0.588	0.534	0.569	0.566	0.703	0.886
sc3	0.678	0.596	0.549	0.579	0.628	0.758	0.911

* item removed to improve discriminant validity

Table A2.3. Discriminant Validity Check through the Square Root of AVE.

Construct	Affect	Attitude	Behavior	Habit	Intention	Roles	Self Concept
Affect	0.946						
Attitude	0.562	0.879					
Behavior	0.674	0.557	0.932				
Habit	0.646	0.620	0.753	0.793			
Intention	0.625	0.607	0.718	0.741	0.957		
Roles	0.654	0.688	0.573	0.604	0.651	0.880	
Self Concept	0.756	0.656	0.622	0.668	0.664	0.798	0.861

The AVE square roots are represented as the bolded, diagonal elements. Off-diagonal elements in the table represent the correlations between the constructs. To establish discriminant validity, the diagonal elements must be greater than the off-diagonal elements for the same row and column (Staples *et al.* 1999).

Table A2.4 MTMM Method for Analysis of Formative Indicators.

Construct	#	(1)	(2)	(3)	(4)	(5)	Ben	(6)	(7)	(8)	Pen	(9)
evbelben1	(1)											
evbelben2	(2)	0.623										
evbelben3	(3)	0.307	0.197									
evbelben4	(4)	0.335	0.269	0.833								
evbelben5	(5)	0.273	0.202	0.710	0.721							
benefits	Ben	0.361*	0.201*	0.957	0.849	0.877						
evbelpen1	(6)	-0.087	0.010	-0.151	-0.033	-0.107	-0.151					
evbelpen2	(7)	-0.046	0.061	-0.124	0.003	-0.072	-0.119	0.948				
evbelpen3	(8)	-0.105	0.013	-0.129	-0.039	-0.133	-0.148	0.754	0.766			
penalties	Pen	-0.093	0.011	-0.152	-0.035	-0.116	-0.156	0.993	0.950	0.827		
norms1	(9)	0.202	0.168	0.451	0.408	0.361	0.448	-0.246	-0.236	-0.220	-0.251	
norms3	(10)	0.179	0.091	0.436	0.431	0.356	0.440	-0.238	-0.223	-0.202	-0.240	0.727
norms4	(11)	0.138	-0.004	0.284	0.302	0.274	0.309	-0.282	-0.234	-0.310	-0.298	0.571
norms5	(12)	0.136	0.001	0.273	0.280	0.300	0.312	-0.232	-0.195	-0.297	-0.252	0.584
norms	Norm	0.199	0.111	0.462	0.448	0.382	0.468	-0.274	-0.253	-0.248	-0.279	0.874
socfac1	(13)	0.199	0.100	0.490	0.396	0.443	0.511	-0.330	-0.329	-0.285	-0.334	0.449*
socfac2	(14)	0.188	0.088	0.525	0.429	0.432	0.530	-0.327	-0.314	-0.278	-0.330	0.444
socfac3	(15)	0.215	0.066	0.447	0.365	0.394	0.467	-0.277	-0.263	-0.282	-0.288	0.410
socfac4	(16)	0.193	-0.031	0.381	0.261	0.364	0.415	-0.341	-0.281	-0.268	-0.341	0.396
socfac5	(17)	0.086	-0.002	0.206	0.172	0.219	0.231	-0.239	-0.189	-0.233	-0.247	0.283
socfac6	(18)	0.106	-0.059	0.238	0.210	0.325	0.300	-0.273	-0.203	-0.271	-0.283	0.325
socfactors	Sfac	0.224	0.057	0.507	0.408	0.481	0.543	-0.375	-0.345	-0.342	-0.383	0.499
fc1	(19)	0.137	0.091	0.429	0.379	0.424	0.458	-0.191	-0.194	-0.254	-0.209	0.279
fc2	(20)	0.146	0.087	0.069	0.033	0.067	0.080	-0.104	-0.088	-0.061	-0.100	0.017
fc3	(21)	0.091	0.054	-0.005	-0.081	-0.063	-0.023	-0.105	-0.097	-0.089	-0.106	0.039
faccond	Fcon	-0.100	-0.056	0.094	0.128	0.110	0.100	0.050	0.033	-0.014	0.040	0.073

#	(10)	(11)	(12)	Norm	(13)	(14)	(15)	(16)	(17)	(18)	Sfac	(19)	(20)	(21)
(1)														
(2)														
(3)														
(4)														
(5)														
Ben														
(6)														
(7)														
(8)														
Pen														
(9)														
(10)														
(11)	0.676													
(12)	0.685	0.854												
Norm	0.959	0.766	0.752											
(13)	0.400	0.298	0.328	0.443										
(14)	0.481	0.340	0.326	0.496	0.882									
(15)	0.547	0.406	0.371	0.535	0.614	0.712								
(16)	0.470	0.424	0.412	0.487	0.502	0.548	0.690							
(17)	0.374	0.446	0.386	0.395	0.344	0.353	0.416	0.560						
(18)	0.396	0.391	0.436	0.413	0.376	0.382	0.452	0.637	0.767					
Sfac	0.545	0.447	0.455	0.571	0.881	0.856	0.839	0.776	0.609	0.671				
(19)	0.274	0.279	0.220	0.306	0.272	0.252	0.276	0.301	0.230	0.232	0.330			
(20)	0.032	0.050	0.024	0.033	0.027	0.036	0.068	0.122	0.097	0.055	0.070	0.171		
(21)	-0.009	-0.045	-0.018	0.001	0.009	0.017	0.077	0.098	-0.024	-0.008	0.038	0.150	0.479	
Fcon	0.072	0.068	0.062	0.080	0.070	0.053	0.019	-0.024	0.006	0.037	0.047	0.167*	0.914	-0.624

* Item dropped due to poor loading

Appendix 3 Instruments (Study 2)

Introductory Text: Usage of Malware Applications

Malware: is software designed to infiltrate a computer without the owner's informed consent. Software is considered malware based on the perceived intent of the creator rather than any particular features.

Malware includes computer viruses, worms, trojan horses, most rootkits, spyware, dishonest adware, crimeware, and other malicious and unwanted software.

Fear (Osman et al. *1994)*

1. The malware on my computer will never go away
2. Something terrible will happen with my computer due to the malware on it
3. Though malware is annoying and potentially harmful, I'm going to be OK
4. I am afraid of my information being sent to unknown persons
5. The malware on my computer will decrease with time
6. My computer has a serious malware problem
7. My computer might be seriously infected with malware
8. The amount of malware on my computer is terrifying
9. I am afraid of malware
10. My computer might become unusable due to malware
11. My computer might become slower due to malware

Threat (Witte et al. *1996)*

Severity of Threat

1. I believe that malware is a severe threat to my computer
2. I believe that malware is a serious threat to my computer
3. I believe that malware is significant threat to my computer

Susceptibility to Threat

1. I am at risk for getting malware on my computer
2. It is likely that I will get malware on my computer
3. It is possible that I will contract malware on my computer

Efficacy (Herath & Rao 2009)

1. I would feel comfortable using an anti-malware application on my own
2. If I wanted to, I could easily use an anti-malware application on my own.
3. I would be able to use an anti-malware application even if there was no one around to help me

Danger Control Responses (Witte et al. *1996)*

Intentions to use Anti-Malware Application

1. I intend to use an anti-malware application on my computer in the next month
2. I am likely to use an anti-malware application on my computer in the next month
3. I plan to use an anti-malware application on my computer in the next month

Existing Anti-Malware Application-related Behaviors

1. I currently use an anti-malware application on my computer
2. I consistently use an anti-malware application on my computer
3. I regularly use an anti-malware application on my computer

Fear Control Responses (Witte et al. *1996)*

Defense Avoidance

1. When I first heard about malware, my first instinct was to:
    a) "Want to" / "not want to" think about malware
    b) "Want to" / "not want to" do something to keep my computer from getting it

Reactance

1. To what degree do you:
    a) Think the message about malware is realistic
    b) Feel the message about malware not applicable to you
    c) Feel the message about malware is exaggerated
    d) Think the message about malware is overstated

Social Influence (Johnston & Warkentin 2010)

1. People who influence my behavior think that I should use an anti-malware application
2. In general, people I know have supported using an anti-malware application

Subjective Norm

1. My family members think I should use an anti-malware application
2. My friends think that I should use an anti-malware application
3. My colleagues at work or school think that I should use an anti-malware application

Descriptive Norm

1. I believe other computer users use an anti-malware application
2. I am convinced other computer users use an anti-malware application
3. It is likely that the majority of other computer users use an anti-malware application

Cost (Myyry et al. *2009)*

1. Finding an anti-malware application would be time consuming
2. Installing an anti-malware application would take work time
3. Using an anti-malware application would be time consuming
4. Operating an anti-malware application makes working on my computer more difficult

5. Using an anti-malware application inconveniences me while working on my computer
6. There are too many overheads associated with using an anti-malware application
7. Using an anti-malware application would require considerable investment of effort other than time

Benefit (Myyry et al. *2009)*

1. Not using an anti-malware application saves me time
2. Not using an anti-malware application saves me money
3. Not using an anti-malware application keeps me from being confused
4. Using an anti-malware application would slow down the speed of my access to the Internet
5. Using an anti-malware application would slow down my computer
6. Using an anti-malware application would interfere with other programs on my computer
7. Using an anti-malware application would limit the functionality of my Internet browser

Habits (Verplanken & Orbell 2003)

1. I do it frequently
2. I do it automatically.
3. I do it without having to consciously remember.
4. It makes me feel weird if I do not do it.
5. I do it without thinking.
6. It would require effort not to do it.
7. It belongs to my (daily, weekly, monthly) routine.
8. I start doing it before I realize I'm doing it.
9. I would find it hard not to do.
10. I have no need to think about doing it.
11. It's typically for "me."
12. I have been doing it for a long time.

Appendix 4 Supplementary Data Validation Procedures (Study 2)

This is not meant for publication in the journal, but can be included as an online appendix if desired. It is meant to aid the reviewers in the examination of this study.

Table A4.1. T-statistics for Convergent Validity of Reflective Constructs.

Latent Construct	Indicator	t-statistic
Avoidance	avd1	5.623 ***
	avd2	0.505 (d)
	avd3	0.505 (d)
Behavior	beh1	43.274 ***
	beh2	82.170 ***
	beh3	67.981 ***
Cost	cost1	1.360 (d)
	cost2	2.705 **
	cost3	2.852 **
	cost4	2.088 **
	cost5	1.822 *
	cost6	1.901 *
	cost7	2.722 **
Descriptive norm	dnorm1	18.737 ***
	dnorm2	19.313 ***
	dnorm3	17.525 ***
Efficacy	eff1	6.406 ***
	eff2	8.450 ***
	eff3	5.687 ***
Fear	fear1	1.596 (d)
	fear2	10.083 ***
	fear3	3.580 ***
	fear4	2.345 *
	fear5	1.382 (d)
	fear6	3.548 ***
	fear7	7.074 ***
	fear8	2.558 *
	fear9	8.240 ***
	fear10	8.554 ***
	fear11	1.287 (d)

Latent Construct	Indicator	t-statistic	
Habit	habit1	19.058	***
	habit2	10.711	***
	habit3	6.415	***
	habit4	13.693	***
	habit5	13.416	***
	habit6	7.600	***
	habit7	11.857	***
	habit8	9.496	***
	habit9	16.431	***
	habit10	4.455	***
	habit11	9.341	***
	habit12	16.836	***
Intention	int1	30.874	***
	int2	44.090	***
	int3	30.942	***
Reactance	ract1	4.202	***
	ract2	1.349	(d)
	ract3	1.357	(d)
	ract4	2.411	*
Reward	rew1	3.592	***
	rew2	3.198	**
	rew3	3.009	**
	rew4	2.058	*
	rew5	1.045	(d)
	rew6	1.237	(d)
	rew7	1.938	(d)
Severity	sev1	27.225	***
	sev2	28.932	***
	sev3	13.340	***
Social influence	sinf1	11.838	***
	sinf2	36.305	***
Susceptibility	susc1	15.135	***
	susc2	8.886	***
	susc3	10.174	***

*** $p < .001$; (d) dropped item

Table A4.2. Discriminant Validity with Latent Scores for Reflective Indicators.

Indicators	Avoidance	Behavior	Cost	Desc. Norm	Efficacy	Fear	Habit	Intention	Reactance	Reward	Severity	Social influence	Susceptibility
avd1	0.9966	0.2244	-0.0323	0.3373	0.2642	0.2389	0.1984	0.3199	-0.2421	-0.1617	0.1855	0.3684	0.2764
avd2	-0.2664*	-0.1215	0.1265	-0.0249	-0.1342	0.0275	-0.1129	-0.0414	0.2585	0.2595	0.0738	-0.0824	-0.0099
avd3	0.2664*	0.1215	-0.1265	0.0249	0.1342	-0.0275	0.1129	0.0414	-0.2585	-0.2595	-0.0738	0.0824	0.0099
beh1	0.2316	0.9315	-0.1466	0.4174	0.5520	0.0784	0.5082	0.5102	-0.0131	-0.2751	0.0837	0.4530	0.1156
beh2	0.1901	0.9591	-0.1929	0.4016	0.5143	0.0502	0.5559	0.4798	-0.0206	-0.3111	0.0627	0.4253	0.0991
beh3	0.2311	0.9438	-0.1828	0.4133	0.5312	0.0621	0.6286	0.5063	-0.0380	-0.2751	0.0926	0.4060	0.0940
cost1	0.2126	0.0072	0.3766*	0.2410	0.0787	0.3059	0.0671	0.0922	-0.1446	0.1527	0.3422	0.2133	0.2757
cost2	-0.0717	-0.2022	0.8568	-0.0788	-0.1912	0.2001	-0.0545	-0.1064	0.0824	0.4060	0.2933	-0.0156	0.0402
cost3	0.0461	-0.0956	0.6923	0.1318	-0.0844	0.1837	0.0080	-0.0721	0.0463	0.3503	0.2281	0.1259	0.1927
cost4	0.0341	-0.0293	0.5688*	0.1061	0.0201	0.3227	0.0621	-0.0653	-0.0215	0.3171	0.2293	0.1027	0.1999
cost5	-0.0948	-0.0297	0.5253*	-0.0155	-0.0381	0.2105	-0.0087	-0.1067	0.1407	0.3868	0.1739	0.0207	0.1202
cost6	-0.1023	-0.0417	0.5421*	-0.0003	-0.0163	0.0813	-0.0180	-0.1362	0.3062	0.5381	0.1354	-0.0347	0.0551
cost7	0.0097	-0.1345	0.7128	0.0671	-0.0833	0.2495	-0.0122	-0.0834	0.0048	0.3493	0.2052	0.0527	0.1139
dnorm1	0.3606	0.3594	-0.0156	0.8642	0.2071	0.1427	0.2634	0.2407	-0.1599	-0.1690	0.1731	0.4514	0.2819
dnorm2	0.2262	0.3925	0.0217	0.8442	0.2849	0.0963	0.3262	0.3173	-0.0559	-0.0398	0.2512	0.4604	0.2719
dnorm3	0.2656	0.3588	0.0375	0.8485	0.2388	0.0605	0.2905	0.2595	-0.1099	-0.0649	0.1242	0.4490	0.2506
eff1	0.2996	0.4987	-0.0274	0.3266	0.7387	0.2367	0.3497	0.4424	-0.2302	-0.2129	0.2324	0.3791	0.2117
eff2	0.1977	0.3374	-0.1276	0.1562	0.7925	-0.0357	0.2873	0.3863	-0.0383	-0.1249	0.0279	0.1964	0.0589
eff3	0.0907	0.4224	-0.2240	0.1338	0.7574	-0.1968	0.3978	0.4250	-0.0393	-0.0969	-0.1163	0.1916	-0.0294
fear1	-0.0003	-0.0525	0.2036	-0.0070	-0.1515	0.2815*	-0.0733	-0.1254	-0.0046	0.1383	0.1048	-0.0573	0.1005
fear2	0.2089	0.0911	0.2248	0.0712	0.0562	0.7281	0.1116	0.1116	-0.1742	0.0203	0.4547	0.1766	0.3168

Indicators	Avoidance	Behavior	Cost	Desc. Norm	Efficacy	Fear	Habit	Intention	Reactance	Reward	Severity	Social influence	Susceptibility
fear3	0.1393	0.0362	0.0386	-0.0007	0.0372	0.4973*	0.0681	-0.0226	-0.1663	-0.0720	0.2656	0.0471	0.0844
fear4	0.1941	0.0895	0.1382	0.1200	0.1134	0.4085*	0.0880	0.0525	-0.0064	0.0038	0.2460	0.1281	0.2175
fear5	0.0801	0.0580	0.0029	0.0272	0.0209	0.2383*	0.0193	0.0010	-0.1702	-0.1495	0.1399	0.0855	0.1337
fear6	-0.0011	0.0170	0.2047	0.0275	-0.0275	0.4919*	-0.0471	0.0664	0.0736	0.1679	0.2209	0.0773	0.2765
fear7	0.1386	0.0037	0.1598	0.0500	0.0116	0.6653	-0.0126	0.0001	0.0581	0.1061	0.3691	0.0841	0.3970
fear8	0.0109	-0.1018	0.1591	-0.0807	-0.1399	0.4277*	-0.0799	-0.1429	0.1070	0.1074	0.1012	-0.0009	0.1039
fear9	0.1534	-0.0288	0.2502	0.0844	-0.0897	0.6595	-0.0181	-0.0670	-0.0042	0.0210	0.5163	0.0461	0.2513
fear10	0.1350	0.1016	0.1304	0.1445	0.1332	0.6855	0.0905	0.0737	-0.0701	0.0237	0.5008	0.1579	0.2468
fear11	0.0732	0.0484	0.0342	0.0693	-0.0185	0.2633*	0.0585	0.0577	0.0463	-0.0230	0.1552	0.1096	0.0950
habit1	0.1826	0.5998	-0.0889	0.2911	0.4193	0.0512	0.7693	0.3805	-0.1060	-0.1474	0.0444	0.3626	0.0501
habit2	0.1505	0.4614	-0.0212	0.2770	0.3297	0.0843	0.6896	0.3055	-0.1230	-0.0955	0.0605	0.3169	0.0991
habit3	0.0253	0.2960	0.0115	0.1544	0.2265	-0.0449	0.5765*	0.2102	0.0715	0.0339	-0.0012	0.2083	-0.0549
habit4	0.0626	0.3679	0.0455	0.1965	0.3217	-0.0225	0.7462	0.2420	-0.0567	-0.0136	0.0045	0.2517	-0.0363
habit5	0.1610	0.3762	-0.0640	0.2792	0.3505	-0.0031	0.7481	0.2756	-0.0279	-0.1266	0.0170	0.2919	0.0352
habit6	0.0383	0.2743	-0.0063	0.1611	0.2230	-0.0102	0.6346*	0.1814	0.0579	0.0034	0.0182	0.1787	-0.0815
habit7	0.1348	0.4428	-0.0495	0.1872	0.3228	0.0909	0.7405	0.2628	-0.0035	-0.1073	0.0077	0.2177	0.0008
habit8	0.1563	0.3157	0.0748	0.1500	0.2739	0.1107	0.6933	0.2737	0.0294	-0.0348	0.0929	0.2898	-0.0148
habit9	0.1332	0.4517	0.0500	0.2697	0.2719	0.0704	0.7820	0.3161	-0.0404	-0.0930	0.0691	0.3684	-0.0440
habit10	0.1504	0.2323	-0.0265	0.2131	0.1790	-0.0635	0.5025*	0.2357	-0.0625	-0.0360	-0.0007	0.2192	0.0176
habit11	0.1046	0.2828	0.0253	0.2017	0.2575	0.0644	0.6575*	0.2636	0.0276	0.0624	0.0609	0.2142	0.0081
habit12	0.2794	0.5923	-0.0945	0.3699	0.4531	0.0845	0.7558	0.3489	-0.0684	-0.2180	0.0129	0.3749	0.0841
int1	0.2456	0.4663	-0.1197	0.2608	0.5180	-0.0026	0.3566	0.9079	-0.1400	-0.1361	0.0394	0.3119	0.1377

Indicators	Avoidance	Behavior	Cost	Desc. Norm	Efficacy	Fear	Habit	Intention	Reactance	Reward	Severity	Social influence	Susceptibility
int2	0.3379	0.4995	-0.1059	0.3216	0.5356	0.0603	0.3721	0.9275	-0.1955	-0.1397	0.0877	0.4396	0.1799
int3	0.2803	0.4769	-0.1367	0.2911	0.4562	0.0348	0.3852	0.8991	-0.1151	-0.1392	0.1067	0.4361	0.1712
ract1	-0.2530	-0.0351	0.0955	-0.1180	-0.1558	-0.0683	-0.0568	-0.1705	0.9913	0.2982	-0.0610	-0.1570	-0.0982
ract2	0.2530	0.0351	-0.0955	0.1180	0.1558	0.0683	0.0568	0.1705	-0.6913*	-0.2982	0.0610	0.1570	0.0982
ract3	-0.0664	0.0707	0.0817	-0.1057	0.0665	-0.0548	0.0514	0.0435	0.5677*	0.2011	-0.0929	-0.1223	-0.0034
ract4	-0.1593	0.0542	0.0910	-0.1265	-0.0277	-0.0828	0.0167	-0.0398	0.9089	0.2800	-0.0468	-0.1618	-0.0645
rew1	-0.1087	-0.2544	0.4288	-0.0598	-0.1868	0.0330	-0.1331	-0.1083	0.2320	0.8552	0.0566	-0.1444	0.0360
rew2	-0.0766	-0.2399	0.4243	-0.1077	-0.1767	0.1229	-0.0909	-0.1007	0.2021	0.7801	0.0898	-0.0519	0.0481
rew3	-0.2866	-0.1869	0.3111	-0.2133	-0.1124	-0.0944	-0.0621	-0.1314	0.3785	0.7081	0.0032	-0.1145	-0.1118
rew4	-0.0349	-0.1058	0.4565	0.1247	-0.0297	0.1263	0.0304	-0.0969	0.1513	0.5104*	0.1155	0.0315	0.1164
rew5	0.0282	0.0767	0.4123	0.1152	0.0495	0.2579	0.0238	-0.0077	0.0731	0.3260*	0.2449	0.0641	0.2179
rew6	0.0503	0.0069	0.3584	0.0992	0.0514	0.1869	0.0175	-0.0226	0.0269	0.3648*	0.1866	0.0136	0.1917
rew7	-0.0538	-0.1209	0.3754	0.0901	-0.0476	0.1682	-0.0637	-0.0707	0.0709	0.4840*	0.1946	0.0104	0.1660
sev1	0.1511	0.1082	0.2722	0.1772	0.1287	0.5111	0.0561	0.0710	-0.0406	0.0693	0.8752	0.1658	0.4259
sev2	0.1484	0.0323	0.3102	0.1550	0.0457	0.5336	0.0350	0.0461	-0.0258	0.1001	0.8807	0.1518	0.4153
sev3	0.1480	0.0751	0.2287	0.2178	0.0428	0.5458	0.0273	0.1021	-0.0905	0.0426	0.7872	0.2361	0.4411
sinf1	0.3596	0.3442	0.0811	0.3419	0.2450	0.1783	0.3037	0.3345	-0.1302	-0.0628	0.1990	0.8012	0.1553
sinf2	0.2810	0.4177	0.0035	0.5392	0.3433	0.1254	0.3847	0.3991	-0.1544	-0.1235	0.1739	0.8941	0.2478
sus1	0.2916	0.0659	0.1379	0.2915	0.0596	0.4469	0.0400	0.1434	-0.1128	0.0697	0.5854	0.1903	0.7860
sus2	0.1525	0.1050	0.0685	0.2050	0.1523	0.2671	-0.0202	0.1651	-0.0730	-0.0526	0.2727	0.2236	0.7359
sus3	0.1516	0.0906	0.0879	0.2148	0.0897	0.2330	0.0173	0.1067	-0.0360	0.0113	0.2221	0.1536	0.8058

* item removed to improve discriminant validity

Table A4.3. Discriminant Validity Check through the Square Root of AVE.

Constructs	Avoidance	Cost	Desc Norm	Efficacy	Existing Behavior	Fear	Habit	Intention	Reactance	Reward	Severity	Social Influence	Susceptibility
Avoidance	1.000												
Cost	-0.016	0.770											
Desc Norm	0.337	0.017	0.852										
Efficacy	0.264	-0.169	0.286	0.763									
Existing Behavior	0.224	-0.199	0.435	0.563	0.945								
Fear	0.230	0.254	0.122	0.038	0.059	0.719							
Habit	0.212	-0.043	0.350	0.469	0.626	0.075	0.746						
Intention	0.320	-0.116	0.320	0.553	0.528	0.042	0.410	0.912					
Reactance	-0.236	0.067	-0.135	-0.132	-0.010	-0.079	-0.062	-0.148	0.852				
Reward	-0.163	0.440	-0.147	-0.201	-0.285	0.046	-0.157	-0.138	0.337	0.804			
Severity	0.186	0.318	0.215	0.086	0.085	0.643	0.049	0.085	-0.064	0.066	0.849		
Social Influence	0.368	0.047	0.532	0.353	0.452	0.163	0.421	0.435	-0.178	-0.128	0.216	0.849	
Susceptibility	0.277	0.123	0.315	0.122	0.108	0.420	0.037	0.179	-0.099	0.000	0.505	0.244	0.776

The AVE square roots are represented as the bolded, diagonal elements. Off-diagonal elements in the table represent the correlations between the constructs. To establish discriminant validity, the diagonal elements must be greater than the off-diagonal elements for the same row and column (Staples *et al.* 1999).

Table A4.4. MYMM Method for Analysis of Formative Indicators.

Items		(1)	(2)	(3)	Subj Norm
snorm1	(1)	1.0000			
snorm2	(2)	.7017	1.0000		
snorm3	(3)	.6502	.7645	1.0000	
Subj norm		.8819	.9109	.8962	1.0000

Appendix 5. Instruments (Study 3)

Scenarios

Excess Control

1. Nykänen is a mid-level software development manager in a software development company. A large portion of Nykänen's salary is based on the performance of the developers under him. However, several high-profile projects for the company are slipping behind on their schedules. Nykänen has regularly received a sizable bonus by always having projects completed on time. In the past, Nykänen has allowed his team to bypass minor tests in order to stay on schedule and receive bonuses for his team. However, with so little time left for a given project, he tells his Quality Assurance tester to sign off on all code as if it has already been tested. Due to skipping all the testing, Nykänen and his team all receive bonuses for completing the high-profile project on time.
2. Nykänen is a mid-level software development manager with his own team of developers. His team is under a strict deadline that is crucial to the release of an application for a major client, and the other modules cannot be completed until his team completes the development of their module. Nykänen's annual bonus is strongly influenced by the success of his work with this major client. Nykänen thinks that the only way that the team will be able to meet their deadline is to skip some of the quality tests that he thinks are not very important for their module. In order to complete their module on time, Nykänen informs his team to skip these tests.

Lack of Control

3. Nykänen has recently been hired by a software development company. As the company has more clients and contracts than it is able to fill, they often provide significant bonuses to employees who work ahead of schedule and thereby enable the company to take on additional contracts. Nykänen has noticed that the employees who generally get these bonuses tend to skip the majority of the required tests prior to releasing the developed code to the client. On his next major engagement, Nykänen is able to receive a bonus

since he also bypassed the majority of the testing and indicated that the code had passed all tests.

4. Nykänen is a low-level software developer for a well-respected software development company. The company has announced pre-fixed release dates for the major application that Nykänen is helping to develop, test, and modify. Nykänen only receives a bonus if he abides by this set schedule. However, the next release involves a significant change to the underlying program structure, and Nykänen does not think that he can meet the next deadline unless he skips some testing. Due to the time pressure, he skips testing his portion of the product and releases it on time.

Intention (Johnston & Warkentin 2010)

1. I would probably do what Nykänen did in the scenario.[9]
2. I would be likely to do the same as Nykänen did if the same event happened to me.

Control (Curry 2005; Piquero & Piquero 2006)

Control (Piquero & Hickman 1999): Being able to exercise control can be defined as having the ability to limit the behavioral options of others by:

a) withholding or granting things that are useful to them as they try to achieve their goals;
b) imposing or withholding things that are unpleasant to them as they try to achieve their goals;
c) overcoming physical or social structural barriers as you try to achieve your own goals.

Please indicate how much control (given the definition of control above) you assert and experience in the following social arenas:

1. Friendships in general;
2. People you tend to hang out with;
3. Relationships with significant others;
4. Other people (such as neighbors, solicitors, or repair people);
5. Relationships with family members;

[9] All items are measured on a 7-point Likert scale

6. Recreational activities;
7. Physical body (such as avoiding or regulating illness or fatigue, or maintaining your appearance);
8. Physical environment (such as the ability to control heat, coldness, regularity of food, or cleanliness);
9. Society as a whole;
10. Job/place of employment;
11. Salary/pay-scale;
12. Workload;
13. Time at work;
14. Professional reputation;
15. Your boss;
16. Your software development team;
17. Your company's norms.

Situational Provocation (Curry 2005)

1. Learning that I am not receiving a bonus would make me very upset.
2. It is very important to me to get my work done in a timely manner.
3. It is very important to me to receive bonuses for my work.

Violation Motivation (Curry 2005)

1. If I skipped the software testing, I would feel less worried or upset about the likelihood of getting a bonus.
2. If I skipped the software testing, I would probably get a bonus.
3. If I skipped the software testing, I would have more control over the likelihood of receiving a bonus.

Constraints (Piquero & Piquero 2006)

1. How morally wrong is the act portrayed in the scenario?
2. Rate the risk of getting caught by committing the act portrayed in the scenario.

Self-control (Curry 2005)

1. I often act on the spur of the moment without stopping to think;
2. I often do whatever brings me pleasure here and now, even at the cost of some distant goal;
3. I am more concerned with what happens to me in the short run than in the long run;
4. I sometimes find it exciting to do things for which I might get in trouble;
5. Excitement and adventure are more important to me than security;
6. I will try to get things I want even when I know it's causing problems for other people.

Appendix 6 Supplementary Data Validation Procedures (Study 3)

This is not meant for publication in the journal, but can be included as an online appendix if desired. It is meant to aid the reviewers in the examination of this study.

Table A6.1. T-statistics for Convergent Validity of Reflective Constructs.

Latent Construct	Indicator	t-statistic
Constraints	con1	19.919 ***
	con2	28.137 ***
Intentions	int1	158.425 ***
	int2	99.779 ***
Morality	moral1	8.714 ***
	moral2	44.809 ***
	moral3	11.354 ***
Self-control	sc1	4.222 ***
	sc2	8.283 ***
	sc3	2.504 **
	sc4	12.781 ***
	sc5	5.396 ***
	sc6	11.877 ***
Situational provocation	sp1	3.018 **
	sp2	1.808 *
	sp3	4.635 ***
Violation motivation	vm1	22.817 ***
	vm2	32.649 ***
	vm3	27.628 ***

*** p < .001; (d) dropped item

Table A6.2 Discriminant Validity with Latent Scores of Reflective Indicators.

Indicators	Constraints	Control balance	Intentions	Morality	Self-Control	Situational Provocation	Violation motivation
con1	0.859	-0.017	-0.360	0.491	-0.192	-0.075	-0.031
con2	0.861	0.144	-0.446	0.382	-0.261	-0.083	-0.156
conbal	0.074	1.000	-0.155	0.086	-0.128	0.070	0.188
int1	-0.460	-0.137	0.972	-0.434	0.324	0.195	0.271
int2	-0.450	-0.165	0.969	-0.428	0.317	0.218	0.203
moral1	0.332	0.106	-0.387	0.781	-0.255	-0.127	-0.176
moral2	0.521	0.043	-0.402	0.912	-0.140	0.037	0.020
moral3	0.388	0.083	-0.331	0.812	-0.207	-0.0141	-0.059
sc1	-0.096	-0.175	0.259	-0.079	0.653*	0.144	0.129
sc2	-0.244	-0.234	0.280	-0.209	0.782	0.153	0.171
sc3	-0.069	-0.137	0.152	-0.080	0.432*	0.104	0.118
sc4	-0.229	-0.009	0.245	-0.194	0.814	0.236	0.236
sc5	-0.166	0.047	0.189	-0.012	0.703	0.237	0.225
sc6	-0.208	-0.086	0.267	-0.283	0.786	0.330	0.244
sp1	-0.149	0.005	0.305	-0.128	0.314	0.813	0.170
sp2	0.206	0.067	-0.009	0.172	0.021	0.490*	0.080
sp3	-0.140	0.087	0.147	-0.028	0.271	0.919	0.201
vm1	-0.170	0.207	0.303	-0.159	0.261	0.159	0.879
vm2	-0.070	0.146	0.185	-0.025	0.264	0.209	0.924
vm3	-0.025	0.140	0.144	0.040	0.203	0.202	0.894

* item removed to improve discriminant validity

Table A6.3. Discriminant Validity Check through the Square Root of AVE.

	Constraints	Control Balance	Intentions	Morality	Self-Control	Situational Provocation	Violation motivation
Constraints	0.800						
Control Balance	0.074	1.000					
Intentions	-0.469	-0.155	0.971				
Morality	0.507	0.086	-0.444	0.837			
Self-Control	-0.276	-0.104	0.319	-0.236	0.779		
Situational Provocation	-0.160	0.058	0.239	-0.079	0.328	0.897	
Violation motivation	-0.107	0.187	0.244	-0.065	0.278	0.209	0.900

The AVE square roots are represented as the bold, diagonal elements. Off-diagonal elements in the table represent the correlations between the constructs. To establish discriminant validity, the diagonal elements must be greater than the off-diagonal elements for the same row and column (Staples *et al.* 1999).

Appendix 7 Measurement Items (Study 4)

Table A7.1. Pre-experiment Measures.

Construct	Subdimension	Items	Questions
Disposition to trust (second-order formative factor) (McKnight *et al.* 2002)	DT-Benevolence (DTB) (reflective)	DTB1 (d2)	In general, people really do care about the wellbeing of others.
		DTB2	The typical person is sincerely concerned about the problems of others.
		DTB3 (d1)	Most of the time, people care enough to try to be helpful rather than just looking out for themselves.
	DT-Integrity (DTI) (reflective)	DTI1 (d1)	In general, most folks keep their promises.
		DTI2	I think people generally try to back up their words with their actions.
		DTI3	Most people are honest in their dealings with others.
	DT-Competence (DTC) (reflective)	DTC1 (d1)	I believe that most professional people do a very good job at their work.
		DTC2	Most professionals are very knowledgeable in their chosen field.
		DTC3 (d2)	A large majority of professional people are competent in their area of expertise
	DT-Trusting stance (DTTS) (reflective)	DTTS1 (d1)(d2)	I usually trust people until they give me a reason to doubt when I first meet them.
		DTTS2 (d1)(d2)	I generally give people the benefit of the doubt when I first meet them.
		DTTS3 (d1)(d2)	My typical approach is to trust new acquaintances until they prove I should not trust them.
Formalism (Schminke and Wells 1999)	N/A		To what extent do you agree that each of the following character traits is important to you (you value in yourself)?
		FORM1	Principled
		FORM2	Dependable
		FORM3	Trustworthy
		FORM4	Honest
		FORM5 (d2)	Noted for integrity
		FORM6	Law-abiding

(d1) = dropped to improve discriminant validity for Study 1; (d2) = dropped to improve discriminant validity for Study 2

Table A7.2. Post-experiment Measures.

Construct	Subdimension	Items	Questions
Riskiness of computer-abuse scenario	N/A		Indicate how risky you think the computer abuse incident is that your classmate committed:
		RBS1	In general, it would be risky to commit this computer abuse.
Modified from the risk beliefs measure to focus on the riskiness of the scenario itself		RBS2	There would be high potential for loss associated with committing this computer abuse.
		RBS3(d2)	There would be too much uncertainty associated with committing this computer abuse.
		RBS4	Personally committing the computer abuse would involve many unexpected problems.
		RBS5	I would feel unsafe committing this computer abuse.
Risk beliefs (RB)	N/A		Based on the computer-abuse reporting scenario that you just read, please indicate how risky/risk-free it would be to report this abuse to your university's administration:
Original from (Jarvenpaa and Tractinsky 1999b), improved by (Malhotra *et al.* 2004)		RB1	In general, it would be risky to report the computer-abuse incident.
		RB2	There would be high potential for loss associated with reporting the computer-abuse incident.
		RB3(d1)	There would be too much uncertainty associated with reporting the computer-abuse incident.
		RB4	Personally reporting the computer-abuse incident would involve many unexpected problems.
		RB5	I would feel unsafe reporting the computer-abuse incident.
Public self-awareness (Pinsonneault and Heppel 1998)	N/A		In considering whether or not you would report the computer-abuse incident referred to in the scenario, please indicate the degree to which the following concerns would likely apply to you:
		PSA1(d1)	
		PSA2	I would be concerned about my style of doing things.
		PSA3	I would be concerned about the way I present myself.
		PSA4	I would be self-conscious about the way I look.
		PSA5	I would be concerned about what other people think of me.
			I would worry about making a good impression.

Anonymity (second-order formative factor) (Pinsonneault and Heppel 1998) Changed from a group decision context to an individual context of more general context of the degree of anonymity involved in reporting a computer-abuse incident according to a specific scenario.	Diffused responsibility		Given the stated scenario, please state your agreement with the following:
		DF1 (d1)(d2)	All computer-abuse reporting participants would be equally accountable for reporting computer-abuse incidents.
		DF2 (d1)	I believe it would be impossible to make one computer-abuse reporting participant responsible for not reporting a given computer-abuse incident.
		DF3	I believe it would be impossible to ask me personally to justify not reporting computer abuse.
		DF4 (d2)	Reporting computer-abuse incidents would be everybody's affair.
		DF5 (d1)	I believe it would be impossible to blame me personally for not reporting a computer-abuse incident.
		DF6 (d1)	I believe it would be impossible to make me more responsible than others for reporting computer abuse.
	Proximity	PROX1	If I were to report this computer-abuse incident, others could not easily see it on my computer screen.
		PROX2 (d2)	In reporting this incident, it would be near impossible for a computer-abuse reporting participant to see my computer screen while reporting the incident.
		PROX3	It would be very difficult for someone to read my computer-abuse report on my computer.
		PROX4	It would be difficult for a computer-abuse reporting participant to physically see me report the computer abuse.
		PROX5	It would not be possible for a computer-abuse reporting participant to clearly see my keyboard when writing up a computer-abuse incident.
		PROX6 (d1)	I would feel assured that no one could physically observe me in the act of reporting the computer abuse (*e.g.*, looking over my shoulder).

Knowledge of others	KO1	I believe others would NOT be able to identify my computer-abuse reports.
	KO2	I believe that those who have been selected to participate in reporting computer-abuse do not know each other well enough to identify the authors of computer-abuse reports.
	KO3	I believe I would NOT have distinguishing characteristics that would allow other computer-abuse participants to identify my computer-abuse reports.
	KO4 (d1)(d2)	I believe it would be possible to identify the origin of the reports based on the author's personal characteristics.
	KO5	I would NOT recognize the author of most computer-abuse reports.
	KO6	I believe the group participating in reporting computer abuse is large enough that it would be impossible for anyone to identify my computer-abuse reports.
Confidence in the system	CON1 (d2)	I believe the system would NOT malfunction and identify me as the author of my comments.
	CON2	I believe it would NOT be possible to identify me as the author of my comments using the system.
	CON3	I believe that the system would NOT attach a code to comments so that their author could be identified if needed.
	CON4	I believe that no names would be attached to the computer-abuse reports in the system.
	CON5 (d1)	I believe that my comments would not be identified in the system to other campus community members.
Lack of identification[10]	LI1	My personal identity would not be provided in the computer-abuse incident reports.
	LI2	During the process of reporting a computer-abuse incident no one could know who is reporting the incident.
	LI3	My computer-abuse reporting would be entirely secret.
	LI4	No personally identifying information would be found in my computer-abuse reports.

[10] In contrast to their other conceptualizations, Pinsonneault and Heppel (1998) conceptualized identification as a dichotomous state (identified or not identified). We expanded their conceptualization to a perceptual measure to be congruous with their other anonymity subconstructs so that it too could be represented in a perceptual range.

Belief that problem ought to be reported Modified from (Park *et al.* 2008) [11]	N/A	OTR1 (d2) OTR2 OTR3 (d1)	I would believe that something should be done to make more information about the computer-abuse incident known to my university administration. I believe that it would really matter whether information about the computer-abuse incident is made known to my university administration. Even if it is not me, I believe someone should tell my university administration about the computer-abuse incident.
Perceived responsibility to whistle-blow CA incident Modified from (Park *et al.* 2008)	N/A	RTW1 RTW2 RTW3	I believe that I would have the personal responsibility to report the computer-abuse incident to my university administration. I believe that it would be my responsibility to report the computer-abuse incident to my university administration. I believe that it would be my personal duty to report the computer-abuse incident to my university administration.
Willingness to whistle-blow CA incident Modified from (Park *et al.* 2008)	N/A	WTW1 WTW2 WTW3 (d2)	Please indicate your likely willingness to IMMEDIATELY (*i.e.*, RIGHT NOW) report the computer-abuse incident to your university administration. At this time, how likely are you to go directly to your university administration by yourself to report the computer incident? Please indicate how likely it is that you would tell your university administration about the computer-abuse incident.
Trusting beliefs (second-order formative factor) Modified from trust in an Internet vendor to trust in university (or organizational) administration	TB-Benevolence (TBB) (reflective)		In respect to reporting the computer-abuse incident discussed in the written scenario, please indicate how you think the university administration would react to your report (note: "organizational administration" was used for professional study):
		TBB1 TBB2 TBB3	I believe that my university administration would act in my best interest. If I required help, my university administration would do its best to help me. My university administration is interested in my wellbeing, not just its own.

[11] We changed their original items from the context of reporting bad news about a software project to one's boss to reporting a computer-abuse incident to university administration. (Importantly, their items were grounded in whistle-blowing theory and literature.)

from (McKnight *et al.* 2002)	TB-Integrity (TBI) (reflective)	TBI1 TBI2 (d2) TBI3 TBI4	My university administration would be truthful in its dealings with me. I would characterize my university administration as honest. My university administration would keep its commitments. My university administration would be sincere and genuine.
	TB-Competence (TBC) (reflective)	TBC1 (d) TBC2 TBC3 (d) TBC4 (d)	My university administration would be competent and effective in handling my report of computer abuse. My university administration would perform its role of dealing with the reported computer abuse very well. Overall, my university administration would be capable and proficient in handling the reported computer abuse. In general, my university administration would be very knowledgeable about dealing with reported computer abuse.
Trust in computer-abuse reporting tool (Grazioli and Jarvenpaa 2000)	N/A	TQN1 TQN2* TQN3 TQN4* TQN5 TQN6*	Please evaluate the likely quality of information that you believe would come out of the computer-abuse reporting system: Accurate Misleading Truthful Deceptive Factual Distorted

* = reverse-scaled item; (d1) = dropped to improve discriminant validity for Study 1; (d2) = dropped to improve discriminant validity for Study 2

Appendix 8 Model Validation (Study 4)

Establishing Factorial Validity

In this section, we jointly report the results of establishing factorial validity for both studies. A key step before assessing factorial validity, which has recently come to light in IS research, is to determine which constructs are formative and which are reflective (Petter *et al.* 2007). We used (Diamantopoulos & Winklhofer 2001) as the basis for determining where we had formative and reflective constructs. All of the constructs in our model are reflective. We thus followed the latest established procedures for establishing factorial validity for reflective indicators.

To do so, we analyzed factorial validity using partial least squares (PLS), using PLS-GRAPH version 3.0. To establish the factorial validity of our reflective indicators, we followed procedures by (Gefen & Straub 2005). To establish convergent validity, we generated a bootstrap with 200 resamples. We then examined the *t*-values of the outer model loadings; all of the outer loadings in both studies were significant at the .05 α level (see Table A8.1), with the exception of one of the anonymity items in Study 1, which was dropped. These results indicate strong convergent validity for the reflective constructs in both studies' models.

To establish discriminant validity of our reflective indicators, we used two established techniques: (1) correlating the latent variable scores against the indicators (Tables A8.2A and A8.2B) and (2) calculating the average variance extracted (AVE) (see Tables A8.3A and A8.3B). Both analyses indicate very strong discriminant validity. Most of the constructs demonstrated high levels of discriminant validity for both approaches. Several items were dropped to further improve discriminant validity.

Finally, to establish reliability, PLS computes a composite reliability score as part of its integrated model analysis (Table A8.3C). This score is a more accurate measurement of reliability than Cronbach's alpha because it does not assume that loadings or error terms of the items to be equal (Chin *et al.* 2003). Each reflective construct in our research model demonstrated high levels of reliability that exceeded the standard thresholds.

Testing for Common Methods Bias

All data was collected using a similar-looking online survey; thus, we still needed to test for common method bias to establish that it is not a likely problem in our data collection. To do so, we used two approaches.

The first approach, which is increasingly in dispute, was to conduct Harman's single factor test (Podsakoff *et al.* 2003). This test required that we run an exploratory unrotated factor analysis on all of the first-order constructs. The aim of the test is to see if a single factor emerges that explains the majority of the variance in the model. If so, then common methods bias likely exists on a significant level. The result of our factor analysis for Study 1 produced 89 distinct factors, the largest of which accounted for only 13.5% of the variance of the model; Study 2 produced 69 distinct factors, the largest of which accounted for only 20.3% of the variance.

The second approach, which is more accepted, is simply to examine a correlation matrix of the constructs (see measurement model statistics) and to determine if any of the correlations are above 0.90, which would be strong evidence that common methods bias exists (Pavlou *et al.* 2007). In no case were the correlations near this threshold.

Given that our data passed both tests of common methods bias, we conclude there is little reason to believe that the data in either study exhibit negative effects from common methods bias.

Manipulation Checks

To make our model testing more generalizable, we introduced variation into our data by giving participants several experimental manipulations for the riskiness of the scenario and for the various forms of anonymity. (Because manipulations were assigned on a random basis, manipulation treatment sizes were not equal). However, the ANOVA procedure is robust to unequal treatment sizes, so differences in cell sizes did not substantively affect our manipulation tests (Fidell & Tabachnick 2003). These manipulations were through the explicit descriptions of these various aspects in the scenario. To ensure that our participants received these manipulations, we used several validated measures. These independent manipulations were examined in a series of ANOVA tests. The results of these tests and the related comparisons are summarized in Table A8.4. All

manipulations were highly effective and significant, except for the manipulation for diffused responsibility in Study 1.

Mediation Checks

An important final check in our models was to check for mediation. Four constructs should serve as mediators: trust in the report-receiving authority, personal responsibility to report, perceived risk of reporting, and trust in the tool (only for Study 2). We followed the simple test of mediation proposed by Baron and Kenny: "A variable functions as a mediator when it meets the following conditions: variations in levels of the independent variable significantly account for variations in the presumed mediator (*i.e.*, Path a), variations in the mediator significantly account for variations in the dependent variable (*i.e.*, Path b), and when paths a and b are controlled, a previously significant relation between the independent and dependent variables (*i.e.*, Path c) is no longer significant, with the strongest demonstration of mediation occurring when Path c is zero" (pg. 1176) (Baron & Kenny 1986). Full mediation occurs when the IV no longer has a significant effect when the mediator is included; partial mediation occurs when the IV still has a significant effect but when its effect is diminished. The following provides the results of these tests for both studies.

Study 1: All three constructs passed the Path a check. All three constructs pass the Path b check, with the exception of perceived risk of reporting (at $\beta = -0.029$, $t = 0.92$ n/s). Thus, perceived risk of reporting is dropped as a potential mediator. Neither disposition to trust nor responsibility to report have significant Path c coefficients, so further testing is not necessary for these. However, anonymity has a significant path with willingness (at $\beta = 0.167$, $t = 4.64$***). By adding in Path a and Path b for anonymity, Path c decreases in strength but remains significant (at $\beta = 0.129$, $t = 3.25$**). These results support all of our proposed mediation relationships with the exception of perceived risk of reporting, which drops out of the model. Trust in the report-receiving authority acts as a full mediator in the relationship with one's disposition to trust and willingness to report; however, it acts as a partial mediator in the relationship with anonymity and willingness to report. Thus, a path between anonymity and willingness to report is added to the results.

Study 2: All four constructs passed the Path a check. All four constructs passed the Path b check, with the exception of perceived risk of reporting (at $\beta = -0.055$, $t = 1.20$ n/s). Thus, perceived risk of reporting was dropped as a potential

mediator. Finally, disposition to trust, anonymity, and confidence in the system did not have significant Path c coefficients, so further testing was not necessary to establish trust in *reporting-receiving authority* and *trust in tool* as mediators. We thus tested all three paths involved with personal responsibility. Path a was significant (at $\beta = 0.714$, $t = 17.90$***), Path b was significant (at $\beta = 0.463$, $t = 5.82$***), and Path c became insignificant (at $\beta = 0.104$, $t = 1.56$ n/s). These results support all of our proposed mediation relationships with the exception of perceived risk of reporting, which dropped out of the model.

Moderation Check

Because of the often highly interrelated relationships between risk and trust, we were surprised that perceived risk of reporting had no bearing on willingness to report in either model, even though this result supports traditional whistle-blowing theory. Thus, it is prudent to test whether perceived risk of reporting acted instead as a negative moderator with every predictor of willingness to report.

To do so, we followed the latest techniques for testing these potential interaction terms by creating both a baseline model and an interaction model, using the product-indicator approach detailed in (Chin *et al.* 2003). This is the most effective approach in identifying interaction terms in complex path models because it adds three critical improvements to measuring interaction effects. First, this approach models paths between each exogenous and endogenous construct—a critical step because "when the main effect variables are missing in the analysis, interaction path coefficients are not true interaction effects" (pg. 196) (Chin *et al.* 2003). Second, it standardizes or centers the individual items for the moderation scores[12]. Third, no information is eliminated from the model. All the interaction indicators stand alone without being summarized and are free to vary on their own to take advantage of PLS analysis. Whether or not moderators exist in a model is assessed by a hierarchical process similar to that used in first-generation statistical techniques. First, two models—one with the moderator relationship and one without (Chin *et al.* 2003)—are constructed and compared. In creating the

[12] "Standardizing or centering indicators helps avoid computational errors by lowering the correlations between the product indicators and their individual components." \cite{Chin:2003wb}. Standardizing is used if it is thought that the indicators measure their constructs equally well. Because we had no theoretical reason to believe that there were unequal differences in the specific indicators, standardizing was our methodological choice.

baseline model, the main effects of the interaction term need to be included; thus, perceived risk is included.

In short, perceived risk of reporting did not negatively moderate any element of either model. Thus, we can only conclude that there is no evidence that perceived risk of reporting plays a role in predicting willingness to report. Furthermore, we only report the results of the baseline model in our paper.

Table A8.1. T-statistics for Convergent Validity.

Latent Construct	Subconstruct	Indicator	t-statistic Study 1	t-statistic Study 2
Willing to report	n/a	wtw1	91.08***	87.59***
		wtw2	86.33***	86.58***
		wtw3	121.93***	47.92***
Trusting beliefs	Benevolence	tbb1	28.58***	29.46***
		tbb2	39.64***	27.16***
		tbb3	55.43***	13.48***
	Integrity	tbi1	50.22***	42.16***
		tbi2	39.91***	26.92***
		tbi3	45.17***	35.48***
		tbi4	63.60***	49.28***
	Competence	tbc1	31.81***	16.21***
		tbc2	39.55***	23.36***
		tbc3	32.38***	16.22***
		tbc4	26.14***	11.20***
Responsibility to report	n/a	rtw1	90.84***	65.00***
		rtw2	149.96***	150.78***
		rtw3	122.87***	84.70***
Ought to report	n/a	otr1	67.38***	42.05***
		otr2	68.59***	51.70***
		otr3	48.62***	27.30***
Riskiness of the scenario		rbs1	87.50***	44.83***
		rbs2	97.66***	50.97***
		rbs3	40.14***	9.00***
		rbs4	71.93***	37.09***
		rbs5	71.14***	42.94***

Latent Construct	Subconstruct	Indicator	t-statistic Study 1	t-statistic Study 2
Anonymity	Lack of identification	li1	46.23***	43.68***
		li2	77.64***	78.98***
		li3	111.69***	105.08***
		li4	71.87***	78.29***
	Diffused responsibility	df1	4.60***	4.50***
		df2	20.89***	21.35***
		df3	22.78***	9.92***
		df4	5.66***	2.83**
		df5	32.99***	27.61***
		df6	35.33***	10.92***
	Lack of proximity	prox1	42.44***	41.90***
		prox2	71.10***	39.42***
		prox3	70.69***	41.61***
		prox4	76.81***	63.40***
		prox5	43.42***	31.53***
		prox6	50.94***	69.39***
	Lack of knowledge of others	ko1	38.88***	30.63***
		ko2	46.03***	26.38***
		ko3	41.36***	31.54***
		ko4	1.28 (d)	5.57***
		ko5	22.69***	37.57***
		ko6	45.90***	40.55***
	Confidence in the system	con1	30.32***	40.13***
		con2	49.55***	67.66***
		con3	59.74***	34.26***
		con4	57.88***	32.86***
		con5	54.83***	58.17***
Risk beliefs	n/a	rb1	48.57***	35.12***
		rb2	43.21***	15.33***
		rb3	50.29***	41.81***
		rb4	44.13***	42.11***
		rb5	43.10***	29.81***
Public self-awareness	n/a	psa1	22.64***	20.77***
		psa2	47.51***	40.20***
		psa3	46.54***	21.65***
		psa4	41.48***	28.88***
		psa5	42.56***	18.55***

Latent Construct	Subconstruct	Indicator	t-statistic Study 1	t-statistic Study 2
Formalism	n/a	form1	19.71***	8.43***
		form2	14.40***	6.35***
		form3	18.28***	37.64***
		form4	23.95***	25.22***
		form5	21.63***	5.73***
		form6	16.92***	9.31***
Disposition to trust	Benevolence	dtb1	16.02***	7.75***
		dtb2	19.03***	17.14***
		dtb3	16.32***	14.05***
	Integrity	dti1	26.48***	18.87***
		dti2	18.40***	14.52***
		dti3	27.23***	22.46***
	Competence	dtic1	18.20***	18.50***
		dtic2	17.59***	13.58***
		dtic3	15.78***	7.45***
	Trusting stance	dtts1	17.81***	2.66**
		dtts2	14.75***	3.22**
		dtts3	16.22***	4.93***
Trust in the tool	n/a	tqn1	n/a	18.13***
		tqn2	n/a	13.48***
		tqn3	n/a	34.57***
		tqn4	n/a	7.06***
		tqn5	n/a	31.86***
		tqn6	n/a	16.66***

*** p < .001; ** p < .001; (d) dropped item

Table A8.2A. Study 1: Discriminant Validity with Latent Scores.

Construct	wtw1	wtw2	wtw3	TBB1	TBB2	TBB3	TBI1	TBI2	TBI3	TBI4	TBC1	TBC2	TBC3	TBC4
Willingness to WB	0.910	0.909	0.917	0.451	0.271	0.271	0.196	-0.070	0.142	-0.147	-0.082	-0.354	-0.331	-0.324
Trusting beliefs	0.179	-0.227	-0.005	0.835	0.846	0.907	0.875	0.961	0.925	0.936	0.942	0.806	0.799	0.831
Felt responsibility	0.746	0.624	0.623	0.596	0.570	0.408	0.485	0.044	0.273	0.043	-0.036	-0.375	-0.373	-0.078
Ought to be reported	0.494	0.480	0.764	0.545	0.428	0.464	0.394	0.215	0.261	0.085	0.264	-0.174	-0.145	-0.137
Riskiness of scenario	0.712	0.513	0.512	0.468	0.383	0.319	0.242	-0.017	0.074	-0.162	0.080	-0.152	-0.275	-0.203
Anon: Lack of ID	0.174	0.168	0.308	-0.040	-0.028	-0.073	0.220	0.033	0.362	0.037	0.005	-0.030	0.058	0.225
Anon: Diffused responsibility	0.127	-0.111	-0.223	0.574	0.664	0.529	0.705	0.509	0.424	0.561	0.562	0.368	0.246	0.633
Anon: Proximity	0.506	0.306	0.539	0.389	0.321	0.273	0.475	0.196	0.434	0.096	0.138	-0.089	-0.071	0.069
Anon: Knowledge of others	-0.185	-0.250	-0.339	-0.023	-0.070	-0.098	0.152	0.175	0.107	0.175	0.150	0.451	0.405	0.363
Anon: Confidence in system	0.243	0.166	0.158	0.455	0.604	0.426	0.731	0.308	0.472	0.372	0.326	-0.015	-0.010	0.497
Risk beliefs	0.022	0.154	0.061	-0.088	-0.228	-0.039	-0.266	0.094	0.072	0.048	0.136	0.416	0.465	0.026
Public self-awareness	0.325	0.308	0.328	-0.003	-0.240	-0.054	-0.292	-0.049	-0.053	-0.094	-0.129	0.112	0.163	-0.277
Formalism	-0.482	-0.393	-0.184	-0.011	-0.001	0.075	0.160	0.302	0.192	0.385	0.191	0.331	0.481	0.349
Trusting disposition	-0.092	0.096	-0.040	0.261	0.210	0.294	0.081	0.257	0.084	0.198	0.315	0.509	0.548	0.165

Construct	rtw1	rtw2	rtw3	otr1	otr2	otr3	rbs1	rbs2	rbs3	rbs4	rbs5	li1	li2	li3	li4
WIngness	0.685	0.758	0.662	0.526	0.419	0.655	0.600	0.647	0.533	0.641	0.665	-0.153	0.336	0.281	0.433
Trusting beliefs	0.274	0.163	0.002	0.121	0.039	0.436	0.037	0.062	0.066	0.087	0.111	-0.032	0.086	0.075	0.143
Felt responsibility	0.949	0.987	0.941	0.429	0.415	0.723	0.549	0.506	0.487	0.495	0.514	-0.303	0.312	0.051	0.209
Ought to be reported	0.579	0.718	0.507	0.801	0.866	0.762*	0.525	0.559	0.427	0.569	0.564	-0.295	0.182	0.041	0.105
Riskiness of scenario	0.595	0.565	0.354	0.405	0.291	0.693	0.983	0.990	0.887	0.994	0.985	-0.299	0.028	-0.009	0.113
Anon: Lack of ID	0.113	0.116	-0.054	-0.075	-0.059	0.158	-0.073	-0.015	-0.209	-0.029	0.035	0.752	0.927	0.915	0.953
Anon: Diffused responsibility	0.394	0.351	0.298	0.226	0.040	0.348	0.299	0.295	0.395	0.305	0.288	-0.434	-0.109	-0.066	-0.108
Anon: Proximity	0.600	0.567	0.270	0.335	0.052	0.574	0.547	0.521	0.258	0.479	0.561	0.213	0.809	0.630	0.783
Anon: Knowledge	-0.208	-0.245	-0.299	-0.003	-0.687	-0.300	-0.016	-0.033	-0.132	-0.093	-0.034	-0.035	0.230	0.435	0.320
Anon: Confidence	0.535	0.589	0.526	0.177	0.415	0.475	0.217	0.230	0.347	0.263	0.261	0.029	0.361	0.292	0.270
Risk beliefs	-0.495	-0.488	-0.450	-0.171	-0.281	-0.307	-0.297	-0.217	-0.160	-0.201	-0.203	0.214	-0.016	0.243	0.211
Public self-awareness	-0.137	-0.175	-0.130	0.021	-0.342	-0.136	-0.087	-0.035	-0.197	-0.067	-0.017	0.053	-0.028	0.114	0.199
Formalism	-0.311	-0.204	-0.067	0.057	0.070	-0.331	-0.765	-0.746	-0.735	-0.752	-0.725	0.065	-0.060	-0.011	-0.163
Trusting disposition	-0.305	-0.160	-0.022	0.124	0.161	-0.183	-0.112	-0.102	0.233	-0.056	-0.107	-0.428	-0.498	-0.278	-0.451

Construct	df1	df2	df3	df4	df5	df6	prox1	prox2	prox3	prox4	prox5	prox6	ko1	ko2
Willingness to WB	0.436	-0.512	0.280	0.138	0.065	-0.451	0.326	0.384	0.711	0.520	0.154	0.127	-0.055	-0.356
Trusting beliefs	0.446	0.101	0.140	0.357	0.376	0.351	0.117	0.168	0.291	-0.018	0.263	0.172	0.140	0.248
Felt responsibility	0.659	-0.201	0.718	0.558	0.082	-0.587	0.103	0.259	0.442	0.507	0.221	0.658	-0.248	-0.353
Ought to be reported	0.273	-0.726	0.465	0.189	0.615	-0.178	0.004	0.557	0.463	0.345	0.206	0.055	-0.305	-0.514
Riskiness of scenario	0.653	-0.731	0.528	0.467	0.306	-0.106	0.260	0.727	0.701	0.151	0.252	0.100	0.010	-0.082
Anon: Lack of ID	-0.238	-0.098	0.064	-0.398	-0.142	0.070	0.530	0.261	0.475	0.766	0.688	0.233	0.597	-0.045
Anon: Diffused	0.503*	0.026*	0.704	0.832	0.542*	0.276*	-0.343	0.093	0.123	-0.026	0.359	0.460	0.042	0.288
Anon: Proximity	0.282	-0.433	0.441	0.004	0.085	0.045	0.704	0.726	0.825	0.788	0.804	0.552*	0.540	0.089
Anon: Knowledge	-0.094	0.170	0.021	-0.060	-0.141	0.701	0.422	0.065	0.168	0.062	0.610	0.225	0.905	0.894
Anon: Confidence	0.402	-0.062	0.739	0.590	0.462	-0.158	-0.271	0.162	0.188	0.379	0.491	0.579	-0.110	-0.313
Risk beliefs	-0.241	0.092	-0.775	-0.570	-0.203	0.251	0.328	-0.215	0.129	-0.180	-0.190	-0.639	0.349	0.245
Public self-awareness	-0.090	0.058	-0.636	-0.450	-0.520	-0.001	0.501	-0.109	0.229	-0.030	-0.255	-0.390	0.257	0.242
Formalism	-0.404	0.495	-0.273	-0.247	-0.101	0.153	-0.221	-0.510	-0.595	-0.188	-0.113	-0.050	-0.106	-0.021
Trusting disposition	0.216	0.096	-0.342	0.030	0.182	0.138	-0.147	-0.273	-0.257	-0.673	-0.313	-0.439	-0.153	0.050

Construct	ko3	ko4	ko5	ko6	con1	con2	con3	con4	con5	rb1	rb2	rb3	rb4	rb5
Willingness to WB	-0.271	0.252	-0.417	-0.251	0.239	0.056	0.231	0.241	0.161	0.158	0.221	-0.095	0.009	0.041
Trusting beliefs	0.191	0.170	0.034	0.165	0.482	0.345	0.252	0.469	0.384	0.114	-0.071	0.348	-0.068	0.009
Felt responsibility	-0.314	0.639	-0.244	-0.121	0.518	0.523	0.353	0.584	0.633	-0.453	-0.365	-0.340	-0.453	-0.524
Ought to be reported	-0.289	0.446	-0.484	-0.379	0.493	0.334	0.362	0.407	0.351	-0.221	-0.110	-0.436	-0.442	-0.157
Riskiness of scenario	0.016	0.390	-0.378	0.017	0.366	0.325	0.149	0.325	0.063	-0.057	-0.277	0.056	-0.396	-0.262
Anon: Lack of ID	0.100	-0.028	0.056	0.387	0.316	0.123	0.230	0.248	0.266	0.213	0.318	-0.183	0.271	0.179
Anon: Diffused	0.270	0.407	0.061	0.308	0.641	0.738	0.564	0.781	0.411	-0.369	-0.630	-0.032	-0.740	-0.409
Anon: Proximity	0.248	0.196	0.163	0.430	0.402	0.290	0.095	0.385	0.435	-0.108	-0.096	-0.231	-0.126	-0.188
Anon: Knowledge	0.957*	-0.548*	0.848	0.915	-0.154	-0.097	-0.124	-0.024	-0.281	0.243	0.070	0.243	0.035	0.221
Anon: Confidence	-0.198	0.645	-0.340	0.108	0.968	0.947	0.842	0.979	0.766*	-0.482	-0.468	-0.424	-0.664	-0.421
Risk beliefs	0.224	-0.637	0.066	0.036	-0.498	-0.714	-0.230	-0.513	-0.652	0.963	0.915	0.668*	0.859	0.891
Public self-awareness	0.125	-0.600	0.179	-0.096	-0.646	-0.802	-0.522	-0.646	-0.530	0.727	0.737	0.507	0.793	0.579
Formalism	0.005	-0.292	0.266	-0.075	-0.061	-0.094	0.021	-0.099	0.087	-0.037	0.217	-0.175	0.110	0.187
Trusting disposition	0.161	-0.303	-0.089	-0.045	-0.088	-0.160	0.123	-0.113	-0.422	0.437	0.436	0.461	0.143	0.540

Construct	psa1	psa2	psa3	psa4	psa5	form1	form2	form3	form4	form5	form6	dtb1	dtb2	dtb3
Willingness to WB	0.256	0.231	0.303	0.269	0.464	-0.192	-0.216	-0.322	-0.471	-0.308	-0.334	0.097	0.073	0.038
Trusting beliefs	0.154	-0.142	-0.185	-0.260	0.058	0.456	0.052	0.500	0.487	-0.098	-0.183	0.198	0.124	0.186
Felt responsibility	-0.215	-0.296	-0.054	-0.190	0.078	-0.051	-0.151	-0.154	-0.288	-0.244	-0.038	-0.211	-0.185	-0.189
Ought to be reported	-0.242	-0.231	-0.287	-0.140	0.045	0.131	0.132	-0.116	-0.258	-0.040	-0.245	-0.090	0.007	-0.246
Riskiness of scenario	0.219	-0.229	-0.021	-0.259	-0.039	-0.514	-0.469	-0.641	-0.741	-0.629	-0.712	-0.122	-0.002	-0.065
Anon: Lack of ID	0.172	0.038	0.111	-0.044	0.151	-0.289	-0.112	0.094	0.142	0.137	-0.220	-0.239	-0.480	-0.311
Anon: Diffused	-0.247	-0.691	-0.611	-0.653	-0.483	0.106	-0.008	-0.039	-0.063	-0.269	-0.113	0.047	0.110	0.144
Anon: Proximity	0.147	-0.254	0.064	-0.223	0.223	-0.513	-0.370	-0.250	-0.228	-0.062	-0.386	-0.403	-0.535	-0.491
Anon: Knowledge	0.384	-0.001	0.141	0.063	-0.011	-0.268	-0.019	-0.105	0.006	0.266	0.055	0.069	-0.086	-0.093
Anon: Confidence	-0.485	-0.656	-0.699	-0.686	-0.482	0.112	0.117	0.013	-0.052	-0.249	-0.156	-0.181	-0.150	-0.143
Risk beliefs	0.662	0.850	0.572	0.744	0.540	0.124	0.078	0.122	0.172	0.003	-0.179	0.683	0.521	0.503
Public self-awareness	0.794*	0.917	0.913	0.884	0.826	0.032	-0.114	0.117	0.072	0.142	0.066	0.365	0.228	0.295
Formalism	-0.204	0.220	-0.063	0.260	0.003	0.864	0.757	0.814	0.768	0.784	0.770	0.090	0.035	-0.105
Trusting disposition	0.131	0.469	-0.013	0.431	-0.029	0.600	0.584	0.098	0.043	-0.041	0.018	0.730	0.809	0.390*

Construct	dti1	dti2	dti3	dtic1	dtic2	dtic3	dtts1	dtts2	dtts3
Willingness to WB	0.235	0.147	-0.185	-0.488	-0.260	-0.209	0.062	0.305	-0.125
Trusting beliefs	0.144	0.682	0.058	-0.016	0.200	0.235	-0.036	0.396	-0.206
Felt responsibility	0.037	0.000	-0.456	-0.251	-0.276	-0.305	0.153	0.565	0.083
Ought to be reported	0.159	0.067	0.032	-0.316	-0.020	0.061	0.290	0.181	0.361
Riskiness of scenario	-0.159	0.254	0.060	-0.209	-0.022	-0.179	-0.123	0.013	0.109
Anon: Lack of ID	-0.076	-0.262	-0.565	-0.670	-0.397	-0.211	0.141	0.345	-0.213
Anon: Diffused responsibility	-0.350	0.326	0.025	-0.011	-0.049	-0.164	-0.074	0.084	0.113
Anon: Proximity	-0.026	0.014	-0.497	-0.647	-0.355	-0.310	-0.009	0.392	-0.213
Anon: Knowledge of others	0.008	0.262	0.087	-0.098	0.035	0.010	-0.131	-0.034	-0.302
Anon: Confidence in system	-0.264	-0.025	-0.349	-0.318	-0.351	-0.230	0.333	0.438	0.312
Risk beliefs	0.407	0.428	0.419	-0.002	0.313	0.410	-0.138	-0.142	-0.489
Public self-awareness	0.545	0.337	0.149	-0.054	0.097	0.132	-0.194	0.025	-0.534
Formalism	0.473	0.011	0.080	0.258	0.177	0.423	0.482	0.304	0.220
Trusting disposition	0.590*	0.691	0.818	0.535*	0.660	0.797	0.360*	0.086*	0.186*

*Item removed to improve discriminant validity

Table A8.2B. Study 2: Discriminant Validity with Latent Scores.

Construct	dtb1	dtb2	dtb3	dti1	dti2	dti3	dtic1	dtic2	dtic3	dtts1	dtts2	dtts3	form1	form2	form3
L_trust_di	0.041*	0.725	0.707	0.387	0.698	0.767	0.731	0.684	0.328*	0.171*	0.380*	0.437	0.224	0.145	0.125
L_formalis	-0.146	0.210	0.178	0.015	0.213	0.101	0.155	0.191	0.104	-0.013	0.159	0.184	0.588	0.595	0.836
L_M_RB_sce	-0.061	-0.039	-0.046	-0.093	0.032	-0.055	0.005	0.078	0.021	0.047	0.075	0.141	0.152	0.064	0.179
L_M_Lack_I	-0.092	0.061	0.071	0.103	0.067	0.089	0.092	0.118	0.011	-0.104	-0.018	0.046	-0.048	0.123	0.079
L_M_diffus	0.036	-0.039	0.101	0.093	-0.083	0.049	0.051	0.020	0.037	-0.133	-0.065	-0.027	-0.008	0.035	0.088
L_M_proxim	-0.126	0.059	0.114	-0.071	0.039	0.070	0.068	0.162	0.006	-0.017	-0.091	-0.036	-0.056	-0.019	0.059
L_M_know_o	0.007	0.164	0.106	0.047	0.076	0.094	0.229	0.193	0.104	0.086	0.084	0.108	-0.090	0.035	0.000
L_M_sys_co	-0.021	0.175	0.124	-0.076	0.120	0.131	0.173	0.144	-0.063	0.078	0.146	0.153	-0.055	-0.014	0.025
L_risk_bel	-0.034	-0.117	-0.185	0.087	-0.084	-0.018	-0.116	-0.068	0.052	-0.113	-0.133	-0.099	-0.085	-0.087	-0.030
L_pub_self	0.092	0.216	0.108	0.111	0.083	0.141	0.130	0.138	0.126	-0.031	-0.069	0.015	-0.012	-0.044	-0.067
L_Ought_re	-0.060	0.098	0.087	0.033	0.156	0.097	0.149	0.170	0.096	0.095	0.100	0.174	0.244	0.190	0.253
L_Responsi	-0.157	0.091	0.043	-0.025	0.135	0.092	0.131	0.110	0.094	0.175	0.198	0.225	0.196	0.129	0.215
L_trust_be	-0.105	0.333	0.295	0.032	0.231	0.267	0.316	0.319	0.062	0.160	0.155	0.285	0.139	0.136	0.143
L_willingn	-0.139	0.160	0.155	-0.032	0.197	0.128	0.118	0.100	0.021	0.140	0.177	0.254	0.199	0.073	0.133
L_tqn	-0.104	0.243	0.213	0.044	0.246	0.181	0.232	0.216	0.022	0.170	0.194	0.238	0.148	0.111	0.229

Construct	form4	form5	form6	rbs1	rbs2	rbs3	rbs4	rbs5	li1	li2	li3	li4	df1	df2	df3
L_trust_di	0.189	-0.060	0.252	0.027	0.012	-0.121	0.067	0.018	-0.003	0.103	0.098	0.100	0.203	0.034	0.081
L_formalis	0.811	0.076*	0.589	0.240	0.212	-0.060	0.171	0.282	0.064	0.069	0.164	0.065	-0.004	0.077	0.056
L_M_RB_sce	0.143	-0.014	0.242	0.876	0.883	0.152*	0.883	0.856	-0.027	0.050	0.092	0.024	0.064	-0.004	0.160
L_M_Lack_I	0.108	-0.020	-0.103	0.003	0.025	0.050	-0.017	0.027	0.913	0.950	0.714	0.944	0.033	0.156	0.047
L_M_diffus	0.020	0.205	-0.118	-0.032	-0.079	0.052	-0.009	0.010	0.072	0.088	0.086	0.049	-0.446*	0.765	0.669
L_M_proxim	0.089	0.018	-0.059	-0.103	-0.064	-0.121	-0.053	-0.104	0.043	0.080	0.048	0.068	-0.018	0.144	0.148
L_M_know_o	0.049	-0.101	0.030	-0.041	-0.018	-0.029	0.022	-0.028	0.052	0.104	0.017	0.125	0.021	-0.075	-0.024
L_M_sys_co	0.061	0.012	-0.050	0.057	0.025	-0.160	0.061	0.091	0.082	0.123	0.024	0.124	0.182	0.029	0.075
L_risk_bel	-0.046	0.025	-0.030	-0.164	-0.131	0.079	-0.104	-0.088	0.005	0.015	0.059	0.016	-0.149	0.011	-0.029
L_pub_self	-0.056	-0.017	0.042	-0.156	-0.123	0.077	-0.073	-0.140	0.120	0.109	0.053	0.084	-0.042	0.100	0.025
L_Ought_re	0.205	0.031	0.198	0.352	0.418	-0.016	0.383	0.353	-0.068	0.042	0.070	0.031	0.068	0.033	0.030
L_Responsi	0.166	0.032	0.312	0.348	0.456	0.027	0.467	0.391	-0.131	-0.036	0.065	0.009	0.151	-0.152	-0.061
L_trust_be	0.139	-0.022	0.206	0.187	0.208	-0.031	0.222	0.151	-0.060	0.109	0.010	0.090	0.260	-0.001	-0.045
L_willingn	0.116	-0.039	0.283	0.310	0.397	-0.034	0.349	0.313	-0.116	-0.009	0.024	0.010	0.170	-0.138	-0.058
L_tqn	0.216	-0.054	0.276	0.248	0.243	-0.166	0.227	0.281	-0.076	0.041	0.003	-0.011	0.282	-0.059	0.011

Construct	df4	df5	df6	prox1	prox2	prox3	prox4	prox5	prox6	ko1	ko2	ko3	ko4	ko5	ko6
L_trust_di	-0.022	-0.054	0.050	0.074	-0.045	0.038	0.064	0.071	0.070	0.254	0.101	0.219	0.035	0.176	0.172
L_formalis	0.014	-0.094	0.025	-0.019	-0.037	-0.005	0.014	-0.039	-0.011	0.036	-0.087	0.154	0.059	0.036	-0.009
L_M_RB_sce	-0.072	-0.086	-0.049	-0.087	0.072	-0.054	-0.107	-0.132	-0.080	-0.032	-0.037	0.008	0.159	0.003	-0.099
L_M_Lack_I	0.096	0.091	0.063	0.127	0.096	0.083	0.056	0.084	0.074	0.081	0.136	0.145	0.077	0.092	-0.029
L_M_diffus	-0.004*	0.451	0.677	0.155	0.030	0.170	0.160	0.209	0.122	0.063	-0.019	0.079	0.143	-0.029	0.011
L_M_proxim	-0.010	0.068	0.114	0.896	0.114*	0.904	0.931	0.865	0.926	0.316	0.306	0.290	-0.009	0.207	0.024
L_M_know_o	0.017	-0.034	0.079	0.257	0.130	0.291	0.244	0.240	0.279	0.844	0.826	0.881	-0.249*	0.855	0.423
L_M_sys_co	-0.061	0.069	0.066	0.251	0.034	0.256	0.276	0.160	0.275	0.347	0.315	0.325	-0.117	0.328	0.121
L_risk_bel	-0.081	0.092	0.131	-0.212	-0.080	-0.240	-0.221	-0.148	-0.262	-0.230	-0.224	-0.220	0.058	-0.316	-0.105
L_pub_self	0.031	0.048	0.098	0.031	0.012	-0.012	-0.011	0.072	-0.036	-0.056	-0.064	-0.046	0.155	-0.142	-0.034
L_Ought_re	0.048	-0.176	-0.072	0.043	0.044	0.052	0.012	0.002	0.061	0.085	-0.005	0.113	0.077	0.057	-0.080
L_Responsi	0.014	-0.281	-0.241	-0.042	-0.001	-0.066	-0.050	-0.082	0.002	0.060	-0.065	0.006	0.133	0.008	-0.016
L_trust_be	-0.023	-0.179	-0.067	0.053	0.039	0.039	0.030	-0.052	0.065	0.276	0.166	0.267	0.063	0.257	0.065
L_willingn	0.067	-0.267	-0.248	-0.035	0.000	-0.058	-0.030	-0.102	0.015	0.122	0.027	0.060	0.086	0.091	-0.012
L_tqn	0.072	-0.189	-0.118	0.085	-0.018	0.099	0.029	-0.014	0.072	0.172	0.102	0.240	-0.010	0.291	0.085

Construct	con1	con2	con3	con4	con5	rb1	rb2	rb3	rb4	rb5	psa1	psa2	psa3	psa4	psa5
L_trust_di	-0.014	0.222	0.225	0.147	0.181	-0.158	-0.086	-0.150	-0.149	-0.072	0.092	0.105	0.140	0.140	0.054
L_formalis	-0.060	0.021	0.087	0.027	-0.006	-0.086	-0.063	-0.113	-0.027	-0.066	-0.024	-0.075	-0.114	-0.127	-0.018
L_M_RB_sce	-0.082	0.019	0.027	0.045	0.053	-0.081	0.021	-0.216	-0.083	-0.184	-0.105	-0.079	-0.002	-0.192	0.024
L_M_Lack_l	0.104	0.134	0.127	0.126	0.132	-0.046	0.004	0.010	0.013	0.050	0.055	0.154	0.053	0.086	0.066
L_M_diffus	0.125	0.059	0.051	0.077	0.075	0.084	0.089	0.108	0.104	0.085	0.122	0.135	-0.076	0.140	0.021
L_M_proxim	0.147	0.262	0.176	0.239	0.263	-0.273	-0.131	-0.179	-0.241	-0.171	0.001	-0.011	0.035	-0.002	-0.048
L_M_know_o	0.262	0.403	0.293	0.242	0.389	-0.250	-0.184	-0.268	-0.255	-0.203	-0.042	-0.164	-0.089	-0.112	-0.145
L_M_sys_co	0.227*	0.913	0.882	0.888	0.930	-0.424	-0.350	-0.507	-0.412	-0.416	-0.171	-0.215	-0.093	-0.212	-0.119
L_risk_bel	-0.159	-0.464	-0.434	-0.433	-0.456	0.853	0.740	0.860	0.858	0.853	0.431	0.418	0.334	0.403	0.291
L_pub_self	0.042	-0.176	-0.207	-0.177	-0.218	0.389	0.299	0.418	0.469	0.493	0.754	0.857	0.685	0.817	0.536
L_Ought_re	-0.092	0.091	0.089	0.012	0.071	-0.172	-0.118	-0.219	-0.207	-0.202	-0.076	-0.044	-0.034	-0.100	-0.048
L_Responsi	-0.106	0.104	0.132	0.064	0.088	-0.268	-0.108	-0.326	-0.296	-0.310	-0.264	-0.207	-0.055	-0.310	-0.119
L_trust_be	-0.077	0.222	0.298	0.248	0.239	-0.385	-0.272	-0.360	-0.367	-0.404	-0.187	-0.176	-0.101	-0.202	-0.159
L_willingn	-0.086	0.159	0.208	0.135	0.159	-0.348	-0.216	-0.384	-0.389	-0.396	-0.327	-0.276	-0.109	-0.331	-0.188
L_tqn	0.012	0.332	0.379	0.326	0.359	-0.403	-0.303	-0.474	-0.470	-0.430	-0.208	-0.191	-0.115	-0.234	-0.172

Construct	otr1	otr2	otr3	rtw1	rtw2	rtw3	tbb1	tbb2	tbb3	tbi1	tbi2	tbi3	tbi4	tbc1	tbc2
L_trust_di	0.149	0.169	0.159	0.191	0.170	0.173	0.334	0.318	0.280	0.336	0.222	0.367	0.384	0.309	0.342
L_formalis	0.130	0.270	0.250	0.293	0.284	0.298	0.210	0.167	0.137	0.170	0.018	0.203	0.207	0.099	0.241
L_M_RB_sce	0.191	0.341	0.445	0.477	0.438	0.413	0.214	0.256	0.175	0.193	-0.149	0.146	0.158	-0.013	0.287
L_M_Lack_I	0.072	-0.009	0.016	-0.042	-0.031	-0.043	0.082	0.090	0.035	0.094	0.039	0.111	0.104	-0.020	-0.010
L_M_diffus	0.045	-0.078	-0.093	-0.249	-0.298	-0.282	-0.159	-0.129	-0.029	-0.136	0.117	-0.069	-0.108	-0.078	-0.186
L_M_proxim	-0.020	0.020	0.030	-0.021	-0.058	-0.071	0.033	0.022	0.055	0.012	-0.029	0.027	0.025	-0.016	0.022
L_M_know_o	0.076	0.094	0.006	-0.022	0.010	0.001	0.194	0.211	0.279	0.253	-0.009	0.180	0.168	0.182	0.167
L_M_sys_co	-0.049	0.067	0.082	0.055	0.130	0.142	0.237	0.187	0.237	0.276	-0.031	0.193	0.205	0.126	0.193
L_risk_bel	-0.089	-0.217	-0.262	-0.282	-0.327	-0.305	-0.392	-0.386	-0.310	-0.385	-0.048	-0.347	-0.348	-0.173	-0.319
L_pub_self	0.030	-0.046	-0.164	-0.252	-0.270	-0.298	-0.166	-0.214	-0.091	-0.182	0.085	-0.159	-0.183	0.039	-0.231
L_Ought_re	0.602*	0.892	0.867	0.635	0.636	0.627	0.337	0.307	0.206	0.320	0.044	0.243	0.252	0.162	0.367
L_Responsi	0.295	0.570	0.713	0.944	0.973	0.956	0.429	0.376	0.187	0.357	0.000	0.275	0.344	0.112	0.428
L_trust_be	0.226	0.282	0.348	0.400	0.397	0.404	0.817	0.816	0.698	0.840	0.122*	0.863	0.886	0.478*	0.817
L_willingn	0.272	0.506	0.648	0.739	0.740	0.760	0.549	0.496	0.347	0.509	-0.009	0.432	0.498	0.234	0.579
L_tqn	0.243	0.483	0.429	0.458	0.457	0.479	0.474	0.462	0.378	0.397	-0.013	0.399	0.422	0.304	0.538

Construct	tbc3	tbc4	wtw1	wtw2	wtw3	tqn1	tqn2	tqn3	tqn4	tqn5	tqn6
L_trust_di	0.066	0.334	0.185	0.197	0.011	0.352	0.194	0.286	0.127	0.316	0.215
L_formalis	-0.060	0.028	0.071	0.229	-0.058	0.243	0.214	0.243	0.126	0.300	0.172
L_M_RB_sce	0.055	-0.046	0.095	0.355	-0.054	0.300	0.120	0.292	0.052	0.313	0.183
L_M_Lack_I	-0.078	0.033	0.065	-0.081	0.083	-0.056	0.000	-0.015	0.078	-0.063	0.054
L_M_diffus	0.022	-0.103	-0.147	-0.293	-0.037	-0.109	-0.165	-0.097	-0.079	-0.130	-0.192
L_M_proxim	-0.081	-0.065	-0.061	-0.065	-0.032	0.105	0.071	0.025	0.023	-0.006	0.051
L_M_know_o	-0.025	0.208	0.028	0.073	0.020	0.236	0.162	0.165	0.160	0.168	0.212
L_M_sys_co	0.002	0.066	0.071	0.158	-0.091	0.346	0.340	0.317	0.153	0.291	0.295
L_risk_bel	-0.070	-0.118	-0.244	-0.364	-0.050	-0.381	-0.395	-0.398	-0.291	-0.417	-0.416
L_pub_self	-0.115	0.004	-0.134	-0.308	-0.040	-0.163	-0.209	-0.186	-0.166	-0.210	-0.211
L_Ought_re	0.111	0.168	0.284	0.567	0.049	0.362	0.346	0.429	0.277	0.421	0.383
L_Responsi	0.049	0.122	0.411	0.734	0.009	0.400	0.354	0.429	0.225	0.430	0.411
L_trust_be	0.080*	0.366*	0.351	0.576	0.138	0.506	0.405	0.523	0.193	0.525	0.372
L_willingn	0.077	0.239	0.501	0.957	0.108*	0.546	0.406	0.561	0.261	0.542	0.454
L_tqn	0.087	0.213	0.374	0.571	0.071	0.779	0.777	0.846	0.663	0.815	0.769

Table A8.3A. Study 1: Calculating of Discriminant Validity through the Square Root of AVE.

Construct	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)
Disposition to trust (1)	0.521 (0.722)													
Riskiness of scenario (2)	.232	0.788 (0.888)												
Anon: Lack ID (3)	.173	.015	0.782 (0.884)											
Anon: Diffused responsibility (4)	.274	.311	.202	0.637 (0.798)										
Anon: Proximity (5)	.150	.101*	.364	.212	0.747 (0.864)									
Anon: Knowledge of others (6)	.240	.103*	.325	.249	.486	0.636 (0.798)								
Anon: Confidence in system (7)	.268	.138	.349	.265	.373	.368	0.712 (0.844)							
Risk beliefs (8)	.086*	.179	.020	.131	-.017	.039	-.139	0.720 (0.849)						
Public self awareness (9)	.145	.136	.104*	.150	.045	.080	-.008	.420	0.699 (0.836)					
Ought to be reported (10)	.282	.421	.033	.355	.206	.120	.202	.185	.119	0.865 (0.930)				
Responsibility to report (11)	.249	.468	.035	.303	.111	.089*	.216	.079	.123	.629	0.890 (0.943)			
Trust beliefs (12)	.481	.230	.175	.325	.221	.259	.338	-.070	.052	.357	.374	0.686 (0.828)		
Willingness to WB (13)	.308	.444	.106*	.296	.189	.140	.237	.007	.098*	.494	.687	.476	0.863 (0.929)	
Formalism (14)	.470	.231	.165	.290	.181	.282	.236	.149	.148	.356	.296	.429	.269	0.576 (0.759)

Table A8.3B. Study 2: Calculation of Discriminant Validity through the Square Root of AVE.

Construct	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)	(15)
DT (1)	0.484 (0.696)														
FORM (2)	.268	0.500 (0.707)													
RBS (3)	.018	.239	0.781 (0.884)												
LI (4)	.111	.026	.014	0.869 (0.932)											
DF (5)	.068	.020	.020	.103	0.448 (0.669)										
PROX (6)	.093	-.010	-.102	.085	.175	0.823 (0.907)									
KO (7)	.185	.011	-.001	.124	.011	.301	0.744 (0.863)								
CONF (8)	.204	-.023	.054	.148	.100	.257	.373	0.830 (0.911)							
RB (9)	-.132	-.091	-.136	.008	.082	-.237	-.284	-.483	0.695 (0.834)						
PSA (10)	.173	-.025	-.138	.110	.131	.007	-.092	-.210	.502	0.627 (0.792)					
OTR (11)	.172	.298	.432	-.001	-.054	.034	.055	.079	-.264	-.118	0.824 (0.908)				
RTW (12)	.157	.299	.468	-.052	-.241	-.045	.001	.103	-.315	-.282	.708	0.916 (0.957)			
TB (13)	.388	.218	.223	.075	-.095	.039	.276	.260	-.428	-.204	.341	.411	0.700 (0.837)		
WTW (14)	.226	.244	.380	-.050	-.251	-.034	.112	.203	-.409	-.324	.625	.767	.570	0.929 (0.964)	
TQN (15)	.286	.262	.272	-.003	-.123	.045	.238	.362	-.479	-.244	.486	.491	.511	.591	0.605 (0.778)

Table A8.3C. Composite Reliability

Construct (latent variable)	Composite reliability Study 1	Composite reliability Study 2
Disposition to trust	0.867	0.881
Riskiness of scenario	0.949	0.935
Anon: Lack ID	0.935	0.964
Anon: Diffused responsibility	0.778	0.736
Anon: Proximity	0.936	0.959
Anon: Knowledge of others	0.897	0.936
Anon: Confidence in system	0.908	0.951
Risk beliefs	0.912	0.919
Public self awareness	0.903	0.894
Ought to be reported	0.928	0.903
Responsibility to report	0.960	0.970
Trust beliefs	0.960	0.942
Willingness to WB	0.950	0.963
Formalism	0.890	0.831
Trust in tool	n/a	0.901

Table A8.4. Summary of Manipulation Checks.

Measure	Condition 1: μ (SD) [n]	Condition 2: μ (SD) [n]	F-statistic (p-value)	Manipulation significant?
Study 1: Riskiness of scenario	High: μ = 5.72 (SD = 1.22) [n = 272]	Low: μ = 3.50 (SD = 1.80) [n = 297]	F(1,569) = 289.74 p < 0.000	Yes
Study 2: Riskiness of scenario	High: μ = 6.51 (SD = 0.86) [n = 97]	Low: μ = 4.65 (SD = 1.42) [n = 105]	F(1,202) = 124.44 p < 0.000	Yes
Study 1: Anon: Lack of ID	High: μ = 4.25 (SD = 1.70) [n = 296]	Low: μ = 3.48 (SD = 1.96) [n = 273]	F(1,569) = 24.84 p < 0.000	Yes
Study 2: Anon: Lack of ID	High: μ = 5.03 (SD = 1.73) [n = 100]	Low: μ = 3.53 (SD = 1.96) [n = 102]	F(1,202) = 26.08 p < 0.000	Yes
Study 1: Anon: Diffused responsibility	High: μ = 4.17 (SD = 1.49) [n = 280]	Low: μ = 4.13 (SD = 1.34) [n = 289]	F(1,569) = 0.13 p = 0.715	No
Study 2: Anon: Diffused responsibility	High: μ = 4.45 (SD = 1.35) [n = 109]	Low: μ = 4.88 (SD = 1.31) [n = 93]	F(1,202) = 5.22 p < 0.000	Yes
Study 1: Anon: Proximity	High: μ = 3.07 (SD = 1.58) [n = 280]	Low: μ = 4.26 (SD = 1.60) [n = 289]	F(1,569) = 79.71 p < 0.000	Yes
Study 2: Anon: Proximity	High: μ = 2.78 (SD = 1.84) [n = 101]	Low: μ = 5.13 (SD = 1.36) [n = 101]	F(1,202) = 106.70 p < 0.000	Yes
Study 1: Anon: Knowledge of others	Class: μ = 3.84 (SD = 1.29) [n = 272]	University: μ = 4.24 (SD = 1.34) [n = 297]	F(1,569) = 12.91 p < 0.000	Yes
Study 2: Anon: Knowledge of others	Department: μ = 3.06 (SD = 1.43) [n = 112]	Company: μ = 4.27 (SD = 1.39) [n = 90]	F(1,202) = 36.47 p < 0.000	Yes
Study 1: Anon: Confidence in system	Good: μ = 4.14 (SD = 1.42) [n = 287]	Poor: μ = 3.15 (SD = 1.35) [n = 282]	F(1,569) = 72.23 p < 0.000	Yes
Study 2: Anon: Confidence in system	Good: μ = 4.59 (SD = 1.50) [n = 98]	Poor: μ = 2.72 (SD = 1.30) [n = 104]	F(1,202) = 90.15 p < 0.000	Yes

Table A8.5A. Study 1: Measurement Model Statistics.

Constructs	μ	SD	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)
Disposition to trust (1)	4.47	0.95													
Formalism (2)	5.84	0.93	.470												
Risk beliefs scenario (3)	4.46	1.90	.232	.231											
Anonymity: Lack ID (4)	3.88	1.87	.173	.165	.015										
Anonymity: Diffused (5)	4.15	1.41	.274	.290	.311	.202									
Anonymity: Proximity (6)	3.67	1.69	.150	.181	.101	.364	.212								
Anonymity: Others (7)	4.05	1.33	.240	.282	.103	.325	.249	.486							
Anonymity: Confident (8)	3.65	1.47	.268	.236	.138	.349	.265	.373	.368						
Risk beliefs (9)	3.89	1.36	.086	.149	.179	.020	.131	-.017	.039	-.139					
Public self-awareness (10)	3.59	1.43	.145	.148	.136	.104	.150	.045	.080	-.008	.420				
Ought to report (11)	4.44	1.55	.282	.356	.421	.033	.355	.206	.120	.202	.185	.119			
Responsibility to report (12)	3.67	1.59	.249	.296	.468	.035	.303	.111	.089	.216	.079	.123	.629		
Trusting beliefs (13)	4.36	1.32	.481	.429	.230	.175	.325	.221	.259	.338	-.070	.052	.357	.374	
Willingness to WB (14)	3.13	1.65	.308	.269	.444	.106	.296	.189	.140	.237	.007	.098	.494	.687	.476

Table A8.5B. Study 2: Measurement Model Statistics.

Constructs	μ	SD	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(10)	(11)	(12)	(13)	(14)	(15)
DT (1)	4.71	0.88														
FORM (2)	6.30	0.59	.268													
RBS (3)	5.54	1.50	.018	.239												
Anon: LI (4)	4.27	2.20	.111	.026	.014											
Anon: DF (5)	4.65	1.35	.068	.020	.020	.103										
Anon: PROX (6)	3.96	1.53	.093	-.010	-.102	.085	.175									
Anon: KO (7)	3.60	1.53	.185	.011	-.001	.124	.011	.301								
Anon: CONF (8)	3.63	1.68	.204	-.023	.054	.148	.100	.257	.373							
RB (9)	4.16	1.37	-.132	-.091	-.136	.008	.082	-.237	-.284	-.483						
PSA (10)	3.66	1.37	.173	-.025	-.138	.110	.131	.007	-.092	-.210	.502					
OTR (11)	5.33	1.21	.172	.298	.432	-.001	-.054	.034	.055	.079	-.264	-.118				
RTW (12)	4.82	1.48	.157	.299	.468	-.052	-.241	-.045	.001	.103	-.315	-.282	.70			
TBC (13)	4.60	1.20	.388	.218	.223	.075	-.095	.039	.276	.260	-.428	-.204	.341	.411		
WTW (14)	4.41	1.72	.226	.244	.380	-.050	-.251	-.034	.112	.203	-.409	-.324	.625	.767	.570	
TQN (15)	4.49	1.10	.286	.262	.272	-.003	-.123	.045	.238	.362	-.479	-.244	.486	.491	.511	.591

Appendix 9 Scenarios Documentation

Study 1. Students at Large University

Scenario introduction

Suppose that xx University is trying to improve security and risk management of all of its computer systems. This is a big deal because computer abuse and security violations have cost xx millions of dollars, which increases your tuition. As part of this initiative xx has asked students to voluntarily disclose the various abuses that students have witnessed other students doing that have undermined the integrity and performance of xx computer systems. By disclosing this information to your xx's leadership, you can help xx greatly improve its system security and risk management procedures, which will be a great benefit to xx that can potentially save millions of dollars and decrease tuition.

Given this hypothetical background, you will be given a short description of a scenario that describes exactly how this disclosure system would work in reporting the computer abuses of your fellow students. Please carefully read each section of the scenario description, as each section provides careful control for our study. Your helpful responses will help us determine factors that would most strongly encourage people to report computer abuse of others to their employers.

Table A9.1. Text for the Student Manipulation Levels.

Manipulation	Text for the levels
Riskiness of the computer abuse scenario	Low risk Computer Abuse Incident That Another Student Has Committed: Your classmate, Jerry, has played games during class, which is against xx student policy. High risk Computer Abuse Incident That Another Student Has Committed: Your classmate, John, has intentionally “hacked” or broken into a secure financial system to gain access to confidential xx information and personnel information to which he had no privileges nor legal right to access. He has specifically violated Federal privacy laws.
Privacy / identification	Low (personal ID publically revealed) Your name WILL be associated with your report of computer abuse and a record of your report will be accessible to anyone at xx (IT employees, students, professors, administrators, alumni) via a Web browser. High (personal ID not revealed) Your name will NOT be associated with your report of computer abuse and no one at xx (including IT employees, students, professors, alumni) will be able to figure out who submitted the record.
Diffused responsibility	High-diffused (low conveyed responsibility to report from institution) In making the computer abuse reporting system available, xx’s administration has stated that all reporting is entirely voluntary. No one will be held responsible for failing to report abuse incidents that they have witnessed. Low-diffused (high conveyed responsibility to report) In making the computer abuse reporting system available, ASU's administration has stated that all students have a high moral and ethical responsibility to report the abuses of other students. They have stated that if you do not report abuse for which you are aware, they will hold you personally and legally responsible for aiding any such abuse.

Manipulation	Text for the levels
Proximity	Low proximity in report recipient's location to participant's location To report a computer abuse incident, you can use any computer and any Web browser from any location at any time or day (even from home). You can report an incident without seeing or encountering anyone from xx administration or your fellow students. High proximity in reporting location To report a computer abuse incident you have to physically enter a "reporting" room at the main xx administration building where all students reporting an incident must use especially dedicated computers. The room is staffed by an administrator who sits just a couple of feet from the computer in plain view. All of the computers in the room are situated so that anyone can easily view any monitor or keyboard in the room.
Knowledge of others	High knowledge (only small class participating) You have been asked to be among the first in the xx campus community to participate in the computer abuse-reporting system. Only you and the members of a small class or seminar that you recently took (where you know most of the class members and they know you) are going to participate in the system for a month, before they roll it out to the entire university. Accordingly, the volume of reported computer incidents will be very low for the first month and you might recognize the writing style of those submitting incidents, or you might recognize the people behind the incidents. Low knowledge (entire university participating) All of the members of your xx campus community (thousands of administrators, professors, and students) will be asked to start using the computer-abuse system at the same time. Accordingly, there will be an extremely high volume of computer incidents reported, and the likelihood of your recognizing the incidents or the people behind them is extremely low.
Confidence in reporting system	Low quality / low confidence system The reporting system has been developed on campus by student volunteers. It has never been used before and they are still trying to iron out several problems and bugs in the system. By using the system, you can help them discover and fix new problems. They are discovering new problems every day. high quality / high confidence system The reporting system has already been successfully used for over five years at 400 other major universities and corporations. It has been developed by IBM, and the system has a long history of reliability and exact performance. No bugs have been reported in the system for over two years.

Study 2. Working Professionals

Scenario introduction

Suppose that your organization where you work is trying to improve security and risk management of all of its computer systems. This is a big deal because computer abuse and security violations have cost your organization millions of dollars. As part of this initiative they have asked employees to voluntarily disclose the various abuses that employees have witnessed other employees doing that have undermined the integrity and performance of organization computer systems.

The process of disclosing "computer abuse" information is done through a specially designed computer system where you will be able to enter information to disclose the computer abuse event.

By disclosing this information to your organization's leadership, you can help your organization greatly improve its system security and risk management procedures, which will be a great benefit to the overall organization and potentially save millions of dollars. Not to mention, if lots of employees participate, your organization could save millions of dollars by minimizing future computer abuse losses, which will greatly improve the financial standing of your organization.

Given this background, you will be given a short description of a scenario that describes exactly how this disclosure system would work in reporting the computer abuses of your fellow employees. Please carefully read each section of the scenario description, as each section provides careful control for our study. Your helpful responses will help us determine factors that would most strongly encourage people to report computer abuse of others to their employers.

Table A9.2. Text for the Professional Manipulation Levels.

Manipulation	Text for the levels
Riskiness of the computer abuse scenario	Low risk Computer Abuse Incident That Another Employee Has Committed: Your co-worker, Jerry, has played games during a department meeting, which is against organization policy. High risk Computer Abuse Incident That Another Employee Has Committed: Your co-worker, John, has intentionally "hacked" or broken into a secure financial system to gain access to confidential organization information and personnel information to which he had no privileges nor legal right to access. He has specifically violated Federal privacy laws.
Privacy / identification	Low (personal ID publically revealed) Your name WILL be associated with your report of computer abuse and a record of your report will be accessible to anyone at your organization (IT employees, managers, and all other employees) via a Web browser. High (personal ID not revealed) Your name will NOT be associated with your report of computer abuse and no one (including IT employees, managers, and all other employees) will be able to figure out who submitted the record.
Diffused responsibility	High-diffused (low conveyed responsibility to report from institution) In making the computer abuse reporting system available, your organization's administration has stated that all reporting is entirely voluntary. No one will be held responsible for failing to report abuse incidents that they have witnessed. Low-diffused (high conveyed responsibility to report) In making the computer abuse reporting system available, your organization's administration has stated that all employees have a high moral and ethical responsibility to report the abuses of other employees. They have stated that if you do not report abuse for which you are aware, they will hold you personally and legally responsible for aiding any such abuse.

Manipulation	Text for the levels
Proximity	Low proximity in report recipient's location to participant's location To report a computer abuse incident, you can use any computer and any Web browser from any location at any time or day (even from home). You can report an incident without seeing or encountering anyone from management or your fellow employees. High proximity in reporting location To report a computer abuse incident you have to physically enter a "reporting" room at your main building where all employees reporting an incident must use especially dedicated computers. The room is staffed by an organization manager who sits just a couple of feet from the computer in plain view. All of the computers in the room are situated so that anyone can easily view any monitor or keyboard in the room.
Knowledge of others	High knowledge (only small portion of department participating) You have been asked to be among the first in the organization to participate in the computer abuse-reporting system. Only you and the members of a small subsection of your current department (where you know most of your co-workers and they know you) are going to participate in the system for a month, before they roll it out to the entire organization. Accordingly, the volume of reported computer incidents will be very low for the first month and you might recognize the writing style of those submitting incidents, or you might recognize the employees behind the incidents. Low knowledge (entire organization participating) All of the employees of your entire organization and affiliated organization (potentially thousands of managers and employees) will be asked to start using the computer-abuse system at the same time. Accordingly, there will be an extremely high volume of computer incidents reported, and the likelihood of your recognizing the incidents or the people behind them is extremely low.
Confidence in reporting system	Low quality / low confidence system The reporting system has been developed only for your organization by a bunch of inexperienced summer IT interns who have returned to their campuses and no longer work for the IT department. It has never been used before and they are still trying to iron out several problems and bugs in the system. By using the system, you can help them discover and fix new problems. They are discovering new problems every day. high quality / high confidence system The reporting system has already been successfully used for over five years at 400 other major corporation. It has been developed by IBM, and the system has a long history of reliability and exact performance. No bugs have been reported in the system for over two years.

562. Sarala, Marian (2010) Elongation of Scots pine seedlings under blue light depletion

563. Vance, Anthony (2010) Why do employees violate is security policies? : insights from multiple theoretical perspectives

564. Karppinen, Katja (2010) Biosynthesis of hypericins and hyperforins in *Hypericum perforatum* L. (St. John's wort) – precursors and genes involved

565. Louhi, Pauliina (2010) Responses of brown trout and benthic invertebrates to catchment-scale disturbance and in-stream restoration measures in boreal river systems

566. Hekkala, Riitta (2011) The many facets of an inter-organisational information system project as perceived by the actors

567. Niittyvuopio, Anne (2011) Adaptation to northern conditions at flowering time genes in *Arabidopsis lyrata* and *Arabidopsis thaliana*

568. Leppälä, Johanna (2011) The genetic basis of incipient speciation in *Arabidopsis lyrata*

569. Kivelä, Sami, Mikael (2011) Evolution of insect life histories in relation to time constraints in seasonal environments : polymorphism and clinal variation

570. Kaartinen, Salla (2011) Space use and habitat selection of the wolf (*Canis lupus*) in human-altered environment in Finland

571. Hilli, Sari (2011) Carbon fractions and stocks in organic layers in boreal forest soils—impacts of climatic and nutritional conditions

572. Jokipii-Lukkari, Soile (2011) Endogenous haemoglobins and heterologous *Vitreoscilla* haemoglobin in hybrid aspen

573. Vuosku, Jaana (2011) A matter of life and death - polyamine metabolism during zygotic embryogenesis of pine

574. Petsalo, Aleksanteri (2011) Development of LC/MS techniques for plant and drug metabolism studies

575. Leppälä, Mirva (2011) Successional changes in vegetation and carbon dynamics during boreal mire development

576. Huotari, Noora (2011) Recycling of wood- and peat-ash – a successful way to establish full plant cover and dense birch stand on a cut-away peatland

577. Alahuhta, Janne (2011) Patterns of aquatic macrophytes in the boreal region: implications for spatial scale issues and ecological assessment

Book orders:
Granum: Virtual book store
http://granum.uta.fi/granum/

UNIVERSITY OF OULU P.O.B. 7500 FI-90014 UNIVERSITY OF OULU FINLAND

ACTA UNIVERSITATIS OULUENSIS

ISBN 978-951-42-9560-7 (Paperback)
ISBN 978-951-42-9561-4 (PDF)
ISSN 0355-3191 (Print)
ISSN 1796-220X (Online)

UNIVERSITY of OULU
OULUN YLIOPISTO