OULU 2015
A 655

ACTA UNIVERSITATIS OULUENSIS

Ying Li

USERS' INFORMATION SYSTEMS (IS) SECURITY BEHAVIOR IN DIFFERENT CONTEXTS

UNIVERSITY OF OULU GRADUATE SCHOOL;
UNIVERSITY OF OULU,
FACULTY OF INFORMATION TECHNOLOGY AND ELECTRICAL ENGINEERING

ACTA UNIVERSITATIS OULUENSIS
A Scientiae Rerum Naturalium 655

YING LI

USERS' INFORMATION SYSTEMS (IS) SECURITY BEHAVIOR IN DIFFERENT CONTEXTS

Academic dissertation to be presented with the assent of the Doctoral Training Committee of Technology and Natural Sciences of the University of Oulu for public defence in the OP auditorium (L10), Linnanmaa, on 19 October 2015, at 12 noon.

UNIVERSITY OF OULU, OULU 2015

Acta Univ. Oul. A 655, 2015

Supervised by
Professor Mikko Siponen

Reviewed by
Professor V. Srinivasan Rao
Professor Rossouw von Solms

Opponent
Professor Shuk Ying Ho

ISBN 978-952-62-0938-8 (Paperback)
ISBN 978-952-62-0939-5 (PDF)

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

Cover Design
Raimo Ahonen

JUVENES PRINT
TAMPERE 2015

Li, Ying, Users' information systems (IS) security behavior in different contexts.
University of Oulu Graduate School; University of Oulu, Faculty of Information Technology and Electrical Engineering
Acta Univ. Oul. A 655, 2015
University of Oulu, P.O. Box 8000, FI-90014 University of Oulu, Finland

Abstract

Users' information systems (IS) security behavior continuously draws attentions from scholars and practitioners. While previous studies usually focused on one context (e.g., employees' compliance with IS security policies in an organizational context), little research has focused on the possible explanations for users' IS security behavior if the context changes. To address this gap, this dissertation discusses the role of context in IS security behavior research. An analysis of the differences between the organizational context and the home context suggests a need to study users' IS security behavior solely in a specific context, such as home. This study provides guidelines for applying and developing contextualized theories in IS security behavior research.

Based on the guidelines, this dissertation includes two empirical studies. First, drawing on rational choice theory, it compares specific IS security behavior in two contexts: the work context (N = 210) and the personal context (N = 202). Second, drawing on stewardship theory, this dissertation develops a contextualized theory explaining employees' IS security risk-taking behavior in the organizational context (N = 170).

The findings of this dissertation show different explanations for users' IS security behavior in different contexts and highlight the importance of taking context into account when doing IS security behavior research. The results of each empirical study provide both theoretical contributions to research as well as actionable advice to practice.

Keywords: context, IS security behavior, rational choice theory, stewardship theory

Li, Ying, Tietokoneenkäyttäjien tietoturvakäyttäytyminen eri konteksteissa.
Oulun yliopiston tutkijakoulu; Oulun yliopisto, Tieto- ja sähkötekniikan tiedekunta
Acta Univ. Oul. A 655, 2015
Oulun yliopisto, PL 8000, 90014 Oulun yliopisto

Tiivistelmä

Tietokoneenkäyttäjien tietoturvakäyttäytyminen on jatkuvan kiinnostuksen kohteena niin tutkijoiden kuin käytännön ammatinharjoittajienkin keskuudessa. Aiempi tutkimus on keskittynyt tarkastelemaan tietoturvakäyttäytymistä yleensä yhdessä kontekstissa (esim. työntekijöiden tietoturvaohjeiden noudattaminen organisaatiokontekstissa), kun taas vähemmälle huomiolle on jäänyt se, kuinka kontekstin muuttuminen selittää tietoturvakäyttäytymistä. Tämä väitöskirja vastaa kyseiseen ongelmaan, sillä se käsittelee kontekstin roolia tietoturvakäyttäytymistutkimuksessa. Tutkimuksessa analysoidaan organisaatiokontekstin ja kotikontekstin eroja. Analyysi osoittaa, että on tarpeellista tutkia tietokoneen käyttäjien tietoturvakäyttäytymistä tietyissä konteksteissa, kuten esimerkiksi kotikontekstissa. Tutkimus tarjoaa ohjeita siihen, kuinka kontekstisidonnaisia teorioita sovelletaan ja kehitetään tietoturvakäyttäytymistutkimuksessa.

Väitöskirja sisältää 2 empiiristä tutkimusta, jotka pohjautuvat edellä mainittuihin ohjeisiin. Ensimmäisessä vaiheessa tutkimuksessa sovelletaan rational choice -teoriaa, jonka pohjalta vertaillaan tiettyä tietoturvakäyttäytymistyyppiä 2 kontekstissa: työkonteksti (N = 210) ja henkilökohtaisen käytön konteksti (N = 202). Toiseksi, tutkimus soveltaa stewardship -teoriaa ja kehittää siihen pohjautuen kontekstisidonnaisen teorian, joka selittää organisaation työntekijöiden käyttäytymistä liittyen tietoturvariskin ottamiseen (N = 170).

Väitöskirjan tutkimustulokset esittävät erilaisia selityksiä tietokoneen käyttäjien tietoturvakäyttäytymiselle eri konteksteissa. Tutkimus korostaa sitä, kuinka tärkeää on ottaa konteksti huomioon tutkittaessa tietoturvakäyttäytymistä. Kummankin empiirisen tutkimuksen tulokset tarjoavat teoreettisen kontribuution lisäksi käytännöllisiä neuvoja tietoturvan toteuttamiseen.

Asiasanat: konteksti, rational choice -teoria, stewardship -teoria, tietoturvakäyttäytyminen

Acknowledgements

First of all, I would like to express my deepest gratitude to my supervisor Professor Mikko Siponen. For me, as a PhD student who has just entered the research field, my supervisor has a great positive and profound influence on me. He has always been infecting me with his intelligence, energy, strictness as well as sense of humor. The discussion with him often makes me feel my lack of knowledge, and motivates me to work harder and think deeper. His critical thinking and the courage to challenge convention show a creative spirit that every researcher should pursue. From him, I see a scholar's passion and infinite striving to the research contribution. These influences are the most invaluable wealth for me forever. Also, I am appreciated for his strictness toward my work, which lets me see a better self through efforts. I am so lucky to have met such a supervisor. Until now, I still feel very grateful that he chose me among many outstanding candidates, and took me on board to start the very exciting and fantastic journey into the world of science.

I thank very much the following people who have ever helped me with my research, without their help, this thesis would not be possible. I am thankful to Dr. Nan Zhang who is a very helpful and supportive colleague as well as a close friend. He is always ready to help in whatever way he could. I sincerely thank my follow-up group members, Dr. Seppo Pahnila, Dr. Mari Karjalainen, and Professor Tero Vartiainen. They are very considerate and responsible for tracking the progress of my doctoral study, and provide me with useful experienced advices. I thank the two pre-examiners, Professor V. Srinivasan (Chino) Rao from the University of Texas at San Antonio, and Professor Rossouw von Solms from the Nelson Mandela Metropolitan University in South Africa, for their valuable feedbacks on this thesis. I would like to thank Professor Shuk Ying (Susanna) Ho, from the Australian National University, for serving as the opponent in the defense. I appreciate the visiting senior scholars that my supervisor has invited. The communications with them improved my work and meanwhile broadened my horizons. I also want to appreciate the company and the respondents who have participated in my data collection. I also thank the company Scribendi for proofreading my English.

I would like to thank Department of Information Processing Science at the University of Oulu, and Department of Information Systems and Computer Science at the University of Jyväskylä for the financial supports, the good study resources and work facilities during my PhD study. Thanks to the following people in the two universities, who have helped me with the administrative affairs: Professor Markku

Oivo, Professor Kari Kuutti, Marja-Liisa Liedes, Eila Kankaala, Tapio Tammi, Seija Paananen, and Tiina Lampinen.

I want to express my gratitude to my master supervisor Professor Wenli Li from Dalian University of Technology in China, for his encouragement and support for me to pursue the PhD degree. He has continued providing me with good research resources and visiting opportunities.

I thank all the friends and colleagues who have been accompanying me in Finland. They are all very successful in their study and work. I am proud of being their friend. I will never forget the time we have spent together in Oulu and Jyväskylä. The dinners we made together are the most delicious. I believe, years later, these wonderful memories will often come back to me.

Last, I want to dedicate this work to my dearest parents. They are the greatest parents to raise and educate me to become outstanding. Thank you for always standing by me with your unconditional love.

Jyväskylä, August 5th 2015 Ying Li

Abbreviations

AVE	Average variance extracted
CFA	Confirmatory factor analysis
CI	Confidence interval
CMV	Common method variance
EM	Embarrassment
FC	Facilitating conditions
GNF	Growth needs fulfillment
IS	Information systems
IT	Information technology
LTO	Long-term orientation
MN	Monitoring
PLS	Partial least squares
RCT	Rational choice theory
ISRB	IS security risk-taking behavior
ISRI	IS security risk-taking intention
TB	Task benefit
TC	Task cost
TRF	Trusted relationship fulfillment
USPP	Use of strong personal password
USWP	Use of strong work password
VI	Value identification

Contents

1 Introduction

The ubiquitous use of information technology in modern life leads to many information system (IS) security problems. For example, computers infected by malware could be controlled remotely, putting the stored confidential files in danger (Provos *et al.* 2007). Hijacked computers can be used to distribute illegal material or launch attacks against other computers. As another example, identity theft on social networking sites would lead to a wide range of victims if the cloned identity accesses the contacts' sensitive personal information (Jansson & von Solms 2013) or sends spam to their contacts (Bilge *et al.* 2009). Such security issues could be caused by users' unsecure behaviors when they are using an IS. Users' IS security-related behaviors are so various and complex that they can hardly be defined by a unified explanation. One important reason is that the contexts where users engage in the behavior vary. Context provides rich information that may influence how theories are applied and developed (Hong *et al.* 2013). Therefore, understanding the role of context in IS security behavior research is crucial.

1.1 Research gaps

Abundant research has focused on users' IS security in the organizational context, usually under names such as "computer abuse," "compliance or violations of IS security policies," and "misuse." In contrast, researchers have paid little attention to users' behavior in other contexts, such as at home or on public computers. Users may make different decisions according to the situation or conditions in the context. However, little research has investigated the differences between contexts (e.g., organization and home) and how the differences may lead to different explanations for the behavior.

Further, from a theory perspective, theories are also sensitive to context. Previous IS security research has largely applied theories such as rational choice theory (Bulgurcu *et al.* 2010, Vance & Siponen 2012) and deterrence theory (D'Arcy *et al.* 2009) from reference fields like economics and criminology. Few of these studies have discussed whether the assumptions of the original theories are appropriate in an IS security context. If the assumptions are invalid, the inferences will be problematic. For this reason, more contextualized theories and specific explanations for IS security behavior are needed. In order to understand IS security behavior in different contexts, an approach is needed to develop contextualized theories.

1.2 Overview of chapters

This dissertation aims to address the important role context plays in IS security behavior research, specifically by showing how context differences result in different explanations for behavior, how theory is context sensitive, and how new theory is applied in the context of IS security. To this end, we designed three studies (one conceptual, two empirical). Each chapter presents one study, all of which are briefly summarized below.

The first study addressed the need to pay attention to the home context in IS security behavior research. We posited four types of use and nine contextual factors to reflect the different explanations needed in the home context compared with users' behavior in an organizational context. Based on the discussion, we proposed seven avenues for research to call for more research on home users.

The second study discussed the approach to develop a contextualized theory. Taking rational choice theory as an example, we elaborated on two levels of assumptions (i.e., core assumption and auxiliary assumption) and their connections with the IS security context. In order to show that different contexts require different contextualized theories, we designed a comparative empirical study. We tested the rational choice-based model using 217 respondents for the work group and 210 respondents for the personal group.

The third study adopted a temporal perspective, discussing the time feature of IS security risk-taking behavior in an organization and then identifying the specific factors that influence IS security risk-taking behavior. We developed and tested a contextualized model drawing on stewardship theory (Davis *et al.* 1997, Hernandez 2012). This study collected data from a global company with 170 respondents from six countries.

1.3 Study 1. A call for home users' information security behavior

1.3.1 Research gap

Home users' security should be an important research topic in IS security research, not only from the perspective of protecting home users' personal or work information on their home computers, but also because hijacked home computers have become an ideal breeding ground for hackers attacking organizations and distributing illegal or morally questionable material. Despite the importance of studying home users' security behavior, the primary focus of the behavioral IS

security research has been on an organizational context. While this research in organizational contexts is important, we argue that the home user context requires more attention by scholars. While similarities exist between home users' IS security behavior and employees' compliance with IS security procedures in the organizational context, it is necessary to understand their differences so that research and practice on home users' security behavior can develop further. We argue that previous research has largely ignored such differences.

1.3.2 Understanding IS security behavior by type of use

To understand individuals' information security behavior differences, we distinguished and analyzed four types of use by two dimensions—place and task. Based on the framework, we discussed nine possible contextual factors that reflect differences in users' IS security behavior in different contexts (see Fig. 1): awareness training, IS security policy, information technology (IT) support, monitoring, fear factors, safety climate, mandatory control, network security, and sharing computers.

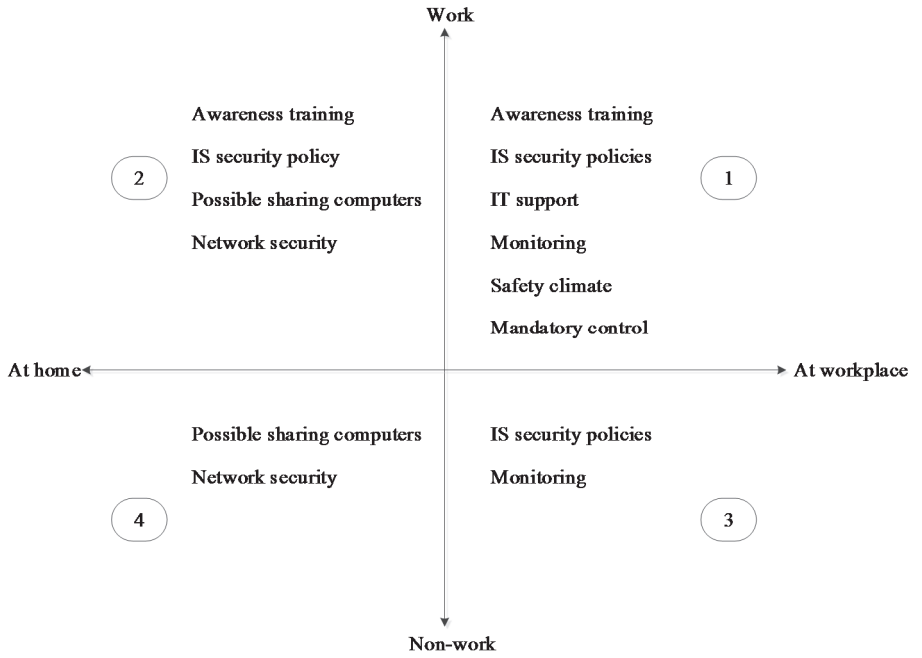

Fig. 1. Features of four contexts.

1.3.3 Contribution

This study highlights the need to study home users' IS security behavior. The proposed types of use are preliminary context differences that need to be investigated when studying the home users. Further, we identified nine contextual factors for future empirical studies to examine their different impacts on users' security behavior in the organizational context and the home context. Based on the discussion, we conclude by proposing research agendas for future research.

1.4 Study 2. Users' IS security behavior in different contexts: a contextualized rational choice approach and comparative empirical evidence

1.4.1 Research gap

IS security behavior is an important research stream in IS research. The research of this area has widely applied reference theories from non-IS fields, such as criminology, economics, and psychology. Popular theories include rational choice theory (RCT), deterrence theory, protection motivation theory, and neutralization theory. While the use of reference theories has been a successful mode of publication in IS research (Baskerville & Myers 2002), it is important to understand the underlying assumptions of these reference theories, including whether these assumptions are met within the IS security context. By reviewing the IS security behavior studies, we found that little research has specifically discussed the appropriateness of assumptions of the applied theory in the IS security context. A case in point is RCT, which was derived from neoclassical economics or criminology to explain investment or crimes, respectively, and has been applied to explain IS security behavior (Bulgurcu *et al.* 2010, Li *et al.* 2010, Vance & Siponen 2012). Recent IS scholars have also emphasized the importance of context and the development of contextualized theories (Hong *et al.* 2013), suggesting that there exists a general theory that can guide the following contextualization. We argue that no general theory exists because every theory is based on certain assumptions that may be arguable and context-sensitive. It is very important to contextualize a theory by analyzing the context and examining its assumptions within the context.

1.4.2 Rational choice theory overview

The rational choice approach is influential in explaining humans' decision-making in many domains of social life. Under the rational choice paradigm, humans are assumed to be naturally rational and to take purposeful actions. Rational choice generally means choosing among alternative courses of action in accordance with certain rationality assumptions (Voss & Abraham 2000). RCTs explain human behavior by using different rationality assumptions that depend on the features of the context faced by the actors (Voss & Abraham 2000). This arrangement results in a family of rational choice theories that provide different explanations for human behavior. Examples of RCTs are the neoclassical economic approach of rational choice (Becker 1976), deterrence theory (Cornish & Clarke 2014) and rational choice theory (Paternoster & Simpson 1993) in criminology, and the theory of justice (Rawl 1971) in sociology.

1.4.3 Guidelines for developing contextualized theory in IS security behavior research

In order to develop more contextualized theory in IS security behavior research, we suggest four guidelines:

Guideline 1: Analyze the context. We recommend that researchers analyze the IS security context in four critical dimensions—user context, task context, social context, and technology context. These dimensions can help identify the differences in context, as well as the possible contextual factors that should be included in a research model.

Guideline 2: Make core assumptions. The core assumptions are the overarching foundation, which are assumed as valid in the integrated context as well as in each dimensional context.

Guideline 3: Make auxiliary assumptions. The auxiliary assumptions are closely connected to the detailed context, such as the user, task, social, and technology context. Each dimensional context can be more detailed (e.g., users' goals, needs in the user context).

Guideline 4: Derive hypotheses from the assumptions. Hypotheses should be derived from the assumptions made, and not contradict other assumptions.

1.4.4 Theoretical model

Based on the guidelines and the RCT, we conducted an empirical study to illustrate the guidelines. Specifically, we built a research model to compare the use of strong work password (USWP) and the use of strong personal password (USPP). The model intends to show how differently USWP and USPP are influenced by specific contextual factors. As shown in Fig. 2, users' IS security behavior is influenced directly by contextual factors, including the impetus factors of facilitating conditions, embarrassment, monitoring, and task benefit as well as the impediment factor task cost.

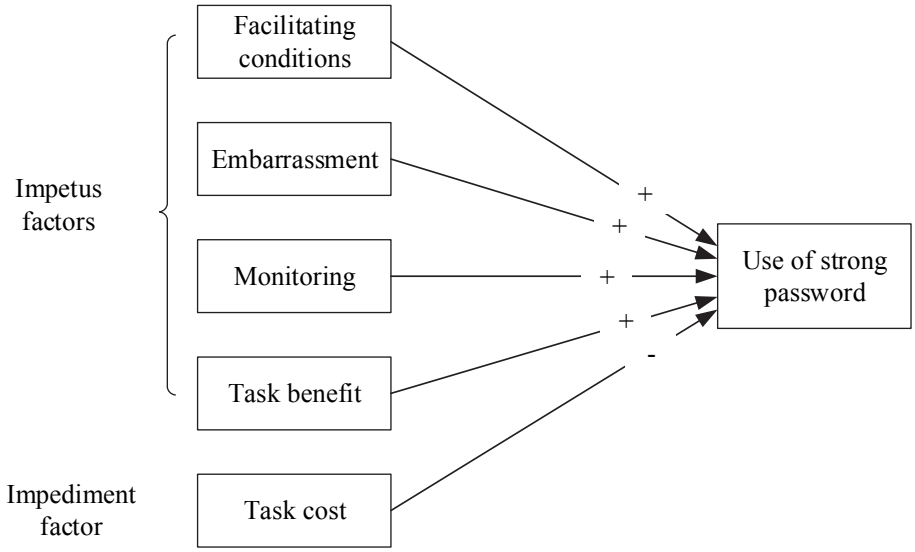

Fig. 2. Rational choice-based research model.

1.4.5 Contribution

This study makes four contributions. First, our work contributes to the theory contextualization approach in IS research by suggesting that researchers appropriately alter the assumptions in the corresponding context. We suggest that examining the appropriateness of assumptions or, if necessary, altering the assumptions in the context is the first step in contextualizing a theory.

Second, we contribute to the RCT development in IS security behavior research. Previous RCT-based IS security behavior studies have rarely discussed the particularity of the IS security context or the appropriateness of assumptions applied in the context. By showing a comparative example of password use in work and personal contexts, we suggest making the specific assumptions explicit rather than implicit.

Third, we suggest analyzing the IS security context in dimensions. We identify four context dimensions that are important in studying IS security behavior, namely, user context, task context, social context, and technology context. We emphasize the importance of analyzing the context and making appropriate assumptions, which can provide more precise theoretical explanations.

Fourth, our comparative empirical results provide evidence for the need to move to contextualized IS security behavior research. Our study indicates that the conclusions in one context may not be generalized to a different context. Our comparative empirical results show that the influential factors in an organizational context (USWP) are quite different from those in a personal context (USPP).

1.5 Study 3. Understanding employees' IS security risk-taking behavior: a temporal perspective

1.5.1 Research gap

Both scholars and practitioners have demonstrated concern over employees' IS security risk-taking behavior (ISRB) (D'Arcy *et al.* 2014, Guo *et al.* 2011, Willison & Warkentin 2013). Although organizations exert great effort to improve security management through actions such as training, enhancing security monitoring, and updating security policies, many employees still fail to comply with the IS security policies. IS security literature has implied that employees are not ignorant about the rightness or wrongness of the behavior. Instead, they know the risk of the behavior but have reasons to choose to take the risk. Because risk is intrinsically embedded in time, the outcomes of current risk unfold in the short or distant future (Das & Teng 1997, Drucker 1972). Many ISRBs may not cause immediate loss, especially when employees are nonmalicious (such as when using a simple password), but the behavior may leave vulnerability for the future. Without considering the possible future consequences of their current behavior, employees may underestimate the seriousness of the threats, which leads to violations.

Unfortunately, little research has adopted such a temporal perspective, which may be an important angle to understand ISRB and its influential factors. This paper aims to address this gap.

1.5.2 Stewardship theory overview

Stewardship is defined as "the extent to which an individual willingly subjugates his or her personal interests to act in the protection of others' long-term welfare" (Hernandez 2012: 174). Given a choice between self-serving behavior and pro-organizational behavior, a steward-like employee will not deviate from the interests of his or her organization. Stewardship theory suggests that steward-like employees are more likely to generate a long-term orientation (LTO), which could lead to pro-organizational behavior (Hernandez 2012). Moreover, individuals' value identification and the satisfaction of higher order needs are important psychological constructs that influence the pro-organizational behavior (Davis *et al.* 1997).

1.5.3 Theoretical model

Fig. 3 presents the theoretical model developed and tested in this study. We based the model on stewardship theory (Davis *et al.* 1997, Hernandez 2012). Since monitoring employees' ISRB in reality is difficult, we used IS security risk-taking intention (ISRI) as a proxy. In the IS security context, we propose that an employee's ISRI is negatively influenced by LTO. Further, LTO is positively influenced by an employee's value identification of avoiding ISRB, trusted relationship fulfillment, and personal growth needs fulfillment.

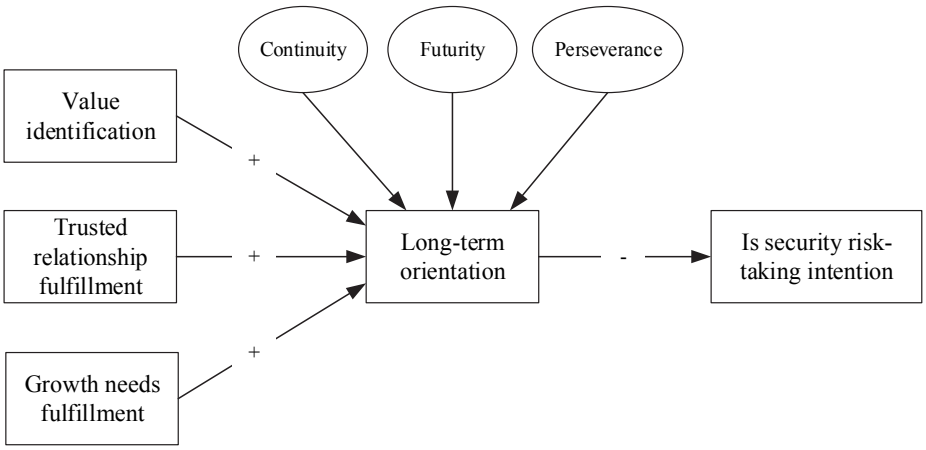

Fig. 3. Stewardship model of employees' IS security risk-taking behavior.

1.5.4 Contribution

This paper makes several contributions to the literature on IS security behavior. First, we adopted a temporal perspective to understand IS security behavior and its influential factors. We highlighted the possible delayed consequences as part of the characteristics of ISRB. Employees with ISRB may not foresee the immediate consequences, but their behaviors leave the organization's IS in a vulnerable state for future attack. In addition, we also applied a temporal perspective to look at the influential factors, such as LTO, and individuals' needs. Our preliminary study enabled us to demonstrate the value of adopting a temporal perspective as a new research avenue to study IS security behavior.

Second, by adopting a temporal perspective, we are the first (to our knowledge) to empirically investigate the role of LTO in the context of an employee's ISRB in an organization. We show that LTO is an influential predictor of ISRI, although no previous research has ever identified it.

Our third contribution is that we are the first to draw on stewardship theory to offer a theoretical explanation and empirical support for the influential factors on employees' ISRB. Drawing on stewardship theory, we argue that LTO, value identification, trusted relationship fulfillment, and growth needs fulfillment are important factors influencing ISRI. We found strong empirical support for our argument.

1.6 Publication status of dissertation chapters

Each chapter represents an independent research study, some of which have already been published or submitted for review. Table 1 summarizes the status of each chapter.

Table 1. Status of dissertation chapters.

Chapter	Co-author	Status
2	Mikko Siponen	Published in Pacific Asia Conference on Information Systems, July 2011
3	Mikko Siponen	Preparing for submission
4	Mikko Siponen	Preparing for submission

1.7 Contributions

This dissertation mainly provides three contributions to IS security behavior literature. First, this dissertation identifies the home user's IS security behavior as a unique phenomenon, different from the behavior in an organizational context. An approach that distinguishes four types of use can provide better understanding on the particularity of the home context. Following the approach, we identify nine contextual factors. The contribution, therefore, is that we emphasize the need for future research to focus on home users' IS security behavior.

Second, this dissertation provides an approach to develop contextualized theory in IS security behavior research. By using the case of rational choice theory, we highlight that the contextualization should start from examining or altering the assumptions of a theory. The empirical results indicate that the theory is different in different contexts.

Third, this dissertation applies a temporal perspective to understand employees' IS security risk-taking behavior in an organizational context. We apply stewardship theory to the IS security context. Following its assumptions, we highlight that long-term orientation is an excellent factor to explain the user's IS security risk-taking behavior, and we also identify three antecedents of long-term orientation.

1.8 Conclusion

Users' IS security behavior continues to receive attention from scholars and practitioners. With the increase in the number of contexts in which users use information technology (IT), security issues are also increasing. However, little

research has focused on users' behavior in different contexts or the impact of context on IS security behavior research. This dissertation mainly proposes approaches to study IS security behavior in different contexts, and also provides empirical evidence of the need for a specific explanation in each specific context. This dissertation advances IS security behavior research by focusing on the role of context and adopting novel theoretical perspectives to understand the behavior.

2 A call for research on home users' information security behavior

2.1 Abstract

The number of home computer users is increasing faster than ever. Home users' security should be an important research topic in IS security research, not only from the perspective of protecting home users' personal or work information on their home computers, but also because hijacked home computers have become an ideal breeding ground for hackers attacking organizations and distributing illegal or morally questionable material. Despite the importance of studying home users' security behavior, the primary focus of behavioral IS security research has been on an organizational context. While this research in the organizational context is important, we argue that scholars should also pay attention to the home context. While similarities exist between home users' IS security behavior and employees' compliance with IS security procedures in an organizational context, understanding their differences is crucial to allowing research and practice on home users' security behavior to develop further. We argue that previous research has ignored such differences. As a first step in remedying the gap in our understanding, we first theorize these differences and consider that at least nine contextual factors may result in an individual's behavior inconsistency in the workplace and at home. Because of this finding, we argue that the same theories may not explain the use of security features in home and organizational contexts. Based on this conceptualization, we present a research agenda for studying home users' security behavior.

2.2 Introduction

The number of home computer users is rapidly increasing. In 2008, the American research firm Gartner reported that the number of personal computers in use around the world had surpassed 1 billion and predicted that this number would double by early 2014. The large number of individual home users represents a significant point of weakness in achieving the security of the cyber infrastructure (Anderson & Agarwal 2010). While home users have a high chance of providing valuable information to intruders (e.g., information on emails, Internet banking, online shopping, instant messaging, and online stock trading), home users' information

security should also be a concern for organizations. Hijacked home computers are great breeding grounds for hackers and distributors of illegal or morally questionable material. Indeed, Stafford and Urbaczewski (2004) reported that 85% of all personal computers are infected by spyware. It is essential for home users to recognize the risks and take appropriate precautions in their computer security.

Despite the importance of studying home users' security behavior, the main focus of behavioral IS security research has been on organizational contexts, studying such issues as "employees' compliance with IS security procedures" (Bulgurcu *et al.* 2010, Herath & Rao 2009a, 2009b, Li *et al.* 2010, Puhakainen & Siponen 2010, Siponen & Vance 2010). While this research in an organizational context is important, we argue that the home context requires more attention by scholars. While similarities exist between home users' IS security behavior and employees' compliance with IS security procedures in an organizational context, understanding their differences is essential to advancing research and practice on home users' security behavior. We argue that previous research has neglected such differences. As a first step in remedying the gap in our understanding, we first theorize these differences and consider at least nine contextual factors that may result in an individual's behavior consistency in the workplace and at home. We further argue that the same theories (or their constructs) may not explain the use of security features in the home and organizational contexts. Finally, we present a research agenda for studying home users' security behavior.

The rest of the chapter is organized as follows. Section 2.3 reviews previous studies about end users' IS security behavior. Section 2.4 theorizes the differences between organizational and home use. Section 2.5 presents an agenda for future research. Section 2.6 summarizes the findings of the paper.

2.3 Previous work on information security behavior

In order to better understand the research status quo of individual information security behavior, we summarize and review the literature in two main categories: research in the workplace setting and research in the home setting.

2.3.1 Previous research in the workplace setting

Behavioral studies regarding IS security have been emphasized in recent years (D'Arcy *et al.* 2009, Mishra & Dhillon 2006, Puhakainen & Siponen 2010, Siponen & Vance 2010, Vroom & von Solms 2004). Three main issues in the context of an

organization have attracted many scholars in the IS field: (1) security awareness training/education, (2) IS misuse/abuse, and (3) security policy compliance.

Awareness training and education on IS security in an organization are most commonly suggested in literature (Puhakainen & Siponen 2010). Some studies have been practitioner-oriented, presenting practical methods and approaches to call employees' attention to IS security. According to the characteristics of human behavioral change, scholars have suggested respective programs in different stages (Desman 2002, Guttman 1995, Telders 1991). Some have focused on the media, such as on the use of video (Mitnick & Simon 2003, Murray 1991, Peltier 2000), booklets and newsletters (Murray 1991, Peltier 2000, Spurling 1995), and screen savers (Spurling 1995). In terms of the forms and contents of an awareness program, Perry (1985) suggested means to impact user behavior, for example, a senior officer attending an IS security seminar, hiring a consultant to review the organization's IS security program, and so on. De Zafra *et al.* (1998) proposed three fundamental training content categories: knowledge of laws and regulations, security program, and system lifecycle security.

Other studies have been theory oriented. Researchers have established models to explain managerial perceptions of systems risk, including IS security training (Goodhue & Straub 1991). The main reason for IS security training is to communicate the severity and the certainty of sanctions to employees (Straub & Welke 1998). Also, some scholars have proposed the steps of an awareness training program (Tudor 2006, Vroom & von Solms 2002). As the fruit of contents, forms, and specific procedures, awareness training and education play important roles in an organization to help employees develop the concept of security in information systems and demonstrate security behavior.

Parker (1976) first defined "computer abuse" as "the unauthorized and deliberate misuse of assets of the local organizational information system by individuals," including the misuse of hardware, software, data, and computer services (D'Arcy *et al.* 2009, Harrington 1996, Lee *et al.* 2004, Straub 1990). Studies on computer abuse and misuse have applied criminology theories such as deterrence theory (Straub 1990), which predicts that abuse will decrease as a function of the severity and certainty of the expected punishment, and situational crime prevention (Willison 2006), which aims to reduce the opportunities for specific computer crimes. Harrington (1996) found that codes of ethics act as deterrents. Computer abuse is commonly seen as deviant within an organization. Deterrence theory and situational crime prevention aim to decrease the occurrence of the deviance. The premise of these theories is that an organization has the same

mechanisms as society, which can regulate the members' behavior through policies and norms.

Studies on security policies and end-user policy compliance are also abundant (Bulgurcu *et al.* 2010, Herath & Rao 2009a, 2009b, Puhakainen & Siponen 2010, Siponen *et al.* 2007, Siponen *et al.* 2010). Organizations expect employees to obey the rules and conduct security behavior when they are at work. This stream of research commonly applies deterrence theory. Studies have found that certainty and security of sanctions positively associate with one's perceived cost of noncompliance (Bulgurcu *et al.* 2010), significantly influencing employees' compliance intention (Herath & Rao 2009b) or behavior (Siponen *et al.* 2007, Siponen *et al.* 2010). Another commonly used theory is protection motivation theory. Protection motivation focuses on the effect of threat appraisals and coping appraisals. In the context of IS security, threat appraisals are assessments of individuals' levels of security risks, while coping appraisals refer to assessments on whether individuals are capable of complying with security policies and whether such compliance is effective in reducing security risks (Siponen *et al.* 2006). Pahnila *et al.* (2007) integrated protection motivation and deterrence to explain security policy compliance in an organization, but found that sanctions had no significant impact on compliance behavior (Pahnila *et al.* 2007). Similarly, Herath and Rao (2009b) also found that detection probability and security risks had significant impacts on employees' compliance intention, but sanction severity did not. Other theories have also greatly contributed to this issue. Siponen and Vance (2010) applied neutralization theory to explain that employees may use neutralized techniques to rationalize their rule-breaking behavior. Bulgurcu *et al.* (2010) analyzed employees' compliance from a cost–benefit view based on rational choice theory.

2.3.2 Previous research in the home setting

Behavioral studies about IS security in the home setting seem deficient in comparison to studies in an organizational context. Anderson and Agarwal (2010) did a two-phase study to examine home computer user security behavior. One study established an integrated model based on protection motivation theory and the theory of planned behavior. The results showed that the relation between normative belief and home users' intention to perform security-related behavior was not supported, although it has been mostly supported in organizational settings. The second phase study drew upon the concepts of goal framing and self-view to

examine how the proximal drivers affect intentions to perform security-related behavior. The results would help design effective marketing messages to encourage home users' security behavior (Harrington *et al.* 2006). Theories applied in studies of home user security behavior have been quite insufficient. Several studies have drawn on the theory of planned behavior (TPB). For example, Ng and Rahim (2005) proposed an extended TPB model focusing on the social influence, especially the mass media's effect on home users' intention to practice computer security. Lee and Kozar (2008) also proposed an extended TPB model to investigate home users' adoption of anti-spyware software. They added constructs drawn from innovation diffusion theory and IT ethics/morality into the model. Theories explaining employees' information security behavior, like deterrence theory and rational choice theory, have not been examined in the home context.

In summary, the key focus of the behavioral IS security research has been on an organizational context. We argue that, while similarities exist between home users' IS security behavior and employees' behavior in the organizational context, it is necessary to understand their differences. Because previous research has neglected such differences, we first theorize that at least nine contextual factors may result in an individual's behavior inconsistency in the workplace and at home. As a result, the same theories may not explain the use of security features in home and organizational contexts. Based on this conceptualization, we present a research agenda for studying home users' security behavior.

2.4 Understanding information security behavior

Due to the increasing popularity of technology, individuals can use computers in a variety of circumstances or contexts. These contexts can be the workplace, home, or other places offering public computers or networks. We argue that individuals' information security behaviors under different contexts may be complex and changeable.

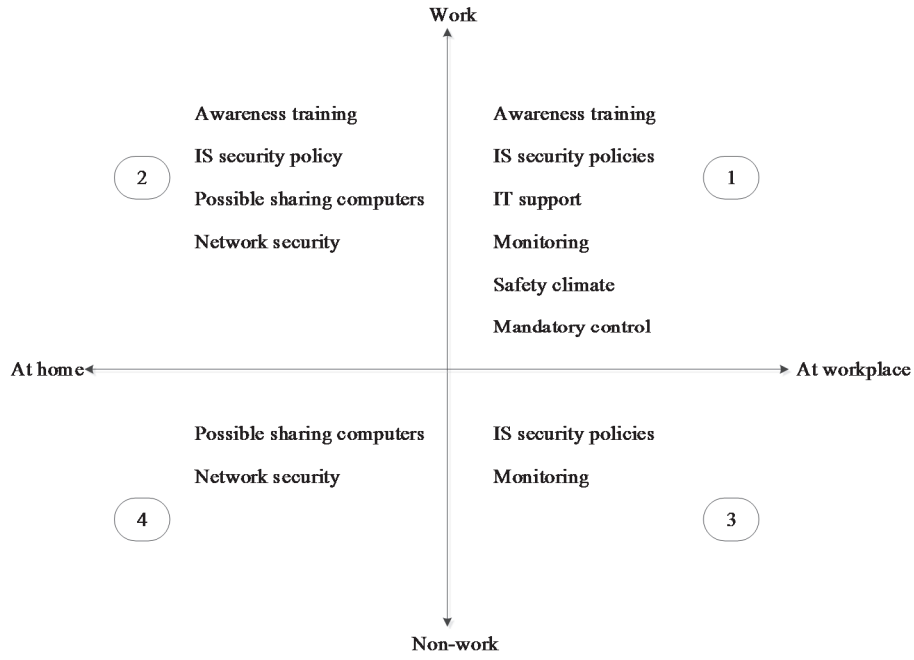

Fig. 4. Features of four contexts.

2.4.1 Individual security behavior inconsistency between home and work

In the home context, individuals can choose whether and how to conduct security behavior. Since the home user's choice is subjective and voluntary, and the environment and conditions differ from those in an organization, home users might exhibit behavior that is inconsistent with that in the workplace. For example, employees do not need to install anti-spyware themselves because the IT administrator does this work, while home users should install it themselves. Home users may judge whether the computer has risks, whether they need the software, and any other factors when they decide to install it. This example shows that, while organizations have IT support, home users do not, and this discrepancy might influence users' decisions and actions to protect their computers. Password habits offer another example. Employees may keep their work-related password secret because of strict security policies that require employees to account for any trouble caused by disclosing work-related passwords to others. However, there may be no

regulations on their personal passwords. People may share non-work-related password to friends, families, or colleagues. This difference relates to the type of use—work at workplace, work at home, non-work at workplace, and non-work at home. The following sections discuss four types of uses, which are not explicitly recognized by existing IS security research.

2.4.2 Type of use: work or non-work

To understand individuals' information security behavior differences, we analyze four types of use that are divided into two dimensions: place and task type (i.e., work or non-work). The flexibility of office models, such as telework, allows people to work anywhere without being confined to a fixed workplace. We chose the workplace and home to discuss because these two locations are typical contexts for most computer users. The second dimension involves the work- or non-work-related tasks that individuals are doing on computers. *Work use* refers to individuals using computers for the purpose of finishing work tasks. *Non-work use* refers to individuals using computers for a personal purpose. Task type (i.e., work or non-work) is a key factor for individuals to determine whether to engage in information security behavior or not. In the following sections, we describe the four types of use and discuss contextual features (see Fig. 4) in detail.

Type of use 1: work at workplace

The information security problems that occur in this situation include employees' noncompliance with organizational security policies. Here, employees do not follow the information security requirements during the working procedure and participate in activities such as gaining unauthorized access, failing to log out when they leave their workstation, or copying confidential data (Siponen & Vance 2010). Another possible noncompliance takes place when people use their computers for personal tasks at the workplace, which we will analyze later. Most of the studies on employees' compliance have not distinguished between these two kinds of noncompliance, and discuss compliance only in a broad sense (Bulgurcu *et al.* 2010, Johnston & Warkentin 2010, Myyry *et al.* 2009).

Type of use 2: work at home

Most information security behavior problems that happen in the workplace cannot be avoided at home since the home provides a much more relaxed work environment for employees. In principal, employees should conform to all work policies and regulations because they should be responsible for their work data no matter where they are working. However, the lack of supervision and management creates a much bigger challenge for an organization in ensuring an employee engages in secure behavior. In this setting, an individual's information security behavior may rely on personal awareness and decisions.

Type of use 3: non-work at workplace

Most organizations are concerned with this problem. Employees use organizational IS resources for personal purposes during and after working hours. This behavior may lead to a waste of IS resources and even a loss of assets. Most organizations expressly prohibit this behavior. Hence, conducting non-work tasks at the workplace can be seen as another kind of noncompliance with procedures. Behavioral studies on abuse and misuse of IS recourses have given rich explanations of this phenomenon (D'Arcy *et al.* 2009, Lee & Lee 2002, Lee *et al.* 2005, Li *et al.* 2010, Tuglular & Spafford 1997, Willison 2006).

Type of use 4: non-work at home

Compared to work at the workplace, non-work at home has different types of use and a different environment for individuals. Individuals have more computer activities at their disposal in the home context. Examples include online shopping, playing online games, web chatting, online stock trading, downloading software and music, and so on. These computer activities provide many enjoyable experiences to the individual, which are different from work activities. Considering the types of use and the context, an individual's attitude toward information security and actual behavior can be different from previous studies in an organizational context. The following section describes at least nine contextual factors that play different roles on the different type of use. By *home use*, we especially refer to type of use 4 (non-work at home).

2.4.3 Contextual factors

With the development of information and communication technologies, people can work with computers both in an organizational workplace and at home. We argue that individuals' information security behavior under different contexts (e.g., between type of use 1 and 4) might be different. The contextual factors have an important impact on individuals' perceptions and could then influence actual information security behavior. In this section, we discuss nine specific contextual factors and their different roles played on the type of use 1 and 4. The nine factors are awareness training, IS security policy, IT support, monitoring, fear factors, safety climate, mandatory control, network security, and sharing computers.

Awareness training

Organizations usually design training programs for security purposes. The programs aim to change employees' attitudes toward IS security, emphasize the importance of IS security, clarify the rules and policies, and highlight employees' responsibilities regarding IS security issues. In terms of content, awareness training commonly includes security events that usually occur in organizations, the risks confronted, the basic concepts of IS security, how to establish good security habits, and recommended supports available when facing security problems. In terms of communication of the awareness or training programs, organizations have many options, such as newsletters, videos, handouts, and leaflets (Murray 1991).

In the home context, end users hardly receive any formal IS security awareness training. Knowledge of IS security mostly comes from self-learning and self-experience. Of course, some people may have received training at their workplace, but no empirical evidence has indicated whether that knowledge transfers to increased home security. In the case of home users, security awareness often arises from panic after end users encounter threats such as viruses, Trojans, and worms, or when they consequently lose data. In addition, social factors may influence home users' security awareness. Ng and Rahim (2005) found that mass media, family, and peers play important roles in promoting computer security. Based on these findings with respect to our first contextual factor, we propose that:

P1: Information security awareness sessions provided by organizations have more influence on type of use 1 than on type of use 4.

IS security policy

IS security policy is an important component of a management system in an organization. Usually, the policy contains regulations on the following aspects: network, devices, data, operation, sanctions, and so on. The policy is not only a guideline for security management, but is also a code of conduct for employees. It instructs employees how to use IS resources correctly and safely, while it deters employees from violating the policy. An IS security policy greatly contributes to keeping IS safe. Policy is therefore an important feature in the organizational context. However, most information security policies are not confined to the workplace. If employees are working outside the office, they also have the responsibility to ensure the safety of organizational materials. Some of the policies take effect no matter where the employees are working. Hence, we propose that:

P2: The effect of information security policy is related to work and hence has more influence on individuals' behavior in type of use 1 than in type of use 4.

IT support

Organizations have the capability to implement a security plan. They invest large amounts of money, time, and resources. The plan makes it easy for employees to get security support on software and hardware, as well as timely human assistance. However, for the end user in the home context, investment in security is limited or non-existent. Insurance for security is missing. Another point is that organizations offer IT support only for work purposes, not for personal tasks unrelated to work. Therefore, IT support exists only in type of use 1. As a result, IT support regarding information security is most limited in type of use 4 with the result that home users need to use their own expertise to secure their personal computers. Therefore, we propose that:

P3: Due to IT support in the organizational context, the level of information security is lesser in type of use 4 than in type of use 1.

Monitoring

Monitoring mechanisms are commonly used in organizations to gain compliance with rules and regulations (Urbaczewski & Jessup 2002). Monitoring systems will

track employees' computer and Internet use, record network activities, and perform security audits (Panko & Beh 2002, Urbaczewski & Jessup 2002). Monitoring as a control method will, to some extent, constrain employees' behavior. Since they know their activities will be recorded, employees will not conduct insecure behavior. Obviously, in the home context, there is no such monitoring mechanism due to privacy protection, so monitoring is not a feasible approach to promote home users' security behavior. Based on this analysis, we propose that:

P4: Due to monitoring in the organizational context, the level of information security is lesser in type of use 4 than in type of use 1.

Fear factors

Fear factors have been examined in papers on IS security management in organizations (Johnston & Warkentin 2010, Lee & Larsen 2009, Li *et al.* 2010, Schuessler 2009, Siponen *et al.* 2007). Researchers have posited two main theories to explain why individuals conduct security behavior due to fear. They are deterrence theory and protection motivation theory. Deterrence theory focuses on formal sanctions that employees receive if they violate security policies. The certainty and severity of sanctions motivate employees' compliance. Protection motivation theory focuses on threat appraisals and coping appraisals. According to this theory, an employee assesses the level of security risks to the organization and whether he or she has the ability to deal with the situation. In terms of context, sanctions occur only in organizations and not at home. In contrast, protection motivation factors are applicable to both an organizational context (Lee & Larsen 2009, Siponen *et al.* 2007) and a home context (Anderson & Agarwal 2010, Woon *et al.* 2005), but the focus of threat appraisal in the home context are the risks confronted by home computers. The fear factors in an organizational context are related to employees' responsibility, but that is not the case in the home context, nor do individuals face sanctions at home. Hence, we propose that:

P5: Fear factors have more influence on individuals' behavior in type of use 1 than in type of use 4.

Safety climate

Zohar (1980) first proposed the idea of a safety climate in an organization and suggested that employees who perceived a strong safety climate in the organization worked more safely. The perception was derived from observance of organizational management as well as the attitudes of superiors and peers (Chan *et al.* 2005). The results of an empirical study by Chan *et al.* (2005) showed that the information security climate encouraged employees' compliance behavior. In comparison, a safety climate is hard to form at home. It relies on each family member's security awareness, desires, and requirements and therefore requires the efforts of all family members. Based on this difference, we propose that:

P6: The safety climate provided by organizations has a greater influence on individuals' behavior in type of use 1 than in type of use 4.

Mandatory control

Mandatory control in an organization describes compulsory procedures established by organizational management to ensure that employees behave in a certain manner (Boss *et al.* 2009). For example, the adoption of anti-spyware or anti-malware on computers in an organization is compulsory because the adoption decision is made by the organization, not the employees. Employees have no rights to choose whether to use the software. However, in the home context, end users have far more independent options. They can choose whether to install protection software or not, as well as what kind of protective technology to use. It is absolutely voluntary. Therefore, we propose that:

P7: Due to IT support in the organizational context, the relevant security behaviors differ between different types of uses, especially between type of use 1 and type of use 4.

Network security

Network security on one hand depends on the safeguards of hardware and software. The IT support that organizations offer, including firewalls and anti-malware software, ensure that organizations are well-prepared for Internet attacks. In the home context, people might invest less on hardware and software, which may result

in a low level of network security. On the other hand, network security relies on the user's maintenance of the system. In an organization, IT specialists explore potential network risks and solve problems. In the home context, unless the user has related knowledge and problem-solving capability, most home users who do not take measures to safeguard networks face the possibility of being attacked by intruders. Hence, we propose that:

P8: The level of network security influences security behaviors in different types of use, especially between type of use 1 and type of use 4.

Sharing computers

Unlike in an organization, where end users may use their own computers, the home context often has several users accessing one home computer. This arrangement increases the difficulty of managing computer security. Therefore, we propose that:

P9: Sharing computers in the home context deceases the level of security behavior in type of use 4, compared to type of use 1.

We summarize the features for each type of use in Fig. 4. For example, if an individual is doing work-related tasks in the workplace (type of use 1), the following contextual factors have an impact on his or her information security behavior: awareness training, IS security policy, IT support, monitoring, safety climate, and mandatory control. However, the influential factors are different in other types of use, e.g., type of use 2, 3 and 4.

2.5 Agenda for future research on home users' information security behavior

Based on our conceptual argument on the differences between home users and organizational employees with respect to information security behavior, we outline a research agenda with seven research streams to investigate home users' information security behavior (especially type of use 4).

The first stream of research endeavors to empirically prove our argument that the nine contextual factors make a difference between the behavior of home and organizational users. One way to justify this argument is to design a theory-testing study, which calls for a model comparison approach in both home and

organizational contexts. Different results in different contexts are expected, which will provide empirical evidence that home users' information security behavior constitutes its own research area.

The second stream of research focuses on the differences between all types of uses. In this chapter, we mainly argued that the different types of uses are not discussed by IS security research, and we provided four potential types of uses. We also argued that there are differences between these, especially between types of use 1 and 4. Future research is needed to study the other types of uses.

The third stream of research is aimed at exploring the types of relevant behavior, which should be studied as "dependent variables," for home users. For example, employees use of anti-spyware software might not be relevant behavior to investigate when studying employees' compliance with organizational IS security procedures, given that it is good security policy that ordinary employees should not have privileges to install any programs. However, the use of anti-spyware software could be a relevant issue for home users. Similarly to Siponen and Vance (2010), who interviewed 56 IS security managers to discover the key problems for employee compliance with organizational IS security policies, future research should explore the required key information security behaviors for home users.

The fourth stream of research could adopt a theory-testing research setting and explore, based on our nine contextual factors, what behavioral theories could best explain home users' information security behavior. A number of potential theories exist in the area of psychology, social psychology, and criminology. In addition to determining which behavioral theories best explain home users' behavior, another possibility is to try to form a unified theory for home users' security behavior à la the unified theory of acceptance and use of technology (Venkatesh *et al.* 2003).

The fifth stream of research is theory development. While the fourth stream of research called for theory testing, we also see that inductive and qualitative approaches are needed. The limitation of the theory-testing setting is that it merely tests if existing theory is supported or not. In contrast, theory development would approach the problem from a clean table without any theories in mind by asking that home users report their reasons for adopting information security measures. Ideally, a qualitative approach would allow researchers to develop new constructs, concepts, and even theories that explain home users' information security behavior. Such in-depth interview studies could also reveal a process that covers the stages for adopting an information security behavior or technique. Possible methods for analyzing the interviews include phenomenography or grounded theory.

The sixth stream of research examines to what extent training the employees have received in their organizations transfers to increased home security. Given that some employees may have received IS security training at their organizations, one might postulate that this knowledge transfers to the home context. On the other hand, IS security training at organizations may not reach the home context for a variety of reasons. First, IS security training at organizations may typically focus on organizational issues (Puhakainen & Siponen 2010). As a result, employees may feel that what they have learned does not apply to the home context; after all, the IS security training at organizations may not have included persuasive messages about the importance of protecting one's home computer. Hence, the topic of whether IS security training at organizations influences home context is an open question for future research.

The seventh stream of research calls for experimental studies. The aim of these studies is to observe how home users' information security behavior can be changed with some kind of treatment, such as theory-based training or campaigning. Following experimental research settings, the participants should be divided into two groups. The experimental group should get a persuasive intervention, while the control group should not. Pre- and post-tests should then be used to evaluate the effect of the treatment. Such experimental research is important because the ultimate goal of the research under the domain of home users' security behavior is not only to explain how things are, but to change them through actions such as training and campaigning.

To sum up, based on our conceptual arguments on the differences between home users and organizational employees, we provided seven directions for future studies. We believe that each of them will contribute to our knowledge on home users' information security behavior.

2.6 Conclusions

The number of home computer users is increasing faster than ever. Home users' security should be an important research topic in IS security research, not only from the perspective of protecting home users' personal or work information on their home computers, but also because hijacked home computers have become an ideal breeding ground for hackers attacking organizations and distributing illegal or morally questionable material. Despite the importance of studying home users' security behavior, the primary focus of the behavioral IS security research has been on an organizational context. While this research in organizational contexts is

important, we argue that the home context requires more attention by scholars. While similarities exist between home users' IS security behavior and employees' compliance with IS security procedures in the organizational context, understanding their differences would allow research and practice on home users' security behavior to develop further. We argue that previous research has not paid attention to such differences. As a first step in remedying the gap in our understanding, we first theorized these differences between the contexts and behaviors of home users and employees at organizations. As a part of this conceptualization, we pointed out that at least nine contextual factors may result in an individual's behavior inconsistency in the workplace and home. Because of this discrepancy, we argued that the same theories may not explain the use of security features in home and organizational contexts. Based on this argumentation, we presented a research agenda for studying home users' security behavior.

3 Users' IS security behavior in different contexts: a contextualized rational choice approach and comparative empirical evidence

3.1 Abstract

The research on users' information systems (IS) security behavior has focused on identifying influential factors of the behavior by applying theories like deterrence theory, protection motivation theory, and rational choice theory (RCT). These theories were originally developed and applied in other contexts, such as criminology, healthcare, and economics, and are contextually sensitive; however, IS security scholars have rarely discussed their assumptions in the IS security context. For example, RCT has been developed in many different contexts, where the discussions began at the assumption level and evolved to the application level, resulting in different versions of RCT. However, IS security behavior research has not done this yet, indicating that the particularity of the IS security context may not be well-considered in the theory development. In this chapter, we present an approach of integrating the IS security context into the use of RCT. This approach implies that the IS security context requires modification of the reference theories from other disciplines as a whole as well as when studying IS security behavior in different specific contexts. To support our argument, we carry out a comparative empirical investigation. By examining the use of strong work password (USWP) and the use of strong personal password (USPP), we show key differences in applying the RCT. The implication for IS security behavior research is to stress the need for further contextual level theorizing.

3.2 Introduction

IS security behavior is an important research stream in IS research. IS scholars have increasingly examined the human aspect of IS security issues, such as IS security policies violations, misuse, computer abuse in organizations, or home users' IS security behavior (Anderson & Agarwal 2010, Bulgurcu *et al.* 2010, Johnston & Warkentin 2010, Siponen & Vance 2010, Straub 1990). The research of this area has widely applied reference theories from non-IS fields, such as criminology, economics, and psychology. Popular theories include RCT, deterrence theory,

protection motivation theory, and neutralization theory. While the use of reference theories has been a successful mode of publication in IS research (Baskerville & Myers 2002), it is important to understand the underlying assumptions of these reference theories, including whether these assumptions are met within the IS security context.

By reviewing the IS security behavior studies, we found that little research has specifically discussed the appropriateness of assumptions of the applied theory in the IS security context. A case in point is RCT, which was derived from neoclassical economics or criminology to explain investment or crimes, respectively, and has been applied to explain IS security behavior (Bulgurcu *et al.* 2010, Li *et al.* 2010, Vance & Siponen 2012). However, the underlying assumptions of the applied RCT were rarely discussed. One key reason for this neglect arises from the deductive research background that attempts to develop generalizable and parsimonious models by extending reference theories to the IS security domain. The borrowed deductive research context does not define what is rational action in the IS security context, but simply applies the previous assumptions to the IS security context; however, these assumptions were originally developed to explain another type of behavior, such as investment or crime. Whether a theory needs modification on the assumption level to fit the context is an issue of concern. The contextualization on the assumption level is not only important in IS security research, but also referential for IS theorists who follow the tradition to introduce theories from other disciplines to explain phenomena in an IS security context.

Recent IS scholars have emphasized the importance of context and the development of contextualized theories (Hong *et al.* 2013). However, Hong *et al.* (2013) suggested that there exists a general theory that can guide the contextualization. We argue that no general theory exists because every theory is based on certain assumptions that may be arguable and context-sensitive. It is very important to contextualize a theory by analyzing the context and examining its assumptions within the context.

To better illustrate our points, we use RCT as an example and show how the theory can be altered by applying different assumptions. By reviewing the literature, we provide some guidelines to develop contextualized theories. In order to demonstrate the necessity of conducting contextualized IS security behavior research, we conduct a comparative empirical study following the guidelines we propose. In the example of password use in work and personal contexts, we discuss their RCT assumptions in the corresponding contexts, and derive hypotheses from

these assumptions. The results indicate that different contexts have different assumptions and therefore require different theorizing.

This chapter is organized as follows. In the next section, we briefly introduce RCT, showing that different assumptions result in different versions of the theory. Next, we discuss the application of RCT in IS security behavior. Then, we review the literature and posit a categorization of the IS security context. Based on the above discussions, we propose guidelines for theory contextualization in IS security context. Then, we conduct a comparative empirical study applying our guidelines. Last, we discuss and conclude our findings.

3.3 Theoretical background

As an example for discussion in this study, we first show how RCT is developed and contextualized in other research fields. The literature review shows profound theoretical differences in developing each own RCT in each field, and the contextualization of RCT often starts from the assumption level. Therefore, the discussion on the role of assumption in contextualizing theory is followed. In addition, as the key element in contextualizing a RCT in IS security context, this section also discusses the important dimensions of IS security context.

3.3.1 Rational choice theory

The rational choice approach is influential in explaining humans' decision-making in many domains of social life. It has been applied to explain IS security behavior (Bulgurcu *et al.* 2010, Li *et al.* 2010, Vance & Siponen 2012). Under the rational choice paradigm, humans are assumed to be naturally rational and to take purposeful actions. Rational choice generally means choosing among alternative courses of action in accordance with certain rationality assumptions (Voss & Abraham 2000). It is worth noting that there is no one rational choice theory, but only rational choice perspectives[1] (Zey 1992). Because RCTs explain human behavior by using different rationality assumptions that depend on the features of the context faced by the actors (Voss & Abraham 2000), researchers have developed a family of rational choice theories that provide different explanations for human behavior. We provide some examples below.

[1] There are different rational choice theories under the umbrella of rational choice perspective. For ease of reference, RCT and RCTs in this dissertation refer to the theories in rational choice perspectives.

The concept of rationality originally stems from economics, which has had the most profound impact on the understanding of rationality. Conventional economics represented by Adam Smith (1732–1790) understood rationality as the seeking of the greatest beneficial choices to meet one's self-interest, which is called the *homo oeconomicus* assumption. On this basis, neoclassical economists developed the rational choice approach using mathematical utility function and operationalizing it to maximize the utility. *Utility* in economics generally refers to the happiness or satisfaction gained from goods or services. Rational actors are seen as "utility maximizers," acting to maximize "the expected utility" (Coleman 1986), "private benefits" (Hardin 1997), wealth (Wittman 1995), "cost-benefit ratios" (Frey & Palacios-Huerta 1997), rent (Tollison 1997), or money income (Opp & Hartmann 1989); alternatively, they may minimize costs, including transaction costs (Williamson 2005) and other "disutilities."

However, as humans' decisions become better understood, scholars have tended to introduce different assumptions about humans' rationality even within the economics field. Simon (1957) posited the concept of "bounded rationality," suggesting that people have limited cognitive capacity for processing information that is available to them. As a result, they do not always choose the optimal choice, but instead they choose a satisficing option that is good enough for them. Under the principles of bounded rationality, Kahneman and Tversky (1979) further proposed the Prospect Theory, suggesting that, in the presence of risk, people put weight on the upcoming outcomes. Kahneman and Tversky (1979) found that people tend to overweigh or underestimate the weight of outcomes not based on the probability of an event but on the impact of events. Becker (1976) suggested that the analysis of rational action in economics would not be limited to material goods and wants or to the market, but extended to "all" social life. Economics has gradually opened to the integration of many forms of human preferences, needs, and desires, according to different research contexts. Some nonmaterial human motives that have received attention in economics include identity (e.g., Akerlof & Kranton 2000), status (e.g., Frank 1985) or respect, self-esteem, and pride (e.g., Khalil 1996, Köszegi 2000, 2006).

In criminology, the conception of rationality/rational choice can be traced back to Cesare Beccaria (1738–1794) and Jeremy Bentham (1748–1832), who are credited as the founders of classical criminology. Bentham developed his theory based on Beccaria, and proposed utilitarianism and the greatest happiness principle.

He formulated an algorithm called felicific calculus to measure the amount of pleasure and pain a specific action causes, suggesting that punishment should be based on the pleasure/pain principle. Rational choice theories of crime explain criminal behavior as a function of expected reward and punishment (Cornish & Clarke 2014), weighted by the subjective probability of detection (Piliavin *et al.* 1986). Cornish and Clarke (2014) suggested that a theory of crime should be crime-specific and that criminal choice is affected by the immediate contextual characteristics. In agreement with this point of view, Paternoster and Simpson (1993) later developed a rational choice model of corporate crime, suggesting that corporate offenders are affected by the context, i.e., by the characteristics and imperatives of their business organization. Social control theory has a strong rational choice flavor in deviance research (Hirschi 1969). The theory highlights the social context where people make rational choice decisions, suggesting that an individual's bonds to conventional social institutions influence deviant behavior.

RCT has been vigorously developed in fields such as sociology and political sciences. These disciplines have developed different rational choice theories as well. Social capital theory is a rational choice-based theory that explains stratification and rests on the assumption that "my connections can help me" (Cross & Cummings 2004, White 2002). Social capital theory concerns the purposeful establishment of relationships and an individual's drive to employ them to generate intangible and tangible benefits in the short- or long-term. The benefits could be social, psychological, emotional, or economical (Lin 1986, 1999, 2000). The theory of justice, which is a political theory, discusses the features of a desirable and feasible societal structure and how to achieve the just distribution of goods in a socio-political arrangement (Rawl 1971). The theory suggests that, when individuals are under the "veil of ignorance," their personal interests are screened out and they are aware of only the general truths about primary goods (Rawl 1971). The assumption of maximizing the justice in this theory is quite different from those assumptions of maximizing self-interest.

Although many other versions of RCT exist, this sampling serves to show that different contexts produce different RCTs. Rational choice is an approach to theory that can result in competing or even contradictory theories (Quackenbush 2004). One reason for the diversity of RCTs is that these theories hold different assumptions. Much of the debate about RCT is fundamentally a debate about the assumption. In the following section, we discuss the role of assumptions in RCT.

The role of assumptions in RCT

An assumption is an untested starting point or belief in a theory that is necessary in order to build a theoretical explanation (Neuman 2009). All theories contain built-in assumptions, which are statements about the nature of things that we cannot observe or do not empirically evaluate. It should be noted that assumptions are the basis of any theory (Quackenbush 2004); as a result, the conclusions of a theory depend on the theory's assumptions.

We distinguish two types of assumptions in RCT. The first is the core assumption, which is the foundation to establish the theory. It must exist, and every following theoretical element must be built on or around the core assumption. The "self-interest" assumption in mainstream economics is an example. It is the behavioral "microfoundation" necessary for theorists to construct the theory (Wittek *et al.* 2013). Theorists need to agree with the foundation in the new context and then can they build theories on it. However, the core assumption is arguable and context-sensitive, meaning that it may not be generalizable to other fields. For example, competing assumptions, such as the "altruism" assumption, have been made in sociological RCT research. Typical core assumptions in RCT include assumptions about rationality (e.g., full rationality, bounded rationality, procedural rationality, social rationality), preference (e.g., selfishness, opportunism, egoism), materialism (e.g., tangible, intangible, physical wellbeing, social wellbeing), and individualism (e.g., natural, social, institutional, structural) (Wittek *et al.* 2013). Such assumptions vary across contexts.

Despite the importance of a core assumption, more is needed to confirm the rationality of behavior. For example, if we assume that "individuals are maximizers of utility," without additional assumptions, it is impossible to know what choices are optimal for a particular decision-maker because we do not know what the utility is. *Utility* may mean something different for different people or for the people in different contexts (e.g., material utility, emotion utility). In order to make a testable hypothesis and verify it, additional assumptions known as auxiliary assumptions must be introduced.

The Duhem–Quine thesis specifically discusses auxiliary assumptions (Duhem 1954, Quine 1951). The main idea is that it is impossible to test a scientific hypothesis in isolation because an empirical test of the hypothesis requires one or more auxiliary assumptions. For example, we assume that the earth is round (core assumption). Then we make a hypothesis that, if we observe a sailboat coming from a far distance, we will first see its masts and then its hull. Actually, this hypothesis

must be tested under a series of auxiliary assumptions, such as that light travels in a straight line and that the seawater lays flat on the surface of earth. Just as the hypothesis is uncertain, the auxiliary assumptions are arguable as well. When empirical evidence fails to support a hypothesis, both the hypothesis and the auxiliary assumptions should be revisited (Quine 1951). An auxiliary assumption can help verify the theory. However, the existence of auxiliary assumptions also implies that a theory that seems plausible in one context may not remain so in another context because auxiliary assumptions are often subject to change over time or across contexts. More importantly, the change of assumptions means that it is no longer the original theory being verified, but a new one.

Previous RCT-based studies in IS security research have rarely specified their underlying assumptions in terms of both core assumptions and auxiliary assumptions, so we emphasize them in this chapter. We suggest that the analysis of context helps make appropriate assumptions, which in turn helps develop our own rational choice-based theories in the IS security context.

RCT in IS security behavior research

As discussed above, differences in context offer researchers the possibility to develop different RCTs, leaving a wide avenue for future research. Since RCT is also a popular theory in explaining IS security-related behavior, we are inspired to examine how existing studies have applied the rational choice approach.

In IS security behavior literature, RCT is an influential theory explaining behavior such as employees' IS security policies compliance or violation in an organization (Bulgurcu *et al.* 2010, Herath & Rao 2009a, 2009b, Hu *et al.* 2011, Li *et al.* 2010, Siponen *et al.* 2010, Vance & Siponen 2012, Willison 2006) or an organization's information security compromise (Ransbotham & Mitra 2009). These studies have been based primarily on economic and criminological approaches of rational choice (Becker 1968, Clarke & Cornish 1985, McCarthy 2002, Paternoster & Pogarsky 2009, Paternoster & Simpson 1993, 1996), conducting the cost–benefit analysis under their corresponding assumptions. Table 2 summarizes RCT-based research in the IS security behavior domain.

Studies from economics perspectives have mainly applied two distinct approaches: the neo-classical economic approach (Bulgurcu *et al.* 2010, Herley 2009) and the behavioral economics approach (Acquisti & Grossklags 2005, Aytes & Connolly 2004). The two approaches are based on different assumptions of human rationality and therefore produce very different findings. With respect to the

forms of benefit and cost, an economics approach usually focuses on tangible value (Ransbotham & Mitra 2009), such as time (Vance & Siponen 2012) or money (Li *et al.* 2010). Other studies have followed the criminological approach or have combined criminology with economics (e.g., Li *et al.* 2010, Vance & Siponen 2012).

The criminological approach of RCT assumes that humans pursue happiness and avoid pain. Representative rational choice factors identified in the literature are sanctions (Herath & Rao 2009a, 2009b), intrinsic benefits (Bulgurcu *et al.* 2010) such as mental pleasure (Hu *et al.* 2011), thrills, or excitement (Vance & Siponen 2012) or negative feelings such as guilt and shame (Bulgurcu *et al.* 2010). Several studies have identified some other forms of benefits and costs from the context, such as work impediment (Bulgurcu *et al.* 2010), relative advantage for job performance (Guo *et al.* 2011), and security risks (Li *et al.* 2010).

These findings suggest that RCT is an important approach to study users' IS security behavior. However, a comparison of the different versions of RCT in other research fields, such as in social science or political science, may reveal a large space for discussion on the RCT approach in the IS security behavior field. Existing studies have not specifically justified the assumptions of economists and criminologists before they were applied to the IS security context. Since the assumptions are context-sensitive, researchers have significant opportunities to advance the RCT approach in the IS security behavior domain by considering differences in contexts and building the RCT on appropriate assumptions. In the next section, we present an approach that incorporates the IS security context into the RCT development.

Table 2. Applications of RCTs in IS security behavior research.

Author & year	Description of work	Indication
Acquisti and Grossklags (2005)	Criticize the application of neoclassical economics for privacy decision-making. Adopt the behavioral economics rational choice approach.	Decision-makers' privacy decisions are made with incomplete information, limited cognitive capabilities, and biases.
Aytes and Connolly (2004)	Propose a rational choice model of unsafe computing practices of undergraduate students based on the bounded-rationality assumption.	Although users appear to be cognizant of the risks, this knowledge does little to curb unsafe behavior.
Bulgurcu *et al.* (2010)	Develop a theory to explain employees' information security policy (ISP) compliance behavior. Use rational choice theory of neoclassical economics as a framework and use TPB to specify the preferences and beliefs.	Benefits of ISP compliance are shaped by intrinsic motivation, safety, and rewards. Cost of compliance is formed into work impediment while the cost of noncompliance is formed into intrinsic cost, vulnerability, and sanctions.
Herath and Rao (2009b)	Develop a model to explain employees' ISP compliance intention based on protection motivation theory and deterrence theory.	The study focuses on the costs of noncompliance. The costs include punishment severity and detection certainty. Other costs from the protection motivation theory are perceived probability of security breach, security breach concern level, and the response cost.
Herley (2009)	Explain users' rational rejection of security advice from purely economic perspective.	Users' rejection is the result of poor tradeoff between the benefit and cost. The long, complex, and growing sets of advice, mandates, policy updates, and tips sometimes carry vague and tentative suggestions, which take too much time and effort for the user.
Hu *et al.* (2011)	Develop a model about security violation behavior in corporate settings with the rational choice theory at its core and elements from other theoretical frameworks at its periphery (i.e., low self-control, moral beliefs, shame, deterrence). The study accepts that rationality is dependent on human limitations and that the utility calculation should consider the subjective costs and benefits.	Benefits include material or intrinsic benefits (e.g., mental pleasure). Costs include risk of formal and informal sanctions, and risk of shame. Additionally, two internal and one external to the individual forces affect the cost and benefit evaluation. They are: individual propensity (i.e., the degree of low self-control), the individual's moral beliefs, and the perceived deterrence (i.e., the perceived certainty, severity, and celerity of sanctions).

Author & year	Description of work	Indication
Li *et al.* (2010)	Develop a model of Internet use policy compliance intention. The authors adopt the economic rational choice theory of Becker (1968) that emphasizes that the economic models of human behavior apply to crime behavior (and other contexts).	Employees are assumed to comply with Internet use policies after a cost–benefit calculation. The costs include formal and informal sanctions and perceived security risks. Perceived benefits of noncompliance are formed into time-saving, money-saving, convenience, and interesting work life.
Ransbotham and Mitra (2009)	Develop a model of information security compromise process from the perspective of the organization. The study adopts the assumption that Internet attackers, like criminals, are rational individuals who weigh the cost–benefits of criminal activity.	Perceived attractiveness (i.e., benefits) includes tangible, iconic, and reprisal value. Costs are associated with the difficulty of realizing the attack, which is associated with measures of access control, vulnerability control, feature control, traffic control, and audit control.
Siponen *et al.* (2010)	Develop a model to explain employees' ISP compliance intention and actual compliance. The model is based on deterrence theory, theory of reasoned action, protection motivation theory, and innovation diffusion theory.	Costs that affect compliance behavior are sanctions, specifically the certainty, severity, and celerity of sanctions, social disapproval, self-disapproval, and impulsivity. The benefits considered are tangible (e.g., money) or intangible (e.g., praise).
Vance and Siponen (2012)	Develop a model of intentional information security policy violations. The study assumes that violations are deliberate choices of the attacker after a calculative decision process.	Perceived benefits in the model include intrinsic ones, such as thrill or excitement, and extrinsic ones, such as time. Costs include formal and informal sanctions and moral values.
Willison (2006)	Develop a model to analyze the relationship between a computer crime offender and the context while committing the crime. The study uses rational choice theory of crime (Cornish & Clarke 1986), and Situational Crime Prevention to explain the offender's behavior in the whole crime-committing procedure and the associated criminal choices.	The study models the computer crime decision-making process, by adapting the model of Cornish and Clarke (1986) for the organizational information security context. The paper provides in-depth analysis of computer crime choices within the process of committing such crime and how security controls might deter the offender in each procedural stage.

Author & year	Description of work	Indication
Willison and Backhouse (2006)	Provide a model of information security risks from the offender's perspective. The offender decides whether a certain context offers an opportunity based on the perceived costs and benefits. The study advances the opportunity structure for corporate computer crimes, using rational choice theory of crime (Cornish & Clarke 1986) and other criminology theories (e.g., situational crime prevention).	The study adopts the rational choice model of crime including the principle of bounded rationality, limited access to information for decision-making, and crime specificity. It elaborates on the opportunity structure for computer crime offenders by adapting the opportunity structure for crime to the corporate computer crime context (e.g., facilitators are connected to the routine activities of the staff and the physical environment).

3.3.2 IS security context

We define the IS security context as the circumstances, conditions, situations, or environments that are external to the IS security-related behavior and enable or constrain it. Recent research has begun to emphasize the role of the situation or context in an investigation of humans' behavior in management and information systems (e.g., Bamberger 2008, Hong *et al.* 2013, Johns 2006). One way to develop theories that provide actionable advice to practice is to take the context into greater consideration (Hong *et al.* 2013, Weber 2003).

Previous work on context dimensions

IS and organizational behavioral research have attempted to group the context effects into different dimensions (e.g., Johns 2006, Polites & Karahanna 2013). The approach makes the complex contextual factors clear, and provides implications for further identifying the effects of each dimension on the observed phenomenon. However, the existing dimensions of context range widely, reflecting different practical needs and philosophical orientations (Griffin 2007). Relevant research fields, such as organizational behavior and human–computer interaction, construct different dimensional structures of context (e.g., Bradley & Dunlop 2005, Johns 2006). In IS security literature, to our knowledge, the dimensions and meanings of the IS security context are still in their infancy.

By reviewing contextual dimensions research in neighborhood areas, we have gained some insights. For example, drawing on classical and environmental psychology, Johns (2006) proposed that the contextual dimension of organizational

behavior is related to the task context (e.g., autonomy, uncertainty, accountability, and resources), the social context (e.g., social density, social structure, and direct social influence), and the physical context (e.g., temperature, lights, the built environment, and décor). Polites and Karahanna (2013) suggested that several contextual factors can influence the formation of IS habit, namely the temporal context, the physical context, the social context, and task definition. In the area of human–computer interactions, researchers have proposed a variety of categorizations of context. Common categories include a user's location and environment, identities of nearby people and objects, and changes to those objects (Brown *et al.* 1997, Dey 1998, Ryan *et al.* 1998, Schilit & Theimer 1994), whereas some studies have used additional categories such as time of the day (Brown *et al.* 1997, Ryan *et al.* 1998). Schilit and Theimer (1994) differentiated among three broad types of context: (1) the computing environment, (2) the user environment, and (3) the physical environment. Bradley and Dunlop (2005) synthesized the understanding of context from multiple disciplines and proposed a model of context, including task, physical, social, temporal, application, and cognitive contexts.

A categorization of the IS security context

The relevant literature mentioned above sheds light on our development of the IS security context framework. We then propose a categorization of the IS security context, which is the basis for theory contextualization. The categorization is summarized from the existing IS security behavior literature. The existing studies have separately investigated different types of contextual factors, representing important aspects of context. Overall, we categorize the IS security context into four dimensions: user context, task context, social context, and technology context. The specific descriptions of each context dimension are as follows.

User context

We define *user context* as the personal factors that are internal to the user and to some degree stable over time and place. Demographical information reflects the basic individual differences between users, including factors such as age, gender, occupation, and education background. Specific demographical groups have been used as proxies for distinctions between user contexts (Pedersen & Ling 2003). IS studies have investigated the differences between teens and adolescents as well as males and females in their IS adoption decisions (Comber *et al.* 1997, Durndell *et*

al. 2000, Durndell & Haag 2002, Ong & Lai 2006, Whitely 1997). In addition, user context would be the internal knowledge/mechanisms underlying the user's cognitive process. These mechanisms may include mood, emotional state (Ziemke 1997), goal, user value, experience, and personality. Taking user value as an example, users may assign different values in different contexts, and the values may affect their actions in different contexts. According to Boztepe (2007), user value can be self-oriented or other-oriented, extrinsic or intrinsic, resulting in four main types of user value: utilitarian, emotional, social, and altruistic. The different values adopted by users may influence how they use IS and their IS security behavior. In IS literature, researchers have noted individual differences such as personality, demographic characteristics, and other individual aspects as the influential factors affecting IS users' beliefs and behaviors (Agarwal & Prasad 1999). Loch and Conger (1996) found that computer experience as a user contextual factor is negatively related to technology misuse. Shropshire *et al.* (2015) found that personality (e.g., conscientiousness and agreeableness) moderates the relationship between security software use intention and actual use.

Task context

In this study, we define *task* as a certain IS security-related practice. The task could be a protective practice aiming to achieve a desired security state (e.g., adopting anti-spyware, using strong passwords), or it could be a risky practice against IS security goals (e.g., downloading cracked software, clicking a suspicious link to a dangerous website). Specifically, task context involves three aspects: task environment, task characteristics, and resources.

The term *task environment* refers to the external security-related environment that may impact the user's IS security behavior. It typically includes factors such as security risks, threats, and vulnerability of IT resources. Researchers have proven that perceptions of task environment significantly impact the employee's compliance with IS security policies (Johnston & Warkentin 2010, Li *et al.* 2010).

Task characteristics include various attributes of IS security practices, such as task type (e.g., job relatedness [Guo 2013] and security-related tasks regarding banking, shopping, and gaming), task value (e.g., advantages of taking precautions), task consequences (e.g., positive or negative), task barriers (e.g., complexity, difficulty, and inconvenience), and task non-routineness (routine versus non-routine) (Karimi *et al.* 2004). Task characteristics could be a direct reason for users to make IS security-related decisions. Empirically, Guo *et al.* (2011) found that

relative advantage for job performance was positively associated with nonmalicious IS security policy violations. Bulgurcu *et al.* (2010) determined that work impediment was positively associated with the employee's perceived cost of compliance but negatively influenced the employee's attitude toward compliance.

Resources constitute a third dimension of the task context. Resources may include time, money, knowledge, and manual assistance that can either facilitate or constrain the target IS security practices. Examples are training, guidelines, and IT assistance in the organization (D'Arcy *et al.* 2009). On the one hand, they provide supports and make the security task easy to accomplish (Herath & Rao 2009b, Pahnila *et al.* 2007). On the other hand, they can be used to deter the misuse of IT (D'Arcy *et al.* 2009).

Social context

The social context includes the social structural and direct social influence on the individual's IS security behavior. *Social structural influence* refers to the influence of an individual's social position on that person (Pfeffer 1991). Social structural position includes network location (e.g., one's position in the organization or in a network of acquaintances or strangers), physical location (e.g., workplace, home, or public), and one's social status indicators (e.g., income, tenure in the organization). The differences in social structure position could be a contextual factor in influencing user IS security behavior. For example, Guo *et al.* (2011) determined that identity match negatively influences user violations of IS security policy; that is, users in the organization related their dealing with security issues and following security policies to their identities as business professionals. Additionally, social structure may extend beyond the formal structure within the organization. The concept can extend to the non-work setting as well. One example could be that, in a family, one individual may take the main role of maintaining computer security rather than the spouse; as a result, one's role could be a social structural factor influencing IS security behavior.

Direct social influence refers to the impact of group norms, values, and beliefs. Direct social influence addresses the norms or pressures arising from the approval or disapproval of other people around the focal person (Herath & Rao 2009a, Pahnila *et al.* 2007). The norms can be formal, such as an organization's IS security policies. For example, if users violate the policies, they could be punished (D'Arcy *et al.* 2009, Herath & Rao 2009a). Other norms are informal and may be formed by

significant others, such as coworkers or peers (e.g., Guo *et al.* 2011, Siponen & Vance 2010).

Technology context

The fourth dimension of IS security context is *technology context*. We define *technology context* as the existence and functionality of hardware and software facilities. Usually, hardware and software combine to affect the user's security behavior. For example, in an organization, employees may be required to work on authorized computers and devices, which is a means to limit users' rights of usage for security purposes. Also, monitoring devices or applications installed on the computer could help to deter employees' misuse of organizational IS resources (D'Arcy *et al.* 2009). In addition to IT equipment and applications, the functionality and performance of hardware and software could influence users' behavior as well. Lee and Kozar (2008) found that computing capacity (e.g., memory size, hard disk capacity) and trialability positively influenced users' attitudes toward adopting security tools.

Cataloguing previous IS security work

In order to show that our dimensions of the IS security context could well cover the existing findings in terms of contextual factors, we summarized their definitions and categorized them into our framework. Appendix 1 provides illustrative examples of contextual factors identified from previous studies. Appendix 2 lists the main studies in IS security behavior and shows that most of them just focused on one or two dimensions in our framework. From Appendix 2, we see that (1) contextual factors require more attention, since previous studies have overlooked the contextual factors in other dimensions, and that (2) dominant studies have been in organizational context, which raises the question of whether it is appropriate to apply the conclusions of the effects of the contextual factors to other contexts (e.g., home).

3.4 A theory-guided approach to developing RCT in the IS security context

We suggest that the development of RCT is a process of contextualization of the theory. Context determines how the theory is applied and developed. As noted in

Hong *et al.* (2013), context has an important value in theory development. Contextualized theory represents high practice relevance, which can provide useful and actionable advice in reality. As Alvesson and Kärreman (2007: 1272) argued, "no theory is always wrong or always right—all are more or less relevant and helpful in different situations." This statement implies that the context differences are the motivations to develop different theories. We argue that analyzing context is the first task in contextualizing a theory. Our suggestion contradicts Hong *et al.*'s (2013) first guideline, which states that a general theory should be selected to guide the contextualization efforts. We argue that theories are hardly general because every theory is grounded upon specific assumptions (core assumptions and auxiliary assumptions), which are all context-sensitive. Theory contextualization should start from identifying the context features and then examining or modifying the assumptions according to the context. Just as there is no single RCT, no one general theory can guide all fields of research because these contextualized theories rest on very different fundamental assumptions. In the following sections, we provide specific guidelines for developing contextualized RCTs in IS security behavior research. Fig. 5 provides an overview of our proposed approach.

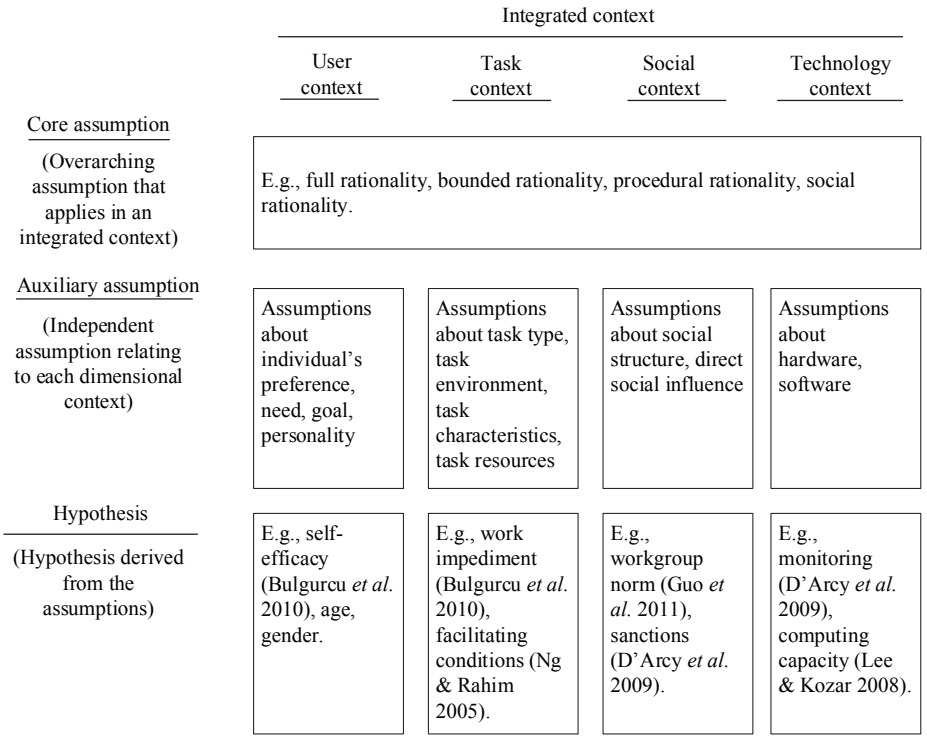

Fig. 5. A context-based decomposed RCT approach.

Guideline 1. Analyze the context

The researcher should first identify the features of context that are relevant to the phenomenon of interest. We define the IS security context as the circumstances, conditions, situations, or environments that can influence IS security-related behavior (see Cappelli & Sherer 1991, Johns 2006, Hong *et al.* 2013, Mowday & Sutton 1993, Welter 2011, Whetten 2009). In order to systematically analyze the context, we recommend the context categorization approach, which is commonly used in IS and relevant research fields such as organizational behavior and human–computer interaction research (Bradley & Dunlop 2005, Johns 2006, Polites & Karahanna 2013). The approach clarifies the complex context and guides the examination of each dimensional context's role. In this study, the categorization approach to context is also important in helping examine the appropriateness of RCT assumptions. IS security behavior literature has verified many contextual

factors in different dimensions (summarized in Appendix 1), which implies that these context dimensions are important in understanding the behavior. Based on these studies, we summarize four dimensions of context: user context, task context, social context, and technology context.

As discussed above, *user context* refers to the internal context of the user, including his or her demographical background (e.g., gender, age, nationality), preferences, goals, needs, and propensity. Willison and Warkentin (2013) highlighted that different explanations should be provided for the IS policy violations with different users' intents, such as the non-volitional noncompliance, volitional (but not malicious) noncompliance, and intentional malicious computer abuse. We suggest that the different treatments should not only be subject to different assumptions about user context, but should extend to other environmental contexts addressing the task, social setting, and technology. The task context includes the task type (e.g., using strong password, locking computer, downloading suspicious files), task environment (e.g., forms of security threats), task characteristic (e.g., positive versus negative consequences, job relatedness, routine versus non-routine), and task resources (e.g., facilitating conditions). The social context includes the social structural influence, such as an individual's social position, and the direct social influence (e.g., from a workgroup or from family). The technology context includes the conditions of hardware and software. This categorization is not intended to be exhaustive, but we aim to highlight the context differences existing on these exemplar dimensions that may influence the development of RCT.

Guideline 2. Make core assumptions

Researchers make core assumptions by considering them in an integrated context (i.e., the overall context that comprises all the context information together). The core assumptions form the overarching foundation and are assumed to be valid in the integrated context as well as in each dimensional context. However, the core assumption does not mean it is context-free. Actually, the integrated context differs from context to context (e.g., in economics and political science), which requires different core assumptions as well. Even studies in IS security behavior research may be situated in totally different integrated contexts, such as the employees' and home users' IS security behavior (Anderson & Agarwal 2010, Bulgurcu *et al.* 2010). For example, Bulgurcu *et al.* (2010) conducted a study in the context of employees' ISP compliance in an organization. Their study applied the neo-classical economic

assumption as the core assumption that individuals determine how they will act by balancing the costs and benefits of their options. In a different research context, Aytes and Connolly (2004) examined unsafe computing practices of undergraduate students. They apply a bounded-RCT assumption that risky computing behavior was a result of individual choices at least weakly guided by considerations of the probability and desirability of choice consequences. Under different core assumptions, even contradictory results have been found. Bulgurcu *et al.* (2010) found that IS security awareness positively influenced employees' attitude to comply, which in turn increased their compliance intentions. However, Aytes and Connolly (2004) found that undergraduate students' awareness of risks did little to curb their unsafe behavior.

Guideline 3. Make auxiliary assumptions

Researchers make auxiliary assumptions by considering them in each dimensional context. The auxiliary assumptions go into greater detail and are closely connected to the detailed context, such as the user, task, social, and technology contexts. Each dimensional context can be more detailed (e.g., users' goals or needs in the user context). Again taking Bulgurcu *et al.*'s (2010) study as an example, the authors made several auxiliary assumptions before they derived their hypotheses. For instance, they made the following assumptions about the user's role: "the ISP stipulates an employee's role and responsibilities in protecting the information and technology resources of the organization" (p. 529), the user's preference: "employees are concerned with the safety of their information and technology resources at work" (p. 531), and the social context: "direct social influence mainly from the executives, colleagues, and managers" (p. 532). We can see that the auxiliary assumptions are very specific and vary in different situations. Those valid assumptions in an organizational context may be relaxed in a home context. Therefore, any changes in these auxiliary assumptions cast doubt on previous findings, and may mean the modification of the theory.

Guideline 4. Derive hypotheses from the assumptions

Hypotheses should be derived from the assumptions made, and they should not contradict other assumptions. A *hypothesis* is a testable version of a theoretical proposition that has not yet been tested or verified with empirical evidence (Neuman 2009). We suggest that every hypothesis can be traced back to certain

assumptions that are harmonious with the adopted theoretical perspectives. The suggestion is noteworthy especially when two and more theoretical perspectives are introduced, which is quite common in IS security behavior studies. Researchers should check all the assumptions and hypotheses to determine whether they are contradictory.

3.5 A comparative empirical study applying the approach

Applying our proposed RCT approach, we conducted a comparative empirical study comparing the use of strong passwords in a work context and a personal context.

3.5.1 Background

In this study, we attempted to show the different assumptions made, examined the model in two contexts, and expected different results. We investigated the use of strong work password (USWP) and the use of strong personal password (USPP) for an example. USWP typically refers to a situation when a password is used for work purposes, such as a password for logging into a work computer, the company email account, or the salary system. In contrast, USPP refers to a situation when a password is used for non-work-related, personal purposes, such as a password for a personal email account, personal Internet banking, or personal instant messenger. We used password behavior as the example because, first, password behavior is an important and representative IS security practice (Sophos 2014, Symantec 2013, Zhang *et al.* 2009). Second, the behavior reflects the user's own decision and action in both settings. In this sense, some IS security practices are not appropriate for the comparison, such as installing anti-virus software on a work computer that may be done by IT specialists in the organization rather than the users themselves.

3.5.2 Comparing the RCT assumptions in USWP and USPP contexts

In the current research context, we posited the core RCT assumption that a user's decision regarding the use of a strong password is the result of assessing the impetus and impediment factors in the context. *Impetus factors* are the factors affecting secure actions that users feel are beneficial, that facilitate activities, or that they are forced to take, such as those that offer advantages for work, IT support, and monitoring. By contrast, impediment factors make it difficult for users to take

secure actions and may include inconvenience or effort. This assumption expands previous assumptions that were adopted from economics and criminology. It takes more contextual factors into account and is not limited to benefit and cost, or happiness and pain. For example, monitoring may be a contextual impetus factor that forces users to use a strong password. However, this factor could not be derived from the economics and criminology assumptions. In this particular study, we regard that this assumption is appropriate in studying both USWP and USPP.

After establishing the core assumption, we analyzed the auxiliary assumptions in USWP and USPP contexts. On the auxiliary assumption level, we noted differences in the four dimensional contexts. Table 3 provides the comparison in detail. We then derived our hypotheses based on these recognized differences.

Table 3. RCT-based theoretical comparison between USWP and USPP contexts.

RCT assumption	Context dimension	USWP context	USPP context	Hypothesis
Core assumption	In the integrated context	Individuals who make decisions regarding IS security behavior by evaluating the impetus and impediment factors in context.		H1, H2, H3, H4, H5
Auxiliary assumption	User context	An employee who has a work responsibility to use a strong work password.	An ordinary user who may voluntarily use a strong personal password.	H4, H5
	Task context	-For protecting work-related data. -Facilitating conditions are from IT specialists in the organization.	-For protecting non-work-related data. -Facilitating conditions are limited and unprofessional.	H1, H4, H5
	Social context	-In an organizational context where the influential people are managers and coworkers.	-In a personal context where the influential people are families and friends.	H2
	Technology context	-Organizational systems that manage employees' work passwords.	-Systems provided by service vendors, which manage personal passwords.	H3

3.5.3 Research model and hypotheses

We built the research model based on the rational choice framework that we proposed above. The model intends to show how specific contextual factors influence USWP and USPP in different ways. As shown in Fig. 6, a user's IS

security behavior is influenced directly by contextual factors, including the impetus factors (i.e., facilitating conditions, embarrassment, monitoring, and task benefit) and an impediment factor (i.e., task cost). We proposed the following hypotheses.

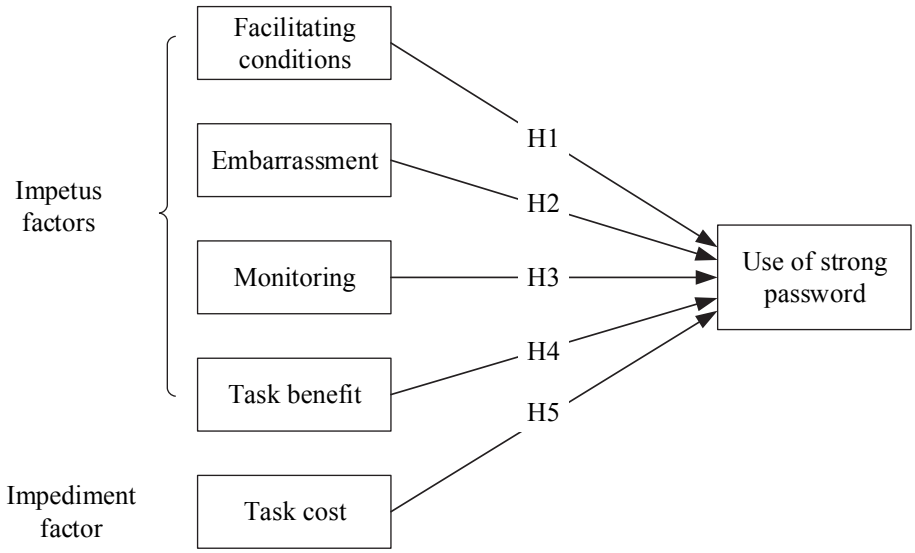

Fig. 6. Research model.

Facilitating conditions

As a type of task resource, facilitating conditions refer to the beliefs about the availability of resources to facilitate behavior (Taylor & Todd 1995). Facilitating conditions are external factors that may promote the performance of a behavior. In a work context, facilitating conditions refer to the organizational support or availability of assistance to individuals who need help in security-related practices and may include the availability of guidelines and manual assistant (Saks & Belcourt 2006, Siponen 2000, Thompson *et al.* 1991). People in the work context have easier access to resources or IT support from the organization, which limits the barriers users face in performing a security behavior. In comparison, such resources are not so easy to obtain in a personal context. Guidelines may be available online, but users must take time and effort to identify. People who can help may be one's friends or a charged service. Moreover, facilitating conditions in the personal context may not be a reliable and professional source, or they may

incur extra costs. Users may feel that obtaining the necessary assistance and resources is more difficult than in a work situation. Ng and Rahim (2005) found that facilitating conditions (e.g., time and financial resources) did not relate to home users' security behavior. Considering the use of a strong password, we suggest that facilitating conditions may likewise have a stronger impact on users in a work context than in a personal context. Therefore, we hypothesize:

H1: Facilitating conditions have a stronger positive impact on USWP than on USPP.

Embarrassment

Grasmick and Bursik (1990) stated that embarrassment is a form of informal sanction when an individual might lose someone's respect if he or she engages in a particular behavior. This embarrassment is a socially imposed punishment, although the most immediate consequence probably is a physiological discomfort. More long-term consequences of embarrassment might include the loss of valued relationships and perhaps a restriction on opportunities to achieve other valued goals over which significant others have some control (Grasmick & Bursik 1990). Therefore, the concern of embarrassment can influence people's IS security behavior. We argue that, for the use of strong passwords, the influence of embarrassment in a work context will be stronger than it is in a personal context. In a work context, the social influence may come from one's supervisor or other colleagues, whose opinions could have important impact on the focal person's performance evaluation or promotion (Siponen & Vance 2010). In a personal context, the social influence may come from family members, friends, and other peers (Hu *et al.* 2011).

In a work context, the disapproval from the work group (including supervisors, colleagues, etc.) may finally influence the individual's performance evaluation in a more formal way. The mistakes an employee has made will lead others to doubt the focal person's sense of responsibility or even work ethics. The negative consequences are serious concerns for an employee in the organizational context; therefore, it is easier for the focal person to feel the embarrassment. We regard that such concerns on the consequences may not exist in a personal context. Since the disapproval of similar mistakes may come from the focal person's family and friends, the focal person is less likely to feel embarrassment because of the intimacy. Instead, the individual may even receive more empathy from his or her close peers.

In this vein, individuals are more likely to feel embarrassment in a work context than in a personal context. Therefore, we hypothesize:

H2: Embarrassment has a stronger positive impact on USWP than on USPP.

Monitoring

Monitoring represents a technology contextual factor. *Monitoring* in this study refers to the function of detecting whether the user's operation of the computer is secure based on a given security criterion. For example, some functions are used to check the complexity of a user's password, or to detect whether the user is browsing an untrusted website. Monitoring as a software facility could provide users with feedback and suggestions for improvement with regard to IS security. As a part of a security control system in the work context, monitoring is one form of organizational IS security countermeasures, which is the first shield to prevent employees' inappropriate computing activities and improve employees' compliance with rules and regulations (Urbaczewski & Jessup 2002). Since monitoring is considered to increase perceived sanctions and employees are deterred from misusing information systems (D'Arcy *et al.* 2009), it helps regulate employees to behave securely. However, in a personal context, the role of monitoring may not be as effective as it is in a work context because it is not based on any management mechanism and people are freer to decide whether to follow given suggestions. Although some websites recommend that users set strong passwords, users often fail to follow these suggestions (Splashdata.com 2013). Therefore, we hypothesize:

H3: Monitoring has a stronger positive impact on USWP than on USPP.

Task benefit and task cost

Viewing the use of a strong password as an IS security task in this study, *task benefit* refers to the favor or advantage of using a strong password, while *task cost* refers to the inconvenience or burden of using a strong password. They are representative task characteristics. According to rational choice theory, individuals usually evaluate the benefit and cost when they make IS security-related decisions (Bulgurcu *et al.* 2010, Hu *et al.* 2011, Li *et al.* 2010, Vance & Siponen 2012). Generally speaking, perceived benefit is a positive incentive to users' security-

related actions, while perceived cost is a negative incentive. We would like to further argue that, for password use, the task cost–benefit considerations could be bounded in certain situations. In a work context, using a strong password is a common practice that does not require employees' considerable judgment on reasonability and feasibility. Rather, it integrates into the work routine as an employee's in-role responsibility. As a result, such task characteristics may not be the key influential contextual factors for the use of a work password. However, in a personal context, users are not bounded by any formal responsibilities. They are in a totally voluntary environment and may more freely choose their passwords based on their preferences. In this sense, task benefit and cost evaluation could be more influential contextual factors for users in the personal setting. Therefore, we hypothesize:

H4: Task benefit has a weaker positive impact on USWP than on USPP.

H5: Task cost has a weaker negative impact on USWP than on USPP.

3.5.4 Methodology

Study and sample

We collected data to test our model through a paper-based survey. In order to compare the USWP and the USPP, we developed two versions of questionnaires accordingly. We tested the questionnaires in two pilot studies with students and teachers at a university in Finland. We collected 34 samples for USWP and 35 samples for USPP for the first pilot test and 30 samples for USWP and 30 samples for USPP for the second one. We further revised the items based on the results and feedback of the two rounds of pilot studies.

For the main data collection, we sent questionnaires by mail to 1665 subjects who were randomly selected from the alumni list of a university in Finland. All of the subjects in this sample frame were at least licentiate from the university and were working in Finland. Specifically, 824 subjects received the USWP questionnaire, of which 217 responded, and 841 subjects received the USPP questionnaire, of which 207 responded. After eliminating some uncompleted and unusable responses, we had 210 responses for USWP, with a response rate of 25.5%,

and 202 responses for USPP, with a response rate of 24.0%. The demographic information of the two samples was fairly consistent (see Table 4).

Table 4. Comparison of demographics between work and personal samples.

Demographical information	Work group (N = 210)		Personal group (N = 202)		*t*-test	
					t value	Sig. (2-tailed)
Gender					-0.47	0.64 n.s.
Male	90	42.9%	82	40.6%		
Female	120	57.1%	120	59.4%		
Age					1.06	0.29 n.s.
18–29	15	7.1%	22	10.9%		
30–39	52	24.8%	63	31.2%		
40–49	72	34.3%	43	21.3%		
50–59	69	32.9%	71	35.1%		
>60	2	1.0%	3	1.5%		
Academic degree					-0.33	0.74 n.s.
Bachelor	23	11.0%	18	8.9%		
Master	144	68.6%	142	70.3%		
Licentiate	17	8.1%	16	7.9%		
Doctor	26	12.4%	26	12.9%		
Computer experience (years)					-0.51	0.61 n.s.
4–6	1	0.5%	1	0.5%		
7–10	12	5.7%	12	5.9%		
11–14	29	13.8%	21	10.4%		
>15	168	80.0%	168	83.2%		

Note: n.s. = not significant.

Nonresponse bias

In order to test the nonresponse bias, we followed the two post-hoc strategies for estimating nonresponse error proposed by Sivo *et al.* (2006). First, we compared the demographic information of the respondents with the whole population on the alumni list. We found no significant differences in gender, age, and academic degree between the two samples. Then, we compared the results between early and late respondents. We asked the participants to return the questionnaire within 10 days after receiving it. We regarded surveys that had been returned within one week as early responses, and the rest were late responses. We found no significant differences in any variables between the two samples. The results indicated that there is no significant nonresponse bias in our study.

Measurement

We used five formative items to measure the dependent variables, USWP and USPP. The survey asked respondents if their passwords met the standards of a strong password; specifically, we asked if the password was not a word from a dictionary or somebody's name, if it was at least eight characters long, if it used upper and lowercase letters, if it used at least one number, and if it used at least one symbol (e.g., '#', '^', '*', etc.). These standards are recommended by organizations like Microsoft (Microsoft.com) and CNET (cnet.com).

For the independent variables, we drew from validated instruments where possible (Straub 1989). All independent variables were reflective. Specifically, facilitating conditions contained three items adapted from Thompson *et al.* (1991). Embarrassment contained two items adapted from Grasmick and Bursik (1990). Monitoring contained three items adapted from D'Arcy *et al.* (2009). We adapted measures from Bulgurcu *et al.* (2010) to measure task benefit with three items and task cost with four items. We modified all items to fit the current context. We used seven-point Likert scales, anchored with "1 = strongly disagree" and "7 = strongly agree." We largely kept the same skeleton of the questions and just changed the concerning behavior (USWP or USPP) to guarantee that the questions measured exactly the same constructs in the two versions of the survey and that they carried the same reliability and validity as well. Since we collected data in Finland, a person who had a degree in the Finnish language translated the questionnaires into Finnish. Several other Finnish native speakers double-checked the questionnaires to make sure the meanings of all items were preserved during translation. Appendix 3 lists all questionnaire items.

3.5.5 Results

We used SmartPLS v3.2.0 (Ringle *et al.* 2015) for model estimations. Partial Least Squares (PLS) employs a component-based approach for model estimation. Compared to the covariance-based structural models, PLS is more flexible and thus is more appropriate for exploratory studies that aim to find new theories or extend the current literature to new contexts (Gefen *et al.* 2000). Further, PLS can estimate both reflective and formative constructs (Chin 1998).

Measurement model

For the reflective constructs, we assessed internal consistency and convergent validity by examining item loading, Cronbach's α, composite reliability, and average variance extracted (AVE) (Gefen & Straub 2005), as shown in Table 5. We compared the values with the commonly accepted guidelines. For reliability, the composite reliability of the constructs was greater than 0.8 (Nunnally 1978), and Cronbach's α was greater than 0.7 (Chin 1998). For convergent validity, indicator loadings exceeded 0.7 (Chin 1998), and the AVE for each construct exceeded 0.5. The only exception was the third item of facilitating conditions for the personal group (FC3), which had a loading (0.48) that fell below the 0.70 threshold. We retained this item for two reasons. First, according to Chin (1998), a loading would be considered acceptable if the loadings of other items for the same construct were high. Second, the loading was still higher than the cutoff point of 0.4 recommended by some scholars (Hulland 1999, Straub *et al.* 2004). Furthermore, the square root of AVE was greater than 0.7 for each construct (see Table 7).

Table 5. Measurement model results.

Construct	Item	Loading	*t*-statistic	Cronbach's α	Composite Reliability	AVE
			Work group			
Facilitating	FC1	0.93	39.10***	0.83	0.90	0.75
conditions (FC)	FC2	0.94	65.95***			
	FC3	0.72	11.46***			
Embarrassment	EM1	0.94	60.40***	0.85	0.93	0.87
(EM)	EM2	0.92	37.16***			
Monitoring (MN)	MN1	0.86	33.20***	0.89	0.93	0.82
	MN2	0.92	61.60***			
	MN3	0.94	83.31***			
Task benefit (TB)	TB1	0.95	78.76***	0.95	0.97	0.91
	TB2	0.95	84.36***			
	TB3	0.96	80.58***			
Task cost (TC)	TC1	0.92	6.63***	0.95	0.96	0.86
	TC2	0.95	6.68***			
	TC3	0.90	6.14***			
	TC4	0.95	6.71***			
			Personal group			
Facilitating	FC1	0.97	4.50***	0.79	0.86	0.69
conditions (FC)	FC2	0.95	4.38***			
	FC3	0.48	1.67			
Embarrassment	EM1	0.95	53.98***	0.78	0.90	0.81
(EM)	EM2	0.84	11.98***			
Monitoring (MN)	MN1	0.90	47.69***	0.86	0.91	0.78
	MN2	0.85	21.26***			
	MN3	0.90	37.68***			
Task benefit (TB)	TB1	0.92	41.68***	0.93	0.96	0.88
	TB2	0.97	175.32***			
	TB3	0.93	43.64***			
Task cost (TC)	TC1	0.91	42.89***	0.95	0.97	0.88
	TC2	0.97	171.77***			
	TC3	0.91	43.62***			
	TC4	0.95	93.79***			

Note: *** $p < 0.001$.

For the discriminant validity, all items loaded higher on their respective constructs than on the other constructs, and the cross-loading differences were much higher than the suggested threshold of 0.1 (Gefen & Straub 2005) (see Table 6). The square root of the AVE of each construct was higher than the inter-construct correlations (Fornell & Larcker 1981) (see Table 7). The correlations among all constructs were

all well below the 0.90 thresholds, suggesting that all constructs were distinct from each other (Herath & Rao 2009a).

Table 6. Loadings and cross-loadings.

Construct	Item	FC	EM	MN	TB	TC
			Work group			
Facilitating	FC1	**0.93**	0.13	0.38	0.30	0.04
conditions (FC)	FC2	**0.94**	0.19	0.40	0.27	0.09
	FC3	**0.72**	0.09	0.26	0.17	0.12
Embarrassment	EM1	0.17	**0.94**	0.14	0.42	-0.24
	EM2	0.13	**0.92**	0.08	0.40	-0.20
Monitoring (MN)	MN1	0.41	0.05	**0.86**	0.27	0.04
	MN2	0.31	0.18	**0.92**	0.37	-0.09
	MN3	0.39	0.09	**0.94**	0.32	-0.04
Task benefit (TB)	TB1	0.27	0.43	0.32	**0.95**	-0.33
	TB2	0.25	0.40	0.34	**0.95**	-0.30
	TB3	0.29	0.43	0.35	**0.96**	-0.30
Task cost (TC)	TC1	0.09	-0.21	-0.02	-0.29	**0.92**
	TC2	0.10	-0.19	0.01	-0.30	**0.95**
	TC3	0.07	-0.25	-0.09	-0.34	**0.90**
	TC4	0.08	-0.22	-0.01	-0.28	**0.95**
			Personal group			
Facilitating	FC1	**0.97**	0.19	0.27	0.20	-0.15
conditions (FC)	FC2	**0.95**	0.18	0.27	0.17	-0.13
	FC3	**0.48**	0.07	0.21	0.08	-0.14
Embarrassment	EM1	0.18	**0.95**	0.28	0.30	-0.08
	EM2	0.15	**0.84**	0.30	0.16	-0.07
Monitoring (MN)	MN1	0.25	0.25	**0.90**	0.26	-0.21
	MN2	0.19	0.33	**0.85**	0.15	-0.09
	MN3	0.31	0.28	**0.90**	0.19	-0.13
Task benefit (TB)	TB1	0.20	0.23	0.22	**0.92**	-0.34
	TB2	0.17	0.26	0.24	**0.97**	-0.34
	TB3	0.19	0.28	0.21	**0.93**	-0.32
Task cost (TC)	TC1	-0.13	-0.10	-0.21	-0.31	**0.91**
	TC2	-0.16	-0.06	-0.16	-0.33	**0.97**
	TC3	-0.15	-0.09	-0.16	-0.37	**0.91**
	TC4	-0.14	-0.06	-0.14	-0.33	**0.95**

Table 7. Inter-construct correlations and the square root of the AVE.

Construct	USP	FC	EM	MN	TB	TC
			Work group			
USWP	-					
FC	0.34	**0.87**				
EM	0.28	0.16	**0.93**			
MN	0.46	0.41	0.12	**0.91**		
TB	0.33	0.29	0.44	-0.24	**0.95**	
TC	-0.23	0.09	0.35	-0.03	-0.33	**0.93**
			Personal group			
USPP	-					
FC	0.15	**0.83**				
EM	0.29	0.19	**0.90**			
MN	0.35	0.29	0.32	**0.88**		
TB	0.55	0.20	0.27	0.24	**0.94**	
TC	-0.41	-0.15	-0.08	-0.18	-0.36	**0.94**

Note: Bold items are the square root of the AVE.

USP refers to USWP and USPP respectively.

Internal consistency reliability does not apply to assess the reliabilities of formative dependent variables (Bollen 1989, Bollen & Lennox 1991). To determine validity, we first referred the contents to the commonly accepted standards of strong passwords by well-known websites (e.g., Microsoft, CNET). We also discussed the items with professors who are experts in information security research and have previous work experiences in the industry to ensure the contents of the formative items are meaningful and reasonable. In order to identify possible multicollinearity issues, we further tested the variance inflation factor (VIF) levels. The highest VIF was less than 1.9, which is below the 3.3 threshold, suggesting that a high multicollinearity is not present (Petter *et al.* 2007). We also assessed the statistical significance of the outer weights. With bootstrapping of SmartPLS, the results in Table 8 show that the formative indicators were significant except USWP2 and USWP4 for the work password group, and USPP1 and USPP4 for the personal password group. Since their loadings were all significant and they have been identified as necessary features of a strong password, we retained the indicators in the formative construct as suggested by Hair *et al.* (2013).

Together the above results suggest good measurement properties for both work and personal groups.

Table 8. Item weights and loadings for formative measures.

Construct	Item	Weight	*t* value	Loading	*t* value
			Work group		
Use of strong password	USWP1	0.32*	2.44	0.55***	4.59
	USWP2	0.17	1.42	0.41***	3.30
	USWP3	0.60***	5.05	0.82***	11.24
	USWP4	-0.01	0.07	0.29*	2.10
	USWP5	0.43***	2.88	0.62***	5.46
			Personal group		
	USPP1	0.03	0.23	0.40***	3.91
	USPP2	0.29**	2.94	0.58***	6.78
	USPP3	0.63***	7.11	0.87***	21.63
	USPP4	0.16	1.19	0.66***	7.99
	USPP5	0.31***	3.91	0.51***	6.04

Note: * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$ (two-tailed test).

Structural model

We first tested the structural model for the work and personal samples separately. We performed a bootstrap resampling procedure (500 samples), with sample size set equal to the work and personal sample sizes (N = 210 and N = 202, respectively). Results of the model with two samples are shown in Fig. 7.

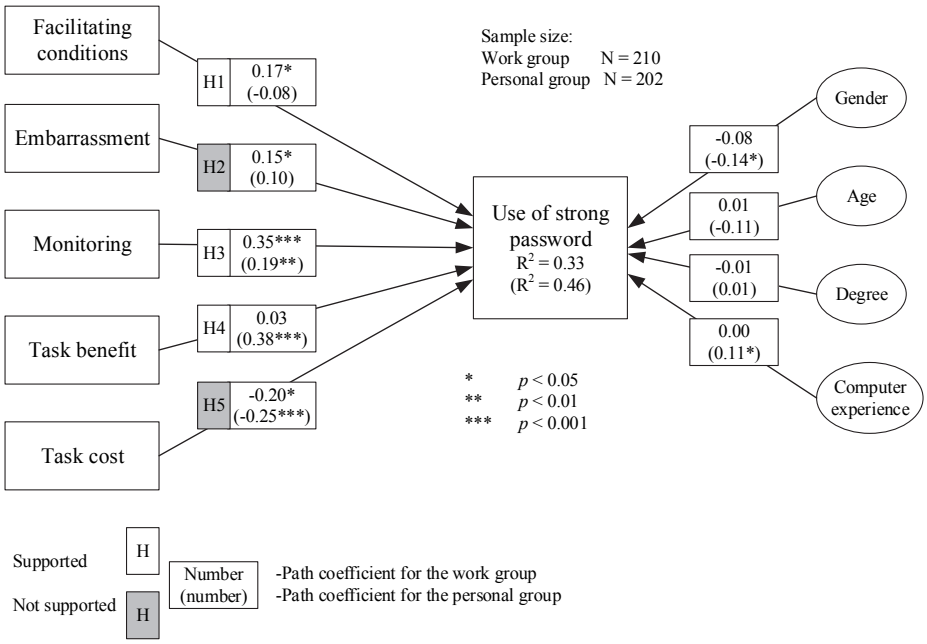

Fig. 7. Structural model.

Multi-group analysis for differences across work and personal groups

In order to test our hypotheses associated with differential contextual impacts, we did additional analysis to compare the path coefficients between the two samples. Specifically, we applied one-way ANOVA to compare all the construct means first. In Table 9, the results revealed significant differences in the use of strong passwords and monitoring between the USWP and USPP groups. Further, the results of Levene's test showed that the two factors exhibited different variance across the two groups. Due to the different variance in the dependent variable across the two groups, we used the Smith-Satterthwait (S-S) test with a pooled error term (Chin 2000). The S-S test can identify the difference of the same set of paths across groups. Results showed that three pairs of paths were different between the two groups (see Table 10). Specifically, H1, H3, and H4 were supported, while H2 and H5 were rejected. Thus, the analysis provided some evidence of the different contextual influences on the password behavior in the two contexts. For the control variables, we found that gender, age, degree, and computer experience had no significant

impact on USWP. In comparison, gender had a significant impact on USPP. However, the influence was not significantly different from that in the work context.

Table 9. Comparisons of construct means.

Construct	Levene's test for equality of variances		Mean		*t*-statistic	Significant differences?
	F	Sig.	Work	Personal		
USP	4.02	$p < 0.05$	5.06	4.73	2.47*	Yes ($p < 0.05$)
FC	0.04	$p = 0.85$	4.16	3.94	1.13	No
EM	1.83	$p = 0.18$	2.34	2.13	1.34	No
MN	7.97	$p < 0.01$	3.84	2.97	4.22***	Yes ($p < 0.001$)
TB	0.02	$p = 0.89$	5.23	5.38	-0.59	No
TC	0.52	$p = 0.47$	3.57	3.59	-0.07	No

Note: * $p < 0.05$ (two-tailed test), *** $p < 0.001$ (two-tailed test).

Table 10. Path coefficient differences.

Path	Path coefficient			*t*-statistic	Significant differences?
	Work		Personal		
FC → USP	0.17*	>	-0.08	2.50††	Yes (H1 is supported.)
EM → USP	0.15*	>	0.10	0.67	No (H2 is not supported.)
MN → USP	0.35***	>	0.19**	1.74†	Yes (H3 is supported.)
TB → USP	0.03	<	0.38***	3.59†††	Yes (H4 is supported.)
TC → USP	-0.20*	<	-0.25***	0.51	No (H5 is not supported.)
Gender → USP	-0.08	N/A	-0.14*	0.56	No
Age → USP	0.01	N/A	-0.11	1.44	No
Degree → USP	-0.02	N/A	0.01	0.26	No
Experience → USP	0.00	N/A	0.11	1.12	No

Note: ††† p' < 0.001 (one-tailed test), †† p' < 0.01 (one-tailed test), † p' < 0.05 (one-tailed test),
*** $p < 0.001$ (two-tailed test), ** $p < 0.01$ (two-tailed test), * $p < 0.05$ (two-tailed test).

Common method variance

During the data collection, we took several measures to reduce the possibility of common method variance (CMV). Specifically, we used neutral wording for the items and multiple items for each construct. We ensured the anonymity of the respondents and requested that they answer as honestly as possible. For the collected data, we tested the CMV using two statistical approaches. First, we used Harman's one-factor test (Podsakoff *et al.* 2003) and found that the majority of data variance could not be accounted for by one general factor; that is, the first factors of the work and personal samples explained only 24.9% and 28.2% of the total

variance respectively, suggesting no significant common method bias. Second, the correlation matrix (see Table 7) shows that all correlations were below 0.55, while CMV is evidenced by extremely high correlations (r > 0.90) (Bagozzi *et al.* 1991). These tests collectively provide the evidence that CMV is not a serious problem for this study.

3.6 Discussion

The empirical results supported three out of five hypotheses. Facilitating conditions, monitoring, and task benefit have significantly different impacts on the password behavior between the work and personal groups (see Table 8). Contrary to our expectations, task cost and embarrassment had no significantly different effect on password behavior across the two contexts. In the following, we first discuss the results in the two contexts separately, and then discuss the results of comparisons.

On the one hand, our study revealed that, in the work context, individuals consider facilitating conditions, monitoring, embarrassment, and task cost in their decisions regarding USWP. These contextual factors embody the strength of organizational management, which in turn influence employees' behavior. In comparison, the contextual factors related to the task, such as task benefit and task cost serving one's own preferences, could have an impact on behavior, but the strength of the effects may be influenced by other contextual factors. For task benefit, a post-hoc analysis showed that, if we include only task benefit and task cost as independent variables in the model, the effect from task benefit became significant (path coefficient = 0.25, $p < 0.05$). This result is consistent with most previous studies (Bulgurcu *et al.* 2010, Li *et al.* 2010, Vance & Siponen 2012). However, when taking consideration of other context factors (i.e., facilitating conditions, embarrassment, and monitoring) together, the effect from task benefit became insignificant, which is consistent with our conjecture. In our results, task cost significantly influenced USWP, and the influence was stronger than we expected (path coefficient = -0.25, $p < 0.001$), so that the difference of the effect across the two contexts was not significant. We have discussed that, in the work context, task cost including inconvenience and perceptions of being burdensome would not have much impact on employee's USWP. On the contrary, the result showed its strong impact. One explanation could be that employees rank productivity ahead of security. The inconvenience brought by using a strong password would lower productivity. As a result, it is possible that employees feel sensitive to the inconvenience.

On the other hand, the results in the personal context revealed that individuals mainly consider task benefit, task cost, and monitoring in USPP. Due to the voluntary characteristic of the personal context, individuals are more likely to decide according to their own preferences. Therefore, benefit and cost play important roles in the personal setting. Monitoring as an application (e.g., the software checking the complexity of a user's password or providing suggestions for creating a strong password) could also influence USPP. However, the influences from the other two contextual factors, facilitating conditions and embarrassment, were insignificant. This result was unsurprising because, for individuals in a personal context, the facilitating conditions are either costly or not professional and their peers would not exert much pressure on individuals' USPP.

The results of the comparisons indicated that the two contexts indeed cause some differences in explanations for the use of strong password. Facilitating conditions and monitoring had significantly stronger impacts on USWP than on USPP, while task benefit had significantly a weaker impact on USWP than on USPP. Thus, H1, H3, and H4 were supported. Although H2 and H5 were not supported by the current data, we could see that embarrassment had a significant effect on USWP, but an insignificant effect on USPP; conversely, task cost had a significant effect at a 0.001 level on USPP, but only at a 0.05 level on USWP. The differences between the two groups showed some trends to be significant. If the sample size were large enough, the significance of differences could become possible.

In terms of the control variables, we found that all four variables had no significant influence on USWP, but gender significantly influenced USPP. The results showed that males were more likely to use a strong personal password than females were. This finding is consistent with the adoption of IT in voluntary settings, suggesting that males typically display higher levels of self-efficacy toward computers or the Internet than females (Comber *et al.* 1997, Durndell *et al.* 2000, Durndell & Haag 2002, Ong & Lai 2006, Whitely 1997). Together, these findings indicate that males may have a stronger ability to manage complex passwords than females. In the work setting, the gender difference was not significant because both males and females are required to manage password security.

3.6.1 Implications for research

In the preceding sections, we discussed the development of rational choice theory in IS security behavior research. We also highlighted that the contextualization of

the theory begins with the modification of assumptions by considering the IS security context. Then we provided four guidelines to develop a contextualized RCT. Based on the comparative results from our study of USWP and USPP, we managed to show that the explanations for behavior differ in different contexts and following different assumptions. Building upon these activities, our research makes the following contributions.

First, our work contributes to the theory contextualization approach in IS research by suggesting that researchers alter the assumptions appropriately in the corresponding context. Although recent work by Hong *et al.* (2013) has provided insightful guidelines for contextualizing IS theory, they did not discuss the contextualization on an assumption level. They asserted that there exists a general theory and that all the contextualization is conducted within the general theoretical foundation. However, by reviewing the literature of rational choice theory, we found that no general theory exists because every theory is based on certain assumptions that are context-sensitive. If these assumptions do not fit the context, the theory based on them will be problematic. We suggest that examining the appropriateness of assumptions and, if necessary, altering the assumptions in context is the first task in contextualizing a theory. Our findings not only guide RCT development, but they also have implications for other theories, especially those reference theories that were originally developed in non-IS contexts. For example, deterrence theory is popular in explaining IS security behavior, but studies that have applied the theory have produced mixed results (D'Arcy *et al.* 2009, Guo *et al.* 2011, Hu *et al.* 2011, Siponen & Vance 2010). The original deterrence theory has a long tradition in criminology with assumptions that intend to explain deliberate crimes. However, the theory may not be appropriate to explain nonmalicious IS security policy violations, which may be one reason for the mixed findings in empirical investigation. Future research can examine the theory's original assumptions and judge whether they fit the context under study.

Second, we contribute to RCT development in IS security behavior research. Previous RCT-based IS security behavior studies have rarely discussed the particularities of the IS security context or the appropriateness of assumptions applied in the context. By showing a comparative example of password use in work and personal contexts, we suggest making the specific assumptions explicit rather than implicit. On the one hand, this approach helps verify the theory. Since each hypothesis is derived from the assumptions made, if a hypothesis is not supported by empirical results, both the hypothesis and assumptions can be reexamined. On the other hand, it creates opportunities to develop new RCT theories. Researchers

have largely based existing IS security behavior studies on the assumptions from economics and criminological versions of RCT. Actually, these assumptions largely limit the explanations for IS security behavior. The rationality of IS security behavior may involve facets such as different values, preferences and beliefs, and physical and social reality. Future research can identify the differences in these aspects and develop new theories.

Third, we suggest analyzing the IS security context in dimensions. We identify four context dimensions that are important in studying IS security behavior: user context, task context, social context, and technology context. We have emphasized the importance of analyzing the context and making appropriate assumptions, which can provide more precise theoretical explanations. These dimensions help future researchers to compare the context differences and check the assumptions in each dimensional context. This approach also helps derive hypotheses about the contextual factors, which are important influential factors on IS security behavior. Previous studies that have included contextual factors in only one or two dimensions have provided limited understanding of contextual influences on IS security behavior and may have neglected some important contextual factors. We suggest future researchers to pay more attention to each dimensional contextual factor.

Fourth, our comparative empirical results provide evidence for the need to move to contextualized IS security behavior research. Existing research has focused on only a single context, such as the organizational context or the home context, or has presented generic models that are free of context. Such research could not reflect the differences between one context and another. Our study indicates that the conclusions in one context may not be generalized to a different context. For example, organizational policies or sanctions in the organizational context do not exist in the home context. Our comparative empirical results also show that the influential factors for USWP are quite different from those in the personal context (USPP). It is possible that contradictory explanations can be provided under two different assumptions in two different contexts. We look forward to future research that may provide interesting results and explanations.

3.6.2 Limitations and future research

Our study had some limitations. First, we used RCT as an example, aiming to elaborate the importance of theory contextualization on the assumption level, but we did not discuss its assumptions in details. Actually, RCT has various

assumptions that result in very different theories in fields such as economics, sociology, and political science, among others (Hechter & Kanazawa 1997, Korobkin & Ulen 2000, McCarthy 2002). Future research can check these assumptions made in reference fields and judge whether they are appropriate in an IS security context. Second, the categorization of the IS security context in guideline 1 is not intended to be exhaustive; rather, it is meant to suggest that future researchers should examine the context in dimensions. Future research can explore other dimensions that influence IS security behavior. Third, the empirical study had several limitations. One is the small sample size; in fact, the non-supported hypotheses might become supported if the sample size is large enough. Another limitation is that the comparative study does not examine all the possible contextual differences, but simply aims to show some examples to prove that the differences exist. Future research can examine other context differences.

3.7 Conclusion

By discussing the use of RCT in IS security behavior research, we highlighted the role of assumptions in theory contextualization. We presented guidelines for checking the theory assumptions in an IS security context. We then illustrated the approach by describing a comparative empirical study that theorizes the use of strong passwords in work and personal contexts. Our study provides implications for future scholars to guide them in conducting better contextualized research.

4 Understanding employees' IS security risk-taking behavior: a temporal perspective

4.1 Abstract

Employees' information systems (IS) security risk-taking behavior (ISRB) usually puts organization's IS resources at risk. Although a number of studies have focused on the behavior, the IS security behavior literature has long overlooked the temporal nature of risk, meaning that the outcomes of ISRB may unfold as time passes. This study adopts a temporal perspective to understand employees' ISRB, positing the construct of long-term orientation (LTO) as a belief that influences employees' ISRB decisions. Drawing on stewardship theory, which explains the situation in which employees willingly serve the organization's long-term welfare, we explain the role of LTO on ISRB, and we further theorize that LTO can be driven by a set of intrinsic motivations. Our empirical results suggest that LTO decreases employees' IS security risk-taking intentions. Three antecedents of LTO (i.e., value identification, trusted relationship fulfillment, and growth needs fulfillment) have significant positive impacts on LTO. We also discuss implications for the research and practice of IS security.

4.2 Introduction

Employees' behavioral threats to an organization's IS security continuously draw concerns from scholars and practitioners. Insider threats remain as one of the most tough security issues for organizations. A recent report indicated that 30% of organizations' data breaches were caused by trusted but negligent insiders, which is ranked as second only to malware as the most important threat to organizations' information security (Ponemon Institute 2015). Ernst and Young (2014) found that employees are regarded as the top vulnerability to increase an organization's risk exposure.

Many recent studies have suggested that employees' volitional but nonmalicious security violations (e.g., using easy-to-guess passwords, using unencrypted personal portable devices to store the organization's data) are representative behavioral threats in organizations (D'Arcy *et al.* 2014, Guo *et al.* 2011, Willison & Warkentin 2013). Although organizations exert great effort to improve their security management through actions such as training, enhancing

security monitoring, and updating security policies, employees still fail to comply with their IS security policies. Typical reasons for these failures are benefits such as saving time or the convenience of the abuse (Li *et al.* 2010), using neutralization techniques such as defense of necessity (Barlow *et al.* 2013, Siponen & Vance 2010), work impediments (Bulgurcu *et al.* 2010), and security-related stress (D'Arcy *et al.* 2014). These studies have implied that employees are not ignorant about the rightness or wrongness of the behavior. Instead, they know the risk of the behavior but have reasons to choose to take the risk. However, risk is intrinsically embedded in time, meaning that the outcomes of current risk unfold in the short or distant future (Das & Teng 1997, Drucker 1972, Gerber & von Solms 2005, Royal Society 1983, 1992). Many IS security risk-taking behaviors (ISRBs) may not cause immediate loss, especially when employees are nonmalicious, such as using a simple password, but the behavior may leave the vulnerability for the future. Without considering the possible future consequences of their current behavior, employees may underestimate the seriousness of the threats, which leads to violations. Unfortunately, little research has adopted such a temporal perspective, which may be an important angle to understand ISRB and its influential factors. This chapter aims to address this gap.

Against this backdrop, this study offers a new avenue for understanding ISRB from a temporal perspective. First, we introduce the concept of long-term orientation (LTO) into the IS security context. We define LTO as a mindset viewing the outcomes of ISRB over a long period of time that includes three dimensions: continuity, futurity, and perseverance. Drawing on stewardship theory, which explains situations in which individuals serve organizational long-term welfare (Davis *et al.* 1997, Hernandez 2012), we argue that LTO is an important psychological construct of employees to avoid ISRB. Second, based on stewardship theory, we further identify three antecedents of LTO: value identification, trusted relationship fulfillment, and growth needs fulfillment. We explicate that value identification and the fulfillment of higher order needs are important intrinsic motivations for employees to generate LTO. We empirically test our research model by examining 170 employees in a global company. The results well support all our hypotheses. Our study contributes to IS security behavior literature by introducing a new theoretical research perspective, new constructs, and a new understanding of ISRB. Our findings also provide valuable implications for practice.

The chapter is organized as follows. The next section presents the theoretical background including the literature review on ISRB and the theoretical foundation. Then we discuss the research model and develop the hypotheses before presenting

the data analysis and results. Finally, we discuss our findings, implications for research and practice, and limitations, and conclude our study.

4.3 Theoretical background

In order to better understand employees' ISRB, in this section, we first discuss the characteristics of the behavior, and review the related studies in existing literature. Second, we introduce the key concept in this study—LTO. Third, we explain stewardship theory, which is the base theory of this study.

4.3.1 IS security risk-taking behavior

IS security risk-taking behavior (ISRB) refers to those intentional behaviors that may put organizational information systems at risk, although the actors do not have malicious purposes (Guo 2013). Previously used terms, such as nonmalicious security violation (Guo *et al.* 2011) and volitional (but not malicious) noncompliance (D'Arcy *et al.* 2014, Willison & Warkentin 2013), have similar meanings as ISRB, but here we use ISRB to highlight the concept of risk. Previous IS security literature has described ISRB as the most common IS security policy violation in organizations and noted that it covers a wide range of insecure behaviors, such as using personal unencrypted USB drives, delaying backups, and failing to change passwords regularly.

Characteristics of IS security risk-taking behavior

Guo *et al.* (2011) summarized four characteristics of ISRB (which they termed "nonmalicious security violations"): (1) intentional, (2) self-benefiting without malicious intent, (3) voluntary rule breaking, and (4) possibly causing damage or security risk. Based on these four characteristics, we made two more observations in terms of IS security management. First, since ISRB is a behavior without malicious intent, the threat and damage from ISRB are usually indirect, with the result that consequences may unfold in the future. Unlike the security-damaging behavior that occurs on purpose and causes direct damage to the organization's IS security (Guo 2013), ISRBs often cause damage indirectly. ISRB could increase the vulnerabilities of an IS in the future rather than harming it immediately and directly. For example, people use easy-to-guess passwords for work accounts because they cannot remember complex passwords or for reasons other than a

desire to see the organizational IS hacked. Technically speaking, an easy-to-guess password cannot harm the system directly, but it indeed increases the possibility of future intrusions by hackers. Second, ISRB is hardly regulated by security controls, such as monitoring and punishment. Due to the diversity of ISRB, IS security policies can hardly define all such behaviors beforehand, especially those new forms of ISRBs of which the organization is not yet aware, let alone establish effective countermeasures. On the other hand, ISRB may be embedded into the routine work process, such as sending unencrypted emails, which is a routine in work. It is inappropriate to use draconian laws for such trivial behaviors, for it will dramatically increase regulatory costs, which is uneconomic, and it may also cause employees to be uncomfortable about work, resulting in a decrease in work efficiency. For these reasons, the traditional control approach has limitations in terms of ISRB regulation.

Prior research on ISRB

Previous studies have often used ISRB scenarios, albeit with different behavior terminology, to describe the target security behavior. Using unencrypted portable media, sharing passwords, and failing to backup, just to name a few, have been discussed intensively (e.g., Siponen & Vance 2010, Vance *et al.* 2012, Workman *et al.* 2008). We summarized the behaviors these studies examined, the theoretical perspectives they applied, and their key findings in Appendix 4. The widely applied theories in ISRB research are deterrence theory (Gibbs 1975), neutralization theory (Sykes & Matza 1957), protection motivation theory (Rogers 1975), and rational choice theory (Paternoster & Simpson 1993, 1996). Researchers have applied each of these theories to explain ISRB from different perspectives.

Deterrence theory suggests that ISRB, like other security behaviors, can be decreased by increasing employees' perceived certainty, severity, and celerity of sanctions. Thus, organizations can increase employees' perceptions of sanctions by specifying the policies or guidelines as well as monitoring or performing security audits (D'Arcy *et al.* 2009, Hovav & D'Arcy 2012). However, researchers have reached no consistent conclusion regarding the influence of sanction perceptions on ISRB. Some studies have found no connections between sanction perceptions and ISRB (D'Arcy *et al.* 2009, Hovav & D'Arcy 2012, Johnston *et al.* 2015, Siponen & Vance 2010). Such findings may reflect the ISRB's characteristics mentioned in previous sections. The results of previous studies indicated that, in reality, employees might not be aware of the sanctions imposed on their ISRBs

when most of them are usually nonmalicious, not serious violations, and the consequences are not immediate most of the time. The results also provide evidence that the policies and technical countermeasures applied by the organizations may not effectively reduce ISRB in the sense of deterrence. Further, employees can use neutralization techniques (Piquero *et al.* 2005, Sykes & Matza 1957) to reduce the perceived harm of their policy violations (Siponen & Vance 2010).

In explaining ISRB, protection motivation theory considers the appraisal of threat and coping. The threat appraisal includes the perceived vulnerability (i.e., how an individual feels that a negative event will take place if no measures are taken to counter the problem) and perceived severity (i.e., the degree of physical and psychological harm an illness may seem to cause). The coping appraisal includes the self-efficacy (i.e., an individual's ability or judgment of his or her capabilities to carry out the coping response actions) and response efficacy (i.e., the effectiveness of the recommended coping response in reducing threat to an individual) (Rogers *et al.* 1983, Siponen *et al.* 2014). Protection motivation theory focuses on the extrinsic motivations (i.e., external threat or risk) to explain ISRB. While these are key factors, protection motivation theory overlooks the possible intrinsic motivations of individuals for preventing ISRB.

The rational choice perspective explains ISRB mainly with the economic and criminological approach of rational choice (Becker 1968, Clarke & Cornish 1985, McCarthy 2002, Paternoster & Pogarsky 2009, Paternoster & Simpson 1993, 1996). This perspective assumes that humans are rational actors who conduct the cost–benefit analysis to maximize their self-interest. Specifically, the economics approach of RCT usually focuses on tangible value (Ransbotham & Mitra 2009), such as time (Vance & Siponen 2012) or money (Li *et al.* 2010). The criminological approach of RCT assumes that humans pursue happiness and avoid pain. Representative rational choice factors identified in the literature are sanctions (Herath & Rao 2009a), intrinsic benefits (Bulgurcu *et al.* 2010) such as mental pleasure (Hu *et al.* 2011), thrill, or excitement (Vance & Siponen 2012), or negative feelings, such as guilt or shame (Bulgurcu *et al.* 2010). While these findings are all based on the assumption that individuals are self-interested, other studies have indicated that individuals may also be willing to serve others' interests, especially in the complex organizational life. As employees may benefit from the development of their organizations, it is possible that employees are willing to serve the organizational interest ahead of their individual interest, especially when there is a conflict between these competing interests on IS security issues (e.g., a trade-

off between work efficiency and security). Existing studies lack explanations of ISRB based on the organization-serving assumption.

A review of the IS security behavior literature has revealed that little research explains ISRB from a temporal perspective (i.e., focusing on the temporal feature of risk). As a result, the literature may lack an important explanation for employees' ISRB. In this next section, we introduce the theoretical background from a temporal perspective.

4.3.2 Long-term orientation

As we discussed before, the consequences of ISRB may unfold as time passes; hence, temporal consideration may be important in related decision-making. Therefore, in this section, we discuss the concept of temporal consideration of an employee.

Rationale for studying LTO

Researchers have widely discussed the temporal consideration in decision-making in various fields, such as psychology, marketing, and firm management, using terms like "managing for the long run" (Miller & Le Breton-Miller 2005), future orientation (Das & Teng 1997), consideration of future consequences (Strathman *et al.* 1994), conceptions of the future (Karniol & Ross 1996), and long-term orientation (Bearden *et al.* 2006, Gómez-Mejía *et al.* 2007, Lumpkin *et al.* 2010, Zahra *et al.* 2004). Although both short-term and long-term orientation are important for decision-making regarding information security behaviors, in this chapter, we focus on long-term orientation (LTO). The primary reason for this choice is that LTO is an important perspective to understand ISRB especially when its consequences may unfold across time. Further, when previous security behavior studies emphasized the importance of the immediacy of either threats or sanctions, they rarely discussed the long-term impact or the consistency of the security behaviors. Management literature has suggested that decisions with a short-term orientation emphasize efficiency, whereas decisions with a LTO emphasize effectiveness (Covin & Slevin 1989, Venkatraman 1989, Wang & Bansal 2012). As to organizational IS security, we assume that organizations value effectiveness more than efficiency because the efforts put into IS security may not result in immediate gains. IS security countermeasures actually aim to prevent the threats and risks before they happen, which emphasizes the usefulness of the control

measures in terms of successful regulating the employees' security behaviors. These goals require organizations to focus more on effectiveness (Beebe & Rao 2005, Dhillon 1999, Dhillon & Moores 2001) and managing for the long run. Therefore, focusing on LTO could be more meaningful in our research context.

Conception of LTO

Previous literature has viewed LTO in several ways. Lumpkin and Brigham (2011) described it as a dominant logic, which is "a mindset or a world view or conceptualization of the business and the administrative tools to accomplish goals and make decision in the business" (Prahalad & Bettis 1986: 491). Lumpkin and Brigham (2011) defined LTO as "the tendency to prioritize the long-range implications and impact of decisions and actions that come to fruition after an extended time period" (Lumpkin *et al.* 2010: 245). Bearden *et al.* (2006) defined LTO as "the cultural value of viewing time holistically, valuing both the past and the future rather than deeming actions important only for their effects in the here-and-now or the short term" (p. 457). Das and Teng (1997) described a similar concept, future orientation, as "individuals' psychological attributes regarding their perception of the future and the flow of time" (Cottle 1976, Das 1986, 1987, 1991, 1993, Fraisse 1963, Kastenbaum 1961, Klineberg 1968). Based on these definitions, in the current context, we define LTO as a mindset viewing the outcomes of ISRB over a long period of time.

In this vein, mindset determines how an individual engages events or views reality (Armstrong & Hardgrave 2007, Culbert 1996). Goodpaster (2007) elaborated that mindsets in the context of business "carry thoughts and values into action" (Goodpaster 2007: 35). Decision-makers with a LTO mindset are mindful that the consequences of many of their choices will be realized only after an appreciable delay (Le Breton-Miller & Miller 2006). Previous research has suggested that a LTO mindset has significant implications for people's choice of behavior. Studies have found that people with a LTO within an organization achieve better joint outcomes in integrative negotiations (Mannix *et al.* 1995) and are less likely to deplete organizational resources (Mannix 1991, Mannix & Loewenstein 1993). Employees who consider more about the future consequences are less likely to violate organizational rules (Takemura & Komatsu 2012).

Dimensions of LTO

LTO is a multidimensional construct. Drawing from Lumpkin and Brigham (2011), LTO is composed of three dimensions: (1) continuity, which involves bridging from the past to the future; (2) futurity, which reflects a concern for future consequences; and (3) perseverance, which highlights how present decisions and actions affect the future. We discuss the three dimensions in more detail below.

Continuity is the belief that whatever is long-lasting and endures has value (Lumpkin & Brigham 2011). People with continuity beliefs respect traditions and past experience and believe that what was right in the past is worthy of preservation in the future. Continuity reflects an interest in tradition. Bearden *et al.* (2006) developed a measure of LTO and found the item "I value a strong link to the past" to be an important indicator of LTO. Furthermore, continuity emphasizes the present and future through repetition (such as making the same choice at "all times" or "every time") to convey the ongoingness and repetitiveness of actions. Individuals believe that it is valuable to repeat the choice as it was made before. The belief of continuity helps align ongoing decisions with existing consensus, such as the strategies and policies made in organizations (Moss *et al.* 2014). Hershfield *et al.* (2012) found that people who hold continuity beliefs are more likely to make ethical decisions.

Futurity is the belief that the process of forecasting, planning, and evaluating the long-range consequences of current actions has utility (Lumpkin & Brigham 2011). Individuals with futurity beliefs pay more attention to, care more about, and give greater weight to the possible future outcomes of their current behavior when making decisions about how to behave (Joireman *et al.* 2006, Shipp *et al.* 2009). Zimbardo *et al.*'s (1997) five-factor model may be used to identify an individual's future orientation (D'Alessio *et al.* 2003, Zimbardo & Boyd 1999, Zimbardo *et al.* 1997). Zimbardo and colleagues described that individuals with future orientation actively plan for and strive to meet future goals. They see themselves as achievers, tend to be conscientiousness, and have a preference for consistency. Individuals with futurity beliefs generally avoid sensation-seeking, aggression, impulsivity, and risk-taking because such behaviors are antithetical to future success (Gupta *et al.* 2012, Zimbardo *et al.* 1997). Previous empirical studies have also proven that decision-makers who have a high degree of futurity belief would make less risky decisions (Das & Teng 1997).

Perseverance is the belief that efforts made today will pay off in the future (Lumpkin & Brigham 2011). People with perseverance beliefs are typically willing

sacrifice immediate benefits in order to get long-term benefits. Individuals believe that certain behaviors are worthwhile because of future benefits, even though immediate outcomes are relatively undesirable or require immediate costs. They are willing to sacrifice immediate benefits like pleasure or convenience to achieve more desirable future states (Strathman *et al.* 1994). Bearden *et al.*'s (2006) study of LTO used items such as "I don't mind giving up today's fun for success in the future" that were suggestive of perseverance. The trade-offs between short-term costs and long-term benefits have been discussed in the context of organizations extensively. Researchers have considered organizational citizenship behavior to be a social dilemma (Joireman *et al.* 2006) in which short-term individual and long-term collective interests are at odds (Komorita & Parks 1994, Messick & Brewer 1983). Joireman *et al.* (2006) found that employees who place greater value on future outcomes than immediate outcomes are more likely to engage in organizational citizenship behavior.

4.3.3 Stewardship theory and LTO

Although literature has indicated that LTO relates to risk behavior and organizational behavior, the theoretical basis for why an employee generates LTO and what factors motivate LTO are associated with a stewardship philosophy (Davis *et al.* 1997, Le Breton-Miller & Miller 2011).

Why do employees generate LTO?

Hernandez (2012) has defined *stewardship* as "the extent to which an individual willingly subjugates his or her personal interests to act in protection of others' long-term welfare" (p. 174). Given a choice between self-serving behavior and pro-organizational behavior, a steward-like employee will not depart from the interests of his or her organization. The assumptions are based on the covenantal relationship between employees and their organizations. A covenantal relationship suggests that employees and organizations make a commitment to a shared set of values and maximization of the wellbeing of both the employee and the organization (Joireman *et al.* 2006, Van Dyne *et al.* 1994). It binds both the organization and its employees to work toward a common goal, without taking advantage of each other (Caldwell *et al.* 2002, Caldwell & Karri 2005, DePree 2011, Hernandez 2012).

From the employees' perspective, employees could have higher order needs, such as growth, achievement, affiliation, and self-actualization in organizational

life. Such needs must be fulfilled through the organization's success (Davis *et al.* 1997). However, it takes time for an organization to succeed and for individuals to fulfill such needs; as a result, employees may generate a long-term vision. Hernandez (2012) suggested that LTO is a key psychological mechanism of stewardship, and represents the time horizon of stewardship theory. Stewardship theory helps explain managers' stewardship behavior (Davis *et al.* 2007), employee stewardship, and prosocial behavior (Pearson & Marler 2010). Schepers *et al.* (2012) found that frontline employees' perceptions of stewardship toward customers positively influenced both their in-role and extra-role behavior.

What generates an employee's LTO?

Since LTO plays an important role in an employee's pro-organizational decision-making, it is worthy of discussing what factors facilitate employees to create a LTO. Hernandez (2012) suggested that a LTO can be driven by two systems: control and reward. For the control systems, fostering relationship-centered collaboration helps establish an infrastructure for working together, and collaborating members continually evolve through social networks; together, these activities promote collective responsibility for work outcomes, which requires an awareness of various stakeholder perspectives. The two structural factors are enacted through ongoing social processes, which typically necessitate a LTO (Hernandez 2012). For the reward systems, intrinsic benefits from working toward the organizational goals and from generating self-efficacy and self-determination also necessitate the long-term investment of resources and efforts (Hernandez 2012). As our study focuses on employee ISRB, which is a form of independent task rather than a collaborative task, the relationship-centered collaboration and collective responsibility may not apply to our current context. Instead, we focus on the intrinsic benefits that emphasize personal psychological factors, which we regard as fundamental causes of behavior.

Scholars have proposed that higher order needs, intrinsic factors, and identification are important in motivating individuals to become stewards of the organization (Davis *et al.* 1997, Hernandez 2012). The fulfillment of the higher order needs can be seen as intrinsic rewards for steward-like employees. These rewards include opportunities for growth, achievement, affiliation, and self-actualization (Davis *et al.* 1997), which can be found in need theories (Alderfer 1972, Maslow *et al.* 1970, McClelland 1975, McGregor 1966). These rewards are similar in that they are time-consuming and difficult to obtain through the

individual's own power. Since a steward-like employee's interests and the organization's interests are consistent, such an individual's needs can be satisfied via the organization's achievements over a relatively long period. Davis *et al.* (1997) also recognized that identification with and commitment to the organization can facilitate an individual's motivation to promote the success of the organization (Hernandez 2012).

4.4 Hypotheses development

Based on the theoretical background and considering our specific research context (i.e., employees' ISRB in organizations), we further developed our hypotheses. Since it is difficult to monitor employees' ISRB in reality, we used IS security risk-taking intention (ISRI) as a proxy. We propose that employees' ISRI is negatively influenced by a LTO. Further, the LTO is positively influenced by employees' value identification of avoiding ISRB, trusted relationship fulfillment, and personal growth needs fulfillment. The research model is shown in Fig. 8.

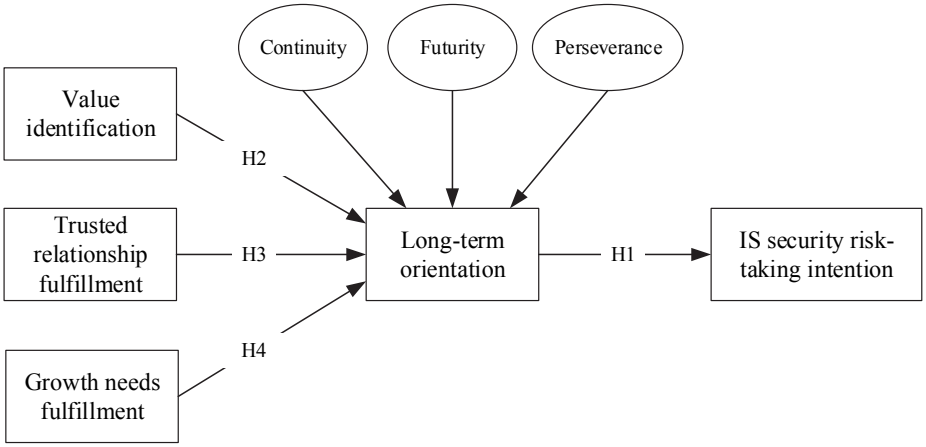

Fig. 8. Stewardship model of employees' IS security risk-taking behavior.

Long-term orientation

In the current context of ISRB in organizations, the term *LTO* refers to an employee's mindset that the long-term consequences of the IS security risk-taking decision should be considered. Since employees and organizations share the same

goals of IS security, employees who have a high degree of LTO will think more about the possible consequences of their ISRB, including its threats to the organization in the future. Therefore, they are less likely to have ISRI. Previous research found that employees with a LTO often behave well beyond current legal requirements, avoiding the compliance costs that come with stricter laws (Wang & Bansal 2012). Employees with high consideration of future consequences are more likely to engage in prosocial behavior (Insko *et al.* 1998, Joireman *et al.* 2006, Joireman *et al.* 2004, Strathman *et al.* 1994) and to be more safety-conscious (Graso & Probst 2012).

Since LTO has three dimensions (i.e., continuity, futurity, and perseverance), an employee's degree of LTO is likely to affect his or her ISRI in three ways. First, an employee with high degree of continuity may believe that avoiding ISRB at work in the past had value; therefore, persisting in the behavior is still valuable for now and future. Such persistence would cause the employee to try to avoid ISRI every time he or she confronts risky situations. Second, an employee with high degree of futurity may take both current and future consequences of behavior into consideration. For example, when an employee thinks about using a personal unencrypted USB stick to store confidential corporate data, he or she may consider whether the data could be leaked if the USB stick fell into the wrong hands in the future. Since employees with a high degree of futurity value the future impact of the current behavior, the undesired future outcomes may prevent the ISRI. Third, an employee with high degree of perseverance may believe that it is worth sacrificing the immediate fun or convenience if it can ensure IS security in the long run. Sometimes, it is time-consuming or burdensome to comply with IS security policies (Bulgurcu *et al.* 2010). Due to that ISRB may be highly embedded into work, e.g., using an unencrypted USB stick, it may be costly to keep avoiding such behaviors in routine work. However, if employees have the belief of perseverance, they may value the effectiveness of their actions, believe that the efforts made today will pay off in the future, and therefore overcome the current inconvenience. As a result, employees with such beliefs may have more chances to sacrifice the immediate benefits to keep avoiding ISRI in order to contribute to a long-term safety environment. Together, employees' LTO (formed by continuity, futurity, and perseverance) may negatively influence their ISRI. Thus, we hypothesize that:

H1: An employee's long-term orientation is negatively associated with the employee's IS security risk-taking intention.

Value identification

In the current context, *value identification* refers to the extent to which employees identify with the meaning and value of IS security that the organization preaches. Value identification is an important psychological profile of a steward-like employee. Employees who identify with the organizational values are motivated to help achieve the long-term interests of the organization (Davis *et al.* 1997). Research has shown that identification is positively associated with organizational citizenship behaviors, work effort, and cooperation (Bartel 2001, Dukerich *et al.* 2002, Mael & Ashforth 1992, O'Reilly & Chatman 1986). A strong identification with and a belief in an organization's goals enhance the employee's willingness to exert considerable effort on behalf of the organization (Mowday *et al.* 2013). In general, researchers have agreed that identification leads to employees' behaviors that help organizations accomplish their objectives (Besharov 2014).

Regarding the tendency to avoid ISRB in work, as we analyzed before, it usually takes time and effort to evaluate the effectiveness of IS security measures and the outcomes of employees' behavior. Employees who recognize and accept the underlying value of the security behavior may better understand the consequences of ISRB and its possible influence in the future and, as a result, may think that they should consistently avoid ISRB. We propose that value identification will make employees recognize the necessity of considering the long-term consequences of ISRB. Thus, we hypothesize that:

H2: An employee's value identification of ISRB avoidance is positively associated with the employee's long-term orientation.

Trusted relationship fulfillment

Trusted relationship fulfillment refers to an employee's perception of the extent to which avoiding ISRB fulfills his or her need for developing a trusted relationship. A trusted relationship is a higher order need that a steward-like employee pursues in an organizational environment (Davis *et al.* 1997). Maintaining relationships is a dynamic process. People must continually invest time and effort to maintain an established relationship. Therefore, if an individual perceives that a behavior can help him or her to enhance a relationship, he or she may think it is worth engaging in such behavior consistently.

In the current context, avoiding ISRB in work can help the employee to establish a trusted relationship since the behavior usually protects confidentiality and the integrity of work data and therefore protects the work of other colleagues. Employees who rarely engage in ISRB may be regarded as responsible and trusted coworkers (Flowerday & von Solms 2006). However, the trusted relationship requires time to establish. As a result, individuals who perceive the benefits of avoiding ISRB in terms of trusted relationship development may generate a LTO and believe that continuing to avoid ISRB is meaningful. In this case, they take into consideration the long-term influence of ISRB on the maintenance of the trusted relationship. Thus, we hypothesize that:

H3: An employee's trusted relationship fulfillment is positively associated with the employee's long-term orientation.

Growth needs fulfillment

Growth needs fulfillment refers to an employee's perception of the extent to which avoiding ISRB is able to fulfill his or her need for growth. In the current context, *growth* typically refers to the knowledge of IS security and the ability to deal with security-related situations. IS develops very quickly. Learning to use new technology and solving problems in a new system can give people the feeling of achievement and therefore increase the individual's willingness to keep using the system (Au *et al.* 2008). The feeling of self-growth arises when people take on and meet what they view as an optimal challenge (Deci & Flaste 1995). These findings about higher order needs and performance are consistent with the assumptions of stewardship theory, which notes that an employee's personal needs are met by working toward organizational, collective ends (Davis *et al.* 1997). In the context of ISRB, employees who have growth needs are willing to master security-related knowledge and are able to deal with different risky situations and solve security problems, which offers employees opportunities to demonstrate their capabilities at work. For example, in order to avoid downloading suspicious files from the Internet, employees should be able to find more secure sources instead. In order to practice this capability, employees may be willing to think more about the possible consequences of ISRB, including the consequences in the future, which may generate a LTO. Thus, we hypothesize that:

H4: An employee's growth needs fulfillment is positively associated with the employee's long-term orientation.

Control variables

According to Bono and McNamara (2011), control variables should meet three conditions for inclusion in a study (Becker 2005, James 1980). First, there is a strong expectation that the variable be correlated with the dependent variable owing to a clear theoretical tie or prior empirical research. Second, the control variable should be correlated with the hypothesized independent variable(s). Third, the researcher must present a logical reason for why the control variable is not a more central variable in the study, either a hypothesized one or a mediator. If a variable meeting these three conditions is excluded from the study, the results may suffer from omitted variable bias.

Our model includes six control variables that meet the above three conditions: gender, age, type of contract, years of working in the company, years of computer use, and IT knowledge. Previous literature confirmed that younger people and males are more likely to engage in illicit behavior (Leonard & Cronan 2005, Leonard *et al.* 2004, Piquero & Tibbetts 1996, Pratt *et al.* 2006). IS literature has also suggested that computer experience is negatively related to technology misuse (Loch & Conger 1996). We further predict that lack of IT knowledge may be a reason for ISRB, and it may relate to an individual's needs for growth. Years of working in the company and type of contract may be relevant to an employee's stewardship behavior. Research has indicated that longer employment may promote a long-term orientation (Miller & Shamsie 2001, Zahra 2005).

4.5 Methodology

We used scenarios to test our proposed hypotheses. We applied the scenario method because it provides more details and contextual specificity (Nagin & Paternoster 1993) while remaining a nonintrusive way to respond to sensitive issues (Nagin & Pogarsky 2001). In addition, Piquero and Hickman (1999) suggested that the scenarios should not be uncommon to respondents.

4.5.1 Measurement

Scenario design

In order to make realistic and believable scenarios, we designed the scenarios together with the security managers from the company where we collected the data. First, the security managers listed the IS security problems that concerned them, covering a wide range of issues such as secure use of mobile devices, secure emailing, secure behavior when traveling, and secure use of the Internet. Based on their list, we composed the specific scenarios. Then, the security managers evaluated whether these scenarios were relevant to their situations and helped edit them. After two rounds of modification, we finalized three scenarios that were regarded as the most relevant to the company. The specific scenarios are shown in Appendix 5.

Instrumentation

Guided by Siponen and Vance (2014) who suggested measuring specific examples of IS security policy violations to get more accurate measures, we used specific scenarios as described above. In addition, we measured both the dependent variable and the independent variables in specific ways. For example, to measure intention, we asked, "If you were Newman, what is the likelihood that you would have copied the file onto a personal unencrypted USB stick?" To measure continuity, we asked respondents to evaluate statements such as, "It is valuable that I always avoid the behavior without exception." In the survey, we explained that "the behavior" referred to Newman's action as described in the scenario (e.g., copying the file onto a personal unencrypted USB stick). We measured the dependent variable—ISRI using two items adapted from D'Arcy *et al.* (2009).

We treated LTO as a formative construct. Conceptually, the three dimensions (i.e., continuity, futurity, and perseverance) share similarities to the extent that they describe a single construct (LTO), but they also each explain a different facet of the LTO construct (Brigham *et al.* 2014). Therefore, we formatively constructed LTO by three reflective first-order constructs (i.e., continuity, futurity, perseverance). We measured continuity (LTO_C), futurity (LTO_F), and perseverance (LTO_P) using two items adapted from Brigham *et al.* (2014). We measured value identification (VI) using two items adapted from Davis *et al.* (1997). We measured trusted relationship fulfillment (TRF) using two items adapted from Deci *et al.* (1991). We

adapted the three items that measured growth needs fulfillment (GNF) from Alderfer (1972). We assessed the measures for dependent and independent variables using a seven-point Likert scale. Except for the scale of ISRI1 that was anchored from 1 (“very unlikely”) to 7 (“very likely”), the rest of the item scales were anchored from 1 (“strongly disagree”) to 7 (“strongly agree”). For the control variables, for gender, male was coded as 1 and female coded as 2. Age was categorized into 1 (18–25), 2 (26–35), 3 (36–45), 4 (46–55), 5 (56–65), and 6 (66 and above). For the type of work contract, a fixed term contract was coded as 1, and a permanent term contract was coded as 2. We measured IT knowledge using a seven-point Likert scale ranging from 1 (“very low”) to 7 (“very high”). Region of country was categorized into 1 (Canada), 2 (Hong Kong), 3 (Singapore), 4 (South Africa), 5 (United Kingdom), and 6 (United States). We measures both years of working in the company and years of computer use in years. The full instrument is provided in Appendix 5.

Pilot study

We conducted a pilot study before the primary data collection. Since the wordings were just slightly different among the three scenarios, we used one scenario (i.e., unauthorized portable devices for storing corporate data) to pilot the survey. We invited our faculty members, Ph.D. students, and any researchers familiar with the topic to complete the survey and provide comments on our questions. The pilot sample size was 39. We assessed reliability by using Cronbach’s α, and the convergent and discriminant validity by using principal components analysis. The assessment indicated acceptable results for the instrument.

4.5.2 Sample and data collection

We conducted the primary data collection at a global insurance company that owns offices in more than 70 countries, has more than 3500 employees, and serves more than 160 countries. The security manager suggested that we randomly send the survey to 670 employees in the following six countries: Canada, Hong Kong, Singapore, South Africa, United Kingdom, and United States. We composed the survey in English and made it available online. We sent an email to each selected employee that contained the survey link as well as a brief introduction about the survey’s purpose and assurance of anonymity. We randomly assigned each respondent to one of the three scenarios and corresponding questions. The duration

of the data collection was 18 days. We received 170 responses, a response rate of 25.4%, after a single reminder on the tenth day. The demographic information is shown in Table 11.

Table 11. Demographic information.

Demographics	Frequency (N = 170)	Percentage
Gender		
Male	89	52.4%
Female	81	47.6%
Age		
18–25	4	2.4%
26–35	34	20.0%
36–45	45	26.5%
46–55	53	31.2%
56–65	31	18.2%
66 and above	3	1.8%
Type of work contract		
Fixed term	35	20.6%
Permanent term	135	79.4%
IT knowledge		
1 (Very low)	4	2.4%
2	13	7.6%
3	24	14.1%
4	54	31.8%
5	44	25.9%
6	18	10.6%
7 (Very high)	13	7.6%
Country of origin		
Canada	8	4.7%
Hong Kong	10	5.9%
Singapore	15	8.8%
South Africa	3	1.8%
United Kingdom	34	20.0%
United States	100	58.8%
Participants in each scenario		
Scenario 1	56	32.9%
Scenario 2	50	29.4%
Scenario 3	64	37.6%

To test the nonresponse bias, we followed the post-hoc strategy for estimating nonresponse error proposed by Sivo *et al.* (2006). We compared the early one-third of the respondents (N = 56) and the last one-third of the respondents (N = 56) on all their answers, shown in Table 12. All *t*-test comparisons between the means of the early and late responses showed no significant differences, which indicates that the nonresponse bias is not a problem in this study.

Table 12. Mean comparison between early and late responses.

Variable	Mean		*t*-statistic	Significant difference?
	Early responses (N = 56)	Late responses (N = 56)		
ISRI1	2.63	2.14	1.403	No
ISRI2	2.82	2.46	0.958	No
LTO_C1	5.61	6.02	-1.757	No
LTO_C2	5.79	5.95	-0.647	No
LTO_F1	5.48	5.84	-1.505	No
LTO_F2	5.54	5.86	-1.407	No
LTO_P1	5.89	5.93	-0.176	No
LTO_P2	5.82	5.96	-0.66	No
VI1	5.71	5.98	-1.139	No
VI2	5.91	6.23	-1.464	No
TRF1	5.43	5.61	-0.658	No
TRF2	5.3	5.32	-0.061	No
GNF1	5.18	5.63	-1.595	No
GNF2	4.86	5.23	-1.304	No
GNF3	4.86	5.27	-1.431	No
Gender	1.46	1.5	-0.375	No
Age	1.52	-0.05	0.497	No
Contract	-3.71	-1.75	-0.495	No
IT knowledge	4.18	4.32	-0.541	No
Years of using computer	20.82	21.54	-0.535	No
Years in company	6.27	8.13	-1.311	No

4.6 Data analysis and results

We used SmartPLS v3.2.0 to analyze our research model (Ringle *et al.* 2015). We chose the partial least square-based structural equation modeling (PLS-SEM) technique because the LTO in our model is a multidimensional second-order construct (MacKenzie *et al.* 2005), for which SEM methods are better suited. We chose PLS because it is more amenable for handling LTO, which is a formative construct.

4.6.1 Measurement model

For the reflective constructs, we assessed internal consistency and convergent validity by examining item loading, Cronbach's α, composite reliability, and average variance extracted (AVE) (Gefen & Straub 2005). We compared the results

(see Table 13 and Table 14) with the commonly accepted guidelines. For reliability, the composite reliability of the constructs was greater than 0.8 (Nunnally 1978), and Cronbach's α was greater than 0.7 (Chin 1998). For convergent validity, indicator loadings exceeded 0.7 (Chin 1998), and AVE for each reflective construct exceeded 0.5. We performed a bootstrap with 1000 resamples and examined the *t*-values of the outer model loadings. All the indicators exhibited loadings that were significant ($p < 0.001$), denoting strong convergent validity.

Table 13. Descriptive statistics.

Construct	Subconstruct	Mean	Standard deviation	Cronbach's α	Composite reliability	AVE
IS security risk-taking intention	N/A	2.65	1.89	0.85	0.93	0.87
Long-term orientation	Continuity	5.62	1.25	0.90	0.95	0.91
	Futurity	5.85	1.06	0.77	0.90	0.81
	Perseverance	5.82	1.23	0.84	0.93	0.86
Value identification	N/A	5.83	1.21	0.88	0.94	0.89
Trusted relationship fulfillment	N/A	5.06	1.48	0.91	0.96	0.92
Growth needs fulfillment	N/A	5.39	1.33	0.83	0.90	0.75

Table 14. Convergent validity for reflective measures.

Construct	Subconstruct	Indicator	Loading	*t*-statistic
IS security risk-taking intention	N/A	ISRI1	0.93	16.80***
		ISRI2	0.94	17.23***
Long-term orientation	Continuity	LTO_C1	0.95	74.36***
		LTO_C2	0.96	46.85***
	Futurity	LTO_F1	0.90	14.39***
		LTO_F2	0.91	20.15***
	Perseverance	LTO_P1	0.93	36.02***
		LTO_P2	0.93	21.37***
Value identification	N/A	VI1	0.94	36.31***
		VI2	0.95	31.98***
Trusted relationship fulfillment	N/A	TRF1	0.95	28.42***
		TRF2	0.96	21.96***
Growth needs fulfillment	N/A	GNF1	0.92	14.04***
		GNF2	0.84	10.70***
		GNF3	0.83	8.91***

Note: *** $p < 0.001$.

For the discriminant validity, all items loaded higher on their respective constructs than on the other constructs, and the cross-loading differences were much higher than the suggested threshold of 0.1 (Gefen & Straub 2005) (see Table 15). The square root of the AVE of each construct was higher than the inter-construct correlations (Fornell & Larcker 1981) (see Table 16). The correlations among all constructs were all well below the 0.90 thresholds, suggesting that all constructs were distinct from each other (Herath & Rao 2009a).

Table 15. Loadings and cross loadings.

Construct	Subconstruct	Item	ISRI	LTO_C	LTO_F	LTO_P	VI	TRF	GNF
IS security risk-	N/A	ISRI1	**0.93**	-0.56	-0.29	-0.45	-0.47	-0.40	-0.39
taking intention		ISRI2	**0.94**	-0.58	-0.38	-0.47	-0.54	-0.50	-0.31
Long-term	Continuity	LTO_C1	-0.57	**0.95**	0.53	0.54	0.75	0.53	0.54
orientation		LTO_C2	-0.59	**0.96**	0.64	0.62	0.78	0.59	0.57
	Futurity	LTO_F1	-0.30	0.48	**0.90**	0.61	0.54	0.47	0.37
		LTO_F2	-0.36	0.63	**0.91**	0.52	0.71	0.46	0.44
	Perseverance	LTO_P1	-0.44	0.56	0.61	**0.93**	0.55	0.55	0.35
		LTO_P2	-0.47	0.58	0.56	**0.93**	0.51	0.58	0.39
Value identification	N/A	VI1	-0.50	0.77	0.64	0.50	**0.94**	0.54	0.47
		VI2	-0.52	0.75	0.67	0.57	**0.95**	0.60	0.51
Trusted relationship	N/A	TRF1	-0.45	0.54	0.47	0.56	0.55	**0.95**	0.49
fulfillment		TRF2	-0.47	0.59	0.52	0.61	0.60	**0.96**	0.52
Growth needs	N/A	GNF1	-0.36	0.60	0.42	0.37	0.55	0.49	**0.92**
fulfillment		GNF2	-0.28	0.42	0.38	0.35	0.39	0.43	**0.84**
		GNF3	-0.32	0.48	0.36	0.31	0.39	0.44	**0.83**

Table 16. Latent variable correlations and the square root of AVE.

Construct	ISRI	LTO	VI	TRF	GNF
IS security risk-taking intention	**0.87**				
Long-term orientation	-0.61	-			
Value identification	-0.54	0.83	**0.89**		
Trusted relationship fulfillment	-0.48	0.65	0.60	**0.92**	
Growth needs fulfillment	-0.37	0.59	0.52	0.53	**0.75**

Note: Bold items are the square root of the AVE.

In the model, long-term orientation is a second-order construct. It is a reflective-formative type of hierarchical component model. Long-term orientation is formatively constructed by three reflective first-order constructs (i.e., continuity, futurity, perseverance). We followed the two-stage approach suggested by Ringle *et al.* (2012) to test the hierarchical component model. First, we used the repeated indicators approach to obtain the latent variable score for the lower order components. Second, we used the latent variable scores as the formative indicators of the second-order construct (Wetzels *et al.* 2009).

We validated our formative construct, long-term orientation, separately from the reflective constructs. As shown in Table 17, the weights of indicators contributing to long-term orientation were all significant, which denotes good validity. Second, we examined the variance inflation factor (VIF) statistic for the

three indicators. The VIF score was no more than 1.9, well below the 3.3 threshold (Petter *et al.* 2007), which means that multicollinearity does not exist in the model and that the model has good reliability. Based on these tests results, we conclude that long-term orientation has sufficient construct validity and reliability.

Table 17. Item weights for formative measures.

Construct	Item	Weight	*t* value
Long-term orientation	LTO_C	0.77***	9.61
	LTO_F	0.16*	2.08
	LTO_P	0.18*	2.45

Note: * $p < 0.05$, *** $p < 0.001$.

Our validation results suggest that all reflective measures demonstrated satisfactory reliability and construct validity and that the formative measures demonstrated satisfactory construct validity and no significant multicollinearity. Therefore, all of the measures were valid and reliable.

Common method variance

We also assessed the common method variance (CMV). Because we collected the data from a single source (i.e., an individual employee) at a single point in time, CMV could unduly sway the results (Podsakoff *et al.* 2003). We attempted to mitigate this bias by adopting multiple techniques. Specifically, we used both procedural remedies and statistical remedies.

As for procedural remedies, we first conducted pilot studies for the questionnaire to eliminate ambiguous items. Second, we informed the participants that their responses would be confidential and assured them that there were no right or wrong answers. Third, we used technical scenarios to let the participants imagine the situation described before making their decisions rather than asking them about their own behavior directly, which is a nonintrusive method. Finally, we randomly sorted the question order to reduce hypothesis guessing.

As for statistical remedies, since each method used by previous studies has its advantages and disadvantages (Chin *et al.* 2012), we used several methods to identify the problem collectively. First, we conducted Harman's one-factor test by including all items in a principal components factor analysis (Podsakoff *et al.* 2003). Evidence for CMV exists when one factor accounts for most of the covariance. The results revealed four factors with no single factor accounting for a majority (<50%)

of variance, suggesting no substantial CMV among the scales. Second, we used a partial correlation method (Lindell & Whitney 2001, Podsakoff *et al.* 2003). Given that we did not include any constructs that were completely theoretically unrelated to one or more constructs in our model, we followed Pavlou *et al.* (2007) to use a construct that was weakly related to other constructs as the marker variable. We used its average correlation with the principal study variables (r = 0.026) as the CMV estimate. Following Malhotra *et al.* (2006), we developed a CMV-adjusted correlation matrix and examined the CMV-adjusted structural relationships in our research model.[2] We found no changes in significance after accounting for the distinct construct, suggesting the effect of CMV was minimal. Finally, we followed Lindell and Whitney (2001), Malhotra *et al.* (2006), Richardson *et al.* (2009), and Williams *et al.* (2010) to conduct a confirmatory factor analysis (CFA) marker test in AMOS 22. Specifically, to assess method variance, we specified a hypothesized method factor as an underlying driver of all of the indicators in the measurement model. The fit indices of the model including the method factor were not significantly better than the original one ($\chi^2 = 24.976$, df = 15, $p = 0.0503$). All the results mentioned above collectively suggest that the CMV was not serious in our study.

4.6.2 Theoretical model test

The main effects model

Our PLS results of the full model are consistent with our theory, as shown in Fig. 9. Long-term orientation has a significant negative effect (path coefficient = -0.58, $p < 0.001$) on IS security risk-taking intention, supporting H1. Value identification has a significant positive effect (path coefficient = 0.64, $p < 0.001$) on long-term orientation, supporting H2. Trusted relationship fulfillment has a significant positive effect (path coefficient = 0.17, $p < 0.05$) on long-term orientation, supporting H3. Growth needs fulfillment has a significant positive effect (path coefficient = 0.17, $p < 0.05$) on long-term orientation, supporting H4.

[2] Within the framework of marker-variable analysis, a method factor is assumed to have a constant correlation with all of the measured items. Under this assumption, a CMV-adjusted correlation between the variables under investigation, r_a, will be computed by partialling out r_m, from the uncorrected correlation, r_u. In particular, with a sample size of n, r_a and its t-statistic can be calculated as follows: $r_a = (r_u - r_m) / (1 - r_m)$, $t = r_a / \text{sqr}\,(1-r_a^2) / (n-3)$.

Long-term orientation explained 41% of the variance in IS security risk-taking intention. Value identification, trusted relationship fulfillment, and growth needs fulfillment collectively explained 74% of the variance in long-term orientation. None of the control factors were significant in this study. In summary, the results provide support for all hypotheses we proposed. Detailed results are provided in Table 18.

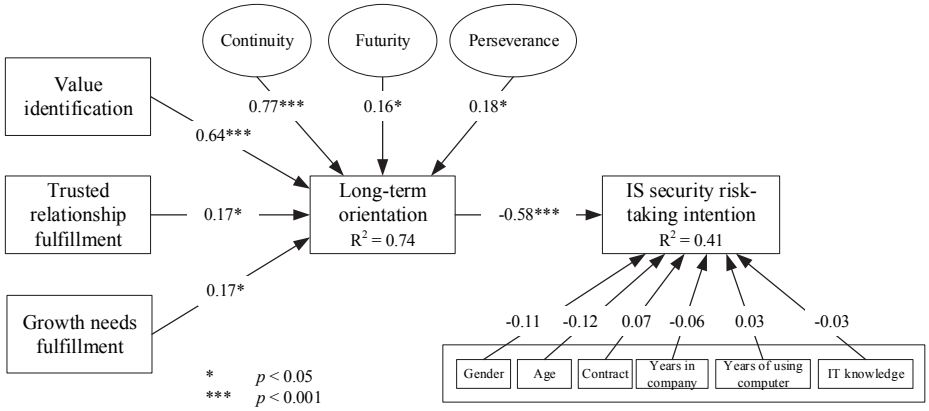

Fig. 9. Structural model results.

Table 18. Summary of hypotheses, path coefficients, and significance levels.

Tested path	Path coefficient	*t*-value	Significant?
Hypotheses			
H1. Long-term orientation → IS security risk-taking intention	-0.583***	9.75	Yes (H1 is supported.)
H2. Value identification→ Long-term orientation	0.64***	9.53	Yes (H2 is supported.)
H3. Trusted relationship fulfillment → Long-term orientation	0.17*	2.34	Yes (H3 is supported.)
H4. Growth needs fulfillment → Long-term orientation	0.17*	2.31	Yes (H4 is supported.)
Control variables			
Gender	-0.11 (n.s.)	1.65	No
Age	-0.12 (n.s.)	1.73	No
Contract	0.07 (n.s.)	1.46	No
Years in company	-0.06 (n.s.)	0.94	No
Years of using computer	0.03 (n.s.)	0.41	No
IT knowledge	-0.03 (n.s.)	0.52	No

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$, n.s. = not significant.

The mediation effect

We conducted mediation analysis following the bootstrapping approach by Hayes (2012). Bootstrapping method is an advanced approach to test the mediation effect, which has several advantages in addition to greater statistical power. First, the indirect effects can be measured directly rather than merely inferred to exist through a sequence of tests, as seen in the traditional Baron and Kenny method (Baron & Kenny 1986, Hayes 2009). Second, unlike the traditional Sobel method, it does not assume that the mediation effect is normally distributed. This factor is important because studies have shown that indirect effects frequently exhibit asymmetric distributions. In such cases, using a test that assumes a normal distribution results in lower statistical power (MacKinnon *et al.* 2002).

To test our hypotheses, we used bootstrapping to construct confidence intervals (CIs) of the mediation effects. Testing mediation effects with bootstrapping is similar to the Baron and Kenny method in that three paths are evaluated: (1) the path from the independent variable to the mediating variable (path *a*), (2) the path from the mediating variable to the dependent variable (path *b*), and (3) the path from the independent variable to the dependent variable (path *c*, or *c′* when considered simultaneously with paths *a* and *b*).

The bootstrapping process involves resampling with a replacement from the obtained sample several thousand times. For each resample, the coefficient of path *a* is multiplied by the coefficient of path *b*. The product of *ab* is the estimate of the indirect effect in the resample (MacKinnon *et al.* 2002). The coefficient for *c′* is also saved. The process is repeated k times, where k is a number equal to at least 1000 and preferably equal to or greater than 5000 (Hayes 2009). At the end of the bootstrapping process, thousands of values for *ab* and *c′* are obtained.

Next, the values for *ab* and *c′* are sorted from largest to smallest and a percentile-based CI is constructed (ci%). This is done by identifying the ordinal positions of *ab* and *c′* that correspond to the bounds of the CI, using the formula k(0.5 - ci/200) for the lower bound and the formula 1 + k(0.5 + ci/200) for the upper bound (Hayes 2009). In our case, we obtained 5000 resamples and specified a 95% CI. For the sorted *ab* values, the lower bound of the CI was represented by the *ab* value in the 125th position.

For the *ab* CI, if zero is not between the lower and upper bound, then one can state with ci% confidence that the indirect effect is not zero (MacKinnon 2008). It is possible to determine whether full or partial mediation occurred by examining the CI for *c′*. If *ab* is non-zero and *c′* is zero, this result indicates full mediation. If both *ab* and *c′* are non-zero, then this result is evidence of partial mediation (Shrout & Bolger 2002).

We followed the above procedures to bootstrap the effects of our three factors on long-term orientation (path *a* 1–3) using PROCESS (Hayes 2012) and a macro to obtain 5000 resamples. We did the same for the effect of long-term orientation on IS security risk-taking intention (path *b*) and for the effects of our three factors on intention (*c′* 1–3). Table 19 reports the 95% CIs for each path; whether zero was obtained in the CI, indicating mediation; and whether full or partial mediation was observed. The results show that the effect of each factor was fully mediated by LTO.

Table 19. Bootstrapped CI tests for mediation.

Variable	Mediation test (*ab*)			Full/partial mediation test (*c'*)			Type of mediation
	2.5% lower bound	97.5% upper bound	Zero included?	2.5% lower bound	97.5% upper bound	Zero included?	
Value identification	-0.639	-0.223	No	-0.326	0.105	Yes	Full
Trusted relationship fulfillment	-0.470	-0.219	No	-0.309	0.004	Yes	Full
Growth needs fulfillment	-0.562	-0.216	No	-0.168	0.131	Yes	Full

4.7 Discussion

The empirical results supported all our hypotheses. In this section, we highlight our main findings based on the empirical results. First, we found that long-term orientation had a significant negative impact on employees' ISRI in the organization. This finding indicates that employees who hold the three long-term-related beliefs in mind are less likely to conduct information ISRB. The underlying reasons for this finding are that: (1) these employees respect the value of consistent good IS security practices, (2) they take the future consequences of current behavior into account, and (3) they are willing to sacrifice immediate benefit to achieve long-term IS security goals. This finding is consistent with previous studies suggesting that long-term orientation decreases an individual's risk-taking behaviors, including entrepreneurs' risk decisions (Das & Teng 1997), risky behaviors (e.g., smoking, drinking, using drugs) in life (Keough *et al.* 1999), and employees' rule violation in organizations (Takemura & Komatsu 2012). Previous research has found that LTO promotes an individual's positive behaviors, such as self-regulation behavior in the health domain (Buhrau & Sujan 2014, Park *et al.* 2012), organizational citizenship behavior (Balliet & Ferris 2013, Joireman *et al.* 2006), and higher quality work (Graso & Probst 2012), which are in line with our suggestions as well. Previous IS research has found that a user's consideration of long-term consequences positively influences the current usage of a personal computer because the outcomes of using the computer in the future can pay-off the current efforts in learning the system (Thompson *et al.* 1991, 1994).

Second, we found that the more employees identify with organizational IS security goals and policies, the more likely they are to generate a long-term orientation toward ISRB-avoiding activities. This result indicates that employees with value identification will not only consider the ongoing behavior outcomes, but also pay attention to the future consequences of their acts, which is a reflection of

a deep understanding of and strong agreement with organizational IS security policies. In IS research, Bateman *et al.* (2011) found that, when the members of a virtual community recognize the value of the community, they will persist in staying in the community.

Third, we found that the fulfillment of two types of employee needs (i.e., the need for trusted relationships and the need for growth) significantly influenced the emergence of an employee's LTO. These findings indicate that, although avoiding ISRB may require more effort on the employees' part, they will think that avoiding ISRB consistently is meaningful (1) if they feel that such behavior will help them be recognized as trustworthy and reliable workers in the organization or (2) if it challenges their abilities to deal with risky situations. More importantly, our findings confirm that the two types of needs require time to fulfill, therefore leading to LTO.

Finally, we found no significant impact from control variables (i.e., gender, age, type of work contract, IT knowledge, years of using computers, and years of working in the company) on an employee's ISRI.

Implications for research

This chapter makes several contributions to the literature on IS security behavior. First, we adopted a temporal perspective to understand IS security behavior and its influential factors. We highlighted the possible delayed consequences as part of the characteristics of ISRB. Employees with ISRB may not foresee the immediate consequences, but their behaviors leave the organization's IS in a vulnerable state for future attack. Without considering the long-term future consequences, employees may underestimate the seriousness of their behavior, thereby leading to ISRB. Therefore, ISRB especially needs theoretical insights from a temporal perspective, though this discussion is still lacking in existing IS security behavior literature. In addition, we also applied a temporal perspective to look at the influential factors, such as LTO, and individuals' needs. LTO is a psychological construct that contains continuity, futurity, and perseverance beliefs, which all emphasize the concern for a long period of time. For individuals' needs, such as trusted relationships and growth needs, we also suggest that these types of needs cannot be satisfied in the short term, but must be satisfied in the long term. For that reason, the perceived fulfillment of these needs is relevant to LTO. Through our preliminary study, we were able to demonstrate the value of adopting a temporal perspective as a new research avenue to study IS security behavior.

Second, by adopting a temporal perspective, we are the first to our knowledge to empirically investigate the role of long-term orientation in the context of an employee's IS security risk-taking behavior in an organization. We have shown that LTO is an influential predictor of IS security risk-taking intention, although no previous research has ever identified it. Furthermore, we highlighted that LTO and its related concepts discussed in this study may have important implications for future IS security behavior research. First, it may help uncover the mixed findings of control elements in organizations, such as the effect of monitoring, deterrence (D'Arcy *et al.* 2009, Siponen & Vance 2010), and so on. Researchers in criminology have revealed that sanction threats are weak for those criminal offenders who do not consider future consequences since they have a tendency to deliberatively devalue the future or fail to consider the future (Nagin & Pogarsky 2001, 2004). Thereby we suggest that future research should investigate whether LTO moderates the role of deterrence or monitoring on employees IS security behavior.

A second research opportunity related to LTO is to investigate how long the future consequences will unfold in an individual's mind, and its role on IS security behavior. According to construal level theory, the psychological temporal distance changes people's responses to future events by changing the way people mentally represent those events (Liberman & Trope 2014, Liberman *et al.* 2007, Trope & Liberman 2003). In other words, people may think and behave in different patterns according to the psychologically near or distant future consequences. Future research can examine if this psychological temporal distance leads to different explanations for security-related behaviors. Previous research has found that influential factors, such as value or abstractness of information, play different roles in behaviors or intentions for near and distant future events (Eyal *et al.* 2009, Nussbaum *et al.* 2006). Future IS security behavior research can explore if similar factors exist.

A third research opportunity regarding LTO is to identify the appropriate organizational strategies that facilitate employees to generate LTO. Although we have shown that LTO can increase employees' secure behavior, the questions still remain as to what strategies organizations should implement. Liang *et al.* (2013) suggested that organizations can adopt two types of strategies to regulate employees' IS security behavior: promotion focus and prevention focus (Higgins 1997). Promotion focus is driven by the need for growth and development (Johnson & Yang 2010, Liang *et al.* 2013). Steidle *et al.* (2013) found that the growth needs are more likely to be fulfilled by promotion focus strategies rather than prevention

focus strategies. Since we found that LTO is motivated by growth needs fulfillment, future research can examine if a promotion focus regulation strategy can increase employees' LTO.

Our third contribution is that we were the first to draw on stewardship theory to offer a theoretical explanation and empirical support for the influential factors on employees' IS security risk-taking behavior. Previous studies have dominantly applied theories such as deterrence theory and rational choice theory that hold the assumptions that employees are individualistic, opportunistic, and self-serving. Under such assumptions, only those factors that attach to individuals' self-utilities are found, such as punishment or momentary and time benefits. However, little research has considered the possibility that employees can be collectivists, pro-organizational, and trustworthy, as stewardship theory assumes. Stewardship theory provides an alternative understanding of employees' behavior in an organization, suggesting that employees may willingly subjugate their personal interests to protect the organization's long-term welfare (Hernandez 2012), and may be motivated by higher order needs, such as growth, achievement, and self-actualization, as well as by intrinsic rewards (Davis *et al.* 1997). Drawing on stewardship theory, we argue that LTO, value identification, trusted relationship fulfillment, and growth needs fulfillment are important factors influencing IS security risk-taking intention. Our findings provided strong empirical support for our arguments. We believe that stewardship theory can contribute more to IS security behavior research. Other research fields based on stewardship theory have suggested that factors such as psychological ownership, affective commitment (Hernandez 2012), and organizational culture (Davis *et al.* 1997) can influence employees' behavior. Future research can examine their roles in explaining IS security behavior.

Implications for practice

This study offers several important practical implications for IS security management in organization. Generally speaking, our empirical results suggest that a shift in IS security management strategy may be necessary. Although deterrence-based control measures, such as sanctions and monitoring (D'Arcy *et al.* 2009), as well as others, such as IS security policies, mandatoriness (Boss *et al.* 2009, D'Arcy *et al.* 2009) may have some effect on regulating employees' IS security behavior, these strategies merely address employees' responsibilities to comply. However, such strategies overlook employees' intrinsic desire to work in and serve the

organization. Employees could have higher order needs to be fulfilled through the success of the organization, such as the need for growth. In this sense, organizations should apply different strategies to encourage such intrinsic motivations.

Based on our finding that LTO can decrease employees' IS security risk-taking intention, we suggest that organizations design corresponding job descriptions, performance evaluations, and incentive systems. First, organizations can highlight that IS security is a long-term mission in each job description. They should inform employees that potential threats may appear after a period of time and instruct employees to pay attention to whether their behaviors cause potential threats for the future. Second, long period evaluations of an individual's performance might encourage employees to focus on long-term rather than short-term outcomes. Organizations can evaluate the continuous secure behavior logs of employees over a relatively long period of time (e.g., one year) and trace the original causes of security incidents to a specific responsible person (Flowerday & von Solms 2005). It is necessary to evaluate long-term performance with regard to employees' IS security behavior. Third, the organization should also base incentives on a long-term evaluation.

Second, since employees' identification with the IS security policies and the recommended security behaviors can increase LTO, we suggest that IS security management design training programs to emphasize the value of persistent secure behavior. IS security managers can persuade employees not to trust to luck about their problematic behavior at every single time, and make them understand that, although it might not cause the organization immediate loss, such behavior can result in loss sometime in the future. Employees should know they play important roles in their organizations in terms of protecting against information security threats.

Third, with respect to the fulfillment of the two types of higher order needs (i.e., trusted relationship and growth needs) that can lead to LTO, we provide two suggestions for organizations. First, organizations can implement peer evaluations, which can be anonymous, aiming to let individuals know if they are trustworthy or responsible in their work regarding IS security. Since employees care about their relationships with peers and their opinions, they can be motivated to improve their performance. Second, employees should be encouraged to recognize and solve IS security problems on their own. Although organizations have IT specialists, we do not suggest that they totally rely on these specialists because employees may deny responsibility for IS security problems they cause (Siponen & Vance 2010) and consequently may have problematic behavior. Our findings indicate that employees

have the intrinsic desire to learn and train themselves. By performing good security practices, their growth needs are fulfilled. Organizations should affirm or reward employees exhibiting such desires.

Limitations

This study has several limitations. First, although IS security risk-taking behavior is the key focus in this study, we measured intention instead of actual behavior as the dependent variable. Intention is regarded as a strong predictor of actual behavior (Fishbein & Ajzen 1975), and numerous IS security behavior studies have measured intention instead of actual behavior (Anderson & Agarwal 2010, D'Arcy *et al.* 2009, Johnston *et al.* 2015, Siponen & Vance 2010). Still, future research could make a valuable contribution by making efforts to collect data of actual behavior. This approach would improve the credibility of the research model and provide more solid evidence for practices. Second, this study used only three hypothetical scenarios to measure ISRB. However, ISRB is not limited to these specific scenarios. Future research could include more types of ISRB to further test the proposed model. Third, although this study focused on ISRB, our research model may provide explanations for other types of security behavior as well. For example, security assurance behavior (SAB), defined by Guo (2013) as "the intentional behaviors that employees actively carry out to protect the organization's information systems, is an active and pro-organizational behavior" (p. 248). Future research could examine whether our research model can generalize to SAB.

4.8 Conclusion

Employees' IS security risk-taking behavior represents a significant concern of organizations regarding their information systems security. Some ISRBs may not cause immediate damage to an organization's IS, but the negative consequences may unfold in the future. Without considering the long-term future, employees may underestimate the seriousness of their risky behavior. Previous research has lacked a temporal perspective to understanding IS security behavior. To fill in the gap, our study discussed the temporal feature of ISRB and highlighted long-term orientation as an important factor that influences employees' decisions to conduct ISRB. Drawing on stewardship theory, we justified the rationality of employees to generate LTO and also identified three antecedents of LTO: value identification, trusted relationship fulfillment, and growth needs fulfillment. The empirical results

well supported our arguments. Our study contributes to IS security behavior literature by being the first to empirically investigate LTO and the first to draw on stewardship theory in the security context. We also contribute to practice by suggesting that organizations evaluate employees' long-term performance regarding IS security and encourage them to train themselves and develop abilities to solve security problems.

5 Conclusion

This dissertation discussed and examined users' IS security behavior in different contexts. Since previous studies have been conducted in one context, such as the organizational context, little research has compared the differences in behavior among different contexts. Moreover, while IS security behavior research has largely applied reference theories from other fields, little research has discussed how to apply and appropriately develop the reference theory in an IS security context. To address these gaps in research, this dissertation addressed the problems both conceptually and empirically. First, we discussed the differences between the organizational context and the home context, and called for more research on home users' IS security behavior. Second, we discussed the application of reference theory in the IS security context. We proposed a categorization of IS security context, and then highlighted that the theory modification should start from the assumption level and fit the IS security context. Then we used an empirical study to provide support for our argument. Last, we conducted a study in an organizational context, adopting a temporal perspective to explore the factors of employees' IS security risk-taking behavior. This study introduced a new theory, stewardship theory, into the IS security field. Based on the stewardship theory, we developed a contextualized theory to explain the target behavior, supported by empirical evidence.

5.1 Key findings

This dissertation includes two empirical studies. The key findings are summarized as follows.

First, users' IS security behavior in work and personal contexts is influenced by different sets of factors. Specifically, the use of a strong work password is influenced by facilitating conditions, embarrassment, monitoring, and task cost. However, the use of a strong personal password is influenced by monitoring, task benefit, and task cost. The results revealed significantly different explanations for users' IS security behavior in different contexts.

Second, we found that long-term orientation is an excellent factor for explaining employees' IS security risk-taking intentions in an organization. The empirical results indicated that employees who hold the three long-term related beliefs in mind are less likely to conduct IS security risk-taking behavior. The reasons underlying this finding are that (1) they respect the value of consistent good

IS security practices, (2) they take the future consequences of their current behavior into account, and (3) they are willing to sacrifice immediate benefits to achieve long-term IS security goals.

Third, we found that the more employees identify with organizational IS security goals and policies, the more likely they are to generate a long-term orientation toward ISRB-avoiding activities. This finding indicates that employees with value identification will not only consider the ongoing behavior outcomes, but also pay attention to the future consequences of their acts, which is a reflection of deep understanding of and strong agreement with organizational IS security policies.

Fourth, we found that the fulfillment of two types of employees' needs (i.e., need for trusted relationships and need for growth) significantly influence the emergence of employees' LTO. The findings indicated that, although doing so may require more effort from employees, they will think that avoiding ISRB is meaningful if such behavior is a way of being recognized as trustworthy and reliable in the organization and if they are challenged to deal with risky situations. More importantly, our findings confirmed that the two types of needs require time to fulfill and therefore lead to LTO.

5.2 Contributions

This dissertation mainly provides three contributions to IS security behavior literature.

First, this dissertation identifies the home users' IS security behavior as a unique phenomenon, different from the behavior in an organizational context. An approach that distinguishes four types of use can provide better understanding of the particularity of the home context. Following the approach, we identified nine contextual factors. Our contribution, therefore, is to emphasize the need for future research to focus on home users' IS security behavior.

Second, this dissertation provides an approach to developing contextualized theory in IS security behavior research. By using the case of rational choice theory, we highlighted that the contextualization should start from examining or altering the assumption of a theory. The empirical results indicate that the theory is different in different contexts.

Third, this dissertation applies a temporal perspective to understand employees' IS security risk-taking behavior in an organizational context. We applied stewardship theory in an IS security context. Following its assumptions, we

identified that long-term orientation is an excellent factor to explain IS security risk-taking behavior, and we also identified three antecedents of long-term orientation.

5.3 Future research agenda

This dissertation has mainly discussed the importance of context in IS security behavior research. Based on our discussions and findings, we further propose several future research directions and relevant research opportunities.

Moving from general context to specific context

We suggest that future research should switch the focus from a general context to a specific context. A great number of previous IS security behavior studies have focused on the context in general, under names such as IS security policy compliance/violation, IS misuse, computer abuse, or security-related behavior. However, IS security behavior can be very specific, such as using a strong password or downloading suspicious files from the Internet. In agreement with Hong *et al.* (2013), we argue that taking context into greater consideration can help develop richer theories and provide actionable advice. One way to conduct contextualized research is to focus more on a specific context than a general context. Taking ISSP violation for instance, it can be considered as a proclivity toward both general violation and specific violation. However, general violation and specific violation may or may not be the same thing. Some studies, such as those by D'Arcy *et al.* (2009), Guo *et al.* (2011), and Siponen and Vance (2010), have selected several types of specific violation behavior to represent general violation behavior; however, they have not examined the differences of these specific violations. There is possibility that individuals do not react in the same way for each specific behavior. For example, given the same policies, an employee who does not lock his or her computer may not necessarily violate other IS security policies, such as using unauthorized USB devices. In addition, the general approach would overlook the details and special explanations for specific behavior. For example, writing down a password may be relevant to memory; however, sharing a password may be relevant to the trust relationship.

The differences between general and specific contexts also exist in the factors for explanation. An individual's perceptions of general and specific stimuli may be different. Attitude studies, for instance, have established that an attitude toward a

particular object may not always be the same as the attitude toward a class of similar objects (Ajzen & Fishbein 2005, Reeve 2005, Zhang 2013). Taking the factor of sanctions in deterrence theory as an example, the perception of a particular sanction may not be the same as the perception of a general sanction. The understanding that "I will get sanctions if I violate the ISSPs" does not necessarily imply that "I will get sanctions if I do not lock the computer." As another example, realizing that a "shared USB stick may harm my computer" may not be the same as saying "John's USB stick may harm my computer." These examples indicate that studying the specific context may provide more precise explanations for IS security behavior. Future research should focus on more specific context.

Comparing IS security behavior in different contexts

Based on the dissertation, we suggest that researchers explore the role of specific contexts by using a comparative approach. The specific context can refer to our categorization of the IS security context (i.e., user context, task context, social context, and technology context) in study 2. One approach to this type of study is to design a theory-testing study in different contexts. Different explanations and results are expected, which will provide empirical evidence that each context constitutes its own research area. Similar examples can be found in IS security behavior and other IS literature (Dinev *et al.* 2009, Hovav & D'Arcy 2012, Hsieh *et al.* 2008, Karahanna *et al.* 1999, Venkatesh *et al.* 2011, Venkatesh & Zhang 2010). Future research can examine the differences in other context dimensions.

Trans-contextual study

According to our findings in study 2, users' IS security behavior varies between work and personal contexts. This result indicates that users may switch their behavioral patterns across contexts. However, questions remain about how the behavior change happens and how IS security behavior is connected and interacts in different contexts. Future research can adopt a dynamic research method to look at how users change their behavior, and what factors lead to the change. As such, we call for a trans-contextual model to explain the phenomenon.

5.4 Conclusion

Scholars and practitioners continue to be concerned with users' IS security behavior. With the increase in the number of contexts in which users use IT, security issues are also increasing. However, little research has focused on users' behavior in different contexts or the impact of context on IS security behavior research. This dissertation mainly proposes the approaches to study IS security behavior in different contexts, and also provides empirical evidence for the specific explanation in each specific context. This dissertation advances IS security behavior research by focusing on the role of context and adopting novel theoretical perspectives to understand the behavior.

List of references

Acquisti A & Grossklags J (2005) Privacy and rationality in individual decision making. IEEE Security & Privacy 3(1): 26–33.

Agarwal R & Prasad J (1999) Are individual differences germane to the acceptance of new information technologies? Decision Sciences 30(2): 361–391.

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

Ajzen I & Fishbein M (1980) Understanding attitudes and predicting social behaviour. Englewood Cliffs NJ, Prentice-Hall.

Akerlof GA & Kranton RE (2000) Economics and identity. Quarterly Journal of Economics 115(3): 715–753.

Alderfer CP (1972) Existence, relatedness, and growth: human needs in organizational settings. New York, FreePress.

Alvesson M & Kärreman D (2007) Constructing mystery: empirical matters in theory development. Academy of Management Review 32(4): 1265–1281.

Anderson CL & Agarwal R (2010) Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions. MIS Quarterly 34(3): 613–643.

Armstrong DJ & Hardgrave BC (2007) Understanding mindshift learning: the transition to object-oriented development. MIS Quarterly 31(3): 453–474.

Au N, Ngai EWT & Cheng TCE (2008) Extending the understanding of end user information systems satisfaction formation: an equitable needs fulfillment model approach. MIS Quarterly 32(1): 43–66.

Aytes K & Connolly T (2004) Computer security and risky computing practices: a rational choice perspective. Journal of Organizational & End User Computing 16(3): 22–40.

Bagozzi RP, Yi Y & Phillips LW (1991) Assessing construct validity in organizational research. Administrative Science Quarterly 36(3): 421–458.

Balliet D & Ferris DL (2013) Ostracism and prosocial behavior: a social dilemma perspective. Organizational Behavior and Human Decision Processes 120(2): 298–308.

Bamberger P (2008) From the editors beyond contextualization: using context theories to narrow the micro-macro gap in management research. Academy of Management Journal 51(5): 839–846.

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

Bandura A (1986) Social foundations of thought and action: a social cognitive theory. Englewood Cliffs NJ, Prentice Hall.

Barlow JB, Warkentin M, Ormond D & Dennis AR (2013) Don't make excuses! Discouraging neutralization to reduce IT policy violation. Computers & Security 39(B): 145–159.

Baron RM & Kenny DA (1986) The moderator–mediator variable distinction in social psychological research: conceptual, strategic, and statistical considerations. Journal of Personality and Social Psychology 51(6): 1173–1182.

Bartel CA (2001) Social comparisons in boundary-spanning work: effects of community outreach on members' organizational identity and identification. Administrative Science Quarterly 46(3): 379–413.

Baskerville RL & Myers MD (2002) Information systems as a reference discipline. MIS Quarterly 26(1): 1–14.

Bateman PJ, Gray PH & Butler BS (2011) Research note—the impact of community commitment on participation in online communities. Information Systems Research 22(4): 841–854.

Bearden WO, Money RB & Nevins JL (2006) A measure of long-term orientation: development and validation. Journal of the Academy of Marketing Science 34(3): 456–467.

Becker GS (1968) Crime and punishment: an economic approach. The Journal of Political Economy 76(2): 169–217.

Becker GS (1976) The economic approach to human behavior. Chicago, University of Chicago Press.

Becker TE (2005) Potential problems in the statistical control of variables in organizational research: a qualitative analysis with recommendations. Organizational Research Methods 8(3): 274–289.

Beebe NL & Rao VS (2005) Using situational crime prevention theory to explain the effectiveness of information systems security. Proceedings of the 2005 software conference, Las Vegas: 1–18.

Besharov ML (2014) The relational ecology of identification: how organizational identification emerges when individuals hold divergent values. Academy of Management Journal 57(5): 1485–1512.

Bilge L, Strufe T, Balzarotti D & Kirda E (2009) All your contacts are belong to us: automated identity theft attacks on social networks. Proceedings of the 18th International Conference on World Wide Web, ACM: 551–560.

Bollen KA (1989) Structural equations with latent variables. New York, Wiley.

Bollen KA & Lennox R (1991) Conventional wisdom on measurement: a structural equation perspective. Psychological Bulletin 110(2): 305–314.

Bono JE & McNamara G (2011) Publishing in AMJ—part 2: research design. Academy of Management Journal 54(4): 657–660.

Boss SR, Kirsch LJ, Angermeier I, Shingler RA & Boss RW (2009) If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. European Journal of Information Systems 18(2): 151–164.

Boztepe S (2007) User value: competing theories and models. International Journal of Design 1(2): 55–63.

Bradley NA & Dunlop MD (2005) Toward a multidisciplinary model of context to support context-aware computing. Human-Computer Interaction 20(4): 403–446.

Brigham KH, Lumpkin GT, Payne GT & Zachary MA (2014) Researching long-term orientation a validation study and recommendations for future research. Family Business Review 27(1): 72–88.

Brown PJ, Bovey JD & Chen X (1997) Context-aware applications: from the laboratory to the marketplace. Personal Communications, IEEE 4(5): 58–64.
Buhrau D & Sujan M (2014) Temporal mindsets and self-regulation: the motivation and implementation of self-regulatory behaviors. Journal of Consumer Psychology 25(2): 231–244.
Bulgurcu B, Cavusoglu H & Benbasat I (2010) Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Quarterly 34(3): 523–548.
Caldwell C, Bischoff SJ & Karri R (2002) The four umpires: a paradigm for ethical leadership. Journal of Business Ethics 36(1–2): 153–163.
Caldwell C & Karri R (2005) Organizational governance and ethical systems: a covenantal approach to building trust. Journal of Business Ethics 58(1–3): 249–259.
Cappelli P & Sherer PD (1991) The missing role of context in OB-the need for a meso-level approach. Research in Organizational Behavior 13: 55–110.
CENT.com The guide to password security (and why you should care). URL: www.Cnet. Com/How-to/the-Guide-to-Password-Security-and-Why-You-Should-Care/. Cited 2015/4/23.
Chan M, Woon I & Kankanhalli A (2005) Perceptions of information security at the workplace: linking information security climate to compliant behavior. Journal of Information Privacy and Security 1(3): 18–41.
Cheng L, Li Y, Li W, Holm E & Zhai Q (2013) Understanding the violation of IS security policy in organizations: an integrated model based on social control and deterrence theory. Computers & Security 39(B): 447–459.
Chin WW (1998) Issues and opinion on structural equation modeling. MIS Quarterly 22(1): Vii–Xvi.
Chin WW (2000) Frequently asked questions–partial least squares & PLS-graph. URL: http://disc-nt.cba.uh.edu/chin/plsfaq.htm. Cited 2015/4/23.
Chin WW, Thatcher JB & Wright RT (2012) Assessing common method bias: problems with the ULMC technique. MIS Quarterly 36(3): 1003–1019.
Clarke RV & Cornish DB (1985) Modeling offenders' decisions: a framework for research and policy. In: Tonry M & Morris N (eds) Crime and justice: a review of research, vol. 19. Chicago IL, University of Chicago Press: 147–185.
Coleman JS (1986) Social theory, social research, and a theory of action. American Journal of Sociology 91(5): 1309–1335.
Comber C, Colley A, Hargreaves DJ & Dorn L (1997) The effects of age, gender and computer experience upon computer attitudes. Educational Research 39(2): 123–133.
Cornish DB & Clarke RV (1986) Situational prevention, displacement of crime and rational choice theory. In: Heal K & Laycock G (eds) Situational crime prevention: from theory into practice. London, HMSO: 1–16.
Cornish DB & Clarke RV (2014) The reasoning criminal: rational choice perspectives on offending. New Brunswick NJ, Transaction Publishers.
Cottle TJ (1976) Perceiving time: a psychological investigation with men and women. New York, Wiley.

Covin JG & Slevin DP (1989) Strategic management of small firms in hostile and benign environments. Strategic Management Journal 10(1): 75–87.
Cross R & Cummings JN (2004) Tie and network correlates of individual performance in knowledge-intensive work. Academy of Management Journal 47(6): 928–937.
Crossler RE (2010) Protection motivation theory: understanding determinants to backing up personal data. 43rd Hawaii International Conference on System Sciences (HICSS). Hawaii, USA: 1–10.
Culbert SA (1996) Mind-set management: the heart of leadership. New York, Oxford University Press.
D'Alessio M, Guarino A, De Pascalis V & Zimbardo PG (2003) Testing Zimbardo's Stanford time perspective inventory (STPI)-short form an Italian study. Time & Society 12(2–3): 333–347.
D'Arcy J & Devaraj S (2012) Employee misuse of information technology resources: testing a contemporary deterrence model. Decision Sciences 43(6): 1091–1124.
D'Arcy J, Herath T & Shoss MK (2014) Understanding employee responses to stressful information security requirements: a coping perspective. Journal of Management Information Systems 31(2): 285–318.
D'Arcy J, Hovav A & Galletta D (2009) User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. Information Systems Research 20(1): 79–98.
Das TK (1986) The subjective side of strategy making: future orientations and perceptions of executives. New York NY, Praeger.
Das TK (1987) Strategic planning and individual temporal orientation. Strategic Management Journal 8(2): 203–209.
Das TK (1991) Time: the hidden dimension in strategic planning. Long Range Planning 24(3): 49–57.
Das TK (1993) Time in management and organizational studies. Time & Society 2(2): 267–274.
Das TK & Teng B-S (1997) Time and entrepreneurial risk behavior. Entrepreneurship Theory and Practice 22(2): 69–88.
Davis JH, Schoorman FD & Donaldson L (1997) Toward a stewardship theory of management. Academy of Management Review 22(1): 20–47.
Deci EL & Flaste R (1995) Why we do what we do: the dynamics of personal autonomy. New York NY, GP Putnam's Sons.
Deci EL, Vallerand RJ, Pelletier LG & Ryan RM (1991) Motivation and education: the self-determination perspective. Educational Psychologist 26(3–4): 325–346.
DePree M (2011) Leadership is an art. New York NY, Crown Business.
Desman M (2002) Building an information security awareness program. Boca Raton, London, New York, Washington, D.C., Auerbach Publications.
Dey AK (1998) Context-aware computing: the CyberDesk project. Proceedings of the AAAI 1998 Spring Symposium on Intelligent Environments: 51–54.

De Zafra D, Pitcher S, Tressler J & Ippolito J (1998) Information technology security training requirements: a role-and performance-based model. NIST Special Publication: 800–816.

Dhillon G (1999) Managing and controlling computer misuse. Information Management & Computer Security 7(4): 171–175.

Dhillon G & Moores S (2001) Computer crimes: theorizing about the enemy within, Computers & Security 20(8): 715–723.

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

Drucker PF (1972) Long-range planning means risk-taking. In: Ewing DW (ed) Long range planning for management. New York, Harper & Row: 3–19.

Duhem P (1954) The aim and structure of physical theory. Princeton NJ, Princeton University Press.

Dukerich JM, Golden BR & Shortell SM (2002) Beauty is in the eye of the beholder: the impact of organizational identification, identity, and image on the cooperative behaviors of physicians. Administrative Science Quarterly 47(3): 507–533.

Durndell A & Haag Z (2002) Computer self efficacy, computer anxiety, attitudes towards the Internet and reported experience with the Internet, by gender, in an East European sample. Computers in Human Behavior 18(5): 521–535.

Durndell A, Haag Z & Laithwaite H (2000) Computer self efficacy and gender: a cross cultural study of Scotland and Romania. Personality and Individual Differences 28(6): 1037–1044.

Ernst & Young (2014) Get ahead of cybercrime EY's global information security survey 2014. URL: http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml. Cited 2015/4/23.

Eyal T, Sagristano MD, Trope Y, Liberman N & Chaiken S (2009) When values matter: expressing values in behavioral intentions for the near vs. distant future. Journal of Experimental Social Psychology 45(1): 35–43.

Fishbein M & Ajzen I (1975) Belief, attitude, intention and behavior: an introduction to theory and research. Reading MA, Addison-Wesley.

Fishbein M & Ajzen I (2005) The influence of attitudes on behavior. In: Albarracín D, Johnson BT & Zanna P (eds) The handbook of attitudes. Mahwah NJ, Erlbaum: 173–221.

Flowerday S & von Solms R (2005) Real-time information integrity= system integrity+ data integrity+ continuous assurances. Computers & Security 24(8): 604–613.

Flowerday S & von Solms R (2006) Trust: an element of information security. In: Fischer-Hubner S, Rannenberg K, Yngstrom L & Lindskog S (eds) Security and privacy in dynamic environments. Boston, Kluwer Academic Publishers: 87–98.

Fornell C & Larcker DF (1981) Structural equation models with unobservable variables and measurement error: algebra and statistics. Journal of Marketing Research 18(3): 382–388.

Fraisse P (1963) The psychology of time. New York NY, Harper & Row.

Frank RH (1985) Choosing the right pond: human behavior and the quest for status. Oxford, Oxford University Press.
Frey BS & Palacios-Huerta I (1997) Not just for the money: an economic theory of personal motivation. Cheltenham, Edward Elgar Publishing.
Gaston S & Accountants CIoC (1996) Information security: strategies for successful management. Toronto, Canadian Institute of Chartered Accountants.
Gefen D & Straub DW (2005) A practical guide to factorial validity using PLS-Graph: tutorial and annotated example. Communications of the Association for Information Systems 16(5): 91–109.
Gefen D, Straub DW & Boudreau M (2000) Structural equation modeling and regression: guidelines for research practice. Communications of the Association for Information Systems 4: Article 7.
Gerber M & von Solms R (2005) Management of risk in the information age. Computers & Security 24(1): 16–30.
Gibbs JP (1975) Crime, punishment, and deterrence. New York, Elsevier.
Gómez-Mejía LR, Haynes KT, Núñez-Nickel M, Jacobson KJL & Moyano-Fuentes J (2007) Socioemotional wealth and business risks in family-controlled firms: evidence from Spanish olive oil mills. Administrative Science Quarterly 52(1): 106–137.
Goodhue D & Straub DW (1991) Security concerns of system users: a study of perceptions of the adequacy of security. Information & Management 20(1): 13–27.
Goodpaster KE (2007) Conscience and corporate culture. Malden MA, Blackwell.
Grasmick HG & Bursik Jr RJ (1990) Conscience, significant others, and rational choice: extending the deterrence model. Law and Society Review 24(3): 837–862.
Graso M & Probst TM (2012) The effect of consideration of future consequences on quality and quantity aspects of job performance. Journal of Applied Social Psychology 42(6): 1335–1352.
Griffin MA (2007) Specifying organizational contexts: systematic links between contexts and processes in organizational behavior. Journal of Organizational Behavior 28(7): 859–863.
Guo KH (2013) Security-related behavior in using information systems in the workplace: a review and synthesis. Computers & Security 32: 242–251.
Guo KH & Yuan Y (2012) The effects of multilevel sanctions on information security violations: a mediating model. Information & Management 49(6): 320–326.
Guo KH, Yuan Y, Archer NP & Connelly CE (2011) Understanding nonmalicious security violations in the workplace: a composite behavior model. Journal of Management Information Systems 28(2): 203–236.
Gupta R, Hershey DA & Gaur J (2012) Time perspective and procrastination in the workplace: an empirical investigation. Current Psychology 31(2): 195–211.
Guttman B (1995) An introduction to computer security: the NIST handbook. Washington, U.S. Government Printing Office.
Hair JF, Hult GTM, Ringle CM & Sarstedt M (2013) A primer on partial least squares structural equation modeling (PLS-SEM). Thousand Oaks, Sage.

Hardin R (1997) The economics of religious belief. Journal of Institutional and Theoretical Economics (JITE)/Zeitschrift für die gesamte Staatswissenschaft 153(1): 259–278.
Harrington SJ, Anderson C & Agarwal R (2006) Practicing safe computing: message framing, self-view, and home computer user security behavior intentions. ICIS 2006 Proceedings: 93.
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.
Hartwick J & Barki H (1994) Explaining the role of user participation in information-system use. Management Science 40(4): 440–465.
Hayes AF (2009) Beyond Baron and Kenny: statistical mediation analysis in the new millennium. Communication Monographs 76(4): 408–420.
Hayes AF (2012) PROCESS: A versatile computational tool for observed variable mediation, moderation, and conditional process modeling. URL: http://www.afhayes.com/public/process.pdf. Cited 2015/4/23.
Hechter M & Kanazawa S (1997) Sociological rational choice theory. Annual Review of Sociology 23: 191–214.
Herath T & Rao HR (2009a) Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. Decision Support Systems 47(2): 154–165.
Herath T & Rao HR (2009b) Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems 18(2): 106–125.
Herley C (2009) So long, and no thanks for the externalities: the rational rejection of security advice by users. Proceedings of the 2009 Workshop on New Security Paradigms Workshop, ACM: 133–144.
Hernandez M (2012) Toward an understanding of the psychology of stewardship. Academy of Management Review 37(2): 172–193.
Hershfield HE, Cohen TR & Thompson L (2012) Short horizons and tempting situations: lack of continuity to our future selves leads to unethical decision making and behavior. Organizational Behavior and Human Decision Processes 117(2): 298–310.
Higgins ET (1997) Beyond pleasure and pain. American Psychologist 52(12): 1280–1300.
Hirschi T (1969) Causes of delinquency. Berkeley, CA, University of California.
Hong W, Chan FKY, Thong JYL, Chasalow LC & Dhillon G (2013) A framework and guidelines for context-specific theorizing in information systems research. Information Systems Research 25(1): 111–136.
Hovav A & D'Arcy J (2012) Applying an extended model of deterrence across cultures: an investigation of information systems misuse in the US and South Korea. Information & Management 49(2): 99–110.
Hsieh JJP-A, Rai A & Keil M (2008) Understanding digital inequality: comparing continued use behavioral models of the socio-economically advantaged and disadvantaged. MIS Quarterly 32(1): 97–126.

Hu Q, Dinev T, Hart P & Cooke D (2012) Managing employee compliance with information security policies: the critical role of top management and organizational culture. Decision Sciences 43(4): 615–660.

Hu Q, Xu Z, Dinev T & Ling H (2011) Does deterrence work in reducing information security policy abuse by employees? Communications of the ACM 54(6): 54–60.

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

Ifinedo P (2012) Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. Computers & Security 31(1): 83–95.

Insko CA, Schopler J & Sedikides C (1998) Differential distrust of groups and individuals. In: Sedikides C, Schopler J & Insko CA (eds) Intergroup cognition and intergroup behavior. Hillsdale NJ, Erlbaum: 75–107.

James LR (1980) The unmeasured variables problem in path analysis. Journal of Applied Psychology 65(4): 415–421.

Jansson K & von Solms R (2013) Phishing for phishing awareness. Behaviour & Information Technology 32(6): 584–593.

Johns G (2006) The essential impact of context on organizational behavior. Academy of Management Review 31(2): 386–408.

Johnson RE & Yang L-Q (2010) Commitment and motivation at work: the relevance of employee identity and regulatory focus. Academy of Management Review 35(2): 226–245.

Johnston AC & Warkentin M (2010) Fear appeals and information security behaviors: an empirical study. MIS Quarterly 34(3): 549–566.

Johnston AC, Warkentin M & Siponen M (2015) An enhanced fear appeal rhetorical framework: leveraging threats to the human asset through sanctioning rhetoric. MIS Quarterly 39(1): 113–134.

Joireman JA, Kamdar D, Daniels D & Duell B (2006) Good citizens to the end? It depends: empathy and concern with future consequences moderate the impact of a short-term time horizon on organizational citizenship behaviors. Journal of Applied Psychology 91(6): 1307–1320.

Joireman JA, van Lange PAM & van Vugt M (2004) Who cares about the environmental impact of cars? Those with an eye toward the future. Environment and Behavior 36(2): 187–206.

Kahneman D & Tversky A (1979) Prospect theory: an analysis of decision under risk. Econometrica 47(2): 263–291.

Karahanna E, Straub DW & Chervany NL (1999) Information technology adoption across time: a cross-sectional comparison of pre-adoption and post-adoption beliefs. MIS Quarterly 23(2): 183–213.

Karimi J, Somers TM & Gupta YP (2004) Impact of environmental uncertainty and task characteristics on user satisfaction with data. Information Systems Research 15(2): 175–193.

Karniol R & Ross M (1996) The motivational impact of temporal focus: thinking about the future and the past. Annual Review of Psychology 47(1): 593–620.
Kastenbaum R (1961) The dimensions of future time perspective, an experimental analysis. The Journal of General Psychology 65(2): 203–218.
Keough KA, Zimbardo PG & Boyd JN (1999) Who's smoking, drinking, and using drugs? Time perspective as a predictor of substance use. Basic and Applied Social Psychology 21(2): 149–164.
Khalil EL (1996) Respect, admiration, aggrandizement: Adam Smith as economic psychologist. Journal of Economic Psychology 17(5): 555–577.
Klineberg SL (1968) Future time perspective and the preference for delayed reward. Journal of Personality and Social Psychology 8(3): 253–257.
Komorita SS & Parks CD (1994) Social dilemmas. Madison, WI, Brown & Benchmark.
Korobkin RB & Ulen TS (2000) Law and behavioral science: removing the rationality assumption from law and economics. California Law Review 88(4): 1051–1144.
Köszegi B (2000) Ego utility and information acquisition. Ph.D thesis. Massachusetts Institute of Technology, Dept. of Economics.
Köszegi B (2006) Ego utility, overconfidence, and task choice. Journal of the European Economic Association 4(4): 673–707.
Kwok LF & Longley D (1999) Information security management and modelling. Information Management & Computer Security 7(1): 30–39.
LaRose R, Rifon NJ & Enbody R (2008) Promoting personal responsibility for Internet safety. Communications of the ACM 51(3): 71–76.
Lazarus RS & Folkman S (1984) Stress, appraisal and coping. New York, Springer.
Le Breton-Miller I & Miller D (2006) Why do some family businesses out-compete? Governance, long-term orientations, and sustainable capability. Entrepreneurship Theory and Practice 30(6): 731–746.
Le Breton-Miller I & Miller D (2011) Commentary: family firms and the advantage of multitemporality. Entrepreneurship Theory and Practice 35(6): 1171–1177.
Lee J & Lee Y (2002) A holistic model of computer abuse within organizations. Information Management and Computer Security 10(2): 57–63.
Lee OKD, Lim KH & Wong WM (2005) Why employees do non-work-related computing: an exploratory investigation through multiple theoretical perspectives. IEEE: 185c.
Lee SM, Lee SG & Yoo S (2004) An integrative model of computer abuse based on social control and general deterrence theories. Information & Management 41(6): 707–718.
Lee Y & Larsen KR (2009) Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. European Journal of Information Systems 18(2): 177–187.
Lee Y & Kozar KA (2008) An empirical investigation of anti-spyware software adoption: a multitheoretical perspective. Information & Management 45(2): 109–119.
Leonard LNK & Cronan TP (2005) Attitude toward ethical behavior in computer use: a shifting model. Industrial Management & Data Systems 105(9): 1150–1171.

Leonard LNK, Cronan TP & Kreie J (2004) What influences IT ethical behavior intentions—planned behavior, reasoned action, perceived importance, or individual characteristics? Information & Management 42(1): 143–158.
Li H, Sarathy R, Zhang J & Luo X (2014) Exploring the effects of organizational justice, personal ethics and sanction on Internet use policy compliance. Information Systems Journal 24(6): 479–502.
Li H, Zhang J & Sarathy R (2010) Understanding compliance with Internet use policy from the perspective of rational choice theory. Decision Support Systems 48(4): 635–645.
Liang H, Xue Y & Wu L (2013) Ensuring employees' IT compliance: carrot or stick? Information Systems Research 24(2): 279–294.
Liberman N & Trope Y (2014) Traversing psychological distance. Trends in Cognitive Sciences 18(7): 364–369.
Liberman N, Trope Y & Wakslak C (2007) Construal level theory and consumer behavior. Journal of Consumer Psychology 17(2): 113–117.
Lin N (1986) Conceptualizing social support. In: Lin N, Dean A & Ensel W (eds) Social support, life events, and depression. Orlando FL, Academic Press: 17–30.
Lin N (1999) Social networks and status attainment. Annual Review of Sociology 25: 467–487.
Lin N (2000) Inequality in social capital. Contemporary Sociology 29(6): 785–795.
Lindell MK & Whitney DJ (2001) Accounting for common method variance in cross-sectional research designs. Journal of Applied Psychology 86(1): 114.
Loch KD & Conger S (1996) Evaluating ethical decision making and computer use. Communications of the ACM 39(7): 74–83.
Lumpkin GT & Brigham KH (2011) Long-term orientation and intertemporal choice in family firms. Entrepreneurship Theory and Practice 35(6): 1149–1169.
Lumpkin GT, Brigham KH & Moss TW (2010) Long-term orientation: implications for the entrepreneurial orientation and performance of family businesses. Entrepreneurship and Regional Development 22(3–4): 241–264.
MacKenzie SB, Podsakoff PM & Jarvis CB (2005) The problem of measurement model misspecification in behavioral and organizational research and some recommended solutions. Journal of Applied Psychology 90(4): 710–730.
MacKinnon DP (2008) Introduction to statistical mediation analysis. New York, NY, Erlbaum.
MacKinnon DP, Lockwood CM, Hoffman JM, West SG & Sheets V (2002) A comparison of methods to test mediation and other intervening variable effects. Psychological Methods 7(1): 83–104.
MacKinnon DP, Lockwood CM & Williams J (2004) Confidence limits for the indirect effect: distribution of the product and resampling methods. Multivariate Behavioral Research 39(1): 99–128.
Mael F & Ashforth BE (1992) Alumni and their alma mater: a partial test of the reformulated model of organizational identification. Journal of Organizational Behavior 13(2): 103–123.

Malhotra NK, Kim SS & Patil A (2006) Common method variance in IS research: a comparison of alternative approaches and a reanalysis of past research. Management Science 52(12): 1865–1883.
Mannix EA (1991) Resource dilemmas and discount rates in decision making groups. Journal of Experimental Social Psychology 27(4): 379–391.
Mannix EA & Loewenstein GF (1993) Managerial time horizons and interfirm mobility: an experimental investigation. Organizational Behavior and Human Decision Processes 56(2): 266–284.
Mannix EA, Tinsley CH & Bazerman M (1995) Negotiating over time: impediments to integrative solutions. Organizational Behavior and Human Decision Processes 62(3): 241–251.
Maslow AH, Frager R, Fadiman J, McReynolds C & Cox R (1970) Motivation and personality. New York, Harper & Row.
McCarthy B (2002) New economics of sociological criminology. Annual Review of Sociology 28: 417–442.
McClelland DC (1975) Power: the inner experience. Oxford, England, Irvington.
McGregor D (1966) Leadership and motivation. Oxford, England, M.I.T. Press.
Messick DM & Brewer MB (1983) Solving social dilemmas: a review. Review of Personality and Social Psychology 4(1): 11–44.
Microsoft.com. Tips for Creating a Strong Password. URL: Http://windows.microsoft.com/En-Us/Windows-Vista/Tips-for-Creating-a-Strong-Password. Cited 2015/4/23.
Miller D & Le Breton-Miller I (2005) Managing for the long run: lessons in competitive advantage from great family businesses. Boston, Harvard Business Press.
Miller D & Shamsie J (2001) Learning across the life cycle: experimentation and performance among the Hollywood studio heads. Strategic Management Journal 22(8): 725–745.
Mishra S & Dhillon G (2006) Information systems security governance research: a behavioral perspective. 1st Annual Symposium on Information Assurance, Academic Track of 9th Annual NYS Cyber Security Conference: 27–35.
Mitnick K & Simon W (2003) The art of deception: controlling the human element of security. New York NY, John Wiley & Sons, Inc.
Moss TW, Payne GT & Moore CB (2014) Strategic consistency of exploration and exploitation in family businesses. Family Business Review 27(1): 51–71.
Mowday RT, Porter LW & Steers RM (2013) Employee–organization linkages: the psychology of commitment, absenteeism, and turnover. New York NY, Academic Press.
Mowday RT & Sutton RI (1993) Organizational behavior: linking individuals and groups to organizational contexts. Annual Review of Psychology 44(1): 195–229.
Murray B (1991) Running corporate and national security awareness programmes. In: Proceedings of the IFIP TC11 Seventh International Conference on IS Security, Amsterdam, North-Holland Publishing Co.: 203–207.
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(2): 126–139.

Nagin DS & Paternoster R (1993) Enduring individual differences and rational choice theories of crime. Law and Society Review 27(3): 467–496.
Nagin DS & Pogarsky G (2001) Integrating celerity, impulsivity, and extralegal sanction threats into a model of general deterrence: theory and evidence. Criminology 39(4): 865–892.
Nagin DS & Pogarsky G (2004) Time and punishment: delayed consequences and criminal behavior. Journal of Quantitative Criminology 20(4): 295–317.
Neuman WL (2009) Social research methods: qualitative and quantitative approaches. 7th edition. MA, Pearson.
Ng B-Y & Rahim M (2005) A socio-behavioral study of home computer users' intention to practice security. 9th Pacifica Acian Conference of Information Systems, Proceedings: 20.
Nunnally JC (1978) Psychometric theory. New York, McGraw-Hill.
Nussbaum S, Liberman N & Trope Y (2006) Predicting the near and distant future. Journal of Experimental Psychology: General 135(2): 152–161.
O'Keefe DJ (1990) Persuasion: theory and research. Newbury Park CA, Sage Publications.
Ong C-S & Lai J-Y (2006) Gender differences in perceptions and relationships among dominants of e-learning acceptance. Computers in Human Behavior 22(5): 816–829.
Opp KD & Hartmann P (1989) The rationality of political protest: a comparative analysis of rational choice theory. Boulder, CO, Westview Press.
O'Reilly CA & Chatman J (1986) Organizational commitment and psychological attachment: the effects of compliance, identification, and internalization on prosocial behavior. Journal of Applied Psychology 71(3): 492–499.
Pahnila S, Siponen M & Mahmood A (2007) Employees' behavior towards IS security policy compliance. 40th Hawaii International Conference: 156.
Panko RR & Beh HG (2002) Monitoring for pornography and sexual harassment. Communications of the ACM 45(1): 84–87.
Park SH, Cho SH & Yoon H (2012) The relationship between future orientation, regulatory focus, and need for cognition and healthy menu choices. International Journal of Human Ecology 13(1): 171–181.
Parker DB (1976) Crime by computer. New York, Charles Scribner's Sons.
Paternoster R (2010) How much do we really know about criminal deterrence? The Journal of Criminal Law and Criminology 100(3): 765–824.
Paternoster R & Pogarsky G (2009) Rational choice, agency and thoughtfully reflective decision making: the short and long-term consequences of making good choices. Journal of Quantitative Criminology 25(2): 103–127.
Paternoster R & Simpson S (1993) A rational choice theory of corporate crime. Routine Activity and Rational Choice: Advances in Criminological Theory 5: 37–58.
Paternoster R & Simpson S (1996) Sanction threats and appeals to morality: testing a rational choice model of corporate crime. Law and Society Review 30(3): 549–583.
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.

Pearson AW & Marler LE (2010) A leadership perspective of reciprocal stewardship in family firms. Entrepreneurship Theory and Practice 34(6): 1117–1124.
Pedersen PE & Ling R (2003) Modifying adoption research for mobile Internet service adoption: cross-disciplinary interactions. Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS), IEEE: 10.
Peltier T (2000) How to build a comprehensive security awareness program. Computer Security Journal 16(2): 23–32.
Perry W (1985) Management strategies for computer security. Newton MA, Butterworth-Heinemann.
Petter S, Straub D & Rai A (2007) Specifying formative constructs in information systems research. MIS Quarterly 31(4): 623–656.
Pfeffer J (1991) Organization theory and structural perspectives on management. Journal of Management 17(4): 789–803.
Piquero AR & Hickman M (1999) An empirical test of Tittle's control balance theory. Criminology 37(2): 319–342.
Piquero AR & Tibbetts S (1996) Specifying the direct and indirect effects of low self-control and situational factors in offenders' decision making: toward a more complete model of rational offending. Justice Quarterly 13(3): 481–510.
Piquero NL, Tibbetts SG & Blankenship MB (2005) Examining the role of differential association and techniques of neutralization in explaining corporate crime. Deviant Behavior 26(2): 159–188.
Piliavin I, Gartner R, Thornton C & Matsueda RL (1986) Crime, deterrence, and rational choice. American Sociological Review 51(1): 101–119.
Podsakoff PM, MacKenzie SB, Lee JY & 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.
Polites GL & Karahanna E (2013) The embeddedness of information systems habits in organizational and individual level routines: development and disruption. MIS Quarterly 37(1): 221–246.
Ponemon Institute (2015) 2014: a year of mega breaches. URL: http://www.ponemon.org/local/upload/file/2014%20The%20Year%20of%20the%20Mega%20Breach%20FINAL3.pdf. Cited 2015/4/23.
Posey C, Bennett B, Roberts T & Lowry P (2011) When computer monitoring backfires: invasion of privacy and organizational injustice as precursors to computer abuse. Journal of Information System Security 7(1): 24–47.
Prahalad CK & Bettis RA (1986) The dominant logic: a new linkage between diversity and performance. Strategic Management Journal 7(6): 485–501.
Pratt TC, Cullen FT, Blevins KR, Daigle LE & Madensen TD (2006) The empirical status of deterrence theory: a meta-analysis. In: Cullen FT, Wright JP & Blevins KR (eds) Taking Stock: The Status of Criminological Theory. New Brunswick, NJ, Transaction: 367–395.

Provos N, McNamee D, Mavrommatis P, Wang K & Modadugu N (2007) The ghost in the browser analysis of web-based malware. Proceedings of the First Conference on First Workshop on Hot Topics in Understanding Botnets: 4.

Puhakainen P & Siponen M (2010) Improving employees' compliance through information systems security training: an action research study. MIS Quarterly 34(4): 757–778.

Quackenbush S (2004) The rationality of rational choice theory. International Interactions 30(2): 87–107.

Quine WV (1951) Main trends in recent philosophy: two dogmas of empiricism. The Philosophical Review 60(1): 20–43.

Ransbotham S & Mitra S (2009) Choice and chance: a conceptual model of paths to information security compromise. Information Systems Research 20(1): 121–139.

Rawl J (1971) A theory of justice. Cambridge, MA, US, Belknap Press/Harvard University Press.

Reeve J (2005) Understanding motivation and emotion (4th ed.). New York, John Wiley & Sons, Inc.

Richardson HA, Simmering MJ & Sturman MC (2009) A tale of three perspectives: examining post hoc statistical techniques for detection and correction of common method variance. Organizational Research Methods 12(4): 762–800.

Ringle CM, Sarstedt M & Straub DW (2012) A critical look at the use of PLS-SEM in MIS Quarterly. MIS Quarterly 36(1): iii-xiv.

Ringle CM, Wende S & Becker J-M (2015) SmartPLS 3. Boenningstedt: SmartPLS GmbH. URL: http://www.smartpls.com. Cited 2015/4/23.

Rivis A & Sheeran P (2003) Descriptive norms as an additional predictor in the theory of planned behaviour: a meta-analysis. Current Psychology 22(3): 218–233.

Rogers RW (1975) A protection motivation theory of fear appeals and attitude change. The Journal of Psychology 91(1): 93–114.

Rogers RW, Cacioppo JT & Petty R (1983) Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation. Social Psychophysiology: A Sourcebook: 153–177.

Royal Society (1983) Risk assessment, report of a Royal Society study group. London, The Royal Society.

Royal Society (1992) Risk: analysis, perception and management, report of a Royal Society study group. London, The Royal Society.

Ryan NS, Pascoe J & Morse DR (1998) Enhanced reality fieldwork: the context-aware archaeological assistant. In: Gaffney V, Leusen MV & Exxon S (eds) Computer applications in archaeology. Oxford, Tempus Reparatum.

Saks AM & Belcourt M (2006) An investigation of training activities and transfer of training in organizations. Human Resource Management 45(4): 629–648.

Schepers J, Falk T, de Ruyter K, de Jong A & Hammerschmidt M (2012) Principles and principals: do customer stewardship and agency control compete or complement when shaping frontline employee behavior? Journal of Marketing 76(6): 1–20.

Schilit BN & Theimer MM (1994) Disseminating active map information to mobile hosts. Network, IEEE 8(5): 22–32.

Schuessler J (2009) General deterrence theory: assessing information systems security effectiveness in large versus small businesses, large versus small businesses. Denton TX, UNT Digital Library.

Sheeran P & Orbell S (1999) Implementation intentions and repeated behaviour: augmenting the predictive validity of the theory of planned behaviour. European Journal of Social Psychology 29(2–3): 349–369.

Shipp AJ, Edwards JR & Lambert LS (2009) Conceptualization and measurement of temporal focus: the subjective experience of the past, present, and future. Organizational Behavior and Human Decision Processes 110(1): 1–22.

Shropshire J, Warkentin M & Sharma S (2015) Personality, attitudes, and intentions: predicting initial adoption of information security behavior. Computers & Security 49: 177–191.

Shrout PE & Bolger N (2002) Mediation in experimental and nonexperimental studies: new procedures and recommendations. Psychological Methods 7(4): 422–445.

Simon HA (1957) Models of man; social and rational. Oxford, Wiley.

Siponen M, Mahmood MA & Pahnila S (2014) Employees' adherence to information security policies: an exploratory field study. Information & Management 51(2): 217–224.

Siponen M, Pahnila S & Mahmood A (2006) Factors influencing protection motivation and IS security policy compliance. IEEE: 1–5.

Siponen M, Pahnila S & Mahmood A (2007) Employees' adherence to information security policies: an empirical study. In: Venter H, Eloff M, Labuschagne L, Eloff J & von Solms R (eds) New approaches for security, privacy and trust in complex environments. Boston, Springer: 133–144.

Siponen M, Pahnila S & Mahmood MA (2010) Compliance with information security policies: an empirical investigation. Computer 43(2): 64–71.

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

Siponen M & Vance A (2010) Neutralization: new insights into the problem of employee information systems security policy violations. MIS Quarterly 34(3): 487–502.

Siponen M & Vance A (2014) Guidelines for improving the contextual relevance of field surveys: the case of information security policy violations. European Journal of Information Systems 23(3): 289–305.

Sivo SA, Saunders C, Chang Q & Jiang JJ (2006) How low should you go? Low response rates and the validity of inference in IS questionnaire research. Journal of the Association for Information Systems 7(6): 351–414.

Son JY (2011) Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. Information & Management 48(7): 296–302.

Sophos (2014) Security Threat Report 2014. URL: Http://www.Sophos.Com/En-Us/Medialibrary/Pdfs/Other/Sophos-Security-Threat-Report-2014.Pdf. Cited 2015/4/23.

Splashdata.com. URL: Http://Splashdata.Com/Press/Worstpasswords2013.Htm. Cited 2015/4/23.

Spurling P (1995) Promoting security awareness and commitment. Information Management & Computer Security 3(2): 20–26.
Stafford TF & Urbaczewski A (2004) Spyware: the ghost in the machine. Communications of the Association for Information Systems 14(49): 291–306.
Steidle A, Gockel C & Werth L (2013) Growth or security? Regulatory focus determines work priorities. Management Research Review 36(2): 173–182.
Strathman A, Gleicher F, Boninger DS & Edwards CS (1994) The consideration of future consequences: weighing immediate and distant outcomes of behavior. Journal of Personality and Social Psychology 66(4): 742–752.
Straub DW (1989) Validating instruments in MIS research. MIS Quarterly 13(2): 147–169.
Straub DW (1990) Effective IS security: an empirical study. Information Systems Research 1(3): 255–276.
Straub DW, Boudreau M-C & Gefen D (2004) Validation guidelines for IS positivist research. The Communications of the Association for Information Systems 13(1): 380–427.
Straub DW & Welke RJ (1998) Coping with systems risk: security planning models for management decision making. MIS Quarterly 22(4): 441–469.
Subramani M (2004) How do suppliers benefit from information technology use in supply chain relationships? MIS Quarterly 28(1): 45–73.
Sykes GM & Matza D (1957) Techniques of neutralization: a theory of delinquency. American Sociological Review 22(6): 664–670.
Symantec (2013) Internet Security Threat Report 2013. URL: Http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf. Cited 2015/4/23.
Takemura T & Komatsu A (2012) Who sometimes violates the rule of the organizations? An empirical study on information security behaviors and awareness. WEIS 2012. Germany.
Taylor S & Todd P (1995) Assessing IT usage: the role of prior experience. MIS Quarterly 19(4): 561–570.
Telders E (1991) Security awareness programs: a proactive approach. Computer Security Journal 7(2): 57–64.
Thompson RL, Higgins CA & Howell JM (1991) Personal computing: toward a conceptual model of utilization. MIS Quarterly 15(1): 125–143.
Thompson RL, Higgins CA & Howell JM (1994) Influence of experience on personal computer utilization: testing a conceptual model. Journal of Management Information Systems 11(1): 167–187.
Thomson M & von Solms R (1998) Information security awareness: educating your users effectively. Information Management & Computer Security 6(4): 167–173.
Tollison RD (1997) Rent seeking. In: Mueller DC (ed) Perspectives on public choice. Cambridge, Cambridge University Press: 506–525.
Trope Y & Liberman N (2003) Temporal construal. Psychological Review 110(3): 403–421.
Tudor J (2006) Information security architecture: an integrated approach to security in the organization. Boca Raton, FL, CRC Press.

Tuglular T & Spafford E (1997) A framework for characterization of insider computer misuse. Unpublished paper, Purdue University.
Urbaczewski A & Jessup LM (2002) Does electronic monitoring of employee Internet usage work? Communications of the ACM 45(1): 80–83.
Vance A & Siponen M (2012) IS security policy violations: a rational choice perspective. Journal of Organizational and End User Computing (JOEUC) 24(1): 21–41.
Vance A, Siponen M & Pahnila S (2012) Motivating IS security compliance: insights from habit and protection motivation theory. Information & Management 49(3): 190–198.
Van Dyne L, Graham JW & Dienesch RM (1994) Organizational citizenship behavior: construct redefinition, measurement, and validation. Academy of Management Journal 37(4): 765–802.
Venkatesh V, Morris MG, Davis GB & Davis FD (2003) User acceptance of information technology: toward a unified view. MIS Quarterly 27(3): 425–478.
Venkatesh V, Thong JYL, Chan FKY, Hu PJH & Brown SA (2011) Extending the two-stage information systems continuance model: incorporating UTAUT predictors and the role of context. Information Systems Journal 21(6): 527–555.
Venkatesh V & Zhang X (2010) Unified theory of acceptance and use of technology: US vs. China. Journal of Global Information Technology Management 13(1): 5–27.
Venkatraman N (1989) The concept of fit in strategy research: toward verbal and statistical correspondence. Academy of Management Review 14(3): 423–444.
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.
Voss T & Abraham M (2000) Rational choice theory in sociology: a survey. In: Quah S & Sales A (eds) The international handbook of sociology. London, Sage: 50–83.
Vroom C & von Solms R (2002) A practical approach to information security awareness in the organization. Proceedings of the IFIP TC11 17th International Conference on Information Security: Visions and Perspectives, Kluwer, B.V.: 19–38.
Vroom C & von Solms R (2004) Towards information security behavioural compliance. Computers & Security 23(3): 191–198.
Wang TY & Bansal P (2012) Social responsibility in new ventures: profiting from a long-term orientation. Strategic Management Journal 33(10): 1135–1153.
Weber R (2003) Editor's Comments. MIS Quarterly 27(1): iii–ix.
Welter F (2011) Contextualizing entrepreneurship—conceptual challenges and ways forward. Entrepreneurship Theory and Practice 35(1): 165–184.
Wetzels M, Odekerken-Schröder G & Van Oppen C (2009) Using PLS path modeling for assessing hierarchical construct models: guidelines and empirical illustration. MIS Quarterly 33(1): 177–195.
Whetten DA (2009) An examination of the interface between context and theory applied to the study of Chinese organizations. Management and Organization Review 5(1): 29–55.
White L (2002) Connection matters: exploring the implications of social capital and social networks for social policy. Systems Research and Behavioral Science 19(3): 255–269.
Whitley BE (1997) Gender differences in computer-related attitudes and behavior: a meta-analysis. Computers in Human Behavior 13(1): 1–22.

Williams LJ, Hartman N & Cavazotte F (2010) Method variance and marker variables: a review and comprehensive CFA marker technique. Organizational Research Methods 13(3): 477–514.
Williamson OE (2005) Transaction cost economics. In: Ménard C & Shirley MM (eds) Handbook of new institutional economics. Berlin, Springer.
Willison R (2006) Understanding the perpetration of employee computer crime in the organisational context. Information and Organization 16(4): 304–324.
Willison R & Backhouse J (2006) Opportunities for computer crime: considering systems risk from a criminological perspective. European Journal of Information Systems 15(4): 403–414.
Willison R & Warkentin M (2013) Beyond deterrence: an expanded view of employee computer abuse. MIS Quarterly 37(1): 1–20.
Wittek R, Snijders T & Nee V (2013) The handbook of rational choice social research. Stanford, CA, Stanford University Press.
Wittman DA (1995) The myth of democratic failure: why political institutions are efficient. Chicago, IL, University of Chicago Press.
Woon I, Tan G & Low R (2005) A protection motivation theory approach to home wireless security. ICIS 2005 Proceedings: 367–380.
Workman M, Bommer WH & Straub DW (2008) Security lapses and the omission of information security measures: a threat control model and empirical test. Computers in Human Behavior 24(6): 2799–2816.
Zahra SA (2005) Entrepreneurial risk taking in family firms. Family Business Review 18(1): 23–40.
Zahra SA, Hayton JC & Salvato C (2004) Entrepreneurship in family vs. non-family firms: a resource-based analysis of the effect of organizational culture. Entrepreneurship Theory and Practice 28(4): 363–381.
Zey M (1992) Criticisms of rational choice models. Thousand Oaks, CA, Sage Publications, Inc.
Zhang J, Luo X, Akkaladevi S & Ziegelmayer J (2009) Improving multiple-password recall: an empirical study. European Journal of Information Systems 18(2): 165–176.
Zhang P (2013) The affective response model: a theoretical framework of affective concepts and their relationships in the ICT context. MIS Quarterly 37(1): 247–274.
Ziemke T (1997) Embodiment of context. Proceedings of ECCS. Manchester, UK: 446.
Zimbardo PG & Boyd JN (1999) Putting time in perspective: a valid, reliable individual-differences metric. Journal of Personality and Social Psychology 77(6): 1271–1288.
Zimbardo PG, Keough KA & Boyd JN (1997) Present time perspective as a predictor of risky driving. Personality and Individual Differences 23(6): 1007–1023.
Zohar D (1980) Safety climate in industrial organizations: theoretical and applied implications. Journal of Applied Psychology 65(1): 96–102.

Appendices

Appendix 1 Dimensions of IS security context, Chapter 3

Table 20. Review of contextual factors in IS security behavior literature.

Contextual factor	Description	Source
User context		
Agreeableness	Contrasting a pro-social and communal orientation toward others with antagonism, and including traits such as altruism, tender-mindedness, trust, and modesty.	(Shropshire *et al.* 2015)
Conscientiousness	Socially prescribed impulse control that facilitates task and goal-oriented behavior, such as thinking before acting, delaying gratification, following norms and rules, and planning, organizing, and prioritizing tasks.	
Personal ethics	Reflect one's normative expectations about the appropriateness of a situation or action.	(Li *et al.* 2014)
Social status	Age and gender.	(Hovav & D'Arcy 2012)
Self-efficacy	An employee's judgment of personal skills, knowledge, or competency about fulfilling the requirements of the information security policies.	(Bulgurcu *et al.* 2010)
Low self-control	A combination of impulsivity, risk-seeking, and self-centered characteristics of an individual.	(Hu *et al.* 2011)
Habit	Habit is unconscious or automatic behavior, as opposed to intentions or conscious behavior.	(Pahnila *et al.* 2007)
Task context (Task environment)		
Security risks	The perceived level of Internet security risks in the workplace.	(Li *et al.* 2010)
Security risk of violations	End users' evaluation of the security risk that may be caused by their violations of security policies and rules.	(Guo *et al.* 2011)
Vulnerability	Information and technology resources at work are exposed to security-related risks and threats.	(Bulgurcu *et al.* 2010, Crossler 2010, Ifinedo 2012)
Threat severity	Significance of the threat.	(Crossler 2010, Ifinedo 2012, Johnston & Warkentin 2010)
Threat susceptibility	Probability of encountering the threat.	(Johnston & Warkentin 2010)
Task context (Task characteristics)		
Relative advantage for job performance	The extent to which users expect their actions to help them do their job.	(Guo *et al.* 2011)

Contextual factor	Description	Source
Work impediment	IS security precautions may lead to perceptible and often immediate negative consequences to the employee, such as inconvenience and additional effort.	(Bulgurcu *et al.* 2010)
Cost of compliance	Overall expected unfavorable consequences for complying.	(Bulgurcu *et al.* 2010)
Perceived benefit of compliance	The overall expected favorable consequences to an employee for complying with the requirements of the ISP.	
Rewards	Tangible or intangible compensation that an organization gives to an employee in return for compliance with the requirements of the ISP.	(Bulgurcu *et al.* 2010)
Task context (Resources)		
Facilitating conditions	Time and financial resources to practice computer security.	(Ng & Rahim 2005)
	Time, access to policies, support on compliance.	(Pahnila *et al.* 2007)
Resource availability	Organizational support or availability of assistance to individuals who need it, including computer training and online availability of policies (Saks & Belcourt 2006, Siponen 2000, Thomson & von Solms 1998).	(Herath & Rao 2009b)
SETA program	Training or education programs that are based on security policy to convey security-related knowledge, emphasize security policy violations, and raise employees' security responsibility.	(D'Arcy *et al.* 2009)
Social context (Social structural influence)		
Identity match	How end users perceive dealing with security issues and following security policies as related to their identity as business professionals vis-à-vis IS.	(Guo *et al.* 2011)
Image	The degree to which adoption of the innovation is perceived to enhance an individual's status in the social system.	(Lee & Kozar 2008)
Social context (Direct social influence)		
Social influence	The degree to which the individual perceives his or her colleagues and others whose opinions matter support its acceptance and use (Hartwick & Barki 1994, Venkatesh *et al.* 2003).	(Johnston & Warkentin 2010)
Security policies	Guiding statements of goals to be achieved (Gaston & Accountants 1996).	(D'Arcy *et al.* 2009, Lee *et al.* 2004)
Formal sanctions	Formal sanctions include the certainty, severity, and celerity of sanctions for violation of the policy or rules (Son 2011).	(Bulgurcu *et al.* 2010, D'Arcy *et al.* 2009, etc.)
Workgroup norm	The approval or disapproval by a user's workgroup members (e.g., supervisor and peers).	(Guo *et al.* 2011)

Contextual factor	Description	Source
Mandatoriness	The degree to which individuals perceive that compliance with existing security policies and procedures is compulsory or expected by organizational management.	(Boss *et al.* 2009)
Organizational norms	Pertain to the moral climate of an organization for approval or disapproval of certain security behavior.	(Li *et al.* 2010)
Informal risk/sanction	The certainty and severity of the loss of respect from family, relatives, friends and colleagues.	(Hu *et al.* 2011, Siponen & Vance 2010)
Subjective norm/normative beliefs	The belief as to whether or not a significant person wants the individual to do the behavior in question.	(Anderson & Agarwal 2010, Herath & Rao 2009a, etc.)
Descriptive norm/peer behavior	The extent to which one believes that others are performing the desired behavior (Rivis & Sheeran 2003, Sheeran & Orbell 1999).	(Herath & Rao 2009a, 2009b)
Descriptive norm	The belief in the prevalence of others' use of the technology.	(Anderson & Agarwal 2010)
Peer influence	The influence or pressure from sources known to the home computer user (family and peers) to practice computer security.	(Ng & Rahim 2005)
Top management participation	Top managers' behavior and actions in facilitating organizational actions.	(Hu *et al.* 2012)
Technology context		
Physical security system	Including physical entry controls, security of data centers and computer rooms, isolated delivery and loading areas, cable security, equipment maintenance, security of equipment off premises, and secure disposal of equipment (Kwok & Longley 1999).	(Lee *et al.* 2004)
Technical countermeasures	Actions such as tracking employees' computer activities and performing security audits (e.g., monitoring, surveillance).	(Hovav & D'Arcy 2012)
Computer monitoring	Including tracking employees' Internet use, recording network activities, and performing security audits (Panko & Beh 2002, Urbaczewski & Jessup 2002).	(D'Arcy *et al.* 2009, Posey *et al.* 2011)
Computing capacity	Memory size, hard disk capacity, etc.	(Lee & Kozar 2008)
Trialability	Trying out the software before adoption.	

Appendix 2 Applications of IS security context dimensions, Chapter 3

Table 21. Applications of IS security context dimensions.

Author & year	Research context		Contextual factors studied						
			User	Task context			Social context		Technology
	Behavior type	Location	context	TE	TC	TR	SSI	DSI	context
Anderson and Agarwal (2010)	Information security-related behavior	Home	x					x	
Boss *et al.* (2009)	Information security precaution taken	Organization						x	
Bulgurcu *et al.* (2010)	Information security policies compliance	Organization	x	x	x			x	
Cheng *et al.* (2013)	Information security policies violation	Organization	x					x	
Crossler (2010)	Backing up data	Not specified		x	x				
D'Arcy *et al.* (2009)	Information systems misuse	Organization				x		x	x
Guo *et al.* (2011)	Nonmalicious security violations	Organization		x	x		x	x	
Herath and Rao (2009a)	Information security policies compliance	Organization						x	
Herath and Rao (2009b)	Information security policies compliance	Organization	x		x	x		x	
Hovav and D'Arcy (2012)	Information systems misuse	Organization	x				x	x	x
Hu *et al.* (2012)	Information security policies compliance	Organization				x		x	
Hu *et al.* (2011)	Information security policies abuse	Organization	x					x	
Ifinedo (2012)	Information security policies compliance	Organization	x	x	x			x	
Johnston and Warkentin (2010)	Anti-spyware software	Organization	x	x				x	
LaRose *et al.* (2008)	Internet safety behavior	Not specified	x		x			x	
Lee and Kozar (2008)	Anti-spyware software adoption	Not specified	x		x		x	x	x
Lee *et al.* (2004)	Computer abuse	Organization	x					x	x

Author & year	Research context		Contextual factors studied						
			User	Task context			Social context		Technology
	Behavior type	Location	context	TE	TC	TR	SSI	DSI	context
Li *et al.* (2010)	Compliance with Internet use policies	Organization	x	x	x			x	x
Ng and Rahim (2005)	Computer security practice	Home	x		x	x		x	
Pahnila *et al.* (2007)	Information security policies compliance	Organization	x	x		x		x	
Posey *et al.* (2011)	Computer abuse	Organization	x						x
Siponen and Vance (2010)	Information security policies violation	Organization						x	
Straub (1990)	Computer abuse	Organization		x	x	x		x	x
Vance and Siponen (2012)	Information security policies violation	Organization						x	

Note: TE = task environment, TC = task characteristics, TR = task resources, SSI = social structural influence, DSI = direct social influence.

Appendix 3 Measurement instrument, Chapter 3

Use of strong password (Formative)

1. My present work/personal password is a word from a dictionary or somebody's name. (Reverse)
2. My present work/personal password is at least 8 characters long.
3. My present work/personal password uses upper and lowercase letters.
4. My present work/personal password uses at least one number.
5. My present work/personal password uses at least one symbol (e.g., #, &, *, etc.).

Facilitating conditions (FC) (Thompson et al. *1991)*

1. When I need help using strong work/personal passwords, guidance is available to me.
2. When I need help using strong work/personal passwords, instructions are available to me.
3. When I need help using strong work/personal passwords, a specific person (or group) is available for assistance.

Embarrassment (EM) (Grasmick & Bursik 1990)

1. I would feel embarrassed if I didn't use a strong work/personal complex password.
2. It would be a big problem for me if the people around me knew that I did not use a strong work/personal password.

Monitoring (MN) (D'Arcy et al. *2009)*

1. The computer checks the password strength when I set my work/personal password.
2. The computer doesn't accept a simple work/personal password.
3. The computer gives me suggestions to alter my work/personal password if I entered a simple one.

Task benefit (BE) (Bulgurcu et al. *2010)*

1. Using strong work/personal passwords would be favorable to me.
2. Using strong work/personal passwords would result in benefits to me.
3. Using strong work/personal passwords would create advantages for me.

Task cost (TC) (Bulgurcu et al. *2010)*

1. Using strong work/personal passwords would be time-consuming for me.
2. Using strong work/personal passwords would be burdensome for me.
3. Using strong work/personal passwords would be costly for me.
4. Using strong work/personal passwords would be inconvenient for me.

Control variables

1. Gender
    - Male
    - Female
2. Age
    - 18–29
    - 30–39
    - 40–49
    - 50–59
    - 60 and above
3. Academic degree
    - Bachelor
    - Master
    - Licentiate
    - Doctor
4. Years of computer experience
    - 4–6
    - 7–10
    - 11–14
    - 15 and above

Appendix 4 Summary of ISRB-related studies, Chapter 4

Table 22. Summary of ISRB-related studies.

Author & year	Description of behavior	Theoretical perspectives	Key findings
Barlow *et al.* (2013)	Study IT policy violation using ISRB scenarios, such as password sharing.	Neutralization theory (Sykes & Matza 1957), deterrence theory	1) IT policy violation intention is influenced by defense of necessity, but not influenced by denial of injury and metaphor of the ledger. 2) Communication of deterrent sanctions and communication to mitigate neutralization can lead to lower intentions to violate. 3) The deterrence focus and neutralization mitigation focus communications have equal effects on decreasing intention to violate. 4) The framing of scenarios, whether negative or positive framing, has no influence on changing violation intentions.

Author & year	Description of behavior	Theoretical perspectives	Key findings
Cheng *et al.* (2013)	Study IS security policy violations using ISRB scenarios: 1) Copying organization's sensitive data, 2) Workstation logout, 3) Sharing passwords, and 4) Reading confidential files.	Social bond theory (Hirschi 1969), deterrence theory	1) Employees' intention to violate IS security policy is influenced by both formal and informal control. 2) As a formal control, perceived severity of sanction deters the intention; however, perceived certainty of sanctions has no effect on intention. 3) Informal controls, such as attachment to job and organization, commitment, belief, subjective norms, and coworker behavior, are found to negatively influence the violation intention. However, attachment to immediate boss and coworkers, and involvement are found to have no effect on violation intention.
D'Arcy and Devaraj (2012)	Study employee misuse of information technology resources using three ISRB scenarios: 1) Unauthorized access to computerized data, 2) Use of unlicensed software (ISRB), 3) Sending an inappropriate email message (ISRB), and 4) Unauthorized modification of computerized data.	Deterrence theory (Paternoster 2010)	1) Misuse intention is negatively influenced by formal sanctions, social desirability pressure, and moral beliefs. 2) Social desirability pressure and moral beliefs have stronger negative relationships with misuse intention than formal sanctions. 3) Formal sanctions positively influence moral beliefs. 4) The influences of formal sanctions and social desirability pressure are partially mediated by moral beliefs. 5) The employment context and virtual status negatively influences misuse intention, but employment level has no effect on misuse intention.

Author & year	Description of behavior	Theoretical perspectives	Key findings
D'Arcy *et al.* (2009)	Study IS misuse behaviors using scenarios, among which, two scenarios are ISRB: 1) Sending an inappropriate email message (ISRB), 2) Unauthorized access to computerized data, 3) Use of unlicensed software (ISRB), and 4) Unauthorized modification of computerized data.	Deterrence theory (Gibbs 1975)	1) Perceived certainty of sanctions explain IS misuse intention, whereas perceived severity of sanctions have no such effect. 2) User awareness of security policies, SETA program, and computer monitoring can influence both the perceived certainty and severity of sanctions.
D'Arcy *et al.* (2014)	Study IS security policy violation intention using four ISRB scenarios: 1) Password-sharing (ISRB), 2) Password write-down (ISRB), 3) Failure to logoff (ISRB), 4) Copy data to unencrypted USB (ISRB), and 5) Data leakage	Coping theory (Lazarus & Folkman 1984), moral engagement theory (Bandura 1986)	Security requirements perceived as an overload, complex, and uncertain can induce employee rationalizations of ISP violations, which in turn increase susceptibility to the ISP violation.
Guo and Yuan (2012)	Study information security violations using ISRB scenarios: 1) Writing down the password, 2) Unauthorized portable devices for storing and carrying organizational data, 3) Installation and use of unauthorized software, and 4) Using insecure public wireless network for business purposes.	Deterrence theory	1) Personal self-sanctions and workgroup sanctions have significant deterrent effects on employee security violations. 2) Organizational sanctions become insignificant when personal self-sanctions and workgroup sanctions are taken into account.

Author & year	Description of behavior	Theoretical perspectives	Key findings
Guo *et al.* (2011)	Study nonmalicious security violations using ISRB scenarios: 1) Writing down the password, 2) Unauthorized portable devices for storing and carrying organizational data, 3) Installation and use of unauthorized software, and 4) Using insecure public wireless network for business purposes.	Theory of reasoned action (Ajzen & Fishbein 1980), theory of planned behavior (Ajzen 1991), deterrence theory (Gibbs 1975)	1) Nonmalicious security violations (NMSV) intention is influenced by attitude toward NMSV, workgroup norm, and perceived identity match. 2) Attitude toward NMSV is influenced by relative advantage for job performance, perceived security risk, workgroup norm, and perceived identity match. 3) Attitude toward security policy and perceived sanctions are found not relevant to attitude toward NMSV.
Hovav and D'Arcy (2012)	Study IS misuse behaviors using scenarios, among which two scenarios are ISRB: 1) Sending an inappropriate email message (ISRB), 2) Use of unlicensed software (ISRB), 3) Unauthorized access to computerized data, and 4) Unauthorized modification of computerized data.	Deterrence theory	1) National differences in the effect of deterrents on IS misuse intention are found between US and Korean samples. Only perceived certainty of sanctions influences the intention of Korean sample, while only perceived severity of sanctions influences the intention of US sample. 2) Moral beliefs, as informal sanctions, influence the intention of both samples. 3) Two types of security countermeasures, procedural countermeasures and technical countermeasures, influence the sanction factors.

Author & year	Description of behavior	Theoretical perspectives	Key findings
Johnston *et al.* (2015)	Study IS security policy compliance using ISRB scenarios: 1) Using strong password, 2) Using unencrypted USB, and 3) Locking computer when leaving workstation.	Protection motivation theory (Rogers 1975), deterrence theory (Paternoster & Simpson 1993), fear appeals (O'Keefe 1990)	1) Sanctioning rhetoric is able to enhance the effectiveness of a fear appeal, thus leading to stronger intentions to comply with information security policy. 2) Conventional fear appeal rhetorical elements revealed consistent with previous earlier work. 3) Sanction celerity and the formal dimensions of sanction severity and sanction certainty were determined to be non-significant in their predictive influence on compliance intention, while informal sanction severity and informal sanction certainty were found to be significant in their roles as direct determinants of compliance intention.
Siponen and Vance (2010)	Study IS security policy violations using ISRB scenarios: 1) Copying corporate data to personal USB drive, 2) Not locking computer when leaving the workstation, and 3) Sharing work password with coworkers.	Neutralization theory (Sykes & Matza 1957), deterrence theory (Paternoster & Simpson 1996)	1) Employees intend to violate the IS security policies when they use neutralization techniques, including defense of necessity, appeal to higher loyalties, condemn the condemners, metaphor of the ledger, denial of injury, and denial of responsibility. 2) Deterrents are found have no influence on the violation intention, including formal sanctions, informal sanctions, and shame.

Author & year	Description of behavior	Theoretical perspectives	Key findings
Vance and Siponen (2012)	Study IS security policy violations using ISRB scenarios: 1) Copying corporate data to personal USB drive, 2) Not locking computer when leaving the workstation, and 3) Sharing work password with coworkers.	Rational choice theory, deterrence theory (Paternoster & Simpson 1993, 1996)	1) Moral beliefs are an excellent predictor of intention to violate IS security policies. 2) Perceived benefits positively affect intention, but negatively associate with moral beliefs. 3) The impact of formal sanctions on violation intention is not significant.
Vance *et al.* (2012)	Study IS security policy compliance using ISRB scenarios: 1) Reading confidential documents, 2) Failing to report computer virus, 3) Allowing children to play with laptop, 4) Using unencrypted portable media, 5) Locking personal computer, and 6) Sharing passwords.	Protection motivation theory (Rogers 1975), habit theory (Verplanken & Orbell 2003)	1) Past and automatic IS security policy compliance influence the threat appraisals and coping responses, which in turn influence the current intention to comply with IS security policy. 2) Habit has a positive impact on vulnerability, perceived severity, rewards, response efficacy, self-efficacy, and response cost. 3) Perceived security and self-efficacy have positive impacts on compliance intention. Rewards and response efficacy and response cost have negative impacts on compliance intention. The impact of vulnerability on compliance intention is not significant.

Author & year	Description of behavior	Theoretical perspectives	Key findings
Workman *et al.* (2008)	Study omissive security behavior, including failure to change passwords, failure to backup, and failure to update security patches.	Social cognitive theory (Bandura 1977), protection motivation theory (Rogers 1975, Rogers *et al.* 1983)	1) Subjective and objective omissive behaviors are negatively influenced by perceived severity, perceived vulnerability, self-efficacy, perceived response efficacy, and response cost–benefit. 2) Locus of control negatively influences subjective omissive behavior, but does not influence objective omissive behavior.

Appendix 5 Instruments, Chapter 4

Survey introduction

To better understand your habits when working with data and IT systems, we kindly ask for your cooperation in completing this survey. Your feedback is greatly appreciated and will help us to improve [the company's] IT environment.

Please take a moment to complete the survey.

You will be presented with one scenario and some questions related to your behavior in such a situation. The survey concludes with a request for some demographic information. These items should be completed only if you are willing to provide the information; however, having demographic information will allow us to better assess your answers.

Please complete the survey in one step, as it is not possible to continue at a later point in time due to the anonymity reasons.

This survey is in cooperation with [the research team]. They have designed the questionnaire, will analyze the answers for scientific research, and will provide us with the results specifically adapted to our situation. The results will be taken to further improve [company's] IT environment.

Scenarios

In the scenarios, we describe a situation that Newman, an employee of your company, is facing. Please read the scenario carefully first, and then indicate the extent to which you agree with the following statements.

Scenario 1: Unauthorized portable devices for storing corporate data

Newman wants to copy a file and show it to clients at their meeting. A personal unencrypted USB stick is available nearby. The file contains the contract draft. However, the meeting is starting soon, and it takes time to find an encrypted USB stick. Newman decides to copy the file into the personal unencrypted USB stick.

Scenario 2: Sending unencrypted emails

Newman needs to send an encrypted email to a client. The client says that she has difficulties decrypting the email and asks Newman to send her an unencrypted one.

The file contains the contract draft. However, the client says that, if she cannot open the email, she may consider switching to another company. So, Newman decides to send an unencrypted email to her.

Scenario 3: Downloading suspicious files from the Internet

Newman needs to search for some information from the Internet in order to complete some work. A file on a website is thought to contain the required information, but Newman is unsure that the site is trustworthy. The browser also displays a security warning stating that "this file type can potentially harm your computer." However, it takes time to find the information by other means, and the file helps to complete the work more quickly. Newman decides to download it.

Items

Following each scenario, respondents were presented with the following questions. The item wordings were slightly modified to fit each scenario, and all items were measured on seven-point Likert scales.

IS security risk-taking intention (ISRI) (D'Arcy et al. *2009)*

In each question, the expression of "the behavior" refers to Newman's action as described in the scenario above.

1. If you were Newman, what is the likelihood that you would have copied the file into a personal unencrypted USB stick?
2. I could see myself copying the file into a personal unencrypted USB stick if I were in Newman's situation.

Continuity (LTO_C) (Brigham et al. *2014)*

1. It is valuable that I always avoid the behavior without exception.
2. Avoiding the behavior all the time at work is of great worth.

Futurity (LTO_F) (Brigham et al. *2014)*

1. In the long run, it is helpful for my organization to evaluate the consequences of such type of behavior.

2. In the long run, it is valuable for my organization to notice the possible negative consequences caused by such type of behavior.

Perseverance (LTO_P) (Brigham et al. *2014)*

1. I do not mind giving up the current convenience if it could ensure my organization's information security.
2. I do not mind extra work if it could ensure my organization's information security.

Value identification (VI) (Davis et al. *1997)*

1. I think it is accepted that my organization discourages the behavior.
2. I fully understand the necessity of avoiding the behavior in my organization.

Trusted relationship fulfillment (TRF) (Deci et al. *1991)*

1. If my coworkers knew that I avoided the behavior, they might recognize me as a trustworthy coworker.
2. If my colleagues knew that I avoided the behavior, they might recognize me as a responsible coworker.

Growth needs fulfillment (GNF) (Alderfer 1972)

1. It is an opportunity for me to master more information protection skills, if I find alternative secure ways to do the work.
2. It is an opportunity for me to learn more information security knowledge, if I find alternative secure ways to do the work.
3. It is an opportunity for me to show my talents in solving information security problems, if I find alternative secure ways to do the work.

Demographic information

1. Please select your country of origin
   Canada
   Hong Kong
   South Africa

United Kingdom
United States

2. Gender
   Male
   Female
3. Age
   18–25
   26–35
   36–45
   46–55
   56–65
   66 and above
4. Type of work contract
   Fixed term
   Permanent term
5. My knowledge of computers and IT is …
   1 Very low
   2
   3
   4
   5
   6
   7 Very high
6. Years of computer usage _____
7. Years of working time for the company _____

639. Holma-Suutari, Anniina (2014) Harmful agents (PCDD/Fs, PCBs, and PBDEs) in Finnish reindeer (*Rangifer tarandus tarandus*) and moose (*Alces alces*)

640. Lankila, Tiina (2014) Residential area and health : a study of the Northern Finland Birth Cohort 1966

641. Zhou, Yongfeng (2014) Demographic history and climatic adaptation in ecological divergence between two closely related parapatric pine species

642. Kraus, Klemens (2014) Security management process in distributed, large scale high performance systems

643. Toivainen, Tuomas (2014) Genetic consequences of directional selection in *Arabidopsis lyrata*

644. Sutela, Suvi (2014) Genetically modified silver birch and hybrid aspen : target and non-target effects of introduced traits

645. Väisänen, Maria (2014) Ecosystem-level consequences of climate warming in tundra under differing grazing pressures by reindeer

646. Suurkuukka, Heli (2014) Spatial and temporal variability of freshwater biodiversity in natural and modified forested landscapes

647. Cherevatova, Maria (2014) Electrical conductivity structure of the lithosphere in western Fennoscandia from three-dimensional magnetotelluric data

648. Etula, Henna (2015) Paikkatietoon perustuva reitinoptimointi metsäninventoinnin työkaluna Suomessa : menetelmän kehittäminen ja sen hyödyllisyyden arviointi

649. Romar, Henrik (2015) Biomass gasification and catalytic conversion of synthesis gas : characterisation of cobalt catalysts for Fischer-Tropsch synthesis

650. Shao, Xiuyan (2015) Understanding information systems (IS) security investments in organizations

651. Heponiemi, Anne (2015) Catalytic wet air oxidation of industrial wastewaters : oxidation of bisphenol A over cerium supported metal catalysts

652. Tolkkinen, Mikko (2015) Biodiversity and ecosystem functioning in boreal streams : the effects of anthropogenic disturbances and naturally stressful environments

653. Zoratti, Laura (2015) Effect of environmental, developmental and genetic factors on flavonoid and carotenoid profile of Vaccinium berries

654. Hekkala, Anne-Maarit (2015) Restoration of the naturalness of boreal forests

Book orders:
Granum: Virtual book store
http://granum.uta.fi/granum/

UNIVERSITY OF OULU P.O. Box 8000 FI-90014 UNIVERSITY OF OULU FINLAND

ACTA UNIVERSITATIS OULUENSIS

UNIVERSITY of OULU
OULUN YLIOPISTO

ISBN 978-952-62-0938-8 (Paperback)
ISBN 978-952-62-0939-5 (PDF)
ISSN 0355-3191 (Print)
ISSN 1796-220X (Online)