

Xiuyan Shao

UNDERSTANDING
INFORMATION SYSTEMS (IS)
SECURITY INVESTMENTS IN
ORGANIZATIONS

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

A

SCIENTIAE RERUM
NATURALIUM



ACTA UNIVERSITATIS OULUENSIS
A Scientiae Rerum Naturalium 650

XIUYAN SHAO

**UNDERSTANDING INFORMATION
SYSTEMS (IS) SECURITY
INVESTMENTS IN ORGANIZATIONS**

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 11
September 2015, at 12 noon

UNIVERSITY OF OULU, OULU 2015

Copyright © 2015
Acta Univ. Oul. A 650, 2015

Supervised by
Professor Mikko Siponen
Docent Seppo Pahnla

Reviewed by
Professor Chris F. Kemerer
Professor Timo Saarinen

ISBN 978-952-62-0892-3 (Paperback)
ISBN 978-952-62-0893-0 (PDF)

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

Cover Design
Raimo Ahonen

JUVENES PRINT
TAMPERE 2015

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

University of Oulu Graduate School; University of Oulu, Faculty of Information Technology and Electrical Engineering, Department of Information Processing Science

Acta Univ. Oul. A 650, 2015

University of Oulu, P.O. Box 8000, FI-90014 University of Oulu, Finland

Abstract

Increasing information systems (IS) security breaches require investments in terms of IS security techniques/practices or personnel. Prior research on IS security investment has provided economic models based on neoclassical economics to assess how much to invest in IS security. These models assume that the goal of IS security investment is only benefit maximization, and that all of the actors involved are unbiased rational actors with complete information. It is argued in this thesis that these prior models for IS security investment are flawed for two reasons. First, benefit maximization is not an appropriate goal for IS security investment, because the benefits and costs of IS security investment cannot be reliably calculated. Second, decision makers are not unbiased rational actors, because they do not have enough information to make IS security investment decisions. To address these concerns, this thesis outlines a framework for IS security investment, which is based on behavioral economics. This framework makes new assumptions about IS security investment decision makers, and redefines the contextual nature of IS security investment.

As an example of how to operationalize this framework in IS research, this thesis examines IS security investment decision-making by using a theoretical model drawn from reputational herding theory. A field study for empirical testing of the model was conducted, which involved surveying 88 information security experts in Finland. The results of the field study not only confirm the new framework, but also identify several motives that strongly predict IS security investment.

In this thesis the assumptions proposed for the framework have also been also tested in a different research setting: the unauthorized uploading behavior of digital goods. This study involves 220 respondents, and the findings suggest that the proposed assumptions for the framework are also applicable in that new research setting.

Overall, this doctoral thesis contributes to IS research by providing a framework to increase the overall understanding of how IS security managers make decisions with regard to IS security investment; moreover, this thesis presents empirically-grounded implications for how practitioners can improve the quality of their IS security investments.

Keywords: characteristics of IS security investment, empirical test, IS security, IS security investment, new assumption of decision maker

Shao, Xiuyan, Tietoturvainvestointien ymmärtäminen organisaatioissa.

Oulun yliopiston tutkijakoulu; Oulun yliopisto, Tieto- ja sähkötekniikan tiedekunta, Tietojenkäsittelytieteiden laitos

Acta Univ. Oul. A 650, 2015

Oulun yliopisto, PL 8000, 90014 Oulun yliopisto

Tiivistelmä

Jatkuvasti lisääntyvät tietoturvaloukkaukset edellyttävät investointeja tietoturvateknikoihin/käytänteisiin tai henkilöstöön. Aikaisempi tietoturvainvestointitutkimus on kehittänyt neoklassiseen taloustieteeseen perustuvia taloudellisia malleja tietoturvainvestointien määrän arvioimiseksi. Nämä mallit olettavat, että tietoturvainvestointien tavoitteena on ainoastaan hyötyjen maksimointi ja että kaikki toimijat ovat täydellisen tiedon pohjalta toimivia, puolueettomia ja rationaalisia. Tässä väitöskirjassa esitetään, että aikaisemmat tietoturvainvestointimallit ovat puutteellisia kahdesta syystä. Yhtäältä hyödyn maksimointi ei sovellu hyvin tietoturvainvestointien tavoitteeksi, koska sen hyötyjä ja kustannuksia ei voida luotettavasti laskea. Toisaalta päätöksentekijät eivät ole puolueettomia rationaalisia toimijoita, koska heillä ei ole käytettävissään tarpeeksi tietoa tietoturvainvestointipäätösten tekemiseksi. Nämä asiat huomioidaan tässä väitöskirjassa kehittämällä käyttäytymistaloustieteeseen perustuva tietoturvainvestointien viitekehys. Viitekehys esittää uusia oletuksia tietoturvainvestointeja tekevistä päätöksentekijöistä ja tietoturvainvestointien kontekstuaalisesta luonteesta.

Väitöskirjassa havainnollistetaan kehitetyn viitekehysten soveltamisesta tietojärjestelmätieteen tutkimuksessa tarkastelemalla tietoturvainvestointeihin liittyvää päätöksentekoa maineeseen perustuvan laumateorian (reputational herding theory) pohjalta laaditun teoreettisen mallin näkökulmasta. Kenttätutkimuksessa mallin testaamiseksi empiirisesti laadittiin kysely, johon vastasi 88 tietoturva-asiantuntijaa Suomessa. Kenttätutkimuksen tulokset sekä vastasivat uutta viitekehystä että toivat esiin useita tietoturvainvestointeja vahvasti ennustavia motiiveja.

Väitöskirjassa kehitetyn viitekehysten oletuksia testattiin myös toisentyypisessä tutkimusasetelmassa: digitaalisten hyödykkeiden luvaton lataaminen. Tähän tutkimukseen osallistui 220 vastaajaa, ja löydökset osoittavat esitettyjen oletusten olevan hyödynnettävissä myös tässä uudessa tutkimusasetelmassa.

Kaiken kaikkiaan tämän väitöskirjan kontribuutio tietojärjestelmätieteelle on sen tarjoama viitekehys, joka lisää ymmärrystä siitä, kuinka tietoturvapäälliköt tekevät tietoturvainvestointeihin liittyviä päätöksiä. Väitöskirja esittää myös empiiriseen tutkimukseen pohjautuvia käytännön implikaatioita tietoturvainvestointien laadun parantamiseksi.

Asiasanat: empiirinen testaus, Tietoturva, tietoturvainvestoinnin piirteet, tietoturvainvestointi, uudet oletukset päätöksentekijästä

Acknowledgment

This thesis represents my work at Department of Information Processing Science, University of Oulu, during the years 2012-2015. This thesis is the result of many experiences I have encountered at University of Oulu from dozens of remarkable individuals who I wish to acknowledge.

First and foremost I would like to express thank to my primary supervisor Professor Mikko Siponen, who provided me with continuous guidance and support. His professional guidance, insightful advice, and continued patience contributed greatly to the current thesis. I am very lucky to have such a great researcher as my supervisor. I also want to thank my second supervisor, Docent Seppo Pahlila, who has provided me with generous help and guidance during my PhD study period. He gave me lots of encouragement when I encountered great frustration and became despaired.

My follow-up group guided me through all these years. Thank you to Professor Tero Vartiainen, Dr. Mari Karjalainen, and Dr. Juha Kortelainen. I appreciate the time and effort you put into providing constructive feedback in order to improve my doctoral thesis.

Appreciations also will be given to the pre-examinors, Professor Chris Kemerer (University of Pittsburg, USA) and Professor Timo Saarinen (Aalto University, Finland), who provided me with valuable and extensive comments on improving the thesis. I want to thank a company called Scribendi for proofreading the thesis.

This doctoral thesis has been financially supported by our company partners in the SECMEC research project and Department of Information Processing Science. The importance of these funding is gratefully acknowledged.

A good supporting system is important to surviving and staying in research work. Dozens of people have helped me immensely at the department. Professor Raija Halonen provided suggestions on improving and re-organizing the thesis. Professor Kari Kuutti and Professor Markku Oivo helped me in challenging times. Marja-Liisa Liedes helped me with administrative tasks. I also want to thank my colleagues who contributed warm social environment at the department: Asheesh Nigam, Ying Li, Hemin Jiang, Nan (Andy) Zhang, Minna Alasuutari, Dorina Rajanen. It was happy to work with you over the past years. People here are genuinely nice and want to help me out and I'm glad to have interacted with many. If I have forgotten anyone, I apologize.

I especially thank my mom and dad. My parents provided unconditional love and care to me. I love them so much, and I would not have made it this far without them. I also thank my friends for providing support and friendship that I needed.

In particular, I want to thank my husband Xiaohua. He was always there to share my joy when I was happy and to provide shoulder when I encountered difficulties. His encouragement, suggestion and love supported me to go this far. Thank you Xiaohua.

Oulu, July 2015

Xiuyan Shao

Abbreviations

GDT	General deterrence theory
IS	Information systems
IT	Information technology
PLS	Partial least squares
SEM	Structural equation modeling
TPB	Theory of planned behavior
TRA	Theory of reasoned action
VIF	Variance inflation factor

Contents

Acknowledgment	7
Abbreviations	9
Contents	9
1 Introduction	15
1.1 Problem statement.....	15
1.2 Research question and objectives.....	17
1.3 Significance of the research	18
1.4 Structure of the thesis.....	19
2 Previous work	23
2.1 Determining the source material for the literature review	23
2.2 An overview of the literature	24
2.2.1 Decision-theoretic approach.....	24
2.2.2 Game-theoretic approach.....	28
2.3 Analysis of previous work	31
2.3.1 Aim of the analysis.....	31
2.3.2 The neoclassical economics framework of decision- making.....	32
2.3.3 Analysis of existing economic analysis of IS security investment	35
3 Characteristics of IS security investment	37
3.1 IS security investment areas.....	37
3.2 Goal of IS security investment.....	39
3.3 Intangible benefits of IS security investment.....	40
4 Research gaps	43
4.1 Neglect of IS security investment characteristics.....	43
4.2 Conflicts between neoclassical framework and IS security investment characteristics	43
4.3 Problems of preference and complete information assumptions per se	44
4.3.1 Rational preference.....	44
4.3.2 Complete information.....	45
5 A preliminary framework for IS security investment	47
5.1 How does behavioral economics view decision-makers?	47
5.2 Assumptions about IS security investment decision-makers	49
5.3 A preliminary framework for IS security investment.....	50

6	Research methodology	53
6.1	Survey-based research design and data collection procedure	53
6.2	Construct operationalization	54
6.3	Pretest.....	54
7	Motivating IS security investment – A field study	57
7.1	Related work	59
7.1.1	IS security investment studies	59
7.1.2	Herding behavior in IS research	61
7.2	Theoretical framework.....	62
7.2.1	Conceptualization: reputation-based herding	62
7.2.2	A comparison to similar concepts and theories	64
7.2.3	Research model and hypotheses	66
7.3	Methodology	71
7.3.1	Operationalization of constructs	71
7.3.2	Pretest	72
7.3.3	Survey administration.....	72
7.4	Data analysis	73
7.4.1	Measurement model	74
7.4.2	Structural model	82
7.5	Summary of hypotheses and results	83
8	Testing the new assumptions in a new context	85
8.1	A new context: digital piracy in online communities.....	85
8.1.1	Related work.....	85
8.1.2	Research gap.....	86
8.2	Research model and hypothesis	87
8.2.1	Research model	87
8.2.2	Hypotheses	88
8.3	Methodology	91
8.3.1	Research design.....	91
8.3.2	Construct operationalization.....	92
8.3.3	Data collection procedure.....	92
8.4	Data analysis	93
8.4.1	Measurement model	94
8.4.2	Structural model	103
8.5	Summary of empirical findings.....	105
9	The empirically grounded framework of IS security investment	107
9.1	The formation process of the empirically grounded framework.....	107

9.2 The empirically grounded framework of IS security investment.....	108
10 Discussion and conclusions	111
10.1 Contribution of the thesis.....	111
10.1.1 Contributions of the new framework.....	111
10.1.2 Contributions of a reputational herd model in explaining IS security investment motivation.....	112
10.1.3 Contributions of testing the new assumption in another context.....	113
10.1.4 Overall contribution of the thesis.....	113
10.2 Implications for practice.....	115
10.3 Limitations and implications for future research.....	116
10.3.1 Examining different IS security investment motivations.....	117
10.3.2 Identifying measurable impacts for IS security investment.....	118
10.3.3 Understanding IS security investment process.....	119
10.4 Conclusions.....	120
Reference	123
Appendices	139

1 Introduction

This chapter introduces both the topic and the purpose of this research. To begin, a short background description is provided for the study. The second section presents the research question and the main objectives of the doctoral thesis. After that, the chapter proceeds to point out the significance of the thesis. Following this, the chapter concludes with the structure of this thesis.

1.1 Problem statement

Information systems (IS) security breaches in organizations are becoming as common as colds but are far more expensive to treat (2014 Cost of Data Breach Study). To illustrate the critical nature of IS security within organizations, this thesis begins with a real-world example of an IS security breach:

“On April 20, 2011 Sony took the two services offline after an intrusion was detected on the network’s servers. More than 77 million PlayStation Network accounts affected, of which 12 million had unencrypted credit card numbers. According to Sony it still has not found the source of the hack. Whoever they are gained access to full names, passwords, e-mails, home addresses, purchase history, credit card numbers, and PSN/Qriocity logins and passwords...” (CSO Online: The 15 Worst Data Security Breaches of the 21st Century)

Large organizations like Sony are not the only ones to suffer from IS security attacks. The UK’s Department for Business Innovation & Skills’ *2014 Information Security Breaches Survey* reveals that organizations of all sizes suffer from external attacks. While it is difficult for organizations to avoid IS security breaches, it is even more difficult to recover from these breaches. The *2014 Cost of Data Breach Study* reveals that the average cost to a company in 2014 was USD\$ 3.5 million, which was 15% more than what it cost in 2013. As a result, the need to secure organizations’ informational assets has become an increasingly critical issue.

IS security within organizations has received attention from researchers for over a decade. The importance of securing organization’s information assets has resulted in research that is focused on the technical defense (e.g., Anderson 1972, Axelsson 2000, Schlienger & Teufel 2002) and the behavioral aspects (e.g., Straub 1990, Bulgurcy *et al.* 2010, Siponen & Vance 2010, D’Arcy *et al.* 2009) of reducing information security breaches. Technical defense (e.g., encryption, access control, and firewalls) to information security breaches focused on protecting information (e.g., Anderson 1972, Wiseman 1986, Simmons 1994) and intrusion detection

systems (e.g., Denning 1987, Daniels & Spafford 1999, Axelsson 2000). Research that concentrates on the technical aspects of information security alone is inadequate as IS users may not follow technical information security measures (Stanton *et al.* 2003). The importance of the human factor in IS security have been addressed in studies that have investigated behavioral issues in IS security, such as computer abuse (Parker 1976, Straub 1990, Harrington 1996, Lee *et al.* 2004, D’Arcy *et al.* 2008), employees’ compliance with IS security procedures (Bulgurcy *et al.* 2010, Johnston & Warkentin 2010, Herath & Rao 2009, 2009b, Li *et al.* 2010, Siponen & Vance 2010), and appropriate IS security behavior for employees (D’Arcy & Greene 2009, Hyeun-Suk *et al.* 2005, Dinev & Hu 2007).

IS researchers have also examined the economic aspects of IS security apart from technical defense and behavioral concerns. In so doing, prior research has developed models to determine how much to invest on IS security (e.g., Gordon & Loeb 2002, Huang *et al.* 2008, Cavusoglu *et al.* 2008). Those studies can be classified into two categories (Cavusoglu *et al.* 2008): studies in the first category are based on a decision-theoretic approach that utilizes risk or decision analysis models to analyze organizations’ investments to prevent IS security problems (e.g., Gordon & Loeb 2002, Huang *et al.* 2008, Lee *et al.* 2011); studies in the second category are based on a game-theoretic approach that treats IS security investment as a game between organizations and attackers – or interdependent organizations (e.g., Cavusoglu *et al.* 2004, Liu *et al.* 2005, Cavusoglu *et al.* 2009). All the models across both of these categories are based on a neoclassical economics framework of decision-making, which assumes that the goal of IS security investment is benefit maximization and that all the actors involved are unbiased rational actors with complete information.

It is argued in this thesis that the idea of benefit maximization is not a suitable goal for IS security investment. Benefit maximization may be an ideal economic goal, however, in practice, the goals of IS security investment include reducing IS security risk, balancing business needs and IS security requirements, maintaining compliance, and ensuring cultural fit (Kayworth & Whitten 2010). Besides, benefits and costs cannot be reliably calculated for IS security and are based on guesswork (Baskerville 1991; Wood and Parker 2004). Different from information technology (IT) investment, the value of IS security investment comes from “preventing something from happening” (Huang *et al.* 2007), which makes it difficult to measure the benefit of IS security investment. As a result, benefit maximization is not a suitable goal to understand IS security investment.

It is also argued in this thesis that the actors involved in IS security are not unbiased, rational decision makers (contrary to the assumptions of prior research on IS security investment). First, generally speaking, humans' preferences are not stable and may change due to risk, framing, loss (Kahneman & Tversky 1979), and time (Thaler, 1981; Loewenstein & Prelec, 1992). Therefore, the utility functions that applied in decision-theoretical and game-theoretical approaches will also change. Second, the information that IS security investment decision makers use is incomplete, so that decision- and game-theoretic approaches are hard to be applied. Information regarding the risks, costs and benefits of IS security investment are important in decision-theoretic approach, however, it is difficult to have reliable data. As an example, information management standards are the most widely used methods in IS security management (CITE), however, practitioners have no evidence that they can use to analyze the popular IS security investment management standards (Siponen & Willison 2009). When utilizing game-theoretic approach, it is essential to understand hacker's strategy, however, research (Wang *et al.* 2008) shows that it is difficult to determine the rationality of hackers as they may be motivated by a different value system.

1.2 Research question and objectives

Prior research has approached IS security investment by building models based on neoclassical economics framework, with making assumptions about the goal of IS security investment and about the decision-maker. Based on these assumptions, prior research treats the IS security investment problem as a calculation problem. However, financial calculation tools do not fit well the IS security investment problem (Wood & Parker 2004). The overall argument carried out in this thesis is that previous economic models for IS security investment fail to take the specific contextual nature of IS security investment into account. For instance, benefit maximization might be a realistic goal for financial investment in the stock market, but it is a less appropriate goal for IS security.

Remedying this problem requires an improved understanding of the context of IS security investment, which has not been of interest to the previous economic models. Accordingly, the author attempts to answer the following question: *What needs to be considered to understand IS security investment?*

To address this research question, an iterative research process that synthesized the used theories, the preliminary framework, and the empirical material was used. The developed framework attempts to take the contextual nature of IS security

investment into account. In order to do so, the intangible benefit, multiple investment areas, and investment goals of IS security investment were considered. Additionally, a satisfactory solution assumption of decision makers is introduced into the framework. This assumption acknowledges that humans have limitations on making decisions, and seeks a satisfactory solution to address this limitation.

The developed framework depicting the nature of IS security investment sheds light on the research question. The preliminary framework was composed so as to be as holistic as possible, and the empirical studies were used to test the framework. Thereafter, the framework was adjusted accordingly to form an empirically grounded framework. Aspects of this framework relevant to managers are highlighted in the discussion section of this thesis.

1.3 Significance of the research

The main theoretical contribution can be divided into two parts. The synthesis of the preliminary framework (Figure 3, section 5.3) depicting IS security investment decision making provides the first contribution, while the second part is the development of an empirically grounded framework (Figure 13, section 9.2), which is based both on the preliminary framework and the field study that together constitute the empirically grounded framework. The preliminary and the empirically grounded frameworks provide answers to the research question, as they describe and explain how IS security investment decision and what factors are influencing IS security investment.

This main theoretical contribution, i.e. the empirically grounded framework of IS security investment, is delivered via several contributions, which are present next.

The first contribution is providing the basis to discuss IS security investment. Investment areas, investment goals and its intangible nature are three basic characteristics of IS security investment. These concepts were introduced and integrated into the framework. These concepts add new elements that in an elementary sense describe IS security investment, providing the means to start discussing the phenomenon.

Based on the first contribution, *the second contribution* was conceptualized. That is the assumptions of IS security investment decision-makers. These assumptions had to be developed as IS security investment has the above characteristics. Intangible nature of IS security investment suggests inaccurate knowledge and incomplete information that decision-makers can acquire.

Investment goals of IS security investment suggest that decision-makers need to balance different perspectives and achieve a satisfactory decision. These assumptions describe the constraints of decision-makers and provide one way to put the IS security investment research inside the boundary.

The third contribution is the concept of herding behavior. Herding behavior exists in many situations where it is hard to accurately estimate costs and benefits of choices. This thesis empirically confirms that herding behavior as well exists in IS security investment. Herding behavior in IS security investment presents that IS security investment managers do not always seek the maximum benefit for company, instead they search for supplementary strategies in decision-making especially due to intangible nature of IS security investment. On the whole, herding behavior enlightens future research to study other supplementary strategies.

The fourth contribution argues that this research indicates the importance to study IS security investment under a behavioral economic paradigm. Behavioral economic paradigm introduces more realistic considerations than neoclassic economic paradigm, which helps researchers see more aspects and deeper into the phenomenon.

Besides theoretical contributions to the current IS security investment research, this thesis has tried to provide meaningful managerial implication as *the fifth contribution*. CEOs can pay attention to factors that influences IS security investment decision-making. For example, whether IS security managers' cognitive limitations affect their decision-making. Better communication channels should be established so that CEOs could better understand how hard IS security investment managers work, and therefore, asymmetric information could be eliminated.

1.4 Structure of the thesis

This thesis is divided into ten chapters as depicted in Figure 1. The first chapter presents the background and introduces the research question and the structure of the thesis. Following this, Chapter 2 analyzes IS security investment literature. Thereafter, characteristics of IS security investment are presented in Chapter 3. Chapter 4 discusses the gaps in the previous research on IS security investment. In Chapter 5, a preliminary framework providing insights into IS security investment is synthesized and further elaborated on. Chapter 6 introduces the employed research design that was used while conducting the empirical analysis. Chapters 7 and 8 present the empirical analysis. These chapters present the empirical tests of the proposed framework. Chapter 9 synthesizes this analysis and presents an

empirically grounded framework for IS security investment. It draws together the preliminary framework developed in Chapter 5, and modifications are made in accordance with the findings from the empirical tests. Chapter 10 presents both the contributions and limitations of the study as well as a discussion of possible future research in this area.

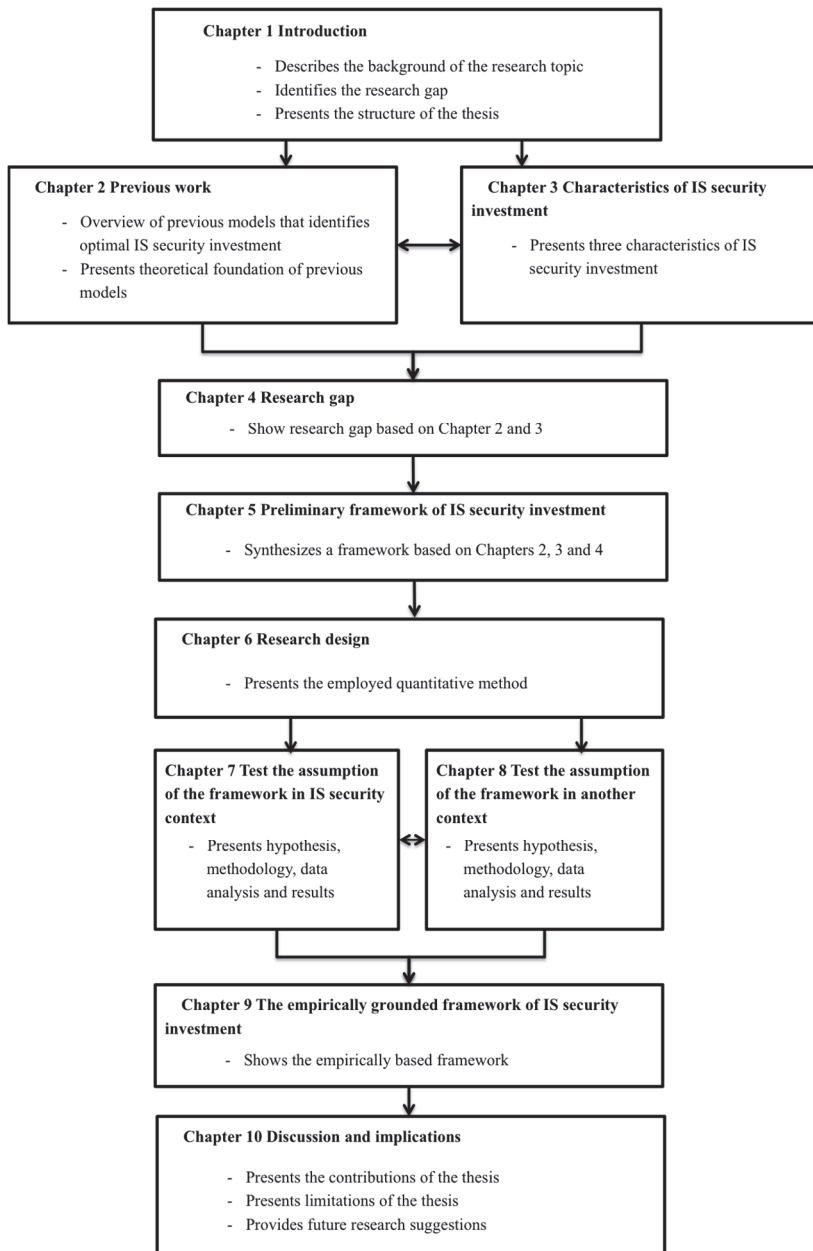


Fig. 1. Organization of the study.

2 Previous work

This chapter reviews previous work on attempts to identify the optimal level of IS security investment. First, this chapter presents the process used to determine the source material for the literature review, after which an overview of the literature then follows. Thereafter, an analysis of the previous work is presented based on a neoclassical economic framework.

2.1 Determining the source material for the literature review

A comprehensive review of the literature will cover all the relevant literature on the topic without being confined to one research methodology, one set of journals or one geographic region (Webster & Watson 2002 p. xv-xvi). With this in mind, the literature review presented in the second chapter of this dissertation aims to cover all existing economic analysis studies of IS security investment. This thesis conducted a systematic literature review using the methods described by Webster & Watson (2002), who focused on the structure of the literature review paper, and by Okoli & Schabram (2010), who focused on the process of conducting a systematic literature review. To identify academic papers on the economic analysis of IS security investment, a search was conducted for papers in the following databases: ACM Digital Library, EBSCO, Google Scholar, IEEE Xplore, ProQuest and Worldcat. Additionally, the databases of a number of well-respected conferences in the Information Systems field, including ICIS, ECIS, PACIS, and AMCIS were also searched.

Full-text searches were conducted up through 2014 using the search term “information systems security investment” and the combination of the search terms “Information” AND “Systems” AND “Security” AND “Investment” as search keys. Furthermore, a search was conducted for earlier papers that were relevant (“going backward”). Where possible, the databases were also used to search for papers in which the papers found were cited (“going forward”). This search process resulted in a collection of 99 academic papers.

During the collection of the academic papers, a practical screen was applied to determine which papers should be kept for further study (Okoli & Schabram, 2010). Applying the screen was alternated with the literature search in order to limit the amount of work involved in “going backward and forward.” A rather tolerant screen was used, since the goal was to obtain a broad overview of the papers published in this domain. The process of screening the papers involved the determination of

whether they accidentally contained the words “information”, “systems”, “security” and “investment”, and whether they really addressed the issue of how much to invest on IS security. During the screening process, a more elaborate understanding was developed, which resulted in increasingly refined rounds of screening while going through the literature. After the screening process, 28 academic papers remained. The selected articles included economic models for making decisions on IS security investments.

2.2 An overview of the literature

To increase our understanding of existing economic analyses of IS security investment, the literature was divided into two categories according to their research approaches as classified by Cavusoglu *et al.* (2008): (1) *decision-theoretic approach*, and (2) *game-theoretic approach*. The rest of this section will provide an overview of the literature.

Prior studies provide analytical tools for organizations to determine an optimal amount to invest on IS security. Both the decision-theoretic approach and the game-theoretic approach are applied in these studies. The decision-theoretic approach uses the traditional risk or decision analysis framework to determine IS security investment level, viewing hackers’ efforts as exogenous. By contrast, the game-theoretic approach treats IS security investment as a game between two players-for example, between organizations and attackers¹, in which case, both the organization’s level of IS security investment level and the hackers’ efforts are endogenously determined. Studies in both approaches offer an understanding of how to determine an optimal level of investment in IS security.

2.2.1 Decision-theoretic approach

Kort *et al.* (1999) developed two models to study optimal investment by firms on IS security. In the first model, the firm has the possibility to reduce criminal losses by building up a stock of security capital. The result shows that in the case of the existence of a long-run steady-state equilibrium, the firm fixes its investment in

¹ The two players are not limited to organizations and attackers. It depends on the problem setting. For example, when the problem setting is about how to protect information from hackers’ attack, the two players are the organization and potential hackers. When the problem setting is about how to protect information when sharing information with dependent partners, the two players are then the organization and the dependent partner.

security equipment, such that the discounted stream of reductions of criminal losses that results from owning an additional unit of security equipment is equal to its marginal security investment expenses. The second model extends the first model by taking a “firm’s reputation in the criminal world” into consideration. If the firm has produced a lot in the past without having invested in security equipment, this firm is known to be a fruitful target for criminals, and therefore, this may increase the likelihood of future criminal losses. By taking different initial values, the second model shows that the introduction of this reputation variable affects the level of investment in security equipment.

Gordon and Loeb (2002) built a model to determine how much to invest in IS security. Their study analyzed the economics of IS security investment by comparing the expected benefits of IS security investment with the monetary investment in security to protect the given information set. The results indicate that, for a given potential loss, a firm should not necessarily focus its investments on the information sets with the highest vulnerability. A firm may be better off concentrating its efforts on information sets with midrange vulnerabilities. This study also suggested that for two broad classes of security breach probability functions, the optimal amount to spend on IS security never exceeds 36.8% of the expected loss resulting from a security breach (and is typically much less than 36.8%).

Huang *et al.* (2006) proposed an economic model that considers simultaneous attacks from multiple external agents with distinct characteristics and derives optimal investments based on the principle of benefit maximization. Their model shows how a firm should allocate its limited security budget to defend against two types of security attacks (distributed and targeted) simultaneously. The result indicates that a firm with a small security budget is better off allocating most or all of its investment on measures against one of the classes of attack; when the potential loss from the targeted attacks and the system vulnerability is relatively large. The firm should allocate most of its budget to prevent such attacks.

Willemson (2006) slightly modified the Gordon & Loeb (2002)’s model² and showed that there are functions that can decrease vulnerability that require investments of up to 50% of the asset value.

² In Gordon & Loeb model, it is assumed that it is impossible to decrease the attack probability to exactly 0, no matter how large amounts of money invested, unless the original vulnerability is 0. Willemson (2006) suggested that when the threat is a possible attack from a specific person, it is possible to get rid of this person by paying to a hit man and having this person killed. Therefore, it is possible to have attack probability to exactly 0.

Huang *et al.* (2008) developed an economic model to analyze the optimal level of investment on information security. Unlike Gordon & Loeb (2002), who assumed that a firm is risk-neutral, Huang *et al.* (2008) considered the firm to be risk-averse. Utilizing the expected utility theory, they compared monetary investment against potential loss from a security breach within an expected utility analysis to determine the security investment level. The results show that there exists a minimum potential loss for non-zero optimal IS security investment, above which optimal investment increases along with potential loss. Furthermore, they showed mathematically that, contrary to the investment made in the risk-neutral case, a risk-averse decision maker might continue to invest in IS security until the spending is close to (but never exceeds) the potential loss.

Huang and Goo (2009) built a general model to manage IS security investment and applied the general model to different scenarios of IS security, including directed attacks, risk-averse decision makers, and attacker propensity. Their results suggested that the relative size of potential losses is an important factor in determining the level of optimal investment and that the total investment may drop when system vulnerability is high. A risk-averse firm would always invest more than the information security risk but never more than the expected loss. Moreover, they suggested that a firm should study its level of risk aversion as well as that of the potential attacker's to determine the most optimal level of IS security investments.

Wang *et al.* (2009) proposed two algorithms, API and OSI, to calculate the accumulative probability of threat to resources and the optimal security investment for each filter in a data center when a single threat exists. The proposed API algorithm is based on a threat flow model that models the probabilistic flow of possible attacks on information systems. The proposed OSI algorithm is based on a risk-neutral assumption that the optimal security investment should maximize the total expected net benefit. They suggested that the two algorithms could be used to evaluate IS security and determine the optimal level of IS security investment for data centers.

Bohme & Felegyhazi (2010) considered penetration testing in determining optimal information security investment. Their result suggested that once started, it is optimal to continue penetration testing until a secure state is reached. Additionally, the penetration testing almost always increases the per-dollar efficiency of security investment.

Huang (2010) extended the current economic models of IS security investment by using a business value to determining a firm's security investment. Huang

(2010)'s model argued that current economic models of IS security investment focus on risk reduction as the primary effect of IS security investments, assuming that they generate no direct business benefit; however, some potential business values, such as brand reputation and data stability, are important considerations in optimizing IS security investment.

Willemsen (2010) extended the Gordon & Loeb (2002)'s model by revising the vulnerability function to better apply Gordon & Loeb's model in practice.

Lee *et al.* (2011) presented a profit optimization model for customer information security investments based on value-at-risk methods and operational risk modeling from financial economics. Their model can be applied to scenarios in which the frequency of information security breaches and financial loss severity distribution can be estimated qualitatively or quantitatively.

Shim (2011) extended the Gordon & Loeb (2002)'s model by considering interdependent security risks. Shim (2011)'s analysis showed that the relationship between the level of security vulnerability and the optimal information security investment is affected by externalities³ caused by a firm's correlated security risks. These externalities lead a firm to, in order to prevent independent security risks, invest a different fraction of the expected loss compared to security investments. This is because a firm should invest a larger fraction of the expected loss from a security breach in the case of negative externalities in order to maximize the expected benefits from security investments, while in the case of positive externalities, a firm should spend a smaller fraction of the expected loss.

Bojanc *et al.* (2012) proposed a mathematical model for the optimal security-technology investment evaluation and decision-making processes based on a quantitative analysis of security risks and digital asset assessments within an organization. Unlike other models used to evaluate security investment, the proposed model allows for a direct comparison and quantitative assessment of different security measures: technological security solutions, the introduction of organizational procedures, training or transfer risk to an external company. The model output data includes return on investment (ROI), net present value (NPV),

³ The characteristic of interdependent security risks generates either positive or negative externalities onto firms' security investments. Examples of negative externalities include the case where hacking attacks targeted at a highly secured server are diverted to other servers, and hence increase the risks of other firms (i.e., targeted attacks). Positive externalities include the case when a firm raises its level of information security by investing more in technical security solutions; the firm's partners security breaches may be lowered via its computer network (i.e., untargeted attacks).

internal rate of return (IRR), as well as a comparison of individual measures with one another.

Huang & Behara (2013) developed an analytic model for the allocation of a fixed budget for information security investment against multiple attacks. The results of these analyses showed that a firm with a limited security is better off allocating most or all of its investment to measures against one of the classes of attack. Further, when information systems are highly connected and relatively open and when the potential loss is large relative to the security budget, managers should focus the security investment on preventing targeted attacks.

Huang *et al.* (2014) studied optimal information security investment in a Healthcare Information Exchange (HIE). They applied classical economic decision analysis techniques and modeled a HIE based on its network characteristics. They found that for an organization in a HIE, only security events with the potential for critical loss are worth protecting, and organizations would only spend a fraction of the intrinsic security risk on protection measures. Even when there is a business benefit from security investment, organizations in a HIE tend to invest based on risk reduction alone.

2.2.2 Game-theoretic approach

While organizations try to patch vulnerabilities in their systems, hackers race to exploit them. Game theory is used to analyze problems in which the payoffs to players (e.g., an organization and a hacker) depend on the interaction between players' strategies. For example, in the IS security investment problem, the firm and the hackers are the players. The firm's payoff from the security investment depends on the extent of hacking to which it is subjected. The hacker's payoff from the hacking depends on the likelihood of getting caught. Thus, the likelihood of the firm getting hacked depends on the likelihood that the hacker will be caught, which, in turn, depends on the level of investment the firm makes in IS security.

Cavusoglu *et al.* (2004) constructed a game tree to describe the interaction between organizations and hackers to determine the choice of security technology, and argued that the game-theoretic approach to determine IS security investment is better than a risk analysis or a cost effectiveness analysis.

Cavusoglu & Raghunathan (2004) presented two modes—the first based on decision theory and the second based on game theory—to assist firms with the process of configuring detection software. According to the decision theory approach, the firm estimates the probability of fraud exogenously and assumes that

its actions do not alter users' behavior. According to the game-theoretic approach, the firm makes its decisions by assuming that these decisions will alter user behavior. The authors found that firms incur lower costs in most situations when they use game theory as opposed to decision theory.

Bandyopadhyay *et al.* (2005) studied information security investment strategies in supply chain firms, which share information assets among themselves and make use of inter-firm network connections to enable quick information sharing. They found that past decisions on information asset sharing intensity affect today's efficient level of investment in security technologies in supply chain firms, and increased chain size widens the gap of investment thresholds between the vendors and the retailers, at which point contamination probability rises.

Cavusoglu *et al.* (2005) studied the value of intrusion detection systems (IDS) in a game-theoretic framework, with the firm and users as the two players. Their results showed that a firm might not realize a positive value from an improperly configured IDS. Additionally, they also found that optimal configuration depends not on the firm's internal cost parameters, but on the external hacker parameters, which highlights the significance of understanding hacker behavior and motivation when employing an IDS.

Liu *et al.* (2005) analyzed information security investment with different information types in two firms that possessed imperfectly substitutable information assets. They found that when these decisions are made independently, holding substitutable information assets causes both firms to overinvest, whereas holding complementary information assets leads to underinvestment.

Cremonini & Nizovtsev (2006) suggested that understanding attackers' behavior has important implications for information security investment strategies.

Hausken (2006) investigated income, interdependence, and substitution effects that affect security investment incentives. The investigation of income effect studied a game between firms and hackers, and it suggested that any investment against an overwhelming threat is a waste; moreover, when the income reduction parameter⁴ increases above a certain level, security investments also increase. The investigation of interdependence studied a game between two interdependent firms, and the findings suggested that because interdependence leads to free riding, each firm cuts down on its own investment and prefers the other to invest. Substitution effect means that the hacker allocates its attack optimally between the two firms. The hackers do not go for the largest asset if this asset is too well protected.

⁴ This parameter scales how much a firm's security investments reduce an attacker's income.

Cavusoglu *et al.* (2008) proposed using game theory to determine IT security investments and compared the decision-theoretic approach with game-theoretic approach on several dimensions, including investment level, vulnerability, and payoffs from investment. They showed that the sequential game results in the maximum payoff to the firm but requires that the firm move first, before the hacker. Even when a game is played simultaneously, the firm enjoys a higher payoff than with the decision theory approach, except when the firm's estimation of a hacker's efforts in the decision theory approach is sufficiently close to the actual hacker's efforts. This study also showed that if a firm learns from previous observations of hackers' efforts and uses this knowledge to predict future hacker efforts by using the decision theory approach, then the gap between the results of decision theory and game-theoretic approaches diminishes over time.

Bohme and Moore (2009) proposed a model for security investment that reflects the dynamic interaction between a defender and an attacker. The defender faces uncertainty and repeatedly targets the weakest link. The model explains that underinvestment might reasonably occur when a) reactive investment is possible; b) uncertainty exists about the attacker's relative capability to exploit different threats; c) successful attacks are not catastrophic; and d) the sunk cost to upgrade the defense configuration is relatively small.

Liu *et al.* (2011) studied the relationship between decisions made by two similar firms with regard to knowledge sharing and investment in information security. The analysis showed that the nature of the information assets possessed by the two firms, complementary in one case and substitutable in the other, played a crucial role in influencing these decisions. In the complementary case, firms have a natural incentive to share security knowledge, and no external influence is needed to induce sharing; however, the investment levels are lower than optimal. In the substitutable case, firms fall into a prisoners' dilemma in which they do not share security knowledge despite it being beneficial for both of them to do so; even when the firms share information following recommendations, the level of investment is suboptimal.

Pal and Hui (2011) proposed a security investment model for the Internet in which Internet users account for the positive externality posed to them by other Internet users and make security investments in situations in which they do not have complete information about the underlying connecting topology of their neighbors or their security investments. Their model, which is based on a game-theoretic approach, found that better connected Internet users exert less effort but earn higher

utilities than their less connected peers with respect to security improvement when user utility functions exhibit strategic substitutes.

Gao *et al.* (2013a) investigated how firms invest in information security within the Cournot and Bertrand competition, constructing a differential game in which hackers become knowledgeable over time by disseminating security knowledge, while firms can inhibit it through security investments. Their study showed that greater effectiveness in inhibiting knowledge dissemination may not necessarily leads to a higher investment, and that the investment is more effective in the Cournot competition.

Gao *et al.* (2013b) utilized a differential game-theoretic framework in which hackers disseminate security knowledge within a hacker population over time. They found that the hacker invests the most in the simultaneous differential game, whereas the firm invests the most in the sequential differential game; moreover, both the firm and the hacker enjoy their highest payoff in the sequential differential game when the hacker is the first mover.

2.3 Analysis of previous work

In this section, previous work is analyzed within the neoclassical economics framework. The neoclassical economics framework is presented in the following section (see Table 1).

2.3.1 Aim of the analysis

While prior work developed economic models to help firms make decisions on IS security investment, there is a lack of a comprehensive review of the literature. A comprehensive review would be useful for practitioners, as they do not necessarily have enough time to browse the large amount of published material. By analyzing extant IS security investment studies, this thesis aims at better understanding the literature to help practitioners choose IS security investment models that are suitable for the aims and cultures of their organizations. Such an analysis is also of value to the research community in that it will indicate which areas of IS security investment have been studied and for which the need for future research is of greatest importance.

The analysis used in this thesis employs a neoclassical economics framework in order to achieve two goals. The first aim is to point out existing analyses of IS security investment that propose an optimal investment level of IS security. This is

useful for both practitioners and scholars wishing to explore the various models further. In addition to recognizing various IS security investment models, a deeper understanding of these models is of value. Lack of understanding of the available IS security investment models is manifest, for example, in the use of models unsupported by adequate empirical evidence on their practical effectiveness.

The second aim of this analysis is to contribute to the understanding of the theoretical background behind the economic analysis of IS security investment. This is useful for both scholars and practitioners, as such knowledge explains why a particular level of investment is proposed for IS security. In addition, the identification of appropriate models for IS security investment decision-making is important.

2.3.2 The neoclassical economics framework of decision-making

A literature review that aims to increase understanding can benefit from the use of an analytical tool like a conceptual framework to identify gaps in knowledge and theoretical bias (Rowe 2014). In particular, if the mapping was clear and well-known prior to the literature review, a review that uses an original and relevant analytical lens is very likely to lead to the identification of knowledge gaps and theoretical bias, should these exist.

A neoclassical economics framework of decision-making has been chosen here. The neoclassical economics paradigm has proven to be a valuable approach for evaluating a variety of issues with individual and social decision-making.

The origin of neoclassical economics is classical economics, including the work of Adam Smith (1776) and David Ricardo (1817). Classical economics proposes that the value of a product depends on the costs involved in producing that product. However, a change in economic theory from classical to neoclassical occurred called the “marginal revolution.” Marginal utility was discovered independently and simultaneously in Jovons’s *Theory of Political Economy* (1871), Menger’s *Principles of Economics* (1871), and Walras’s *Elements of Pure Economics* (1874). The framework of neoclassical economics can be summarized as follows: individuals make choices at the margin, where the marginal utility of a good or service is either the gain from an increase or the loss from a decrease in the consumption of that good or service (Rittenberg & Tregarthen, 2012). For example, consumers attempt to maximize their gains from the purchase of goods by increasing their purchases of a good until what they gain from an extra unit of that good is just balanced by what they have to give up to obtain it. In this way,

consumers maximize utility. Similarly, producers attempt to produce units of a good so that the cost of producing the incremental or marginal unit is just balanced by the revenue it generates. In this way, producers maximize profits.

Simon (1997, p. 17) summarized the neoclassical framework of decision-making as this: the decision maker has a comprehensive, consistent utility function (*preferences*), knows all the alternatives that are available for choice, can compute the expected value of utility associated with each alternative (*complete information*), and chooses the alternative that maximizes expected utility (*utility maximization*). Figure 2 depicts the neoclassical framework of decision-making.

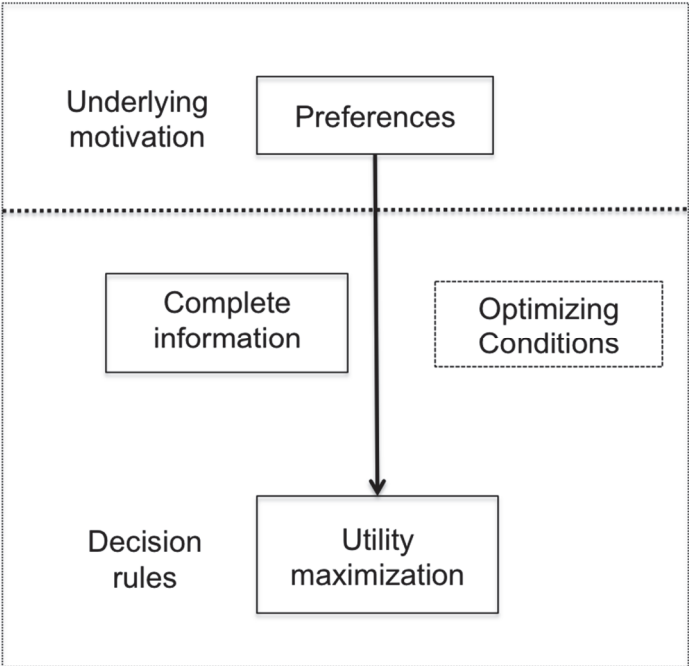


Fig. 2. Depiction of the neoclassical framework for decision-making

Table 1 summarizes the concepts related to the neoclassical economics framework for decision-making. Preferences are often described by their utility function or payoff function, and thus, preferences are expressed as the relationship between utilities and payoffs (Barten *et al.*, 1982). When individuals face a set of exhaustive and exclusive options to choose from, they can rank the options in terms of their

preferences, describe their preferences by utility function, and select the option with maximal utility.

Utility maximization can be traced back to Smith's (1776) "Economic Man" in *The Wealth of Nations*, which suggested that economic men are self-interested, who attempt to maximize utility as a consumer and economic profit as a producer. Economics, as the study of the allocation of scarce resources among unlimited and competing users (Arrow, 1962), maintains the maximization of utility/payoff assumption as one of its central assumptions.

Complete information refers to the situation in which people have full and relevant information about what exactly will occur as a result of any choice made (Case & Fair, 1989, p. 103). For example, suppose that an individual is making a purchase decision; and the individual knows all the information that is relevant to the purchase decision, such as the price of every commodity, the inventory of every commodity, and the individual's own demand and preference. With game theory, the complete information assumption suggests that every player knows the payoffs and strategies available to other players.

The decision rules for neoclassical optimization are described by a set of first order necessary conditions that equate marginal benefits and marginal costs, subject to the second order conditions (Opaluch & Segerson, 1989). These decision rules describe optimizing behavior and provide insights into the trade-offs faced in decision-making.

Table 1. Neoclassical framework of decision-making

	Description	Sources
Preferences	Given a set of exhaustive and exclusive options to choose from, an individual can rank the options in terms of his/her preferences, this preference structure is internally consistent, and there should be at least one maximal option. Preferences are often described by utility function or payoff function.	Barten <i>et al.</i> (1982)
Utility maximization	Individuals maximize utility. Firms maximize profits.	Smith (1776); Simon (1997)
Complete information	People have full and relevant information about exactly what will occur due to any choice made. In game theory, every player knows payoffs and strategies of every other player.	Case & Fair (1989)
Optimizing condition	Neoclassical optimization are described by a set of first order necessary conditions that equate marginal benefits and marginal costs, subject to the second order conditions.	Opaluch and Segerson (1989)

2.3.3 Analysis of existing economic analysis of IS security investment

In this section, an analysis of IS security investment literature is presented. This analysis investigates how prior work applied the neoclassical economics framework for decision-making. A detailed table of this analysis is presented in Table 19 in Appendix 1.

Preferences are often described by their utility function or payoff function (Barten *et al.*, 1982). In prior work, rational preference is usually described as a function of benefit/utility/profit. For example, Gordon and Loeb (2002) built a function of expected benefit for information security investment. Huang *et al.* (2008) developed a function of expected utility. Cavusoglu *et al.* (2004) developed functions of expected payoff for both the firm and the hacker. Cremonini and Nizovtsev (2006) established a function of expected payoff for hackers.

Maximization of utility/profit is also assumed in prior work. In decision-theoretical studies, firms are usually assumed to maximize their expected net benefits (e.g., Gordon & Loeb 2002; Willemson, 2006) or profits (e.g., Bohme & Felegyhazi, 2010; Lee *et al.*, 2011). In game-theoretical studies, both players are assumed to maximize their payoffs (e.g., Cavusoglu *et al.*, 2004) or profits (e.g.,

Hausken, 2006; Cavusoglu *et al.*, 2008). In some studies, firms have been assumed to minimize their costs⁵ (e.g., Cavusoglu & Raghunathan 2004; Bandyopadhyay *et al.*, 2005; Cavusoglu *et al.*, 2005; Liu *et al.*, 2005; Liu *et al.*, 2011).

Complete information is not clearly mentioned in decision-theoretical studies. But in game-theoretical studies, complete information is implicitly applied. The solution to the game involves the maximization (or minimization) of a polynomial function. Therefore, the firm needs to know the hacker's payoff function, and vice versa (e.g., Cavusoglu *et al.*, 2004, Cavusoglu & Raghunathan, 2004; Bandyopadhyay *et al.*, 2005; Cavusoglu *et al.*, 2005; Liu *et al.*, 2005; Cremonini & Nizovtsev, 2006).

With regard to optimizing conditions, prior work described a set of first order necessary conditions that equate marginal benefits and marginal costs, subject to the second order conditions. For example, Huang *et al.* (2008) differentiated expected utility function from security investment to find the first-order equilibrium, which yields the conditions in which to find the optimal security investment. Cavusoglu *et al.* (2008) differentiated the payoff functions for both firm and hacker with respect to security investment to find the first-order equilibriums. By solving the first-order equilibriums, they were able to determine the optimal investment level for the firm and the optimal effort level for the hacker in the simultaneous game.

To sum up, prior work on IS security investment was based on the neoclassical framework of decision-making, by assuming decision makers have a rational preference (using a comprehensive and consistent utility/payoff function), have complete information (in the game-theoretical approach), and seek maximum benefits/payoffs.

⁵ In economic models, when facing a budget constraint, maximizing utility/profit is equivalent to minimizing the cost to reach an optimal choice.

3 Characteristics of IS security investment

This chapter discusses three characteristics of IS security investment, including (1) IS security investment areas; (2) intangible benefits of IS security investment; and (3) goals of IS security investment. Table 2 summarizes the characteristics of IS security investment.

Table 2. Characteristics of IS security investment

	Description
Distribution	<ul style="list-style-type: none">– IS security training/education to improve employees' security behaviors– IS security policy development– IS security technologies
Goal	<ul style="list-style-type: none">– Reduce the risk to an acceptable level– Balance the need to secure information assets against the need to facilitate the business function– Maintain compliance– Ensure cultural fit
Intangible benefits	<ul style="list-style-type: none">– Value of IS security investment lies in "preventing something from happening," not in "making something happen"– Payoff period of IS security investment is ambiguous

3.1 IS security investment areas

Since information systems connect various parties and stakeholders, IS security is not an isolated concern. Although most organizations have long been using security technologies, it is well known that technology tools alone are not sufficient. IS security cannot be achieved only through technological tools, and effective organizational IS security depends on all three components, namely: people, processes, and technology (Hamill *et al.*, 2005).

Many important security breaches occur from employees' computer misuse/abuse or violation of IS security procedures. Practitioners and researchers have started to realize that employees as well as other insiders are most likely to perpetrate IS security incidents (Information Security Breaches Survey, 2014; Puhakainen, 2006; Siponen & Vance, 2010). Industry statistics suggest that between 50%–75% of security incidents originate from within an organization (Ernst & Young, 2003; InformationWeek, 2005), often perpetrated by disgruntled employees (Standage, 2002). However, many organizations do not have plans for

responding to insider threats, and those that do are not highly effective (Information Security Breaches Survey, 2014). If employees do not comply with IS security procedures, security solutions lose their usefulness. The number of security breaches that involve internal misuse of IS resources highlights the need for employees to be aware of IS security. In order to ensure that employees comply with their companies' IS security procedures, different approaches have been advanced in the literature, such as the use of sanctions and deterrence (Straub, 1990; Siponen *et al.*, 2007), marketing campaigns (McLean, 1992), and training (Puhakainen & Siponen, 2010). Of these, IS security training is the most common approach to improve employees' IS security behavior (Puhakainen & Siponen, 2010).

Another area that needs investment is IS security policy development. The information security policy has been called the precondition to implementing all effective security deterrents (Straub, 1990) and may be more vital to reducing computer crime than devices like firewalls and intrusion detection systems (Buss & Salerno, 1984). Of all the controls necessary to protect organizational information from threats, the information security policy may be the most important one (Höne & Eloff, 2002; Whitman & Mattord, 2005), because IS security policies can be the basis for litigation or internal measures that punish IS misbehavior. However, the development of an IS security policy is not easy. An unclear IS security policy will confuse employees. Puhakainen (2006) reported a situation in which employees refused their responsibility to comply with a policy to encrypt confidential e-mails, rationalizing that the policy was unclear. Information security policies are sometimes framed in a life-cycle context with an emphasis on development, enforcement, and maintenance while advising that the security policy be consistent with business objectives (Hare, 2002; Howard, 2003).

A third area that needs investment is IS security technology. Most companies have deployed traditional security tools, such as application firewalls, web content filters, malware or virus-protection software, secure remote access (VPN), secure browsers, compliance testing, network access control software, identity management technology, encryption of desktop PCs, and so on. Yet these traditional security tools may not be effective in stopping today's threats. Safeguards that monitor data and assets (for example, behavioral profiling and monitoring, use of a virtual desktop interface, security information and event management technologies, protection/detection solutions for APTs, data loss prevention tools, asset-management tools, and centralized data stores) can provide ongoing intelligence into ecosystem vulnerabilities and dynamic threats.

To sum up, IS security investment should be made in at least the three above mentioned areas to ensure that information receives protection: IS security awareness training for employees, IS security policy development, and IS security technology. The first two areas (employee IS security training and IS security policy development) are for the prevention of internal IS security breaches, and the third area (IS security technology) is for the prevention of external IS security breaches.

3.2 Goal of IS security investment

Since IS security breaches can cause enormous losses to organizations, investments in IS security are then made to block the potential damaging attacks and breaches. However, it should be noted that no matter how much and how well a firm spends on IS security, there is no guarantee that all potentially damaging attacks and breaches will be prevented (Huang *et al.*, 2007). Therefore, the first goal of IS security investment is to reduce the risk to an acceptable level.

The financial and reputational losses associated with large-scale data breaches make executives acutely aware of the need to protect corporate information assets. IS security investment is helpful in building an organization's reputation and saving economic losses. Chai *et al.* (2011) have shown that IS security investment leads to positive abnormal returns for firms, and the abnormal returns are higher after the Sarbanes–Oxley Act (SOX) than any of those preceding it. However, overprotection of data may cause problems in business, such as low productivity of employees, which hinder business operations. So the second goal of IS security investment is to align investment with business goals and objectives, simultaneously securing information assets while still allowing the business to maintain regular function.

The third goal for IS security investment is to ensure compliance. Security managers are faced with the complex challenge of meeting multiple compliance requirements from a growing array of federal, state, and industry standards. For example, the Australian Government information security management core policy states, with regard to the mandatory requirement for compliance:

Agencies must ensure that agency information security measures for all information processes, ICT systems and infrastructure and adhere to any legislative or regulatory obligations under which the agency operates.

Therefore, IS security investment is not exclusively about reducing risks; rather it is a balancing act between operations (business requirements), governance (security requirements), and compliance (legal compliance).

The fourth goal for IS security investment is to maintain cultural fit. As discussed above, one area in which to invest in IS security is in the education and training of employees' IS security awareness. Employees usually tend to behave in ways consistent with corporate values. Cultural conflict may occur, however, when the values associated with IS security awareness training/education do not match those of the company. If IS security awareness training/education do not fit the organizational culture, employees may behave inconsistently with IS security policies and standards. Therefore, IS security investment programs should be deployed in harmony with the prevailing cultural values of their organizations. Otherwise, conflicts may occur between the demands of the IS security program and the values of the organizations.

To sum up, the four primary goals of IS security investment include reducing the risk to an acceptable level, aligning with business goals and objectives, maintaining compliance, and ensuring cultural fit. The goals should be considered when training employees' IS security awareness, developing IS security policy, and implementing IS security technology.

3.3 Intangible benefits of IS security investment

Although it may be possible to quantify the costs of IS security investment, it is difficult to quantify the benefits from IS security investment. One reason is that IS security investments usually do not generate economic benefits in the sense of revenue generation or cost reduction. Huang *et al.* (2007) concluded that IS security investment has an intangible return, because the value of IS security investment lies in "preventing something from happening," not in "making something happen." Thus, the payoff of IS security investment can only be measured by "avoiding potential loss." When no security attacks occur, it is difficult to say whether the investment is working. For example, an important role of IS security technology is prevention; yet, it is difficult to determine whether reduced threats result from the implementation of IS security technology or from the lack of outsider threats at that time.

Second, the payoff period of IS security investment is ambiguous. The payoff period refers to the length of time required to recoup the funds expended in an investment, or to reach the break-even point. Some types of benefits require a

longer period of time to be identified. Take IS security policy development, for example; as the development of an IS security policy is sometimes framed in a life-cycle context with an emphasis on development, enforcement, and maintenance, it is difficult to measure whether the policy development is effective while it is an ongoing process. Additionally, a goal of IS security policy development is to ensure that employees clearly understand it and will thus comply with it. However, employees' compliance with IS security policy is connected with training. Hence, employees' compliance with IS security policy is a conjunct benefit of training and policy development.

For the reasons above, traditional economic analyses of the value of IT investment (Barua *et al.*, 1991; Brynjolfsson & Hitt, 1996; Pavlou *et al.*, 2005) as well as conventional accounting measures (Gordon & Loeb, 2002) often do not apply to IS security.

4 Research gaps

Three gaps in research are discussed in this chapter. The first gap in the research arises from the ignorance of IS security investment characteristics in prior work. The second problem arises from the conflicts between neoclassical economics assumptions between IS security investment characteristics. The third problem arises from the neoclassical economics assumptions *per se*, which have been challenged as lacking realism (Gurrien, 2002; Sapir, 2002; Hodgson, 2002).

4.1 Neglect of IS security investment characteristics

In Chapter 2, it is noted that prior work is based on the neoclassical framework for decision-making, by assuming that decision makers have a rational preference and complete information to seek the maximum benefit/utility. However, prior work did not consider IS security investment characteristics. Table 20 in Appendix 2 presents a detailed analysis about this.

Most previous studies considered general IS security investment without addressing specific areas (e.g., Gordon & Loeb, 2002; Wang *et al.*, 2009; Willemson, 2010, etc.). Some studies considered only IS security technology as the area in which to invest. For example, Kort (1999) considered security equipment investment, Bojanc *et al.* (2012) considered security technology investment, Cavusoglu *et al.* (2004, 2005) considered intrusion detection system investment, and Hausken (2006) considered information security technology investment.

Prior work considered the maximization of benefits (or minimization of the costs) as the investment goal of IS security investment. No other investment goals were addressed.

None of previous studies discussed the intangible benefits of IS security investment.

4.2 Conflicts between neoclassical framework and IS security investment characteristics

The utility/payoff maximization assumption implies that a decision maker can compute the value of utility associated with IS security investment. However, the assumption conflicts with the intangible benefits of IS security investment, IS security investment goals, and IS security investment areas.

First, the intangible benefits of IS security investment determine that it is difficult to value the anticipated consequences accurately. Even risk analysis, which has been the key technique for justifying the benefits of IS security investment, is considered to be simple guesswork (Baskerville, 1991). Because the basic concepts of risk analysis (risk probabilities and loss estimates) are highly interpretive—often gleaned whole by the professional from an unstructured study of the complex multivariate organizational landscape. Therefore, it is impossible to compare the utilities/payoffs and select the greatest. Additionally, losses from IS security investment breaches can potentially be significant, and their recovery may require an unspecified length of time. The long-term effects of IS security breaches may also make it difficult to accurately estimate the related monetary damages. For example, Lee *et al.* (2011) found that it is difficult to quantify monetary damages related to customers.

Second, utility/payoff maximization conflicts with IS security investment goals and areas. IS security should be invested to align with business need, but there are more objectives to be achieved than just the maximization of profit. Improving employees' IS security awareness may not directly add value to a business, but it is still important. In addition, there are certain other important aspects (such as organizational culture) that need attention, even though they cannot be evaluated by profits.

4.3 Problems of preference and complete information assumptions per se

4.3.1 Rational preference

A comprehensive, consistent utility function means that a decision maker has a stable, well-defined preference. Consistent preference refers to the assumption that, in the presence of complete information, people act as if they could look up their preferences in a book and respond to situations accordingly: choose the item most preferred; pay up to the value of an item to obtain it; sell an item if offered more than its value; and so on (Tversky & Thaler 1990).

However, the assumption of consistent preference is challenged by the presence of many anomalies (Tversky & Thaler, 1990). Prospect theory (Kahneman & Tversky, 1979) shows that humans' preferences may reverse in response to risk, framing, and loss. Kahneman and Tversky (1979) found that humans are risk-

averse in front of gains, but risk-seeking in front of losses; moreover, they found that humans change their preferences in front of different framing and that most people are more sensitive to losses than gains.

Additionally, experimental studies suggest that people have time-inconsistent preferences (Thaler, 1981; Loewenstein & Prelec, 1992). Humans prefer immediate utility over delayed utility (Frederick et al, 2002). This means that when two rewards are distant in time, people act relatively patiently (e.g., they prefer two apples in 101 days, rather than one apple in 100 days). However, when both rewards are expected sooner, they act more impatiently (e.g., they prefer one apple today, rather than two apples tomorrow). Hence, these individuals place greater weight on earlier rewards as it gets closer.

Khan *et al.* (2012) studied the effects of time-inconsistent preferences on investments in information technology infrastructure. They found that managers are more likely to exercise options early when the net payoffs are low, and that managers are more likely to exercise a growth option early in its life when a project is performing well. Given that there is a long-term effect related to the loss of IS security investment, there is reason to believe that managers' preferences will change in the long term.

4.3.2 Complete information

The costs of searching for information are enormous, and therefore, information is considered to be asymmetric and incomplete in the real world (Stiglitz, 1985). As a result, different parties cannot access each other's information without cost. The increasing complexity of the socio-economic environment makes it progressively less possible for a single decision maker to consider all the relevant aspects of a problem.

Likewise, information is asymmetric in IS security investment. Wang *et al.* (2008) argued that the rationality of hackers is difficult to capture, as they may be motivated by a different value system. They may be rational, but not in financial terms. For example, they may be driven by motivations other than money, and as such, it can be difficult for IS security managers to determine a hacker's cost function for attacking the system. Indeed, research shows that hackers are typically motivated by ideological values (Xu *et al.*, 2013).

Information is also incomplete in IS security investment. An IS security investment decision is usually made without all the necessary information. For example, implementing IS security investment management standards is justified

by appealing with best practice, practitioners have no evidence to analyze the popular IS security investment management standards (Siponen & Willison, 2009). Even the “research process,” if there is one, is not explained (Siponen, 2006). Thus, practitioners have no information with which to evaluate IS security investment management standards.

In sum, previous studies have applied a problematic theoretical background that conflicts with IS security investment characteristics. The next section outlines guidelines for future research on IS security investment, highlighting IS security investment characteristics.

5 A preliminary framework for IS security investment

Chapter 4 shows that the neoclassical economics framework of decision-making is not an appropriate framework on which to base IS security investment research; moreover, the chapter shows that prior work did not consider IS security investment characteristics. The aim of this chapter is to develop a new framework for IS security investment, which overcomes the gaps in the research discussed in Chapter 4.

This chapter draws together the constituent factors to be included in the preliminary framework for depicting IS security investment. First, assumptions about the IS security investment decision makers are proposed based on behavioral economics; these assumptions are intended to overcome the problems associated with the neoclassical economics assumptions about decision makers. Thereafter, a discussion of the consistency of IS security investment characteristics and assumptions about decision makers follows. The subsequent section provides a description of the preliminary framework that depicts IS security investment and attempts to shed some light on the research question.

5.1 How does behavioral economics view decision-makers?

Behavioral economics increases the explanatory power of economics by providing more *realistic* psychological foundations, and it is believed that, with all things being equal, better predictions are likely to result from theories that are based on more *realistic* assumptions (Camerer & Loewenstein, 2002). Three bounds of human nature are studied in behavioral economics: bounded rationality, bounded willpower, and bounded selfishness (Mullainathan & Thaler, 2000).

As an early critic of the economic model that posits that people have unlimited information processing capabilities, Simon (1955) suggested the term “bounded rationality” to describe a more realistic concept of human problem solving capabilities. Since economic actors have limited brainpower and time, they cannot be expected to solve difficult problems optimally. It is then “rational” for economic actors to adopt rules of thumb as a way to increase the efficiency of cognitive

faculties. There are a number of examples regarding judgment and choice⁶ that illustrate that people are not as rational as assumed by neoclassical economics. Indeed, judgment diverges from rationality in many ways (see Kahneman, Slovic, & Tversky, 1982). Some illustrative examples include overconfidence, optimism, anchoring, extrapolation, and making judgments of frequency or likelihood based on salience (the availability heuristic) or similarity (the representativeness heuristic). Many of these departures from rational choice are addressed by prospect theory (Kahneman & Tversky, 1979), a descriptive theory of how people make choices under uncertainty. Prospect theory states that people make decisions based on the potential value of losses and gains rather than on the final outcome, and that people evaluate these losses and gains using certain heuristics.

Neoclassical economics assumes that economic actors make the optimum choice. However, in the real world, humans—even when they know what is best—sometimes fail to make the best choice because of a lack of willpower (Mullainathan & Thaler, 2000). Bounded willpower refers to the tendency to make decisions that are in conflict with one's long-term interests. For example, bounded willpower can lead to addictive behavior, under-saving, or procrastination.

Finally, behavioral economics sees economic actors as bondedly selfish (Mullainathan & Thaler, 2000). Neoclassical economists stress self-interest as the primary motive. For instance, the free rider problems widely discussed in economics are predicted to occur because individuals cannot be expected to contribute to the public good unless their private interests are thus improved. However, people often act selflessly, contradicting the assumption that self-interest is a primary motivating factor. For example, people donate to earthquake stricken areas or do volunteer work.

To conclude, behavioral economics highlights three important ways in which people deviate from the assumptions of neoclassical economics (Mullainathan & Thaler, 2000). *Bounded rationality* reflects the limited cognitive abilities that constrain human problem solving. *Bounded willpower* describes the fact that people sometimes make choices that are not in their long-term best interests. *Bounded self-interest* incorporates the comforting notion that humans are often willing to sacrifice their own interests to help others.

⁶ *Judgment* refers to the processes people use to estimate probabilities, and *choice* refers to processes people use to choose between actions, taking into account any relevant judgments they may have made (Camerer & Loewenstein, 2002).

5.2 Assumptions about IS security investment decision-makers

An earlier chapter revealed that neoclassical economics assumptions about IS security investment decision makers are problematic. New assumptions about IS security investment decision makers have thus been developed based on behavioral economics.

Behavioral economics uses *bounded rationality* to describe human problem solving capabilities (Mullainathan & Thaler, 2000). With regard to IS security investment, a decision maker's *bounded rationality* results not only from cognitive limitations, but also from the intangible nature of IS security. According to bounded rationality, IS security investment decision makers have uncertain perceptions about their own preferences and the environment. First, due to cognitive limitations, a decision maker may allow for a range of attribute weights for the conditional utility functions. Second, because of the intangible nature of IS security, a decision maker is uncertain about risk and value judgments on one or more attributes. Third, due to cognitive limitations as well as the intangible nature of IS security, a decision maker may not be sure about how to evaluate the consequences of an alternative.

Behavioral economics uses *bounded self-interest* to describe the notion that people are often willing to sacrifice their own interests to help others (Mullainathan & Thaler, 2000). In terms of IS security investment, a decision maker's *bounded self-interest* is reflected in the balance of four subgoals of IS security investment. It is assumed that the decision maker will choose an alternative that meets or exceeds a set of minimum criteria, if he or she chooses a satisfactory alternative, but not one that is necessarily unique or the best. In general, this satisficing hypothesis is accompanied with searches for alternatives and for new information (learning). Satisficing is also compatible with incomplete ordering of alternatives and with multiple criteria of choice. An individual's satisfaction with respect to the desired level of aspiration is supported by a range of evidence from experimental economics (e.g., Tversky & Kahneman, 1986).

Therefore, in this chapter a satisfactory solution assumption is developed to overcome the gaps in the neoclassical assumptions about decision makers. Satisfactory solution assumption suggests that *a decision maker, with regard to IS security investment, has inaccurate knowledge and incomplete information about the consequences of IS security investment and makes an IS security investment decision that is expected to be satisfactory.*

The satisfactory solution assumption absorbs concepts from behavioral economics. As illustrated in the satisfactory solution assumption, a decision maker

has incomplete information and inaccurate knowledge about IS security investment, which reflects his limited capability to solve problems. Additionally, a satisfactory solution reflects a decision maker's bounded willpower. Table 3 compares the satisfactory solution assumption with neoclassical assumptions.

Table 3. A Comparison of assumptions

Assumptions about decision makers	Neoclassical economics	Satisfactory solution assumption
Goal	To obtain maximum benefit from IS security investment	To achieve a satisfactory solution
Precondition 1	Complete information about decision maker's own preference and the environment (consequences of IS security investment)	Incomplete information about one's own preferences and the environment
Precondition 2	Complete knowledge, such that decision maker could accurately predict the value of all consequences	Inaccurate knowledge about the consequences of IS security investment due to limited cognitive ability and the intangible nature of IS security investment benefits

5.3 A preliminary framework for IS security investment

A preliminary framework for IS security investment can be divided into two broad categories: assumptions about decision makers and characteristics of IS security investment. These assumptions and characteristics were identified in previous chapters and empirically supported by earlier findings. Figure 3 below shows how the characteristics of IS security investment and underlying assumptions about the decision makers are interconnected.

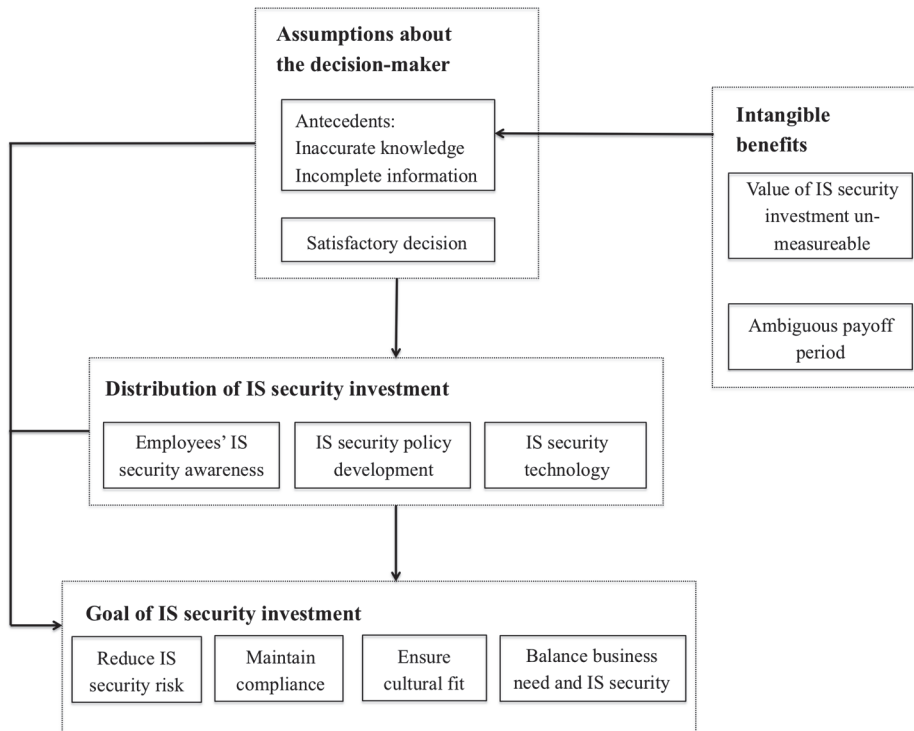


Fig. 3. The preliminary framework of IS security investment.

As shown in Figure 3, the two categories of the preliminary framework (assumptions about the decision makers and characteristics of IS security investment) are connected to each other in multiple ways. First, the intangible nature of IS security investment benefits helps to illustrate that a decision maker of IS security investment has inaccurate knowledge and incomplete information about the consequences of IS security investment. Second, a satisfactory solution of IS security investment needs to consider balancing four subgoals of IS security investment. Third, investing in each of the three areas of IS security (employees' IS security awareness, IS security policy development, and IS security technology) also aims to achieve the four subgoals of IS security investment.

There is an inherent logic in the preliminary framework of IS security investment: gathering information about the benefits of IS security investment is difficult, and hence, there is always a tradeoff between allocating time and resources with gathering further information and proceeding to act on the basis of current information. A similar tradeoff occurs between the investment of time and

resources necessary to enhance a decision maker's computational capacities with education or training. Hence, the decision maker of IS security investment satisfies by seeking an attainable solution through the balance of the four subgoals of IS security investment. In the complicated and changing environment of organizations, IS security investment decision makers are highly unlikely to have the information or computational power to discover or maintain an optimal profit-maximizing solution.

Compared to the neoclassical economic framework that influenced prior work, the preliminary framework developed in this thesis overcomes the research gaps depicted in Chapter 4. The concerns regarding preference and complete information are overcome with the development of a satisfactory solution assumption about decision makers. Furthermore, the satisfactory solution assumption does not conflict with the characteristics of IS security investment.

To summarize this section, the preliminary framework depicted in Figure 3 describes key elements of IS security investment by employing characteristics of IS security investment and assumptions about decision makers.

With the help of Figure 3, this chapter shed some light on the research question presented in Chapter 1. Figure 3 can be used to identify how the characteristics of IS security investment and the assumptions about decision makers influence the decision-making of IS security investment. In later chapters, empirical studies are used to test the assumptions about IS security investment decision makers and how the framework influences decision-making of IS security investment; and thus, an empirically grounded framework can be synthesized accordingly.

6 Research methodology

The central focus of this chapter is on the empirical research design, beginning with an explanation of the delivery of the empirical research. This chapter concludes by providing a description of the survey design, construct operationalization, pretest, and the data collection procedure. A more detailed discussion about the research methodology is presented in sections 7.3 and 8.3.

6.1 Survey-based research design and data collection procedure

The new framework and its assumptions were examined using a survey methodology. First, a field survey was used to collect data for the current research. The field survey occurred over a period of four months, from mid-January 2013 to April 2013. The survey was randomly sent to 1042 Finnish companies. All the respondents were IS security investment managers who were familiar with IS security investment management (for more details, see section 7.3.3). Completed surveys were returned by the respondents using envelopes with pre-paid postage.

In addition to a field survey, another survey was used to collect data to test the assumptions in a different research setting. An online survey was conducted to collect data for the current research. The aim of the online survey was to understand the extent to which the integration of different theoretical perspectives could capture piracy intention. Rather than collecting data through a paper-and-pencil questionnaire, an online survey was used for two reasons: First, the process of uploading unauthorized digital products to online communities relies heavily on Internet use. In this particular context, using online surveys can maintain consistency between the research context and the data collection context. Second, the behavior involved in uploading unauthorized digital products is generally regarded as unethical and/or illegal. Surveys of this type of behavior should take into consideration the anonymity and confidentiality of respondents. Online surveys, in comparison to traditional paper-and-pencil surveys, can better ensure the anonymity of respondents and the credibility of their answers (Kwong, 2009; Lin, *et al.*, 1999). Data was collected from randomly invited people. There were 275 responses obtained through an online channel. Among these responses, 55 were considered to be invalid, as these subjects spent less than 5 minutes⁷ in completing

⁷ We tested and showed that finishing the survey requires at least 10 minutes.

the survey. After removing these 55 invalid responses, 220 valid responses were used in the data analysis.

6.2 Construct operationalization

The reliability of constructs can be improved by using previously validated and tested questions (Straub, 1989, Boudreau *et al.*, 2001). Accordingly, previously validated instruments from the literature were utilized. For the field survey (Chapter 7), the items measuring herding behavior were adapted based on Sun (2013). Reputation items were adapted from Zinko *et al.* (2012). Mandatory measures were adapted from Boss *et al.* (2009). Three items measuring the behavior (i.e., investment) were adapted based on Beaudry and Pinsonneault (2010). For the second survey (Chapter 8), two items were adapted from Venkatesh *et al.* (2008) to measure uploading behavior. Here, the frequency and intensity of uploading behavior were used. Sanctions were considered a formative second-order construct consisting of three dimensions: the first two, punishment certainty and severity, were adapted from D'Arcy *et al.* (2008), and the third, punishment celerity, was adapted from Nagin and Pogarsky (2001). Warm glow was considered to be a formative second-order construct consisting of four dimensions: affective feelings, role merger, subjective norms, and moral norms were all adapted from Ferguson *et al.* (2012). All the measures used a 7-point Likert scale.

However, some constructs had not been previously validated. As such, for this thesis, new instruments were developed for them. Appendix 3 describes in detail how the instruments were developed following the procedures from Mackenzie *et al.* (2012).

6.3 Pretest

For the field survey, a pretest survey was conducted at Oulu University in Finland. A total of 32 responses were collected. The purposes of the pilot study were twofold: to ensure that the questionnaire was properly compiled and to have a reliability assessment of the scales. To achieve the first goal, an open question was included that allow subjects to comment on the wording, content, and length of the questionnaire. Revisions to the questionnaire were made accordingly. To assess the reliability of the scales, Cronbach's alpha (Cronbach, 1970) was utilized, which is, according to Moore and Benbasat (1991), "fairly standard in most discussions of reliability." Thirteen items with low inter-item and item-total correlations, high

“Cronbach’s alpha if item deleted” statistics, or small standard deviation scores (and thus low explanatory power) were deleted with content validity in mind.

For the second survey, a pretest was conducted also at Oulu University in Finland. A total of 39 responses were collected. Items with low inter-item and item-total correlations, high “Cronbach’s alpha if item deleted” statistics, or small standard deviation scores (and thus low explanatory power) were deleted.

7 Motivating IS security investment – A field study

The severity of IS security breaches continues to increase. However, investment in IS security has not kept up its pace. According to *The Global State of Information Security Survey 2014*, loss or damage of internal records jumped 77% in 2012. The 2014 Cost of Data Breach Study revealed that the average cost to a company was USD\$3.5 million in 2014, 15% more than what it cost in 2013. However, despite potential consequences, many companies have not implemented technologies and processes that could provide insight into today's risks (*The Global State of Information Security Survey 2014*). For instance, 31% of respondents (companies) have no centralized data storage; 37% of respondents have no asset-management tools; and 38% of respondents have no data loss prevention tools. Forty-nine percent of respondents use cloud computing, but only 22% include provisions for cloud computing in their security policies. Therefore, the IS security budget represents only 3.8% of total IT expenditure in 2014. Information Security Forum (ISF) 2013 reported that the number one IT security challenge in the future will be insufficient resources for IT security investments.

Prior studies established economic models to solve the problem of inadequate investment in IS security. For example, Gordon and Loeb (2002) suggested using cost-benefit analysis, and Huang *et al.* (2008) suggested using expected utility analysis. However, it is difficult to apply such analyses because IS security investment has intangible benefits, and no reliable actuarial loss statistics exist (Wood & Parker, 2004). The literature on behavioral decision-making suggests that when there is not enough information to make a decision, herding behavior may be the most effective choice (Bikhchandani & Sharma, 2000). Herding behavior exists in various economic situations in which an organization's decision-making is markedly influenced by the decisions of others, such as in financial investment, technology adoption, firms' strategic decisions, and so on (Duan *et al.*, 2009). In IS security investment, managers tend to follow the recommendations and decisions of many "smart cookies," such as IS security investment experts and big companies.

According to management fashion theory, idea entrepreneurs (such as consultants, gurus, journalists, and academics) compete in a market for providing management knowledge. They sense managers' demands for new management techniques and produce discourse that promotes the use of certain techniques to help narrow performance gaps. For example, ISO-IEC 27002 provides best practice recommendations for information security management to all types and sizes of

organizations. Organizations can adopt information security controls by following ISO-IEC 27002 recommendations, one of which is to have an employee security awareness training program. According to *The Global State of Information Security Survey 2015*, in 2014, 51% of companies that responded had a security awareness and training program, and 57% of companies that responded required employees to complete training on privacy policies.

Sometimes organizations may adopt information security technology by following other organizations' practices. Studies have shown that organizations have a tendency to chase the hottest IT (Wang, 2010). *The Global State of Information Security Survey 2014* shows that 88% of respondent companies invest in application firewalls; 70% of respondent companies invest in malware or virus-protection software; and 63% of respondent companies invest in network access control software, identity management technology, and encryption of desktop PCs already in place. Additionally, 19% of respondent companies have no asset-management tools, but they plan to implement these in the next 12 months, and 29% of respondent companies have no identity management strategy, but they also plan to implement these in the next 12 months.

This chapter is a field study to understand IS security investment by drawing on the reputational herding theory (Scharfstei & Stein, 1990). Reputational herding theory suggests that if an investment manager is uncertain about a decision regarding an investment, conformity with other investment professionals is a good choice. This is because of the theory's key assumptions that there are systematically unpredictable components to the value of an investment, and that smart managers make similar decisions. Managers will be evaluated more favorably if they make the same decision as the others: share the blame.

One aim of this chapter is to show the factors that influence IS security managers' investment decisions. IS security investment decisions are usually made by senior managers. Because their investment decisions are not immune to agency and incentive problems, they may imitate others' decisions to enhance their professional reputations if the situation warrants it. Additionally, in many scenarios, IS security investment managers have to make their investment decisions with very limited information; because IS security investments are highly specialized tasks that involve a lot of perspectives, there are also significant information asymmetries between the decision makers (IS security investment managers) and their supervisors (the firm's owner or board). Furthermore, the economic payoffs of IS security investments are difficult to observe or measure in the short term, which

gives managers more room to enhance their reputations at the expense of their companies.

This chapter also discusses the test of the new assumptions developed for the preliminary framework. By demonstrating the significance of herd behavior in IS security investment, this chapter shows that benefit maximization is not the aim (or at least not the only aim) of IS security investment.

7.1 Related work

This section will briefly describe the literature relevant to this study. Previous IS security investment research provided analytical tools to assess how much to invest in IS security and to evaluate the efficiency of the investment; however, previous IS security investment research did not study motivations behind IS security investment. Herding behavior has previously been studied in IS research by applying network effects, informational cascades, and herd behavior theory. However, reputation was not considered in previous work.

7.1.1 IS security investment studies

IS security investment studies have addressed topics ranging from the identification of the optimal level of IS security investment to the effectiveness of IS security investment. Previous studies in these two areas, however, focused more heavily on the analytic tools than on motivation factors for IS security investment.

Optimal IS security investment

As shown in Chapter 2, studies that investigated the optimal level IS security investment utilized the decision-theoretical and game-theoretical approaches and applied neoclassical economics assumptions. In prior work, functions of benefit/utility/profit are usually used to describe rational preference. For example, Gordon and Loeb (2002) built a function of expected benefit of information security investment. Huang *et al.* (2008) used a function of expected utility. Cavusoglu *et al.* (2004) developed functions of expected payoff for both the firm and the hacker. Cremonini and Nizovtsev (2006) established a function of expected payoff for hackers.

In decision-theoretical studies, it is usually assumed that firms will maximize their expected net benefits (e.g., Gordon & Loeb 2002; Willemsen, 2006) or profits

(e.g., Bohme & Felegyhazi, 2010; Lee *et al.*, 2011). In game-theoretical studies, it is assumed that both players will maximize their payoffs (e.g., Cavusoglu *et al.*, 2004) or profits (e.g., Hausken, 2006; Cavusoglu *et al.*, 2008). In some studies, it is assumed that firms will minimize their costs (e.g., Cavusoglu & Raghunathan, 2004; Bandyopadhyay *et al.*, 2005; Cavusoglu *et al.*, 2005; Liu *et al.*, 2005; Liu *et al.*, 2011).

Complete information is not directly mentioned in decision-theoretical studies. But complete information is implicitly applied in game-theoretical studies, in which the solution to the game involves maximization (or minimization) of a polynomial function. For this to occur, the firm needs to know the hacker's payoff function, and vice versa (e.g., Cavusoglu *et al.*, 2004; Cavusoglu & Raghunathan, 2004; Bandyopadhyay *et al.*, 2005; Cavusoglu *et al.*, 2005; Liu *et al.*, 2005; Cremonini & Nizovtsev, 2006).

The effectiveness of IS security investment

In the literature, the effectiveness of IS security investment is usually evaluated in terms of ROI-type metrics (Gordon & Loeb, 2006; Purser, 2004; Mizzi, 2010; Sonnenreich *et al.*, 2006; Davis, 2005). The term "Return on Investment (ROI)," which is defined as the calculation of the financial return from an investment based on the financial benefits and costs of that investment, is usually used to refer to the measures of how effectively capital is being used to generate profit. Focusing more closely on investment security, Davis (2005) developed the term of return on security investment (ROSI), which is defined as the calculation of the financial return from an investment in security, such as an initiative or project, based on the financial benefits and costs of that investment. : Purser (2004), arguing that ROI did not take into consideration the effects of changes in risk associated with business initiatives, proposed the concept of a total return on investment (TROI) to take into account the financial impact of changes in risk. Moreover, Sonnenreich *et al.* (2006) proposed the concept of return on security investment (ROSI), which takes into account risk exposure and risk mitigation in the calculation of ROI, and also outlined techniques to quantitatively measure risk exposure and mitigation. Mizzi (2010) contributed to the discussion of the "viability of security expenditure," "successfulness of attack," and "motivation to attack" and developed the concept of return on information security investment (ROISI).

7.1.2 Herding behavior in IS research

Herding behavior, in which investment decision makers follow the decisions of earlier adopters (Kauffman & Li, 2003; Swanson & Ramiller, 2004), has been observed in IT adoption, such as in the downloading of popular software products (Duan *et al.*, 2009), in the adoption of wiki systems (Sun, 2013), and in general purchasing decision making (Shen *et al.*, 2014). Network effects (Au & Kauffman, 2001; Gallagher & Wang, 2002; Kauffman *et al.*, 2000), information cascades (Duan *et al.*, 2009), and herding behavior (Sun, 2013; Shen *et al.*, 2014) have been used to study such imitative behavior.⁸

Au and Kauffman (2001) examined the adoption of electronic bill presentation and payment technology and suggested that network effects play a significant role: the more billers that adopt the technology, the more consumers are willing to use the services. Gallagher and Wang (2002) studied the way that network externalities influence two-sided software pricing and found that significant positive network externalities exist in the web server market. Kauffman *et al.* (2000) empirically examined the impact of network externalities and other influences that combine to determine network membership and supported the network externalities hypothesis. They found that banks in markets that can generate a larger effective network size and a higher level of externalities tend to adopt a network early, while the size of a bank's own branch network decreases the probability of early adoption.

Walden and Browne (2002) suggested that the concept of informational cascades play a significant role in influencing firms' adoption of electronic commerce technologies. Kauffman and Li (2003) proposed a theoretical framework for the herding behavior observed in IT adoption and identified informational cascades theory as a new perspective to explain the dynamics of IT adoption. Li (2004), taking an explorative approach, focused on examining the influence of informational cascades in IT adoption and the business implications. He also explored various scenarios in IT adoption, in which informational cascades may interact with other mechanisms, such as network effects and word of mouth (WOM) effects. Konana and Balasubramanian (2005) referred to informational cascades theory in developing a social-economic-psychological model to predict technology adoption in online banking. Informational cascades theory is also associated with the institutional theory of mimetic isomorphism, in which institutions tend to imitate one another in technology decision-making (DiMaggio

⁸ A comparison of the three concepts is shown in the next section.

& Powell, 1983; Swanson & Ramiller, 2004; Tingling & Parent, 2002). Both theories share the characteristics of peer influences and uncertainty in the decision-making process. Duan *et al.* (2009) empirically examined informational cascades in the context of online software adoption and found that user behavior in adopting software products is consistent with the predictions of the informational cascades literature.

Sun (2013) developed a longitudinal study of herding behavior in the adoption and continued use of technology. Two concepts were proposed to describe herd behavior in technology adoption: discounting one's own information and imitating others. Sun's findings suggested that the acts of discounting one's own information and imitating others are provoked primarily by the observation of prior adoptions and perceptions of uncertainty regarding the adoption of new technology. Similarly, Shen *et al.* (2014) studied information adoption from the perspective of herd behavior and found that the acts of discounting one's own information and imitating others posit significant influences on the adoption of online reviews.

7.2 Theoretical framework

7.2.1 Conceptualization: reputation-based herding

Herd behavior has been observed in a variety of situations, such as in the selection of retirement investments (Choi *et al.*, 2003), the opening of new bank branches (Chang *et al.*, 1997), the development of prime-time television programs (Kennedy, 2002), and the downloading of software applications (Duan *et al.*, 2009; Walden & Browne, 2007).

Bikhchandani and Sharma (2000) summarize herding as an individual herd when knowledge that others are investing changes one's decision from not investing to making the investment. Sun (2013) extracted two aspects from the definition of herding: imitating others and discounting one's own information. "Imitating others" refers to the notion that a person who is herding observes others and makes the same decisions or choices that the others have made. "Discounting one's own information," in terms of herding, refers to the notion that people may be less responsive to their own private information and favor a processor's action. However, when making a decision, people depend more often on a combination of their own information as well as their observations of the behavior of others. It is less common that people simply discount their own information, as their own

information indicates how the investment would benefit their own needs. Therefore, herd behavior does not necessarily include discounting one's own information. As such, herd behavior is conceptualized in this thesis as imitating others.

Scharfstein and Stein (1990) developed the reputational herding model, in which they suggested that managers with good reputations are more conservative in bucking the consensus and herd to protect their current status. Accordingly, reputation-based herding is conceptualized in this thesis as *a person who concerns for his/her reputation observes others and makes the same decisions or choices that others have made.*

Prior research has identified four antecedents for reputational herd behavior: an ability to analyze an investment decision, a manager's reputation, the strength of prior information, and the level of correlation across informative signals.

Ability to analyze an investment decision. When managers are unable to accurately assess the value of an investment, they may be uncertain about the investment. This may be a result of incomplete information or asymmetric private information (Bikhchandani & Sharma, 2000; Fiol & O'Connor, 2003; Lieberman & Asaba, 2006; Walden & Browne, 2009). Managers are more likely to herd when they are uncertain about the decision that needs to be made (Sun, 2013).

Managers' reputation. Managers with good reputations are more likely to herd. This is because after managers have made an investment decision, their reputations are updated based on two pieces of evidence: (1) whether the manager made a profitable investment and (2) whether the manager's behavior was similar to or different from that of other managers (Bikhchandani & Sharma 2000). If there are systematically unpredictable components of the investment value (as in the case of IS security investment), the first piece of evidence will not be used exclusively. Hence, the second piece of evidence is important as well. Holding the absolute profitability of the investment choice as fixed, managers will be evaluated more favorably if they adopt the decisions of others than if they behave in a contrarian fashion. Thus, an unprofitable decision is not as bad for a reputation when others make the same mistake—they can share the blame if there are systematically unpredictable shocks.

Strength of prior information. A high level of correlation across informative signals refers to the notion that many people have made the same decision. This is a necessary condition for herd behavior to occur.

Correlation across informative signals. When aggregate information is strongly held and reinforced by the actions of the market leader, people are less likely to take an opposing view based on private information.⁹

7.2.2 A comparison to similar concepts and theories

Concepts that refer to people’s mimicking behavior include more than just reputational herd behavior. It is essential to have a comparison of the differences between similar concepts. Table 4 presents a comparison of reputational herd behavior, information cascade, and payoff and network externalities.

Table 4. Comparison of reputational herd behavior, information cascades, and payoff and network externalities

	Reputational Herd Behavior	Information Cascade	Payoff and Network Externality
Definition	Managers concerned about their reputation engaged in IS security investment to enhance their professional reputations.	Managers ignore their own private information that is overwhelmed by publicly observable information and instead mimic other organizations' actions.	A manager's IS security investment affects the payouts to others of doing IS security investment.
Aspect emphasized	Managers' incentives of reputation concern	Information externality and social learning	Network effects
Theoretical foundations	Information economics; contracting; agency theory	Information economics; agency theory; Bayesian learning	Payoff interdependency; economies of scale
Information source	Prior IS security investments from other organizations	Prior IS security investments from other organizations	Those organizations that can benefit from the IS security investments
What information is inferred from others	Estimated value of IS security investment	Estimated value of IS security investment	Benefits from more organizations that invest on IS security
How information is inferred from others	By observation	By observation	By observation and direct communication

⁹ The private information may be the conclusions of an investor’s research effort (Bikhchandani & Sharma, 2000).

	Reputational Herd Behavior	Information Cascade	Payoff and Network Externality
The impact of the number of others	The greater the number, the greater the influence on others	The greater the number, the greater the influence on others	In general, the more prior adopters, the greater the influence of others, and the higher perceived value of the decision. However, it has network congestion.
Motivations	To overcome uncertainty and to maintain reputation	To overcome uncertainty	To enjoy the increased value associated with the enlarged user base

Network externalities tend to reward herding decisions by increasing the payoffs to those who associate themselves with the majority. Herding in the presence of network externalities also decreases the risks of being stranded with user bases that are too small.

Network externalities differ from reputational herding in several ways. First, the value-adding mechanism is not necessary in reputational herding. The motivation for reputational herding is to overcome uncertainty and to maintain a reputation. Additionally, there is no necessary value added by reputational herding. Second, they share different theoretical backgrounds. Reputational herding occurs because of agency problem from information asymmetries, while network externalities result from economies of scale.

Another similar concept is informational cascades. The only difference between reputational herding and informational cascades is that the former places managers' concerns for their reputation in addition to the latter. Informational cascade models demonstrate how herding arises out of information asymmetries and the problems associated with observational learning. And reputational herding models show that herding may be caused by managerial incentive problems and thus builds a bridge between agency theory and rational observational learning.

Figure 4 shows a paradigm of relationships with the three concepts. These concepts are neither exhaustive nor mutually exclusive. Reputational herding is about maintaining a good reputation, and such a desire for a good reputation can cause payoff interactions, making III a subset of II (Scharfstein & Stein, 1990).

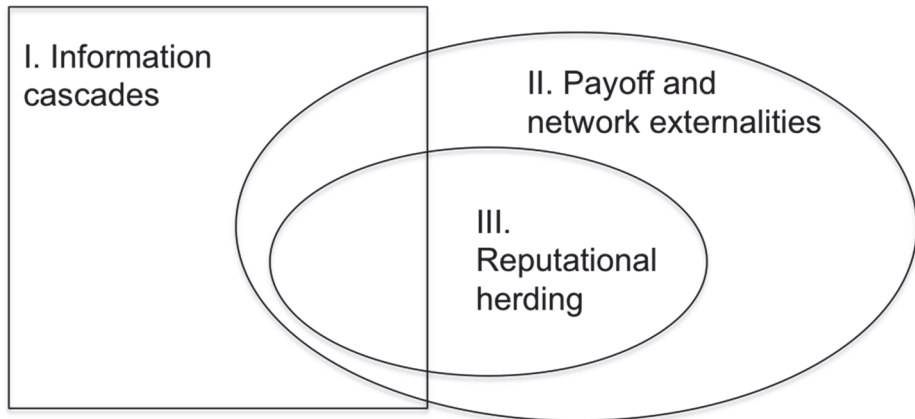


Fig. 4. Hierarchy of the three concepts.

7.2.3 Research model and hypotheses

Research model

In order to better understand IS security investment decision-making in organizations, we use reputational herding theory as previously described (Scharfstein & Stein, 1990) as the basis for our theoretical model (Figure 5). Reputational herding theory was developed first in explaining corporate investment and then argued to be applicable also in the stock market and in decision-making within firms. Although reputational herding theory is a prominent theory in behavioral economics, it has not yet been used in the field of information systems.

The basic idea of reputational herding theory is that if an investment manager is uncertain of his ability to decide on an IS security investment, conformity with other investment professionals is a good choice. This is because of its key assumptions that there are systematically unpredictable components of the investment value and that smart managers make similar decisions. Managers will be evaluated more favorably if they make the same decision of the others, as they can share the blame.

Because of its emphasis on the unpredictability of the value of decisions, reputational herding theory has been theorized to explain decision-making under uncertainty especially well. For the same reason, and because reputational herding theory has been found to be effective in the strategic decision-making context, we

expect it to be well suited for explaining IS security investment, which also involves unpredictability in its value. Our theoretical model and its associated hypothesis will be discussed next.

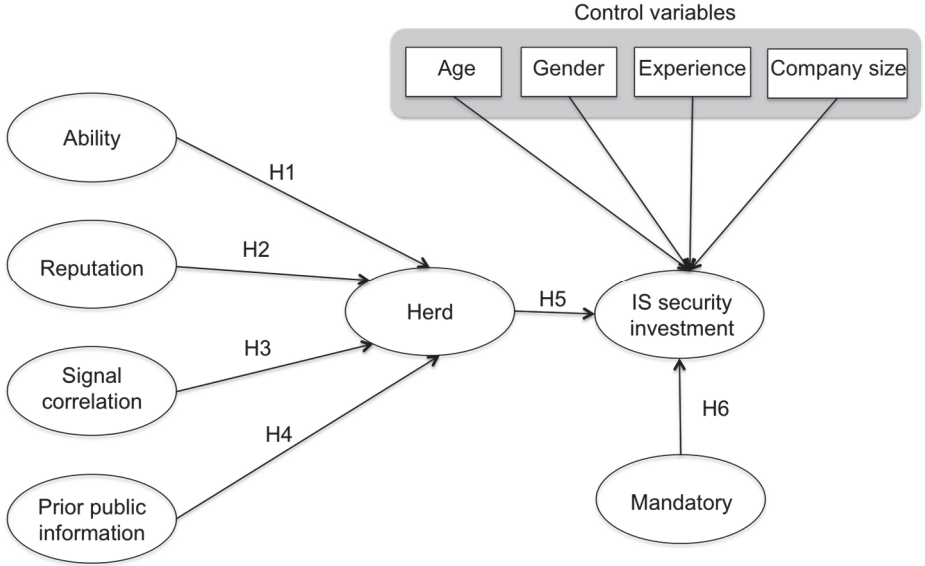


Fig. 5. Theoretical model.

Hypotheses

Antecedents of reputational herding

As mentioned above, reputational herding literature has suggested four conditions for herd behavior: an ability to accurately assess the value of an investment, a manager’s initial reputation in the market, the strength of prior information, and the level of correlation across informative signals.

One reason that herd behavior is common in IS security investment is that it is difficult to accurately predict the value of an IS security investment. The new assumption developed for IS security investment (Chapter 5) suggests that decision makers have inaccurate knowledge about the consequences of IS security investment and incomplete information. This is because of the intangible nature of IS security investment (see Chapter 3), which lead decision makers to be uncertain about investing.

Sun (2013) summarized three types of uncertainties taken from Milliken (1987) to describe the difficulty in accurately predicting the issues related to the adoption of a technology: state uncertainty, effect uncertainty, and response uncertainty. *State uncertainty* is a situation in which managers do not feel confident that they understand what the major events or trends in an environment are or feel unable to accurately determine the probability to the likelihood that particular events or changes will occur. *Effect uncertainty* refers to an inability to predict the effects that a future state of the environment will have on an organization (i.e., an understanding of cause-effect relationships). *Response uncertainty* is an inability to predict the likely consequences of a particular response choice. These three uncertainties may occur in IS security investment decision-making. For example, IS security investment managers may not be sure of a hackers' next attack (state uncertainty). They may be unclear about how serious the damages will be (effect uncertainty). It may also be difficult to determine how efficiently an IS security investment will prevent security breaches (response uncertainty). As a result, it is difficult to accurately predict the value of an IS security investment.

Prior research has shown that when people feel uncertain about a decision, they are likely to herd (Bikhchandani & Sharma, 2000; Graham, 1999; Sun, 2013; Zwiebel, 1995). When managers have a limited ability to predict the value of an IS security investment, they are more likely to follow the decisions of others, doing what others have done. This notion led to the construction of the first hypothesis:

H1: A manager's ability to accurately predict the value of IS security investment is negatively associated with herd behavior.

A manager's reputation in the market is considered to be a second factor that influences herding behavior. Reputation is important to managers because it will bring autonomy, power, and career success (Zinko *et al.*, 2012). Autonomy refers to the freedom that an individual has to carry out work. Reputation exists in order to show that a manager's behavior is predictable and, therefore, that there is no need to closely monitor a manager's actions. As individuals gain a good reputation, they gain power (Gioia & Sims, 1983; Pfeffer, 1992), which may be derived from not only formal but also informal authority; the authority to delegate tasks is an example of these powers. Reputation also has the ability to affect performance evaluations, promotions, and compensation (Ferris *et al.*, 2003).

The labor market updates a manager's reputation from checking whether managers make "smart" decisions. A "smart" decision can be evaluated in terms of

whether it is a profitable decision for the organization or whether the decision is similar to those made in other organizations. As reputation is important to managers, they generally will avoid making “dumb” decisions. However, as previously discussed, it is difficult to accurately predict the value of an IS security investment, and managers may face difficulty in evaluating whether their decisions are profitable. Therefore, managers who have a good reputation tend to make decisions that are similar to the decisions of others in order to maintain their reputations.

This assertion is supported by the results of several studies. Trueman (1994), investigating the reputational incentives that lead stock market analysts to herd with regard to their forecasts of future earnings, found that analysts have an incentive to make forecasts based off of the prior expectation. Similarity, Brandenburger and Polak (1996) showed that a firm with superior information can have a reputational incentive to make investment decisions that are consistent with a prior belief about the profitability of a project.

H2: A manager’s reputation is positively associated with herd behavior.

According to the new assumption proposed in Chapter 2 with regard to IS security investment, decision makers have incomplete information about IS security investments. Managers can make inferences about other organizations’ private information by observing their decisions. Managers have many opportunities, through many channels, to observe other organizations’ IS security investment decisions. For example, many companies make public announcements about their IS security investments in major newspapers (e.g., *The Wall Street Journal*, *The New York Times*, *USA Today*) and magazines as well as other sources, such as wire services. Such public announcements are perceived as sending a positive signal to stakeholders, customers, and attackers and, therefore, have a positive effect on stock prices (Chai *et al.*, 2011).

When managers observe other organizations’ IS security investment decisions, they generally pay attention to the number of organizations that are making the same IS security investment decisions. People often follow the general trends regarding a particular choice, believing in the “wisdom of the crowd.” The higher number of predecessors there are making the same IS security investment decision, the more likely it is that a manager will herd (Bikhchandani *et al.*, 1992; Graham, 1999). At the same time, managers also pay attention to the identity of predecessors. For example, managers may believe in signals from consultants or experts, even

though those “opinion leaders” may never claim to have more information. This notion led to the construction of a third hypothesis:

H3: The level of correlation across informative signals is positively associated with herd behavior.

In the reputational herding model (Scharfstein & Stein, 1990), “prior information” refers to information that has previously been made public that shows the probability of deriving profit from an investment. Hirshleifer (2001) defines the strength of information as the extremeness of information. So, for this thesis, we have defined the strength of prior information as the extremeness of prior public information that shows the probability of deriving profit from an investment.

The reputational herding model suggests that when prior information is strong and consistent with the majority’s actions, the decision maker will tend to follow the actions of the majority. This notion led to the construction of a fourth hypothesis:

H4: The strength of prior information and its consistency with the actions of the majority are positively associated with herd behavior.

Impact of herd behavior on IS security investment

It has been suggested in prior research that investment managers mimic the investment decisions of other managers to avoid the risk of being considered incapable (Graham, 1999; Scharfstein & Stein, 1990). Moreover, if a manager makes an unprofitable investment by following others, such a mistake is not considered to be so bad because the manager can “share the blame” with others who made the same decision. Indeed, herding is considered to be a legitimate strategy for people with good reputations to protect their status (Graham, 1999). In the context of IS security investment, a manager may imitate others in making an investment decision, as even if the decision turns out to be inefficient, the manager is not alone in having made the wrong decision and can thus share the blame with others who also rejected an efficient IS security investment—and thereby, the manager can potentially spare their own reputation. Such a positive association with herd behavior led to the construction of a fifth hypothesis:

H5: Herd behavior is positively associated with a manager’s IS security investment.

Control variable: mandatory

As more people have realized the value of information, the government has enacted various laws to secure information in cyberspace, such as the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act and Health Insurance Portability, Accountability Act Security Rule, and the Sarbanes–Oxley Act. According to the new assumption developed in Chapter 3 on IS security investment, one aim of IS security investment is to ensure compliance. Given this aim, we sought to determine if mandatory requirements would ensure compliance. This investigation led to the formulation of a sixth hypothesis:

H6: Mandatory requirements are positively associated with a manager's IS security investment.

7.3 Methodology

7.3.1 Operationalization of constructs

Measures adapted from prior research

Appendix 4 lists all the measures used in this study. As the reliability of constructs can be improved by using previously validated and tested questions (Straub, 1989; Boudreau *et al.*, 2001), this study utilized instruments that had been previously validated in the literature. The items used to measure herd behavior were adapted based on Sun (2013). Items assessing reputation were adapted from Zinko *et al.* (2012). Items assessing mandatory measures were adapted from Boss *et al.* (2009). Three items used to measure the behavior were adapted based on Beaudry and Pinsonneault (2010).

Self-developed measures

Since there were no previously validated instruments to assess ability, signal correlation, and strength of prior information, new instruments were developed to assess them in this study. Appendix 3 describes in detail how the instruments were developed, following the procedure set from Mackenzie *et al.* (2012). The instrument development process resulted in four items to assess ability, four items to assess signal correlation, and three items to assess the strength of prior information. Appendix 3 presents the whole scale development procedure.

7.3.2 Pretest

A pretest survey was conducted at Oulu University in Finland. A total of 32 responses were collected. The purposes of the pilot study were twofold: first, to ensure that the questionnaire was properly compiled, and second, to conduct a reliability assessment of the scales. To achieve the first goal, an open question was included to allow subjects to comment on the wording, content, and length of the questionnaire. Revisions to the questionnaire were made using these responses. To assess the reliability of the scales, Cronbach's alpha (Cronbach, 1970) was used. Cronbach's alpha is, according to Moore and Benbasat (1991), "fairly standard in most discussions of reliability." Thirteen items with low inter-item and item-total correlations, high "Cronbach's alpha if item deleted" statistics, or small standard deviation scores (and thus low explanatory power) were deleted with content validity in mind.

7.3.3 Survey administration

To test the research model, a field survey was conducted in Finland, a developed country in which a number of organizations are growing increasingly aware of IS security investment issues. The field survey took place over a period of four months, from mid-January 2013 to April 2013. The questionnaire included demographic questions and items for the above constructs.

Organizations invest in IS security solutions to protect valuable information. Therefore, an IS security investment ultimately results in the implementation of the solutions embodied in the survey as implementing IS security investment management standards.

The survey was randomly sent to 1,042 Finnish companies. As an incentive to participate, the organizations were offered to provide them a report of our findings upon conclusion of the study. All of the respondents to this survey were IS security investment managers who were familiar with IS security investment management. Out of the 1,042 surveys distributed to these organizations, 88 responses were obtained, yielding a response rate of 8.44%. Respondents returned completed surveys by using envelopes with pre-paid postage. The required sample size to evaluate our model was 80, according to the "rule of ten" heuristic (Barclay *et al.*, 1995).

Table 5 summarizes the demographic statistics. The respondents had an average age of 45. Among the valid responses, 85.23% were male. A majority of

the respondents had university degrees (76.14%). They had an average of 10.9 years' experience in IS security management, and 64.77% of them had previous experience using IS security investment standards. The organization sizes show a good variety of small, mid-sized, and large organizations. These demographic characteristics suggest that our sample was heterogeneous, which helps to increase the external validity of the thesis.

Table 5. Demographics

		Frequency	Percentage
Age	-	-	Average = 45
IS security management experience (years)	-	-	Average = 10.9
Gender	Male	75	85.23%
	Female	13	14.77%
Education	Vocational	4	4.55%
	College level	17	19.32%
	Bachelor's degree	21	23.86%
	Master's degree	45	51.14%
	Ph.D.	1	1.14%
Previous experience	Yes	57	64.77%
	No	31	35.23%
Organization size (# of employees)	1–100	8	9.10%
	101–249	11	12.5%
	250–499	11	12.5%
	500–999	10	11.36%
	1,000+	48	54.55%

7.4 Data analysis

The collected data was analyzed for this thesis by using partial least squares (PLS) with SmartPLS, version 2.0 (Ringle *et al.*, 2005). There were four reasons for using SmartPLS. First, a structural equation modeling (SEM) technique was chosen to test the hypotheses, rather than regression analysis, because of our conceptualization of herding as a multidimensional second-order construct (MacKenzie *et al.*, 2005), for which SEM methods are better suited. Second, SmartPLS was chosen rather than a covariance-based SEM technique, such as

LISREL, because of the ability of PLS to model second-order constructs that are formatively composed of first-order factors, such as our conceptualization of herding. This type of second-order construct specification is problematic for analysis using LISREL (Chin, 1998), therefore. Third, PLS is more suitable when the purpose of the model is to predict rather than to test an established theory, for which LISREL would be preferred (Chin *et al.*, 2003; Gefen *et al.*, 2005). Fourth, SmartPLS has minimal demands for sample size and residual distribution (Chin *et al.*, 2003).

The data analysis followed a two-stage analysis procedure. In the first stage, the measurement issues (i.e., validity, reliability, common method bias) were assessed to ensure their quality. In the second stage, the structural model was assessed, and the hypotheses were tested (Hair *et al.*, 1998). Furthermore, the model contained one second-order formative construct (i.e., herding), which was created by using the factor scores for the first-order constructs (i.e., discounting one's own information and imitating others; Bock *et al.*, 2005).

7.4.1 Measurement model

Before assessing the hypotheses, extensive pre-analysis and data validation were conducted to assess measurement quality, which includes (1) establishing the factorial validity of the measures, (2) establishing strong reliabilities, and (3) checking for common method bias. Because one of the constructs in our model, herding, was formative, said construct was validated by using techniques designed for formative constructs (Petter *et al.*, 2007). Validation of the reflective constructs is discussed first.

Validation for reflective constructs

Tests of validity and reliability are important for both the assessment and reduction of measurement error. Minimizing these errors improves the explanatory power of these measures.

The fit of the pre-specified model in confirmatory factor analysis (CFA) was examined to determine its convergent and discriminant validities (Gefen & Straub, 2005). Convergent and discriminant validities examine whether the pattern of the loadings of the measurement items correspond to the theoretically anticipated factors.

Convergent validity

Convergent validity is indicated when each of the measurement items loads onto its latent construct with a significant *t*-value (Gefen & Straub, 2005). To establish convergent validity, we generated a bootstrap with 400 resamples and examined the *t*-values of the outer model loadings. In almost every case, each latent variable's indicators strongly converged on the latent variable and were highly significant, as shown in Table 6 below. Two items did not reach levels of significance (DOI1, SI1) and were subsequently removed from later analyses to improve convergent validity.

Table 6. T Statistic for Convergent Validity

Latent Construct	Subconstruct	Indicator	T-Value
Ability	N/A	A2 ← A	3.12***
		A4 ← A	3.10***
		A5 ← A	4.56***
		A6 ← A	5.07***
Reputation	N/A	R1 ← R	3.05***
		R2 ← R	2.84**
		R5 ← R	3.34***
		R6 ← R	3.00***
Strength of information	N/A	SI1 ← SI	0.45 (d)
		SI2 ← SI	2.31*
		SI3 ← SI	2.57*
Signal correlation	N/A	SC3 ← SC	4.76***
		SC4 ← SC	5.57***
		SC6 ← SC	5.64***
		SC7 ← SC	3.89***
Herding	Discounting of one's own information	DOI1 ← DOI	0.9804(d)
		DOI2 ← DOI	1.7879*
		DOI4 ← DOI	1.8928*
		DOI6 ← DOI	1.9889*
	Imitation of others	IO1 ← IO	5.9309***
		IO2 ← IO	7.218***
		IO3 ← IO	7.1422***
		IO4 ← IO	5.0167***
Mandatory	N/A	Mand1 ← Mand	81.1023***
		Mand2 ← Mand	17.4388***
		Mand3 ← Mand	72.6893***

Note: * $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$

As a second check, the latent variable scores were compared against the indicators as a form of factor loadings, and then the indicator loadings and cross-loadings were examined to establish convergent validity. Although this approach is typically used to establish discriminant validity (Gefen & Straub, 2005), convergent validity and discriminant validity are interdependent and help establish each other (Straub *et al.*, 2004). Thus, following Kock (2010), convergent validity is also established when each factor loading for a latent variable is substantially higher than those for other latent variables. This is performed by comparing the latent variable scores against the factor loading indicators (Gefen & Straub, 2005). Table 7 summarizes the loadings.

Table 7. Cross-Loadings of Measurement Items to Latent Constructs for Convergent and Discriminant Validity

Construct	Item	1	2	3	4	5	6	7	8
Ability (1)	A2	0.59	0.04	0.10	0.35	0.27	0.29	0.26	0.46
	A4	0.54	-0.02	0.00	0.16	0.52	0.26	0.52	0.46
	A5	0.82	-0.03	0.27	0.28	0.33	0.37	0.28	0.49
	A6	0.89	0.21	0.31	0.20	0.59	0.37	0.25	0.42
Discounting of one's own information (2)	DOI2	0.12	0.93	0.03	0.21	0.26	0.10	0.23	0.23
	DOI4	0.12	0.96	0.12	0.25	0.23	0.12	0.13	0.27
Imitation of others (3)	IO2	0.34	0.13	0.92	0.33	0.17	0.59	0.11	0.26
	IO3	0.28	0.10	0.92	0.25	0.04	0.42	-0.02	0.25
	IO4	0.24	-0.02	0.82	0.10	0.11	0.40	0.21	0.12
Mandatory (4)	Mand1	0.33	0.16	0.20	0.96	0.24	0.32	0.24	0.46
	Mand2	0.18	0.18	0.22	0.86	0.07	0.28	0.14	0.25
	Mand3	0.30	0.32	0.31	0.95	0.19	0.37	0.22	0.47
Reputation (5)	R1	0.53	0.22	0.09	0.22	0.92	0.43	0.51	0.41
	R2	0.51	0.18	0.13	0.10	0.83	0.39	0.37	0.36
	R5	0.40	0.23	0.08	0.18	0.85	0.31	0.46	0.35
	R6	0.49	0.26	0.12	0.20	0.90	0.33	0.48	0.43
Signal correlation (6)	SC3	0.32	0.02	0.44	0.35	0.18	0.75	0.00	0.21
	SC4	0.33	0.08	0.43	0.37	0.21	0.81	0.18	0.34
	SC6	0.34	0.09	0.42	0.11	0.42	0.74	0.38	0.18
	SC7	0.29	0.19	0.20	0.16	0.47	0.57	0.40	0.32
Strength of information (7)	SI2	0.37	0.20	0.12	0.21	0.55	0.28	0.96	0.41
	SI3	0.16	0.12	0.07	0.21	0.37	0.29	0.89	0.26
Use (8)	U1	0.44	0.22	0.11	0.32	0.44	0.30	0.30	0.89
	U2	0.45	0.23	0.26	0.41	0.27	0.24	0.32	0.90
	U3	0.58	0.26	0.25	0.46	0.51	0.40	0.39	0.92

Discriminant validity

Discriminant validity is shown when: (1) measurement items need to load highly on their theoretical assigned factor but not so highly on other factors, and (2) the square root of every AVE (one for each latent construct) needs to be much larger than any correlation among any pair of latent constructs (Gefen & Straub, 2005).

Two established methods were used to determine the discriminant validity as described in Gefen and Straub (2005), and as demonstrated in Lowry *et al.* (2008; 2009). First, as with convergent validity, the factor loadings were examined, this time to ensure that a significant overlap did not exist between the constructs (see Table 7 above). All loadings were appropriate, given the two dropped indicators in the previous step.

Second, we used the approach of examining the square roots of the AVEs described in Gefen and Straub (2005); the AVE analysis is summarized in Table 8 below. The basic standard followed here is that the square root of the AVE for any given construct (latent variable) should be higher than for any of the correlations that involve the construct (Fornell & Larcker, 1981). The numbers are shown in the diagonal for constructs (bolded). Strong discriminant validity was shown between all constructs.

Table 8. AVE Analysis to Establish Discriminant Validity and Construct Correlation to Test Common Method Bias

	1	2	3	4	5	6	7	8
Ability (1)	0.72							
Discounting of own information (2)	0.13	0.95						
Imitation of others (3)	0.33	0.08	0.88					
Mandatory (4)	0.31	0.24	0.26	0.87				
Reputation (5)	0.55	0.26	0.12	0.20	0.72			
Signal correlation (6)	0.44	0.12	0.54	0.35	0.42	0.93		
Strength of information (7)	0.32	0.18	0.11	0.23	0.52	0.30	0.90	
Use (8)	0.55	0.26	0.24	0.45	0.45	0.35	0.38	0.93

Reliability

Reliability refers to the degree to which a scale yields consistent and stable measures over time (Straub, 1989). Reliability differs from validity in that reliability concerns how a phenomenon is measured, whereas validity concerns what should be measured (Hair *et al.*, 1998).

One method for assessing reliability is the test-retest method. If the measurement is free from errors, then when the measurement is repeated, the results should be the same (Hendrickson *et al.*, 1993). This is executed by using measurements from previous studies. The most commonly used measure of reliability is to assess the internal consistency of the items. SmartPLS computes Cronbach's alpha as well as the composite reliability score, which is evaluated in the same way as Cronbach's alpha (Fornell & Larcker, 1981). This score is a more accurate measurement of reliability than Cronbach's alpha, because it does not assume loadings or error terms of the items to be equal (Chin *et al.*, 2003). However, as a conservative check, Cronbach's alpha can also be used as a basis for comparison. Thus, the two most conservative criteria were used, for which both the coefficients of composite reliability and the Cronbach's alpha should be ≥ 0.7 (Fornell & Larcker, 1981; Kock, 2010; Nunnally & Bernstein, 1994). Both analyses indicate a high reliability rate for all subconstructs, as summarized in Table 9.

Table 9. Construct Reliabilities

Construct	Composite Reliability	Cronbach's α
Ability (1)	0.81	0.76
Discounting of one's own information (4)	0.95	0.89
Imitation of others (5)	0.92	0.86
Mandatory (6)	0.95	0.92
Reputation (8)	0.93	0.90
Signal correlation (9)	0.81	0.70
Strength of information (10)	0.92	0.85
Use (11)	0.93	0.89

Validation for formative constructs

The measurement quality of our formative construct, herding, was evaluated in two ways following the suggestions of Chin (1998) and Diamantopoulos *et al.* (2001). First, the correlations between measurement items were examined for this formative construct. The absolute correlation between the two subconstructs measuring herding (discounting of one's own information and imitating others using latent variable scores) is 0.08 (see Table 8). The relatively low correlation suggests that the herding construct is better represented as a formative construct; a reflective construct would show extremely high correlations (often above 0.8) between its measurement items (Pavlou & Sawy, 2006).

Next, the strength of the relationship between the formative construct and its measurement subconstructs was assessed by using latent variable scores. For herding, both subconstructs had significant path coefficients (or PLS weight) (Fig. 6). The variance inflation factor (VIF) was then computed to assess the multicollinearity of the two subconstructs. VIF values above 10 would suggest the existence of excessive multicollinearity and would raise doubts about the validity of the formative measurement (Diamantopoulos *et al.*, 2001). The VIF values ranged from 0.30 to 0.91 for the two subconstructs measuring herding. Therefore, multicollinearity was not a concern in this study.

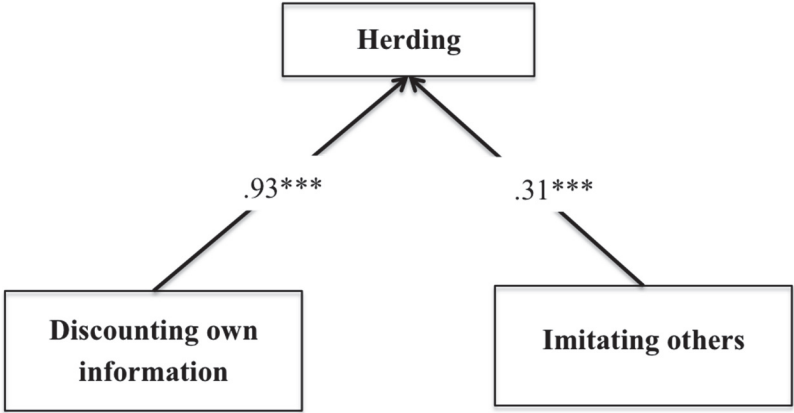


Fig. 6. PLS result for the relationship between herding and its two subconstructs. Completely standardized path coefficients (or PLS weights). *significant at 0.001 level**

Testing for common method bias

To decrease the likelihood of common method bias occurring in our data collection, items within the instrument were randomized so that participants would be less apt to detect underlying constructs, another potential source of common method bias (Cook & Campbell, 1979; Straub *et al.*, 2004). However, all the data was collected using a self-report survey, in which the same subject responds to the items in a single questionnaire at the same point in time. Therefore, this data was likely to be susceptible to common method variance (CNV) or common method bias (CMB), which compromises the credibility of the results of the data analysis (Malhotra *et al.*, 2006). To avoid the CMB threats, it was necessary to test for common method

bias to establish that it was not a likely negative factor in the data remaining for our analysis. To do so, two approaches of increasing validity and rigor were used.

The first approach used here was to simply examine a correlation matrix of the constructs and to determine if any of the correlations were above 0.90, which would serve as evidence that common method bias may exist (Pavlou *et al.*, 2007).¹⁰ In the test, the construct correlation matrix, as calculated by PLS (see Table 8), was examined to determine whether any constructs had an extremely high rate of correlation (more than .90). In our case, none of the constructs correlated so highly. Likewise, this finding indicates that common methods bias was not a problem.

The second approach to testing common method bias was to conduct the test established by Liang *et al.* (2007). This approach was suggested by Podsakoff *et al.* (2003) and carried out for PLS by Liang *et al.* (2007). It is particularly useful because it has been established to overcome the classic issues of assessing common method bias (Liang *et al.*, 2007; Podsakoff *et al.*, 2003). The objective of this technique is to measure the influence of a common latent method factor on each individual indicator in the model versus the influence of each indicator's corresponding construct. More details about this technique, and how to perform it, can be found in Liang *et al.* (2007).

Table 10 provides the detailed analysis that resulted from our common method variance analysis. To interpret these results, the coefficients of the paths between the substantive constructs (λ_s) and the single-indicator constructs, as well as the coefficients of paths from the method factor (λ_m) to the single-indicator constructs, are considered loadings, which are represented by λ in the tables (Liang *et al.*, 2007). Following Liang *et al.* (2007), common method bias could be assessed by examining the statistical significance of the loadings of the substantive factors (λ_s) and of the method factor (λ_m), and by comparing the variance of each indicator as explained by the substantive and method factors. The square of the substantive factor loading (λ_s^2) is interpreted as the percentage of indicator variance, explained by the substantive factor, and the square of the method factor loading (λ_m^2) is interpreted as the percentage of indicator variance explained by the method factor.

Common method bias is a highly unlikely concern when the following three conditions are met: (1) most of the substantive factor loadings are significant, (2) most of the method factor loadings are insignificant, and, arguably the most

¹⁰ The traditional approach to establishing a lack of common method bias is to conduct a Harman's single factor test; however, the validity of this approach is increasingly discredited; thus, we used two more widely accepted methods instead (Pavlou *et al.*, 2007; Podsakoff *et al.*, 2003).

important, (3) the percentage of indicator variance due to substantive constructs is substantially greater than the percentage of indicator variance due to the method construct.

Applying these guidelines, all three required conditions held in our study. Aside from major differences in the frequency and magnitude of the significance of the loadings, the average substantive factor loading (λ_s) was 0.86, whereas the average method factor loading (λ_m) was 0.001. Most importantly, the variance of indicators due to substantive constructs (λ_s^2) was substantially greater than the variance due to the method construct (λ_m^2). These were 75.4% (λ_s^2) and 1.1% (λ_m^2), representing a ratio of nearly 66.98 to 1. Thus, we conclude from this analysis that our data collection had negligible influence due to common method bias.

Table 10. Results of Common Method Bias Test

Construct	Item	Substantive Factor Loading (λ_s)	Variance Explained (λ_s^2)	Method Factor Loading (λ_m)	Variance Explained (λ_m^2)
Ability (1)	A2	0.84***	0.70	-0.13	0.02
	A4	0.88***	0.78	-0.16	0.03
	A5	0.76***	0.58	0.06	0.00
	A6	0.58***	0.34	0.22	0.05
Discounting of one's own information (2)	DOI2	0.95***	0.90	-0.01	0.00
	DOI4	0.95***	0.90	0.01	0.00
Imitation of others (3)	IO2	0.88***	0.78	0.05	0.00
	IO3	0.95***	0.90	-0.07	0.00
	IO4	0.82***	0.66	0.02	0.00
Mandatory (4)	Mand1	0.93***	0.87	0.04	0.00
	Mand2	0.95***	0.90	-0.11	0.01
	Mand3	0.91***	0.83	0.06	0.00
Reputation (5)	R1	0.90***	0.82	0.03	0.00
	R2	0.80***	0.64	0.03	0.00
	R5	0.89***	0.80	-0.04	0.00
	R6	0.90***	0.82	-0.01	0.00
Signal correlation (6)	SC3	0.77***	0.59	-0.07	0.00
	SC4	0.86***	0.75	-0.11	0.01
	SC6	0.75***	0.56	0.01	0.00
	SC7	0.48***	0.23	0.22	0.05
Strength of information (7)	SI2	0.88***	0.78	0.10	0.01
	SI3	0.98***	0.96	-0.10	0.01
Use (8)	U1	1.01***	1.01	-0.13	0.02
	U2	0.91***	0.82	-0.02	0.00
	U3	0.81***	0.65	0.15	0.02
Average		0.86***	0.75	0.001	0.01

7.4.2 Structural model

Given that our data displayed factorial validity and did not display common methods bias, the structural model was then tested. Figure 7 and Table 11 summarize the results of hypotheses testing. In Figure 7, path coefficients are given on each path. R^2 values, which are presented below each dependent variable, reflect the predictive power of the model. The model could explain 23% of the variance in IS security investment and 35% of the variance in herding.

Bootstrapping was performed to compute the *t*-values for each hypothesized relationship and potential impact of the control variables. Among the four control variables, none was found to have a significant impact on IS security investment.

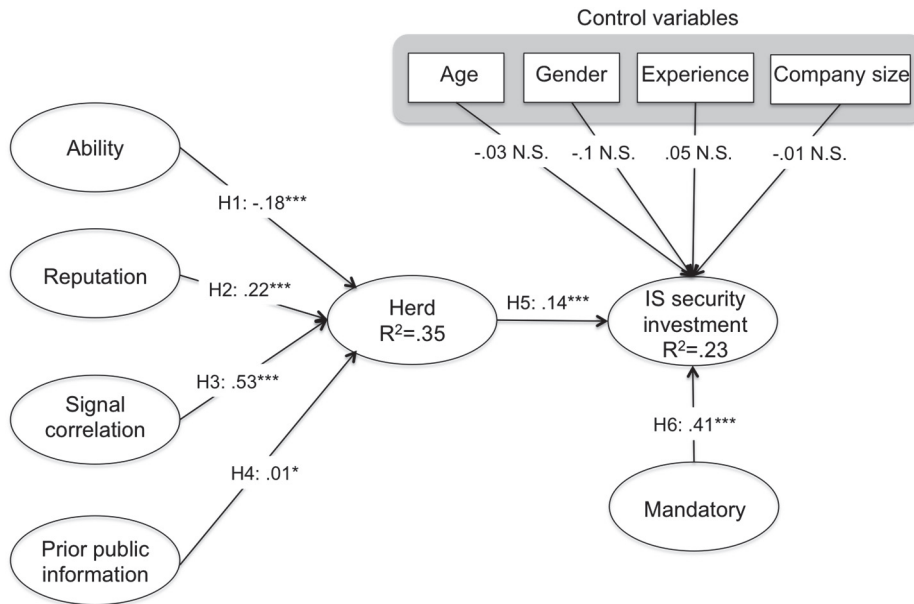


Fig. 7. Research model showing results of PLS analysis.

Table 11. Summary of model results

#	Hypothesis	Coefficient	Supported?
H1	Ability → Herd	-.18***	Yes
H2	Reputation → Herd	.22***	Yes
H3	Signal correlation → Herd	.53***	Yes
H4	Prior public information → Herd	.01*	Yes
H5	Herd → IS security investment	.14***	Yes
H6	Mandatory → IS security investment	.41***	Yes

*** $p < .001$; ** $p < .01$; * $p < .05$; ns: not significant

7.5 Summary of hypotheses and results

Our results support the theoretical model, which will be discussed in turn. First, the results of our model show that herding is a significant motivation for IS security

investment (H5), as suggested by the reputational herding theory (Scharfstein & Stein, 1990). While this is the first application of reputational herding theory to the IS security investment milieu, studies in other fields have focused on herding behavior. For example, Graham (1999) studied herding among investment newsletters by using the data of analysts who published investment newsletters. Their findings suggest that a newsletter analyst is likely to follow *Value Line's* recommendation if the analyst's reputation is high, if the analyst's ability is low, or if the signal correlation is high.

Second, the results show that mandatory government or industry requirements strongly affect managers' IS security investment (H6). While this is a new finding in the area of IS security investment, the result is consistent with IS security behavior studies. Boss *et al.* (2009) studied employees' IS security precaution-taking behavior. Their findings suggest that the perception of security precautions being mandatory is effective in motivating individuals to take these precautions.

The findings for herding and mandatory requirements show that a perceived benefit is not the only motivation for IS security investment, which supports the preliminary framework.

Third, the results also show under which circumstances IS security managers intend to follow the IS security investment decisions made by other companies. The results show that managers' analysis ability, correlations with other companies' practices, and prior public information jointly influence managers' herd behavior. When managers have inaccurate knowledge and incomplete information with which to calculate the consequences of IS security investment (H1), they will tend to follow others' IS security investment decisions. Our results also show that when IS security managers are concerned about their reputation within an organization (H2), they have a significant intention to follow others' decisions. When IS security managers observe a significant number of organizations that have made the same IS security investments, they are more likely to make the same decision (H3). When managers observe that an IS security investment decision is consistent with strong prior information, these managers are more likely to make the same choices as others (H4).

To sum up, the results support the preliminary framework developed for IS security investment in Chapter 5, as well as the reputational herding model.

8 Testing the new assumptions in a new context

The new assumptions for IS security investment developed in Chapter 5 claim that the IS security manager makes investment decisions that are expected to be satisfactory. This chapter will test the new assumptions in a new context by empirically examining whether a decision maker seeks a satisfactory result instead of maximum benefit.

8.1 A new context: digital piracy in online communities

Rapid developments to both online connectivity and digital compression technologies have provided new opportunities for interaction and for the dissemination of information. On the contrary, such advances have increased the unauthorized use of digital products. Recent evidence from the United States indicates that 40% of people have pirated music and 22% have engaged in film piracy, and more than two-thirds of individuals aged between 18 and 29 admit to having engaged in these activities (Karaganis, 2011). Piracy rates are even higher in Europe. Findings from Denmark show that more than three-quarters of people between the ages of 18 and 29 have pirated films or music (Benner & Vuorela, 2012).

Digital piracy is the illegal act of copying digital goods for any reason other than to back up without explicit permission from and compensation to the copyright holder (Higgins, 2006). The rise of digital piracy increases the concerns for both intellectual property rights and lost sales (Bhattacharjee, Gopal, & Sanders, 2003). For instance, the Business Software Alliance investigated the volume and value of unlicensed software used in personal computers in 2011 (BSA, 2012). An extensive survey with 14,700 respondents, which represented 82% of the global PC market, indicated that 57% of the world's PC users admitted to software piracy. In addition, the commercial consequences of this shadow market increased from USD\$58.8 billion in 2010 to USD\$63.4 billion in 2011.

8.1.1 Related work

Scholars seeking to explain and predict digital piracy have applied theories and models from various disciplines, including social psychology (e.g., Taylor *et al.*,

2009), criminology (e.g., Higgins, 2007), and business ethics (e.g., Peslak, 2008), primarily using intention frameworks as foundations for their research.

Research that applied theories from social psychology typically applied the theory of planned behavior (TPB) to the context of piracy (Ajzen, 1985). Results suggest that subjective norms, attitudes, and self-perceptions of behavioral control influence piracy behaviors via intentions (e.g., Cronan & Al-Rafee, 2008; D'Astous *et al.*, 2005; Plowman & Goode, 2009). Extensions of TPB provided similar support, such as Perugini and Bagozzi's (2001) model of goal-directed behavior (e.g., Taylor *et al.*, 2009).

Research that applied theories from criminology conceptualized piracy as criminal behavior. Frameworks such as deterrence theory (Ehrlich 1973) and self-control theory (Gottfredson & Hirschi, 1990) were utilized within this category of research. It has been suggested that perceived risks (e.g., Chiang & Assane, 2007; Pryor *et al.*, 2008; Shanahan & Hyman, 2010), together with self-control and association with peers who engage in piracy (e.g., Higgins, 2005), influence piracy behaviors.

Research that focuses on business ethics employs frameworks like the model of ethical reasoning (Hunt & Vitell, 1986). It has been suggested that ethical judgments and moral intensity variables (e.g., the magnitude of consequences) are related to piracy behaviors (e.g., Lyonski & Durvasula, 2008, Gopal *et al.*, 2004). Market conditions and product attributes also contribute to piracy behavior. For example, price and perceived value were found to be related to piracy intentions (e.g., Chen *et al.*, 2008). Similarly, price and risk were found to be important in determining the ratio of songs pirated to those purchased legally (e.g., Sandulli, 2007). Moreover, satisfaction with variety, legitimacy, and security were found to be negatively related to music piracy, whereas the perceived quality of pirated music was found to be positively related (e.g., Sirkeci & Magnusdottir, 2011).

8.1.2 Research gap

A brief review of the existing literature on digital piracy in IS goes some way toward identifying its antecedents and reveals that a broad variety of factors influence piracy behaviors, including social, legal, and ethical considerations. However, prior research is limited in one important way: it has largely disregarded different digital piracy behaviors.

Most research has not examined the uploading of unauthorized digital products to the Internet. In prior research, digital piracy behavior has usually referred to

downloading behavior. Prior research has shown that individual digital piracy behavior relies heavily on three major theories, namely, general deterrence theory (GDT), theory of planned behavior (TPB) or theory of reasoned action (TRA), and ethical decision-making theory.

However, the motivations for downloading and uploading may be different. For example, Janak (2011) has identified different motivating factors¹¹ for uploading and downloading pirated films. In some online communities, the motivation to download unauthorized digital products may not be as important as the motivation to upload unauthorized digital products.

The motivation for uploading unauthorized digital products depends on how the uploading behavior is understood in online communities. Uploading behavior can be understood as piracy behavior, in which the motivation for downloading behavior can be applied. Uploading behavior in online communities can also be understood as charitable giving, which aims to help other members in these online communities. Besides, uploading unauthorized digital products is also providing resources to all the members in the online community, which can be understood as public goods provision behavior.

Two aims will be achieved in this chapter. First, this chapter provides new insights into the digital piracy literature by separating uploading from downloading behavior and by exploring uploading behavior from different angles. Second, this chapter aims to show that the new assumption is applicable to the new context by testing whether an unauthorized digital product uploader seeks benefits from uploading.

8.2 Research model and hypothesis

8.2.1 Research model

The research model that explains the uploading of unauthorized content to online communities incorporates constructs from general deterrence theory and the theory of warm glow giving (see Figure 8). Previous studies have emphasized the importance of sanctions in determining piracy behavior (Kwan *et al.*, 2010; Peace

¹¹ Janak (2011) proposed the following motivations for uploading: recognition factors, profit factors, hacking and ripping product factors, and attitude factors. For downloading, Janak (2011) proposed the following economic factors: supply factors, socio-psychological factors, and other factors (like opportunity to download, time factor, tryouts, and earlier than distribution studios).

et al., 2003), and the importance of demand for resources and warm glow in affecting contribution to online public goods (Andreoni, 1989; Andreoni, 1990). Therefore, we hypothesize that sanctions, demand for resources, and warm glow impact people’s uploading behavior. In order to test our new assumption, the benefits gained from uploading are also considered in the research model.

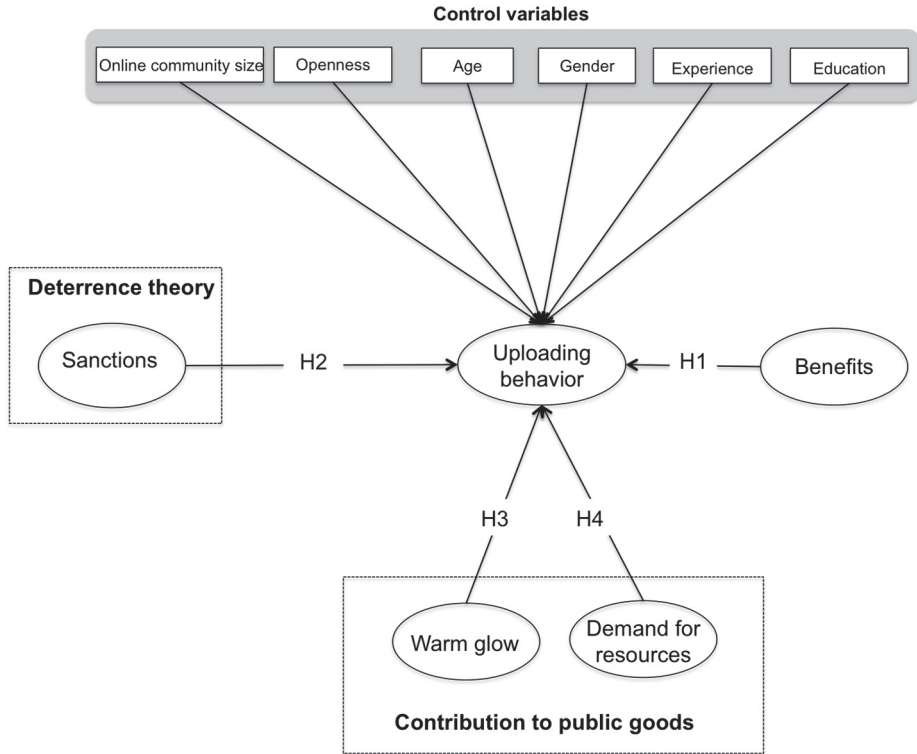


Fig. 8. Research model.

8.2.2 Hypotheses

Examine the new assumption

Our new assumption for IS security investment is that decision makers seek satisfactory results for themselves rather than try to maximize the value from the given options. In order to generalize the new assumption in another setting, we assumed that in the context of uploading unauthorized content to online

communities, decision makers would be satisfied not by receiving benefits, but by other mechanisms.

H1: Benefits have no significant effect on uploading behavior.

Uploading as privacy behavior: Deterrence theory

Uploading unauthorized digital products to online community is a piracy behavior, according to the definition of piracy. Classic deterrence theory focuses on formal (legal) sanctions and posits that the greater the perceived *certainty, severity, and celerity* (swiftness) of sanctions for an illicit act, the more individuals are deterred from that act (Gibbs, 1975). In most criminology literature, sanctions are viewed as an important instrument with which to deter inappropriate behaviors, such as tax evasion (Klepper & Nagin, 1989a, 1989b), juvenile delinquency (Paternoster, 1989), corporate crime (Paternoster & Simpson, 1996), disobedience of regulatory laws (Elffers *et al.*, 2003), and general illegal conduct (Wright *et al.*, 2004). Since individuals are believed to be amenable to sanction-based threats, the punishment-as-deterrence doctrine has been widely accepted by policymakers and the general public (Liska & Steven, 1999).

The impacts of the perception of punishment for digital piracy behavior have also been empirically examined in piracy studies (Chiang & Assane, 2009; Chiou *et al.*, 2005; Christensen & Eining, 1991; Higgins *et al.*, 2005; Kwan *et al.*, 2010; Li & Nergadze, 2009; Peace *et al.*, 2003). These studies have suggested that fear of punishment helps to prevent software piracy and the fear of punishment can be further captured by the probability that the punishment will occur (e.g., punishment certainty) and the losses induced by the punishment (e.g., punishment severity). This notion led to the construction of the following hypothesis:

H2: Perceived sanction is negatively associated with the uploading of unauthorized content to online communities.

Uploading as contributions of public goods: Warm glow and demand for resources

The uploading of unauthorized digital goods to online communities can also be understood as contributing public goods in online communities. A public good is defined as a good for which consumption is non-excludable and non-rivalrous

(Mas-Collel *et al.*, 1995, p. 359). Although a pure public good is rare (Shmanske, 1991), most of the noncommercial online offerings exhibit many attributes of a public good (Kollock, 1999). For online goods, because the cost to exclude consumption is very low, the choice of making the good exclusive or nonexclusive is not about cost. In a noncommercial online network, the good (e.g., the contributed content) is often made nonexclusive so as to maximize its reach. Even though some communities require registration to access the content, it is used not as a way to exclude users, but to enhance the network feature (Kollock, 1999). Therefore, unlike public goods in the physical world, where provision of public goods need actions of a group (e.g., staging a social protest, providing national defense), an individual user's contribution of information is the provision of a public good in the online setting.

When individuals contribute to public goods, there may be many factors influencing them other than altruism. As Olson (1965) noted, "people are sometimes motivated by a desire to win prestige, respect, friendship, and other social and psychological objectives" (p. 60). Becker (1974) observed that apparent charitable behavior can also be motivated by a desire to avoid the scorn of others or to receive social acclaim. The warm glow theory (Andreoni, 1989; Andreoni, 1990) suggests that individuals have two reasons for contributing to the public goods: first, people simply demand more of the public good; second, for their contribution, people get a warm glow, the moral satisfaction people feel as a result of charitable giving (Andreoni, 1990).

Researchers have found that the expectation of receiving personal benefits can motivate users to contribute to the online public good in the absence of personal acquaintance (Constant *et al.*, 1996; Wasko & Faraj, 2005). The concept of reciprocity is often used to explain such contributing behavior (Connolly & Thorn, 1990). It is based on the fact that when people expect to receive a benefit from another, they tend to have the incentive to offer a benefit as well. Wellman and Gulia (1999) and Rheingold (1994) have reported that individuals who regularly contribute knowledge indeed receive help more quickly when they ask for something. Furthermore, the more benefits they demand from the group, the more they would like to pay back. In other words, when a user demands resources (a public good) from a group, that user has incentives to contribute to the group. In our context, when a user hopes to get more resources (shared digital goods), the user has an incentive to upload to the online community.

The impure altruism theory argues that people contribute to the public goods when it is sustained by the sense of positive emotional gain from the action. The

theory posits that when a good exhibits both public and private good characteristics, some people may be motivated to contribute, because the joy of giving more than offsets the cost, as is observed in charity giving. Ferguson *et al.* (2012) found that blood donors' actual donations were associated with feelings of a warm glow. Both Cornes and Sandler (1984, 1994) and Andreoni (1989, 1990) argue, through analytical modeling, that when taking into account the private benefits of giving, including a "warm glow," (i.e., when people take joy in the act of giving itself), a contribution to the public good can be expected in equilibrium. Moreover, the total contribution is more than what a pure altruism theory would predict. These researchers used the term "impure" because the "warm glow" is received directly by the contributor and is thus a seemingly selfish motivation; however, in our context, when a user feels emotionally satisfied by uploading unauthorized digital goods to online communities, the user has an incentive to upload the content.

H3: Warm glow is positively related with the uploading of unauthorized content to online communities.

H4: Demand for resources is positively related with the uploading of unauthorized content to online communities.

8.3 Methodology

8.3.1 Research design

An online survey was conducted to collect data for this study. The aim of the current study was to understand the extent to which the integration of different theoretical perspectives can capture piracy intention. The comprehensiveness of the research framework thus made experiments and case studies inappropriate (Cooper & Emory, 1995). Rather than collecting data through a paper-and-pencil questionnaire, an online survey was adopted for two reasons. First, the uploading of unauthorized digital products to online communities heavily relies on the Internet. In this special context, using online surveys can maintain the consistency between the research context and the data collection context. Second, the behavior involved in uploading unauthorized digital products is generally regarded as unethical and/or illegal. Surveys on this type of behavior should take the anonymity and confidentiality of respondents into consideration. Online surveys, compared with traditional paper-

and-pencil surveys, can better ensure the anonymity of respondents and the credibility of their answers (Kwong, 2009; Lin *et al.*, 1999).

8.3.2 Construct operationalization

Appendix 5 lists all the measures that were used for this chapter. Except for demand for resources, the measures of which were self-developed, the instruments for all the other constructs were adapted from previous studies to fit the context of our study. Two items used to measure uploading behavior were adapted from Venkatesh *et al.* (2008). The frequency and intensity of uploading behavior were used in developing these items. Sanctions were considered to be a formative second-order construct consisting of three dimensions; that is: punishment certainty and severity, adapted from D'Arcy *et al.* (2008), and punishment celerity, adapted from Nagin and Pogarsky (2001). Warm glow was considered to be a formative second-order construct consisting of four dimensions: affective feelings, role merger, subjective norms, and moral norms, all adapted from Ferguson *et al.* (2012). All the measures used the 7-point Likert scales.

8.3.3 Data collection procedure

Data was collected from randomly invited people. In total, 275 responses were obtained through an online channel. Among these responses, 55 responses were considered invalid, because these subjects had spent less than 5 minutes¹² in completing the survey. After removing these 55 responses, 220 valid responses were used in the data analysis.

Table 12 summarizes the demographic statistics. Among the valid responses, 37.2% were male. Over 90% of the participants were between 19 and 29 years old. More than 54.1% held a bachelor's degree or a higher level of education, and most of them had over 5 years of computer experience. Overall, the demographic statistics suggest that our sample is heterogeneous, which helps to increase the external validity of the thesis.

¹² We tested and showed that finishing the survey requires at least 10 minutes.

Table 12. Demographics

		Frequency	Percentage
Gender	Male	82	37.3
	Female	138	62.7
Age	0–18	3	1.4
	19–29	121	55
	30–39	52	23.6
	40–49	31	14.1
	50–59	8	3.6
	≥ 60	4	1.8
Education	Vocational	31	14.1
	College level	70	31.8
	Bachelor's degree	66	30.0
	Master's degree	45	20.5
	Doctorate degree	8	3.6

8.4 Data analysis

PLS was used to test the proposed model and the developed hypotheses for four reasons. First, compared with the first generation statistical analysis tools, PLS allows for the specification of both the relationships among the conceptual factors of interest (e.g., structural model) and the measures underlying each construct (e.g., measurement model), which results in a simultaneous analysis (Chin *et al.*, 2003). Second, the method also enables an analysis of the data in a holistic and systematic manner (Chin *et al.*, 2003). Third, compared with other structural equation modeling (SEM) tools, PLS requires a relatively small sample size, has no restrictions on normal distribution, and is more suitable for formative constructs (Chin *et al.*, 2003). Fourth, due to the formative nature of some of the measures and the non-normality of the data in the present study, the PLS method, rather than other SEM methods, was used. Specifically, SmartPLS version 2.0 was used as the major analysis tool.

Data analysis followed the two-stage analysis procedure. In the first stage, the measurement issues (i.e., reliability, validity, and common method bias) were assessed to ensure their appropriateness; in the second stage, the structural model was assessed, and the hypotheses were tested (Hair *et al.*, 1998). Furthermore, as the model contained two second-order formative constructs (i.e., warm glow, sanctions), the second-order formative construct was created using the factor scores for the first-order constructs (Bock *et al.*, 2005).

8.4.1 Measurement model

Before assessing the hypotheses, extensive pre-analysis and data validation were conducted to assess measurement quality, which included (1) establishing factorial validity of the measures, (2) establishing strong reliabilities, and (3) checking for common method bias. Because two constructs in our model are formative (warm glow and sanctions), the constructs were validated using techniques designed for formative constructs (Petter *et al.*, 2007). Validation of the reflective constructs is discussed first.

Validation of reflective constructs

Tests of validity and reliability are important for both the assessment and reduction of measurement error. Minimizing these errors improves the explanatory power of these measures.

The fit of the pre-specified model in CFA was examined to determine its convergent and discriminant validities (Gefen & Straub, 2005). Convergent and discriminant validities examine whether the pattern of the loadings of the measurement items corresponds to the theoretically anticipated factors.

Convergent validity

Convergent validity is indicated when each of the measurement items loads with a significant *t*-value on its latent construct (Gefen & Straub, 2005). To establish convergent validity, we generated a bootstrap with 400 resamples and examined the *t*-values of the outer model loadings. In every case, each latent variable's indicators strongly converged on the latent variable and were highly significant, as shown in Table 13 below.

Table 13. T statistic for convergent validity

Latent Construct	Subconstruct	Indicator	T-Value
Sanctions	Certainty of sanctions (CTS)	CTS2 <- CTS	49.2156***
		CTS3 <- CTS	65.8372***
		CTS4 <- CTS	45.3858***
	Severity of sanctions (SS)	SS1 <- SS	41.2055***
		SS2 <- SS	28.8788***
		SS3 <- SS	73.8854***
		SS4 <- SS	66.3148***
	Celerity of sanctions (CS)	CS1 <- CS	25.0746***
		CS2 <- CS	57.1455***
		CS3 <- CS	50.3961***
		CS4 <- CS	57.4192***
	Demand for resources	N/A	DPG1 <- Demand
DPG2 <- Demand			29.001***
DPG3 <- Demand			46.883***
Warm glow	Affective feeling (WGAF)	WGAF1 <- WGAF	51.9205***
		WGAF2 <- WGAF	85.2267***
		WGAF3 <- WGAF	31.3397***
		WGAF4 <- WGAF	106.1125***
		WGAF5 <- WGAF	126.7045***
	Role merger	WGRM1 <- WGRM	44.8449***
		WGRM3 <- WGRM	25.0409***
		WGRM4 <- WGRM	77.6096***
		WGRM5 <- WGRM	59.8945***
		WGRM6 <- WGRM	46.4988***
		WGRM7 <- WGRM	34.124***
		Subjective norm	WGSN1 <- WGSN
	WGSN3 <- WGSN		20.8284***
	WGSN4 <- WGSN		33.4858***
	WGSN5 <- WGSN		49.3056***
	WGSN7 <- WGSN		81.8692***
	Moral norms	WGMN1 <- WGMN	45.5017***
		WGMN2 <- WGMN	52.0115***
WGMN3 <- WGMN		91.8946***	
WGMN4 <- WGMN		60.6573***	
WGMN5 <- WGMN		57.0223***	
Uploading	N/A	U1 <- Uploading	97.1495***
		U2 <- Uploading	56.5617***

Note: * $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$

As a second check, the latent variable scores were compared against the indicators as a form of factor loadings, and then the indicator loadings and cross-loadings were examined to establish convergent validity. Though this approach is typically used to establish discriminant validity (Gefen & Straub, 2005), convergent validity and discriminant validity are inter-dependent and help establish each other (Straub *et al.*, 2004). Thus, following Kock (2010), convergent validity is also established when each loading for a latent variable is substantially higher than for other latent variables. This is done by correlating the latent variable scores against the indicators as a form of factor loadings (Gefen & Straub, 2005). Table 14 summarizes the loadings.

Table 14. Cross-loadings of measurement items to latent constructs for convergent and discriminant validity

Construct	Item	1	2	3	4	5	6	7	8	9
Celerity of sanctions (CS)	CS1	0.83	0.68	0.18	0.12	0.70	0.16	0.27	0.18	0.18
	CS2	0.91	0.75	0.21	0.08	0.80	0.17	0.28	0.21	0.21
	CS3	0.90	0.77	0.14	0.03	0.81	0.07	0.21	0.14	0.12
	CS4	0.91	0.77	0.14	0.07	0.84	0.17	0.29	0.20	0.18
Certainty of sanctions (CTS)	CTS2	0.70	0.89	0.16	0.07	0.72	0.15	0.30	0.21	0.17
	CTS3	0.77	0.90	0.22	0.15	0.76	0.25	0.34	0.28	0.24
	CTS4	0.76	0.88	0.14	0.09	0.74	0.17	0.30	0.23	0.21
Demand for resources	DPG1	0.18	0.18	0.88	0.43	0.15	0.60	0.47	0.62	0.58
	DPG2	0.15	0.15	0.84	0.40	0.14	0.47	0.32	0.46	0.44
	DPG3	0.16	0.18	0.88	0.44	0.17	0.56	0.41	0.58	0.55
Uploading	U1	0.13	0.15	0.49	0.94	0.13	0.66	0.65	0.68	0.64
	U2	0.01	0.07	0.42	0.92	0.04	0.55	0.53	0.56	0.53
Severity of sanctions (SS)	SS1	0.81	0.78	0.22	0.10	0.90	0.20	0.32	0.25	0.23
	SS2	0.71	0.69	0.09	0.04	0.84	0.03	0.17	0.07	0.09
	SS3	0.85	0.79	0.18	0.11	0.93	0.18	0.31	0.21	0.21
	SS4	0.79	0.70	0.15	0.07	0.90	0.12	0.28	0.17	0.17
Affective feeling (WGAF)	WGAF1	0.17	0.22	0.59	0.60	0.16	0.93	0.82	0.86	0.89
	WGAF2	0.14	0.19	0.56	0.61	0.13	0.94	0.76	0.86	0.82
	WGAF3	0.11	0.10	0.62	0.56	0.09	0.85	0.64	0.79	0.76
	WGAF4	0.16	0.22	0.58	0.62	0.16	0.95	0.78	0.86	0.83
	WGAF5	0.16	0.22	0.56	0.62	0.15	0.95	0.80	0.88	0.83
Moral norms (WGMN)	WGMN1	0.25	0.31	0.35	0.48	0.28	0.66	0.88	0.69	0.64
	WGMN2	0.25	0.29	0.49	0.62	0.26	0.80	0.92	0.85	0.77
	WGMN3	0.28	0.33	0.41	0.60	0.29	0.78	0.94	0.79	0.76
	WGMN4	0.25	0.32	0.49	0.64	0.26	0.82	0.92	0.84	0.81
	WGMN5	0.31	0.35	0.36	0.54	0.31	0.70	0.91	0.74	0.69

Construct	Item	1	2	3	4	5	6	7	8	9
Role merger (WGRM)	WGRM1	0.20	0.30	0.49	0.60	0.21	0.82	0.80	0.88	0.77
	WGRM3	0.24	0.29	0.66	0.55	0.21	0.75	0.68	0.84	0.70
	WGRM4	0.17	0.23	0.61	0.59	0.15	0.86	0.77	0.92	0.79
	WGRM5	0.17	0.20	0.56	0.61	0.15	0.85	0.77	0.90	0.80
	WGRM6	0.15	0.21	0.58	0.60	0.19	0.82	0.75	0.89	0.80
	WGRM7	0.17	0.21	0.50	0.59	0.14	0.76	0.76	0.86	0.73
	Subjective norm (WGSN)	WGSN1	0.13	0.15	0.61	0.60	0.14	0.80	0.69	0.79
WGSN3		0.14	0.10	0.46	0.50	0.13	0.65	0.58	0.64	0.80
WGSN4		0.22	0.25	0.46	0.51	0.19	0.71	0.68	0.70	0.85
WGSN5		0.17	0.24	0.51	0.52	0.20	0.81	0.72	0.76	0.89
WGSN7		0.18	0.24	0.56	0.59	0.19	0.88	0.80	0.85	0.92

Discriminant validity

Discriminant validity is shown when: (1) measurement items need to load highly on their theoretical assigned factor but not so highly on other factors, and (2) the square root of every AVE (one for each latent construct) needs to be much larger than any correlation among any pair of latent constructs (Gefen & Straub, 2005).

Two established methods were used to determine the discriminant validity, as described in Gefen and Straub (2005) and as demonstrated in Lowry *et al.* (2008; 2009). First, as with convergent validity, the factor loadings were examined, but this time to ensure that a significant overlap did not exist between the constructs (again, see Table 14 above). All loadings were appropriate.

Second, we used the approach of examining the square roots of the AVEs, as described in Gefen and Straub (2005); the AVE analysis is summarized in Table 15 below. The basic standard followed here is that the square root of the AVE for any given construct (latent variable) should be higher than any of the correlations involving the construct (Fornell & Larcker, 1981). The numbers are shown in the diagonal for constructs (bolded). Strong discriminant validity was shown between all constructs.

Table 15. AVE analysis to establish discriminant validity and construct correlation to test common method bias

	1	2	3	4	5	6	7	8	9
Celerity of sanctions (CS)	0.79								
Certainty of sanctions (CTS)	0.64	0.80							
Demand for resources	0.19	0.20	0.75						
Severity of sanctions (SS)	0.69	0.73	0.18	0.79					
Uploading (U)	0.08	0.12	0.49	0.09	0.87				
Affective feeling (WGAF)	0.16	0.21	0.63	0.15	0.65	0.85			
Moral norms (WGMN)	0.29	0.35	0.46	0.30	0.64	0.72	0.84		
Role merger (WGRM)	0.21	0.27	0.64	0.20	0.67	0.72	0.76	0.78	
Subjective norm (WGSN)	0.19	0.23	0.61	0.20	0.63	0.69	0.61	0.67	0.75

Reliability

Reliability refers to the degree to which a scale yields consistent and stable measures over time (Straub, 1989). Reliability differs from validity in that reliability concerns how a phenomenon is measured, whereas validity concerns what should be measured (Hair *et al.*, 1998).

One method for assessing reliability is the test-retest method. If the measurement shows free form errors, then when the measurement is repeated, the results should be the same (Hendrickson *et al.*, 1993). This is executed by using measurements from previous studies. The most commonly used measure of reliability is to assess the internal consistency of the items. SmartPLS computes Cronbach's alpha as well as the composite reliability score, which is evaluated in the same way as Cronbach's alpha (Fornell & Larcker, 1981). This score is a more accurate measurement of reliability than Cronbach's alpha, because it does not assume that the loadings or error terms of the items are equal (Chin *et al.*, 2003). However, as a conservative check, Cronbach's alpha can also be used as a basis for comparison. Thus, the two most conservative criteria were used where both the composite reliability and the Cronbach's alpha coefficients should be ≥ 0.7 (Fornell & Larcker, 1981; Kock, 2010; Nunnally & Bernstein, 1994). Both analyses indicate a high reliability for all subconstructs, as summarized in Table 16.

Table 16. Construct reliabilities

Construct	Composite Reliability	Cronbach's α
Celerity of sanctions (CS)	0.94	0.91
Certainty of sanctions (CTS)	0.92	0.87
Demand for resources	0.90	0.83
Severity of sanctions (SS)	0.94	0.91
Uploading (U)	0.93	0.85
Affective feeling (WGAF)	0.97	0.96
Moral norms (WGMN)	0.96	0.95
Role merger (WGRM)	0.95	0.94
Subjective norm (WGSN)	0.94	0.91

Validation for formative constructs

The measurement quality of our formative constructs, warm glow and sanctions, was evaluated in two ways following the suggestions by Chin (1998) and Diamantopoulos *et al.* (2001). First, the correlations between measurement items for the formative constructs were examined. The absolute correlation between their subconstructs (see Table 15) measuring warm glow (affective feeling, moral norms, role merger, and subjective norm) and sanctions (celerity of sanctions, certainty of sanctions, and severity of sanctions) ranged from 0.61 to 0.73. The relatively low correlation suggests that the herding construct is better represented as a formative construct; a reflective construct would show extremely high correlations (often above 0.8) between its measurement items (Pavlou & Sawy, 2006).

Next, the strength of the relationship between the formative construct and its measurement subconstructs was assessed by using latent variable scores. For warm glow, all subconstructs had significant path coefficients (or PLS weight) (Fig. 9). The VIF was then computed to assess the multicollinearity of the four subconstructs. VIF values above 10 would suggest the existence of excessive multicollinearity and would raise doubts about the validity of the formative measurement (Diamantopoulos *et al.*, 2001). The VIF values varied from 3.52 to 7.83 for the four subconstructs measuring warm glow.

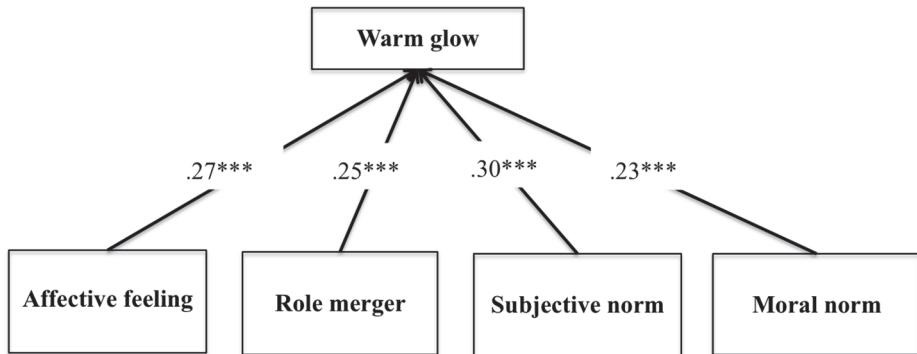


Fig. 9. PLS result for the relationship between warm glow and its four sub-constructs. Completely standardized path coefficients (or PLS weights). *significant at 0.001 level.**

For sanctions, all subconstructs also had significant path coefficients (or PLS weight; Fig. 10). The VIF was then computed to assess the multicollinearity of the three subconstructs. VIF values above 10 would suggest the existence of excessive multicollinearity and would raise doubts about the validity of the formative measurement (Diamantopoulos *et al.*, 2001). However, the VIF values for the three subconstructs measuring sanctions varied from 3.65 to 6.93, and therefore, multicollinearity was not a concern in this study.

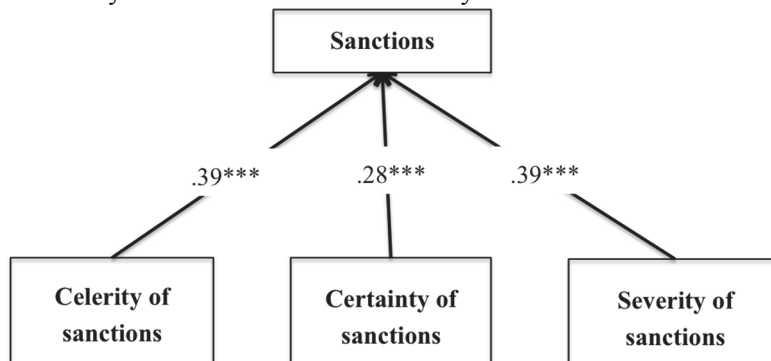


Fig. 10. PLS results for the relationship between sanctions and its three sub-constructs. Completely standardized path coefficients (or PLS weights). *significant at 0.001 level.**

Testing for common methods bias

To decrease the likelihood of common method bias occurring in our data collection, items within the instrument were randomized so that participants would be less apt to detect underlying constructs, another potential source of common method bias (Cook & Campbell, 1979; Straub *et al.*, 2004). However, all the data was collected using a self-report survey, in which the same subject responds to the items in a single questionnaire at the same point in time. Therefore, this data was likely to be susceptible to the common method variance (CNV) or common method bias (CMB), which compromises the credibility of the results of the data analysis (Malhotra *et al.*, 2006). To avoid the CMB threats, it was necessary to test for common method bias to establish that it was not a likely negative factor in the data remaining for our analysis. To do so, two approaches of increasing validity and rigor were used.

The first approach used here was to simply examine a correlation matrix of the constructs and to determine if any of the correlations were above 0.90, which would serve as evidence that common method bias may exist (Pavlou *et al.*, 2007). In the test, the construct correlation matrix, as calculated by PLS (reported above in Table 15), was examined to determine whether any constructs had an extremely high rate of correlation (more than .90). In our case, none of the constructs correlated so highly. This finding similarly indicates that common methods bias was not a problem. We now turn to a more rigorous and definitive second approach.

Our second approach to testing common method bias was to conduct the test established by Liang *et al.* (2007). This approach was suggested by Podsakoff *et al.* (2003) and adapted for PLS by Liang *et al.* (2007). As indicated previously, it is particularly useful because it has been established to overcome the classic issues of assessing common method bias (Liang *et al.*, 2007; Podsakoff *et al.*, 2003). The objective of this technique is to measure the influence of a common latent method factor on each individual indicator in the model versus the influence of each indicator's corresponding construct. More details about this technique, and how to perform it, can be found in Liang *et al.* (2007).

Table 17 provides the detailed analysis that resulted from our common method variance analysis. To interpret these results, the coefficients of the paths between the substantive constructs (λ_s) and the single-indicator constructs, as well as the coefficients of paths from the method factor (λ_m) to the single-indicator constructs, are considered loadings, which are represented by λ in the tables (Liang *et al.*, 2007). Following Liang *et al.* (2007), common method bias could be assessed by

examining the statistical significance of the loadings of the substantive factors (λ_s) and of the method factor (λ_m), and by comparing the variance of each indicator as explained by the substantive and method factors. The square of the substantive factor loading (λ_s^2) is interpreted as the percentage of indicator variance explained by the substantive factor, and the square of the method factor loading (λ_m^2) is interpreted as the percentage of indicator variance explained by the method factor.

Common method bias was a highly unlikely concern here because most of the substantive factor loadings were significant, most of the method factor loadings were insignificant, and the percentage of indicator variance due to substantive constructs was substantially greater than the percentage of indicator variance due to the method construct.

Aside from major differences in the frequency and magnitude of the significance of the loadings, the average substantive factor loading (λ_s) was 0.85, whereas the average method factor loading (λ_m) was 0.25. Most importantly, the variance of indicators due to substantive constructs (λ_s^2) was substantially greater than the variance due to the method construct (λ_m^2). These were 73% (λ_s^2) and 6% (λ_m^2), representing a ratio of nearly 11.4 to 1. We thus conclude from this analysis that our data collection had negligible influence due to common method bias.

Table 17. Results of common method bias test

Construct	Item	Substantive Factor Loading (λ_s)	Variance Explained (λ_s^2)	Method Factor Loading (λ_m)	Variance Explained (λ_m^2)
Celerity of sanctions (CS)	CS1	0.80***	0.64	0.25	0.06
	CS2	0.86***	0.74	0.27	0.07
	CS3	0.85***	0.73	0.19	0.03
	CS4	0.88***	0.78	0.26	0.07
Certainty of sanctions (CTS)	CTS2	0.80***	0.64	0.25	0.06
	CTS3	0.87***	0.76	0.33	0.11
	CTS4	0.83***	0.69	0.27	0.07
Severity of sanctions (SS)	SS1	0.88***	0.78	0.30	0.09
	SS2	0.76***	0.58	0.14	0.02
	SS3	0.90***	0.82	0.28	0.08
	SS4	0.83***	0.70	0.23	0.05
Demand for resources	DPG1	0.88***	0.77	0.24	0.06
	DPG2	0.84***	0.71	0.21	0.04
	DPG3	0.88***	0.78	0.21	0.04

Construct	Item	Substantive Factor Loading (λ_s)	Variance Explained (λ_s^2)	Method Factor Loading (λ_m)	Variance Explained (λ_m^2)
Uploading	U1	0.93***	0.87	0.25	0.06
	U2	0.93***	0.87	0.24	0.06
Affective feeling (WGAF)	WGAF1	0.92***	0.85	0.21	0.04
	WGAF2	0.89***	0.80	0.28	0.08
	WGAF3	0.81***	0.65	0.20	0.04
	WGAF4	0.90***	0.82	0.29	0.09
	WGAF5	0.91***	0.83	0.20	0.04
Moral norms (WGMN)	WGMN1	0.76***	0.57	0.24	0.06
	WGMN2	0.88***	0.78	0.28	0.08
	WGMN3	0.86***	0.75	0.25	0.06
	WGMN4	0.90***	0.80	0.29	0.08
	WGMN5	0.80***	0.64	0.29	0.08
Role merger (WGRM)	WGRM1	0.87***	0.75	0.26	0.07
	WGRM3	0.79***	0.62	0.20	0.04
	WGRM4	0.89***	0.79	0.28	0.08
	WGRM5	0.88***	0.78	0.27	0.07
	WGRM6	0.86***	0.74	0.26	0.07
	WGRM7	0.83***	0.68	0.22	0.05
	WGRM2	0.82***	0.67	0.27	0.07
Subjective norm (WGSN)	WGSN1	0.83***	0.69	0.23	0.05
	WGSN3	0.70***	0.49	0.29	0.09
	WGSN4	0.77***	0.59	0.26	0.07
	WGSN5	0.83***	0.69	0.22	0.05
	WGSN7	0.91***	0.82	0.29	0.09
Average		0.85	0.73	0.25	0.06

8.4.2 Structural model

Given that our data displays factorial validity and does not display common methods bias, the structural model was subsequently tested. Figure 11 and Table 18 summarize the results of hypotheses testing. In Figure 11, path coefficients are given for each path. R^2 values, which are presented below each dependent variable, reflect the predictive power of the model. The model could explain 53% of unauthorized uploading behavior.

Bootstrapping was performed to compute the *t*-values for each hypothesized relationship and for the potential impact of control variables. Among the six control variables, none has a significant impact on IS security investment.

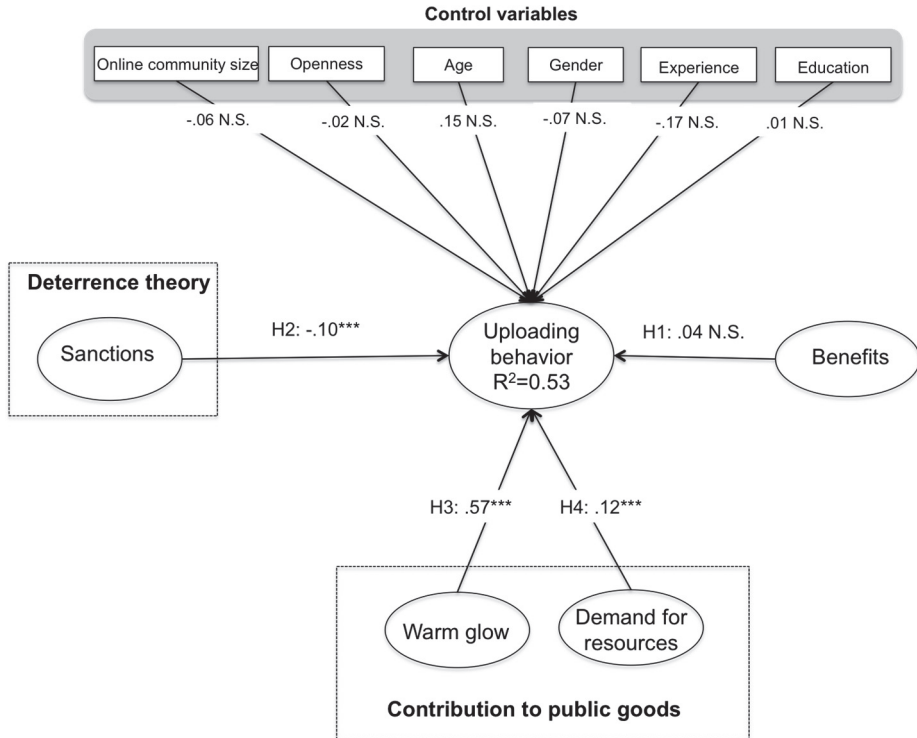


Fig. 11. PLS result.

Table 18. Summary of model results

#	Hypothesis	Coefficient	Supported?
H1	Benefit → Uploading	.04 N.S.	Yes
H2	Sanctions → Uploading	-.10***	Yes
H5	Warm glow → Uploading	.57***	Yes
H6	Demand for resources → Uploading	.12***	Yes

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

8.5 Summary of empirical findings

Our results support the theoretical model as well as the new assumption developed in Chapter 5, which will be discussed in turn.

First, our results suggest that benefits gained from uploading have no significant influence on users' unauthorized uploading behavior (H1). Therefore, we can conclude that users base their decisions to take the risk and upload unauthorized digital goods to online communities not on benefit considerations, but rather on other considerations, which are discussed below.

Second, our results indicate that warm glow leads to an increased in unauthorized uploading (H3). While this is a new finding in the area of information systems, the results are consistent with other related research that relies on impure altruism theory. In other words, if users perceive that they will derive emotional satisfaction from uploading behavior, they may engage in that behavior.

Third, our results indicate that users' demand for resources leads to an increase in unauthorized uploading (H4), which is also consistent with impure altruism theory. This indicates that reciprocity is a strong motivator, one which drives users' uploading behavior.

Fourth, our results suggest that sanctions do have a strong negative effect on uploading behavior (H2), which is consistent with previous piracy studies (Chiang & Assane, 2009; Chiou *et al.*, 2005; Christensen & Eining, 1991).

To conclude, our results support the assumptions of the new framework, indicating that benefit consideration may not be the motivation for users' unauthorized uploading behavior. Instead, satisfaction (warm glow) and demand for resources are shown to be strong motivators for these users.

9 The empirically grounded framework of IS security investment

The purpose of this thesis was to provide insights into IS security investment in organizations. The specific aim of this thesis was to understand, explain, and describe the decision making for investments on IS security. This process was aided by an empirically grounded framework, which also details the IS security investment. This was accomplished by first conceptualizing the decision-making for IS security investment, and then by empirically testing the assumptions in the framework. With this thesis, we sought to contribute to the literature on IS security investment, which lacks a thorough understanding of the characteristics of IS security investment, by providing novel and helpful concepts as well as a guiding framework.

9.1 The formation process of the empirically grounded framework

The first part of the thesis provided an outline of the research by depicting the characteristics of IS security investment and presented the scientific orientation employed. It concluded with a preliminary framework that can be used to describe the decision-making of IS security investment, as was presented in Figure 3.

The second part of the thesis tested the assumption of the framework developed in the first part. The assumptions were first tested in the context of IS security investment and then in a different research context.

This part of the thesis draws together the preliminary framework and empirical findings to form a coherent, empirically grounded framework to depict organizational IS security investment. The outcome was an assumption about the decision makers of IS security investment and the characteristics of IS security investments. The basic ideas that describe the development and formation of the empirically grounded framework are depicted in Figure 12.


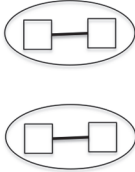
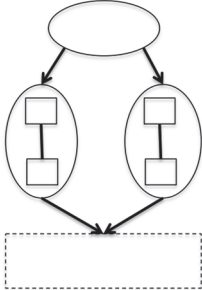
Part I		Chapter 5: Preliminary framework (Figure 5)
Part II		<p>Chapter 7: Verifying the assumption of the new framework in a field study</p> <p>Chapter 8: Verifying the assumption of the new framework in another research context</p>
Part III		Chapter 9: The empirically grounded framework of IS security investment is formed and the preliminary framework is adjusted to be coherent with the empirical findings

Fig. 12. Formation process of the empirically grounded framework.

Figure 12 shows the structure of the thesis and points out how the empirically grounded framework depicted in Figure 13 synthesizes the preliminary framework and empirical findings. In Figure 12, the circle in Part I depicts the preliminary framework, and the ovals in Part II depict the two empirical studies. In Part III, the diagram presents the formation of the empirically grounded framework as an interaction between previously presented elements.

9.2 The empirically grounded framework of IS security investment

This section presents the empirically grounded framework and discusses how it was formed from the interplay between the preliminary framework and the findings of empirical tests.

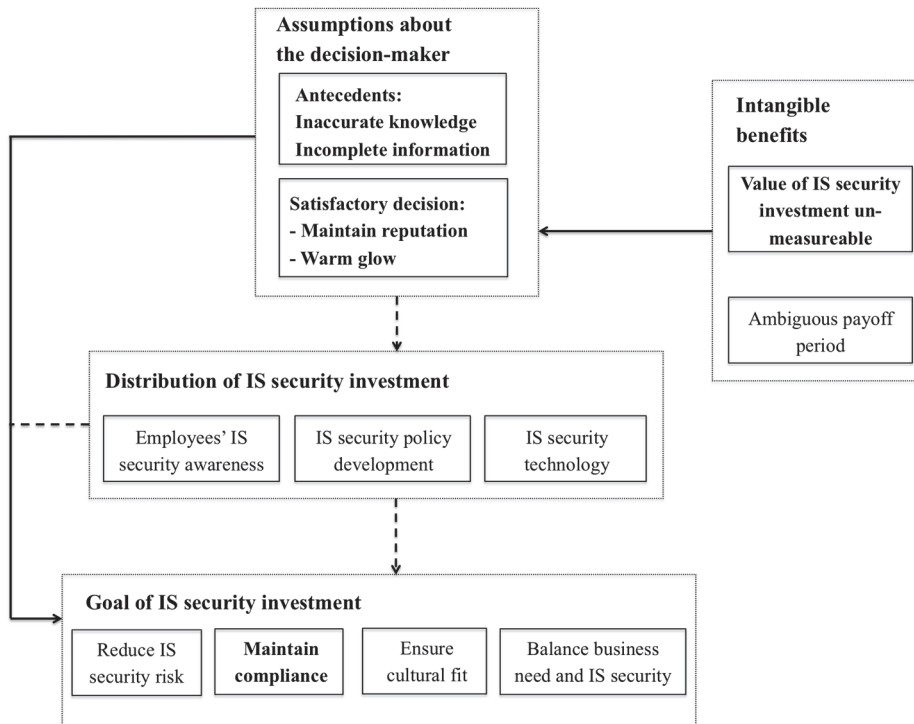


Fig. 13. Empirically grounded framework of IS security investment (dashed line: not tested; solid line: confirmed).

Figure 13 illustrates the structure of the empirically grounded framework for IS security investment. In order to explain IS security investment, Figure 13 incorporates the same factors that were used in the previous preliminary framework (Figure 3). Empirical findings from the two studies not only confirm the validity of the framework, but also provide new information to the framework. Distribution of IS security investment was not tested in the framework because of the nature of the research design.

The findings of the first empirical study confirm some parts of the framework. First, they confirm that maintaining compliance is a strong motive for IS security investment. As shown in the model, mandatory requirements imposed by laws or regulations predict IS security investment within organizations. Second, the findings also show that when decision makers have a limited ability to measure the value of IS security investment, they have an increased tendency to follow other

organizations' practices in order to maintain a good reputation. This confirms the interconnection between the intangible benefits of IS security investment and the assumptions about the decision maker.

The findings of the second empirical study confirm that benefits are not always the goal of human behavior. The results show that warm glow, which is a feeling of satisfaction, can be a strong predictor of unauthorized uploading behavior.

The changes made up until now are illustrated in Figure 13. Next, the thesis illustrates how the framework sheds light on IS security investment decision-making.

Instead of taking IS security investment as a whole, the framework suggests that it be divided into three important areas: measures to improve employees' IS security awareness, measures to develop IS security policy, and IS security technology itself. Accordingly, the goals of IS security investment are derived from the three investment areas. A way to evaluate the results of employees' IS security awareness training is the fitness of the organizational culture and of the IS security culture. When developing IS security policy, the balance of business needs and IS security needs should be kept in mind. The criterion to determine whether or not to implement IS security technology can be whether or not it helps reduce IS security risks. An additional goal of IS security investment is to maintain compliance to mandatory laws or regulations.

Due to congenital difficulties in measuring the value of IS security investment, decision makers lack reliable ways with which to assess the optimal investment level. Additionally, since the decision makers face inaccurate knowledge and incomplete information, they are highly unlikely to have the information or the computational power to discover or maintain the optimal profit-maximizing solution. Any satisfactory decision (such as maintaining a reputation as an IS security expert) can appear to be favorable if no new information can be searched.

10 Discussion and conclusions

This thesis was undertaken to understand, explain, and describe IS security investment in organizations. The purpose of the research was to understand what should be considered in making an investment in IS security.

This chapter draws together the proposed answers to the research question, discusses the limitations of the thesis, and suggests areas for future study. The structure of this chapter is as follows: first, the theoretical and then managerial contributions of this study are discussed. After that the limitations of the thesis and avenues for future research are presented.

10.1 Contribution of the thesis

10.1.1 Contributions of the new framework

How best to make an adequate IS security investment is a topic that has received much attention from researchers. Previous studies in IS security investment have developed economic models to determine how much to invest on IS security (e.g., Gordon & Loeb 2002; Huang *et al.*, 2008). However, it was found in this thesis that prior work has applied a neoclassical framework of decision-making that is not only in conflict with the characteristics of IS security investment, but is also problematic with its assumptions.

In this thesis, a new framework for IS security investment was advanced to fill the research gaps existing in previous studies. The purpose of the new framework here was to analyze the nature of IS security investment at the first level and produce respective guidance on how to manage IS security investment at the second level. With this new framework, three contributions are evident. First, the new framework advances fundamental characteristics of IS security investment, which clarify how IS security investment is different from other investments. This is an important contribution because a decision regarding IS security investment is based on these fundamental characteristics. Second, the new framework develops new assumptions for IS security investment decision makers. While neoclassical economics assumes decision makers as unbiased and rational, our new assumptions acknowledge the limitations of IS security investment decision makers. Compared with previous studies, the new assumptions describe the constraints of IS security investment decision makers and put the IS security investment research inside the

boundary. As the third contribution of the thesis, new theoretical and practical insights are advanced into how IS security investment research can be brought forward. As a new contribution, this thesis illustrates three research directions regarding how to execute IS security investment research based on the proposed new assumption (see section 10.3).

10.1.2 Contributions of a reputational herd model in explaining IS security investment motivation

The first empirical study (in Chapter 7) in this thesis aimed to show why IS security is under-invested in by organizations and to test the new assumption. To explore why IS security is under-invested, the empirical study employs the reputational herding model and the new assumption to establish hypotheses. The results support the new assumption by showing that benefits are not what IS security investment managers chase when making an IS security investment decision. However, to maintain a reputation is an objective that managers are chasing. Since IS security investment managers are uncertain of the intangible costs and benefits of IS security investment, estimating accurately for IS security investment is impossible. Therefore, supplementary strategies are employed in their decision-making. The results indicate that when facing uncertainty in the field of IS security investment, herding can be a supplementary strategy for IS security investment managers, which results in under-investment in IS security. This gives rise to future research that can study any other supplementary strategy that is employed in IS security investment decision-making, as suggested in the first research stream.

Second, this is the first study to adopt the reputational herding model in an IS context, particularly to IS security investment. This work provides a novel view of IS security investment decision-making, one that is applicable to any decision-making situations with uncertainty. This work indicates that the usage of novel theories in IS security research is an important contribution due to the novel insights that these theories provide to extant literature, and by expanding the nomological network of this research field.

Third, this is the first study that provides motivations other than analytic tools for IS security investment. Previous studies developed economic models to estimate the optimal level of IS security investment. However, economic models do not work if any influencing factors are neglected. This empirical study tests and confirms some influencing factors that are not included in previous economic models, for example, IS security managers' ability to accurately calculate the costs

and benefits of IS security investment, IS security managers' reputation, and so on. Future economic models of IS security investment can consider motivation factors inside.

10.1.3 Contributions of testing the new assumption in another context

The second empirical study (in Chapter 8) in this thesis aimed to test the new assumptions in another context by examining whether an unauthorized digital product uploader seeks a satisfactory result instead of maximum benefit from his behavior. The results confirmed the new assumptions. While in the context of IS security investment the satisfactory solution can be to maintain an IS security manager's (decision maker's) reputation, in the context of unauthorized uploading the satisfactory solution is to receive a warm glow from the behavior. When testing the new assumptions in a new context, we see the new assumptions are of generalizability.

Second, when testing the new assumption in a new context, we added a novel theory in the theoretical model to explain the unauthorized uploading behavior, together with the new assumption. Like applying reputational herding theory in Chapter 7, applying the impure altruism theory in Chapter 8 indicates that the novel insights can expand the nomological network of studying unauthorized uploading behavior.

Third, digital piracy studies usually focus on downloading behavior, disregarding different digital piracy behaviors. This empirical study provides new insights to the digital piracy literature by separating uploading from downloading behavior, and by approaching uploading behavior from different angles. The results show that there are different motivations for unauthorized uploading behavior, which was not investigated in digital piracy literature.

10.1.4 Overall contribution of the thesis

This thesis is composed of three parts in the field of IS security investment: developing a new framework for IS security investment research in Chapter 5, testing the new assumption in IS security investment context in Chapter 7, and testing the new assumption in a new setting in Chapter 8. While the first part of the thesis is targeted toward developing the theoretical foundations for IS security investment research, the second part empirically confirms the framework and

provides additional information to the framework. Both parts are needed for the following reasons. First, while previous studies of IS security investment simply view this form of investment to be the same as other investments, the new framework is developed by considering the characteristics of IS security investment, which makes the assumptions realistic for guiding research in IS security investment. Second, the new framework is developed in an analytical way without empirical testing, which makes a test of the new assumption necessary. Third, testing the new framework in a new setting provides the new assumptions the ability to explain other behavioral decision-making in other settings.

The new framework for IS security investment offer valuable contributions for IS security investment research. First, previous studies did not discuss the characteristics that differentiate IS security investment from other types of investments. The new framework, on the other hand, considers these differentiating IS security investment characteristics. Second, the new assumptions of the framework overcomes the unrealistic nature of the neoclassical economic assumption. The new assumptions consider the notion that decision makers have inaccurate knowledge and incomplete information. Third, the new framework advances new theoretical and practical insights as to how future IS security investment research can be conducted. There exist no similar IS security investment studies in the extant literature based on the new framework.

Through an empirical model explaining herd behavior in IS security investment, three main contributions are highlighted. First, although IS security investment is a major concern for organizations, little research has examined the motivations behind IS security investment. This thesis contributes by offering motivations other than costs or benefits. Second, little research has examined the herd behavior in IS security investment. This thesis contributes to the literature by offering the examination of herd behavior in IS security investment in Finnish companies and by increasing our understanding of IS security investment behaviors. Third, the thesis shows the effects of reputational and informational concerns on herding intention to invest on IS security. Fourth, reputational herding theory is demonstrated as an effective predictive model for IS security investment. Further, it is the first study in the field of IS security investment to apply reputational herding theory.

The empirical study of unauthorized uploading behavior contributes to the literature in three ways. First, this empirical study of unauthorized uploading behavior confirms the new assumption, which suggests that decision makers seek a satisfactory solution rather than a maximum benefit. Second, this empirical study

contributes by adding a novel theory in the theoretical model to explain unauthorized uploading behavior. Third, this empirical study contributes by regarding different digital piracy behaviors and by offering different motivations for unauthorized uploading behavior.

10.2 Implications for practice

Two practical implications of the new framework proposed for IS security investment research need to be highlighted. First, it should be admitted that it is not possible to accurately estimate the optimal level of IS security investment due to its characteristics. In practice, IS security investment managers should switch from pondering quantitative data of IS security investment to paying attention to what influences IS security investment decision-making. Second, the new framework suggests that IS security investment managers consider what is actually being done instead of what should be done. Cognitive limitations are inevitable in decision-making. In practice, IS security investment managers can investigate whether those cognitive limitations have affected their decision-making. As proposed with regard to incomplete information, the agency problem between CEOs and IS security investment managers is significant. Better communication channels should be established so that CEOs could better understand how hard IS security investment managers work, and therefore, asymmetric information could be eliminated.

Based on the results of the empirical study, herding strategies are used in making an IS security investment decision. In practice, this means that organizations should admit to the difficulties in estimating accurately the costs and benefits of IS security investment and understand that solely using cost-benefit analysis may make mistakes in IS security investment decision-making. However, it may be more realistic to pay attention to other companies' practices and then make investment decisions.

With respect to the reputational concern of IS security investment managers, we suggest that top management and supervisors should communicate more about IS security investment managers' work, and therefore, the agency problem can be reduced between supervisors and managers.

Regarding the information concern of IS security investment managers, we suggest that paying attention to both public and private information of IS security investment issues helps IS security investment managers make better investment decisions.

10.3 Limitations and implications for future research

All scientific research has limitations that can be pointed out, criticized, and brought forth for discussion. The author has attempted to cope with the limitations of this study. However, there are some inherent limitations that need to be further explained.

First, the framework developed for understanding IS security investment is not fully empirically evaluated. While Chapter 7 confirmed that the motivation of IS security investment is not just to receive benefit, there are other aspects of the new assumption to be tested. For example, the proposed criteria with which the decision makers feel satisfied with IS security investment need to be confirmed. This can be done in future research. Additionally, although we tested the new assumption in another setting, it is still difficult to assert that the new assumption is universally applicable, for example, to all decision-making situations.

Limitations of the latter part of the thesis are typical for quantitative studies. First, as is the case with most IS research, data was collected from within a single country. It may be possible that the results of this study cannot be applied generally to other countries and cultures. A needed avenue of future research is to examine the effects across cultures. Another limitation is the use of field studies as the only methodology of the thesis. While field studies offer the benefits of generalizability by examining professionals in actual organizational settings, there are several weaknesses as well, such as poor internal validity due to an inability to control the independent variables (Stone, 1978). A longitudinal survey or an experiment might be used to provide evidence of causal effects. In addition, the empirical studies were quantitative in nature. The use of surveys allowed us to collect data from a large number of respondents, which would be prohibitive using qualitative methods. However, the depth of understanding provided by surveys is limited compared to that afforded by qualitative research approaches (Orlikowski & Baroudi, 1991). Qualitative studies may help to deepen our understanding of the effects described in this thesis.

The thesis has attempted to open up new avenues of research regarding how to apply and improve the new framework. First, there needs to be further investigation into the different motivations of IS security investment. Second, it may be useful to investigate measures to determine the impact of IS security investment. A third research option might be to investigate the notion that IS security investment in organizations may not be a static decision-making process.

10.3.1 Examining different IS security investment motivations

Most of the existing research in IS security investment has been focused on determining the optimal level of investment. Prior research has been conducted by assuming that decision makers try to maximize the benefits from IS security investment, without examining the real reasons as to why organizations invest in IS security.

There are many underlying reasons, other than the maximization of benefits, that can drive IS security investment. For example, it is a common practice to follow other organizations' customs and influences. Indeed, IS security literature is full of discussions regarding the role of best practices and standards in IS security investment management (Siponen & Willison, 2009; Siponen, 2006; Baskerville, 1993; Siponen, 2005). Hence, it can be assumed that organizations spend money on implementing these standards, thereby following common investment practices. This phenomenon of implementing standards can be explained by the herding theory, as illustrated in this thesis, in which herding is defined as the obvious intent by investors to copy the behavior of other investors (Bikhchandani & Sharma, 2000). With regard to herding in IS security investment, if IS security investment managers have the ability to predict the benefits of an investment, they have no need to follow other security managers' practices regarding that investment. Scharfstein and Stein (1990) find that CEOs' perceptions of managers have an impact on managers' investment decisions. They suggest that if the manager of one firm adopts a particular technology, this creates a reputational externality in the sense that other managers will tend to be biased toward investing in the same technology for reputational reasons. Implementing IS security investment standards may create a reputation externality in IS security investment management; hence, security managers who are concerned about their reputations tend to herd.

Decision makers lack knowledge about the results of IS security investment (Siponen & Willison, 2009); therefore, theories that address the concern of making decisions under uncertainty may be relevant. For example, Black (1986) suggested that when decision makers are unsure about the results of an investment and lack necessary information to analyze potential results, they might invest based on noise. While noise is not truly information, people still make decisions based on noise as if it were. Shleifer and Summers (1990) point to the advice of financial gurus as one example of noise. Menkhoff (1998) showed that investors tend to follow experts' opinions. Take, for example, the task of implementing IS security investment standards. IS security investment managers are willing to invest in

implementing IS security investment standards, which are deemed by experts to be a best practice.

Another theory that may be relevant is agency theory. Agency problems in IS security investment management take place because of asymmetric information. The agent is assumed to have private information to which the principal cannot, without cost, gain access (Baiman, 1990, p. 343). It could be that inactivity (i.e., not using IS security investment standards) is the (best) optimal decision by IS security investment managers' efforts in researching. The difficulty is that the CEOs cannot distinguish between "actively doing nothing" and "simply doing nothing." CEOs may think that the IS security investment manager has not expended any effort to produce information or that he has no ability. It is not surprising that much of the literature shows that agents may take actions to increase principals' perceptions of their abilities (Kanodia, Bushman, & Dickhaut, 1989; Trueman, 1988). Kanodia, Bushman, and Dickhaut (1986) demonstrate that a manager may not give up an investment project found to be unprofitable because dropping it would reveal that the manager did not have accurate information at the time of investment.

To summarize the first research stream, given that management ultimately decides on whether or not an organization can invest in IS security, this research stream examines why management decisions are made. In addition to the aforementioned theories, different theories in behavioral economics, such as cognitive biases, heuristics, and investor's sentiment, can also be utilized to explain and predict the issues in this research stream. In this research stream, testable theories in terms of explaining and predicting (Gregor, 2009) are built with variance or factor models.

10.3.2 Identifying measurable impacts for IS security investment

The extant literature has focused on the economic impacts of IS security investment (Acquisti *et al.*, 2006; Campbell *et al.*, 2003; Cavusoglu *et al.*, 2004; Hovav & D'arcy, 2003, 2005; Tealng & Wattal, 2007). Nevertheless, investment in IS security includes aspects of adopting new technology to protect information, training employees to improve their compliance with security policies, implementing IS security investment standards, and so on. Abnormal returns of stock should not be the only result of IS security investment. Different viewpoints should be taken into account when studying the impact of IS security investment. Kayworth and Whitten (2010) suggest that effective IS security investment requires

a balance between different organizational needs and goals. Before developing an effective IS security investment strategy, it is necessary to first analyze different impacts that have been made by IS security investment.

One theory that may be useful for exploring the research question is external effect theory. In economics, an external effect is a cost or benefit that is incurred by a party who was not involved as either a buyer or a seller of the goods or services in a given transaction. Externality theory is helpful in exploring impacts indirectly caused by IS security investment, and thus allows for a comprehensive understanding of all the impacts of investment. For example, productivity, as well as training, can be considered an external effect. While IS security investment training improves employees' compliance with organizational security policy, spending time on taking care of IS security investment may reduce working productivity. Furthermore, the compatibility of IS security investment systems with other systems greatly affects employees' productivity. External effects are not always negative. Implementing IS security investment management standards in an organization is not only helpful for improving the management of the IS security investment, but it also creates a reputational externality for the security manager and a trust externality from business partners.

Quantitative and qualitative methods could be employed to answer the research questions within this direction of research, including action research, case study research, field studies, grounded theory, and critical research.

10.3.3 *Understanding IS security investment process*

Behavioral theories seek to determine what the actual frame of a decision is, how that frame arises from the decision situation, and how reason operates within that frame (Simon, 1986). Meanwhile, IS security investment may not necessarily be a static decision-making process for organizations. It generally involves several stages in the investment lifestyle, such as selection, control, and evaluation. IS security investment managers are concerned with different factors depending on which of these stages they are at in their decision-making process.

The selection stage is primarily about determining and allocating IS security investment that satisfies IS security investment requirements. In this stage, IS security investment managers make decisions regarding the total amount to invest in IS security as well as regarding the distribution of this investment. Once the investment is identified, the investment management cycle moves into the control stage, which consists of monitoring the investment to determine if the investment

is within the cost and schedule parameters. In this stage, IS security investment managers should use performance metrics to actively track investment cost and performance. The evaluation stage assesses the investment's impact and determines future costs for ongoing investments. The feedback and lessons from the evaluation stage can be used to refine processes within the selection and control phases. The investment can be stopped at any stage if it does not meet the requirement respectively, otherwise the stages keep repeating.

Although the three stages are just suggestions at this point, they seem to all be interrelated. For instance, investing in both IS security investment technology and employee training requires different metrics to control and evaluate. Several alternative theories can be considered to understand the process of making IS security investments. Path dependence theory provides insight from the angle of how previous practice has reinforced the current choice of process. The path dependence theory shows that learning effect, adaptive expectation, and coordination effect lead the reinforcement of previous practice. For example, learning from previous experience helps to improve the ability to manage IS security investment.

The process of making IS security investments would benefit from some of the studies from the first research stream. The issues identified in these studies would help to develop an understanding of each stage of the process. The process of IS security investment would use a variety of methods, such as case studies or action research. In action research, scholars can co-design the investment proposals (action research intervention) and investigate whether or not they are successful.

10.4 Conclusions

The assets of organizations have become increasingly informational in their nature. The need to secure organizations' assets has become an increasingly critical issue. Research in IS security investment has been working on developing analysis tools for evaluating how much to invest on IS security (e.g., Gordon & Lobe 2002; Huang *et al.* 2006, 2008). While focusing on developing analysis tools, however, previous studies fail to pay attention to the differentiating characteristics of IS security investment and investigate the reality of their underlying assumptions.

Prior research shares the common assumption that unbiased decision makers are trying to get the maximum benefit from IS security investment. The benefit maximization assumption has its root in neoclassical economics. However, it is argued in this thesis that the goal of IS security investment is more than to obtain

the maximum benefit. Therefore, it is not adequate to base research on IS security investment problems on a benefit maximization assumption. To address the drawback, as the main contribution, a new framework was proposed in this thesis for IS security investment, based on its own characteristics and new assumptions about decision makers.

Empirical parts of the thesis intended to test the new framework include testing motivations for IS security investment other than obtaining the maximum net benefit. The results show that due to the intangible nature of IS security investment benefits, IS security investment managers can't accurately predict costs and benefits of investment, therefore have the tendency to follow others' decisions on IS security investment. In this case, an IS security investment decision maker's reputation plays an important role. Based on reputational herding theory, this thesis contributes to IS research by presenting a model to understand what IS security investment managers take into account when making an investment decision.

Besides testing new assumptions in the context of IS security investment, this thesis also tests the new assumptions in another IS context. By studying users' unauthorized uploading of digital products to online communities, this thesis finds that a warm glow motivation is stronger than a benefit maximization motivation.

Based on the empirically grounded framework, the thesis outlines a research paradigm on important but not yet studied issues, which would enable practitioners to make better management decisions for IS security investments.

This thesis does not make its contribution by developing new analytical tools for estimating optimal IS security investments, but by developing a new framework with which to understand IS security investment, thus paving the way for future research. More specifically, this thesis contributes in the following ways. First, it considers the contextual factors of IS security investment and realistic assumptions of a decision maker. Second, the thesis empirically shows that in determining how much to invest in IS security, receiving the maximum net benefit is not the goal, but social factors (for example, a concern over reputation) are. Third, this thesis offers new research directions for this field.

Reference

- Acquisti A & Friedman TR (2006) Is there a cost to privacy breaches? An event study. Twenty-Seventh International Conference of Information Systems. URI: <http://aisel.aisnet.org/icis2006/94/>. Cited 2015/3/8.
- Ajzen I (1985) From Intentions to Actions: A Theory of Planned Behavior. In: Action-Control: From Cognition to Behavior. Berlin, Springer Berlin Heidelberg: 11–39.
- Al-Humaigani M & Dunn DB (2003) A model of return on investment for information systems security. Proceedings of the 46th IEEE International Midwest Symposium on Circuits & Systems, Cairo, 483–485.
- Anderson J (1972) Computer security technology planning study. U.S. Air Force Electronic Systems Division Technical Report 73–51.
- Andreoni J (1989) Giving with impure altruism: Applications to charity and Ricardian equivalence. *Journal of Political Economy* 97(6): 1447–1458.
- Andreoni J (1990) Impure altruism and donations to public goods: A theory of warm-glow giving. *The Economic Journal* 100(401): 464–477.
- Arrow KJ (1962) Economic Welfare and the Allocation of Resources for Innovation. In: The Rate and Direction of Inventive Activity: Economic and Social Factors. Universities-National Bureau: 609–626.
- Au YA & Kauffman RJ (2001) Should We Wait? Network Externalities, Compatibility, and Electronic Billing Adoption. *Journal of Management Information Systems* 18(2): 47–63.
- Axelsson S (2000) The base-rate fallacy and the difficulty of intrusion detection. *ACM Transactions on Information and System Security* 3(3): 186–205.
- Baiman S (1990) Agency Research in Managerial Accounting: A Second Look. *Accounting, Organizations and Society* 15(4): 341–371.
- Bandyopadhyay T, Jacob VS & Raghunathan S (2005) Information Security Investment Strategies in Supply Chain Firms: Interplay Between Breach Propagation, Shared Information Assets and Chain Topology. Eleventh Americas' Conference on Information Systems. URL: <http://aisel.aisnet.org/amcis2005/456/>. Cited 2015/3/8.
- Barclay D, Higgins C & Thomson R (1995) The Partial Least Squares Approach (PLS) To Causal Modeling, Personal Computer Adoption and Use As An Illustration. *Technology Studies* 2(2): 285–309.
- Barten AP & Böhm V (1982) Consumer theory. In: Kenneth Arrow and Michael Intrilligator (eds.) *Handbook of mathematical economics*. Vol. II, p. 384.
- Barua A, Kriebel CH & Mukhopadhyay (1991) An Economic Analysis of Strategic Information Technology Investments. *MIS Quarterly* 15(3): 313–333.
- Baskerville R (1991) Risk analysis: an interpretive feasibility tool in justifying information systems security. *European Journal of Information Systems* 1(2): 121–130.
- Baskerville R (1993) Information systems security design methods: implications for information systems development. *ACM Computing Surveys (CSUR)* 25(4): 375–414.

- Beaudry A & Pinsonneault A (2010) The other side of acceptance: studying the direct and indirect effects of emotions on information technology use. *MIS Quarterly* 34(4): 689–710.
- Becker GS (1974) A theory of social interactions. *Journal of Political Economy* 82(6): 1063–1093.
- Benner T & Vuorela M (2012) Netpirat: Jeg Betaler, Hvis Filmen Er God. Retrieved March 5, from <http://politiken.dk/kultur/tvogradio/ECE1558591/netpirat-jeg-betaler-hvis-filmen-er-god/>. Cited 2015/3/8.
- Bhattacharjee S, Gopal RD & Sanders GL (2003) Digital music and online sharing. *Communications of the ACM* 46(7): 107–111.
- Bikhchandani S & Sharma S (2000) Herding behavior in financial markets: A review. IMF Working Paper No. 00/48.
- Bikhchandani S, Hirshleifer D & Welch I (1992) A Theory of Fads, Fashion, Custom, and Cultural Change as Informational Cascades. *The Journal of Political Economy* 100(5): 992–1026.
- Bock GW, Zmud RW, Kim YG & Lee JN (2005) Behavioral Intention Formation in Knowledge Sharing: Examining the Roles of Extrinsic Motivators, Social-Psychological Forces, and Organizational Climate. *MIS Quarterly* 29(1) : 87–111.
- Böhme R & Felegyhazi M (2010) Optimal information security investment with penetration testing. In: *Decision and Game Theory for Security*. Berlin, Springer Berlin Heidelberg: 21–37.
- Böhme R & Moore T (2009) The Iterated Weakest Link--A Model of Adaptive Security Investment. The Eighth Workshop on the Economics of Information Security, London, England. June 24-25.
- Bojanc R & Jerman-Blažič B (2012) Quantitative Model for Economic Analyses of information Security investment in an Enterprise information System. *Organizacija* 45(6): 276–288.
- Bojanc R, Jerman-Blažič B & Tekavčič M (2012) Managing the investment in information security technology by use of a quantitative modeling. *Information Processing & Management* 48(6): 1031–1052.
- 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.
- Boudreau M-C, Gefen D & Straub DW (2001) Validation in Information Systems Research: A State-of-the-art Assessment. *MIS Quarterly* 25(1): 1–17.
- Brandenburger A & Polak B (1996) When managers cover their posteriors: Making the decisions the market wants to see. *Rand Journal of Economics* 27(3): 523–541.
- Brynjolfsson E & Hitt LM (1996) Paradox lost? Firm-level Evidence on the Returns to Information Systems Spending. *Management Science* 42(4): 541–558.
- 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.

- Business Software Alliance (BSA) (2012) Shadow market: 2011 BSA global software piracy study (9th ed.) URI: [http://globalstudy.bsa.org/\(2011/downloads/study_pdf/\(2011_BSA_Piracy_Study-Standard.pdf](http://globalstudy.bsa.org/(2011/downloads/study_pdf/(2011_BSA_Piracy_Study-Standard.pdf). Cited 2015/3/8.
- Buss MD & Salerno LM (1984) Common Sense and Computer Security. *Harvard Business Review* 62 (2): 112–121.
- Camerer CF and Loewenstein G (2002) Behavioral economics: past, present, future. in *Advances in Behavioral Economics*. New York: Russell Sage: 3–51.
- Campbell K, Gordon LA, Loeb MP & Zhou L (2003) The economic cost of publicly announced IS security breaches: empirical evidence from the stock market. *Journal of Computer Security* 11 (3): 431–448.
- Case KE & Fair RC (1989) *Principles of Economics*. Prentice Hall, London.
- Cavusoglu H & Raghunathan S (2004) Configuration of Detection Software: A Comparison of Decision and Game Theory Approaches. *Decision Analysis* 1(3): 131–148.
- Cavusoglu H, Mishra B & Raghunathan S (2004) A model for evaluating IT security investments. *Communications of the ACM* 47(7): 87–92.
- Cavusoglu H, Mishra B & Raghunathan S (2005) The Value of Intrusion Detection Systems in Information Technology Security Architecture. *Information Systems Research* 16(1): 28–46.
- Cavusoglu H, Raghunathan S, & Yue WT (2008) Decision-Theoretic and Game-Theoretic Approaches to IT Security Investment. *Journal of Management Information Systems* 25(2): 281–304.
- Chai S, Kim M & Rao HR (2011) Firms' information security investment decisions: Stock market evidence of investors' behavior. *Decision Support Systems* 50(4): 651–661.
- Chang A, Chaudhuri S & Jayaratne J (1997) Rational Herding and the Spatial Clustering of Bank Branches: An Empirical Analysis. Federal Reserve Bank of New York, Research Paper No. 9724.
- Chen YC, Shang RA & Lin AK (2008) The Intention to Download Music Files in a P2P Environment: Consumption Value, Fashion, and Ethical Decision Perspectives. *Electronic Commerce Research and Applications* 7(4): 411–422.
- Chiang EP & Assane D (2007) Determinants of Music Copyright Violations on the University Campus. *Journal of Cultural Economics* 31(3): 187–204.
- Chiang EP & Assane D (2009) Estimating The Willingness To Pay For Digital Music. *Contemporary Economic Policy* 27(4): 512–522.
- Chin WW (1998) Issues and Opinions on Structural Equation Modeling. *MIS Quarterly* 22(1): vii–xvi.
- Chin WW, Marcolin BL & Newsted PR (2003) A Partial Least Squares Latent Variable Modeling Approach for Measuring Interaction Effects: Results from a Monte Carlo Simulation Study and an Electronic-Mail Emotion/Adoption Study. *Information Systems Research* 14(2): 189–217.
- Chiou JS, Huang C & Lee H (2005) The Antecedents of Music Piracy Attitudes and Intentions. *Journal of Business Ethics* 57(2): 161–174.

- Choi JJ, Laibson D, Madrian BC & Metrick A (2003) Optimal Defaults. *American Economic Review Papers and Proceedings* 93(2): 180–185.
- Christensen AL & Eining MM (1991) Factors Influencing Software Piracy: Implications for Accountants. *Journal of Information Systems* 5(1): 67–80.
- Connolly T & Thorn BK (1990) Discretionary databases: Theory, data and implications. In: *Organizations and Communication Technology*. Newbury Park, CA, Sage: 219–234.
- Constant D, Sproull L & Kiesler S (1996) The kindness of strangers: Usefulness of electronic weak ties for technical advice. *Organization Science* 7(2): 119–135.
- Cook TD & Campbell DT (1979) *Quasi Experimentation: Design and Analytical Issues for Field Settings*. Chicago: Rand McNally.
- Cooper DR & Emory W (1995) *Business Research Methods*. Irwin, Chicago.
- Cornes R & Sandler T (1984) Easy riders, joint production, and public goods. *The Economic Journal* 94(375): 580–598.
- Cornes R & Sandler T (1994) The comparative static properties of the impure public good model. *Journal of Public Economics* 54(3): 403–421.
- Cremonini M & Nizovtsev D (2006) Understanding and influencing attackers' decisions: Implications for security investment strategies. *The Fifth Annual Workshop on Economics and Information Security*. Cambridge, UK.
- Cronan TP & Al-Rafee S (2008) Factors That Influence the Intention to Pirate Software and Media. *Journal of Business Ethics* 78(4): 527–545.
- Cronbach LJ (1970) *Essentials of Psychological Testing*. New York: Harper and Row.
- CSO Online: The 15 worst data security breaches of the 21st century. URI: <http://www.csoonline.com/article/2130877/data-protection/the-15-worst-data-security-breaches-of-the-21st-century.html>. Cited 2015/3/8.
- D'Arcy J & Greene G (2009) The Multifaceted Nature of Security Culture and Its Influence on End User Behavior. *IFIP TC 8 International Workshop on Information Systems Security Research*, Cape Town South Africa, May 29–30.
- D'Arcy J, Hovav A & Galletta DF (2008) User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research* 20(1): 79–98.
- d'Astous A, Colbert F & Montpetit D (2005) Music Piracy on the Web – How Effective Are Anti-Piracy Arguments? Evidence from the Theory of Planned Behaviour. *Journal of Consumer Policy* 28(3): 289–310.
- Daniels TE & Spafford EH (1999) Identification of host audit data to detect attacks on low-level IP. *Journal of computer* 7(1): 3–35
- D'Arcy J, Hovav A & Galletta DF (2009) User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research* 20(1): 79–98.
- Davis A (2005) Return on security investment – proving it's worth it. *Network Security* 11: 8–10.
- Denning D (1987) An intrusion-detection model. *IEEE Transactions on Software Engineering* 13(2): 222–226.

- Diamantopoulos A & Winklhofer HM (2001) Index Construction with Formative Indicators: An Alternative to Scale Development. *Journal of Marketing Research* 38(2): 269–277.
- DiMaggio PJ & Powell WW (1983) The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. *American Sociological Review* 48(2): 147–160.
- Dinev T & Hu Q (2007) The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies. *Journal of the Association for Information Systems* 8(7): 386–408.
- Duan W, Gu B & Whinston AB (2009) Information cascades and software adoption on the Internet: An empirical investigation. *MIS Quarterly* 33(1): 23–48.
- Ehrlich I (1973) Participation in Illegitimate Activities: A Theoretical and Empirical Investigation. *The Journal of Political Economy* 81(3): 521–565.
- Elffers H, Heijden P & Hezemans M (2003) Explaining Regulatory Noncompliance: A Survey Study of Rule Transgression for Two Dutch Instrumental Laws, Applying the Randomized Response Method. *Journal of Quantitative Criminology* 19(4): 409–439.
- Ernst & Young (2003) Global Information Security Survey. New York. URI: https://www2.eycom.ch/publications/items/saas_global_security_survey_2003/de.pdf. Cited 2015/03/08.
- Ernst & Young (2012) Under Cyber Attack: EY's Global Information Security Survey 2013. URI: [http://www.ey.com/Publication/vwLUAssets/EY_-_2013_Global_Information_Security_Survey/\\$FILE/EY-GISS-Under-cyber-attack.pdf](http://www.ey.com/Publication/vwLUAssets/EY_-_2013_Global_Information_Security_Survey/$FILE/EY-GISS-Under-cyber-attack.pdf). Cited 2015/03/08.
- Ferguson E, Atsma F, de Kort W & Veldhuizen I (2012) Exploring the pattern of blood donor beliefs in first-time, novice, and experienced donors: differentiating reluctant altruism, pure altruism, impure altruism, and warm glow. *Transfusion* 52(2): 343–355.
- Ferguson E, Taylor M, Keatley D, Flynn N & Lawrence C (2012) Blood donors' helping behavior is driven by warm glow: more evidence for the blood donor benevolence hypothesis. *Transfusion* 52(10): 2189–2200.
- Ferris GR, Blass FR, Douglas C, Kolodinsky RW & Treadway DC (2003) Personal reputation in organizations. In: J. Greenberg (Ed.), *Organizational behavior: The state of the science* (2nd ed) Mahwah, NJ: Lawrence Erlbaum.
- Fiol M & O'Connor E (2003) Waking Up! Mindfulness in the Face of Bandwagons. *Academy of Management* 28(1): 54–70.
- Fornell CR & Larcker DF (1981) Structural Equation Models with Unobservable Variables and Measurement Error: Algebra and Statistics. *Journal of Marketing Research* 18(3): 382–388.
- Gallaughier JM & Wang Y-M (2002) Understanding Network Effects in Software Markets: Evidence from Web Server Pricing. *MIS Quarterly* 26(4): 303–327.
- Gao X, Zhong W & Mei S (2013a) A differential game approach to information security investment under hackers' knowledge dissemination. *Operations Research Letters* 41(5): 421–425.
- Gao X, Zhong W & Mei S (2013b) Information Security Investment When Hackers Disseminate Knowledge. *Decision Analysis* 10(4): 35–368.

- 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: 91–109.
- Gefen D, Straub DW, & Boudreau M (2000) Structural Equation Modeling Techniques and Regression: Guidelines for Research Practice. *Communications of the Association for Information Systems* (7)7: 1–78.
- Gibbs JP (1975) *Crime, Punishment and Deterrence*. Amsterdam. The Netherlands: Elsevier.
- Gioia DA & Sims HP (1983) Perceptions of managerial power as a consequence of managerial behavior and reputation. *Journal of Management* 9(1): 7–26.
- Gopal RD, Sanders GL, Bhattacharjee S, Agrawal M & Wagner SC (2004) A Behavioral Model of Digital Music Piracy. *Journal of Organizational Computing and Electronic Commerce* 14(2): 89–105.
- Gordon LA & Loeb MP (2002) The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)* 5(4): 438–457.
- Gordon LA & Loeb MP (2006) Budgeting process for information security expenditures, *Communications of the ACM* 49(1): 121–125.
- Gottfredson MR & Hirschi T (1990) *A General Theory of Crime*. Palo Alto, CA: Stanford University Press.
- Graham JR (1999) Herding among Investment Newsletters: Theory and Evidence. *The Journal of Finance* 54(1): 237–268.
- Gregor S (2009) Building theory in the sciences of the artificial. The Forth International Conference on Design Science Research in Information Systems and Technology. Philadelphia, USA, May 06-08.
- Guerrien B (2002) Is There Anything Worth Keeping in Standard Microeconomics. *Post-autistic economics review*, issue no. 12, March 15, 2002, article 1. URI: http://www.btinternet.com/~pae_news/review/issue12.htm. Cited 2015/03/08.
- Gurrien B (2002) Once Again on Microeconomics. *Post-autistic economic review*, issue no. 16, September 16, 2002, article 1. URI: <http://www.paecon.net/PAEReview/issue16/Guerrien16.htm>. Cited 2015/03/08.
- Hair JF, Anderson RE, Tatham RL & Black WC (1998) *Multivariate Data Analysis*, (5th ed.) Upper Saddle River, Prentice Hall.
- Hair JFJ & RE Anderson *et al.* (1998) *Multivariate data analysis*. Upper Saddle River, New Jersey, Prentice Hall Inc.
- Hamill JT, Deckro RF & Kloeber JM Jr (2005) Evaluating information assurance strategies. *Decision Support Systems* 39(3): 463–484.
- Hare C (2002) Policy Development. In: H. F. Tipton & M. Krause (Eds.), *Information Security Management Handbook* (4th ed Vol. 3, 353-383) New York: Auerbach Publications.
- 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.
- Hausken K (2006) Income, interdependence, & substitution effects affecting incentives for security investment. *Journal of Accounting and Public Policy* 25(6): 629–665.

- Hendrickson AR, Massey PD & Cronan TP (1993) On the Test-Retest Reliability of Perceived Usefulness and Perceived Ease of Use Scales. *MIS Quarterly* 17 (2): 227–230
- Herath T & Rao HR (2009a) Protection Motivation and Deterrence: a Framework for Security Policy Compliance in Organizations. *European Journal of Information Systems* 18(2): 106–125. □
- Herath T & Rao HR (2009b) Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures, and Perceived Effectiveness. *Decision Support Systems* 47: 154–165.
- Higgins GE (2005) Can Low Self-Control Help with the Understanding of the Software Piracy Problem? *Deviant Behavior* 26(1):1–24.
- Higgins GE (2007) Digital Piracy: An Examination of Low Self-Control and Motivation Using Short-Term Longitudinal Data. *Cyberpsychology & Behavior* 10(4): 523–529.
- Higgins GE, Fell BD & Wilson AL (2006) Digital Piracy: Assessing the Contributions of an Integrated Self-Control Theory and Social Learning Theory Using Structural Equation Modeling. *Criminal Justice Studies* 19(1): 3–22.
- Higgins GE, Wilson AL & Fell BD (2005) An Application of Deterrence Theory to Software Piracy. *Journal of Criminal Justice and Popular Culture* 12(3): 166–184.
- Hirshleifer D (2001) Investor psychology and asset pricing. *Journal of Finance* 56(4): 1533–1597.
- Hodgson GM (2002) Theoretical Substance Should take Priority over technique. *post-autistic economics review*, issue no. 14, June 21, 2002, article 5. URI: http://www.btinternet.com/~pae_news/review/issue14.htm. Cited 2015/03/08.
- Höne K & Eloff JHP (2002) Information security policy-what do international information security standards say? *Computers & Security* 21(5): 402–409.
- Hovav A & D'Arcy J (2003) The impact of denial-of-service attack announcements on the market value of firms. *Risk Management and Insurance Review* 6 (2): 97–121.
- Hovav A & D'Arcy J (2005) The impact of virus attack announcements on the market value of firms. *Information Systems Security* 13 (3): 32–40.
- Howard PD (2003) The Security Policy Life Cycle: Functions and Responsibilities. In: H. F. Tipton & M. Krause (Eds.), *Information Security Management Handbook* (4th ed Vol. 4, 999) Boca Raton: CRC Press, LLC.
- Huang CD & Behara RS (2013) Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints. *International Journal of Production Economics* 141(1): 255–268.
- Huang CD & Goo J (2009) Investment Decision on Information System Security: A Scenario Approach. *American Conference on Information Systems (AMCIS) 2009 proceedings*.
- Huang CD (2010) Optimal Investment in Information Security: A Business Value Approach. *PACIS 2010 Proceedings*.
- Huang CD, Behara RS & Goo J (2014) Optimal information security investment in a Healthcare Information Exchange: An economic analysis. *Decision Support Systems* 61: 1–11.

- Huang CD, Behara RS & Hu Q (2007) Economics of information security investment. In: *Handbooks in Information Systems*: 53–69.
- Huang CD, Hu Q & Behara RS (2006) Economics of information security investment in the case of simultaneous attacks. The Fifth Workshop on the Economics of Information Security. URI: <http://weis2006.econinfosec.org/docs/15.pdf>. Cited 2015/03/08.
- Huang CD, Hu Q & Behara RS (2008) An economic analysis of the optimal information security investment in the case of a risk-averse firm. *International Journal of Production* 114(2): 793–804.
- Hunt SD & Vitell S (1986) A General Theory of Marketing Ethics. *Journal of Macromarketing* 6(1): 5–16.
- Hyeun-Suk R, Young UR & Cheong-Tag K (2005) I Am Fine But You Are Not: Optimistic Bias and Illusion of Control on Information Security. Twenty-Sixth International Conference of Information Systems, Las Vegas, NV, December 11-14.
- Information Security Breaches Survey (2014) Pricewaterhouse Coopers on behalf of the UK Department for Business Innovation & Skills. URI: <http://www.pwc.co.uk/audit-assurance/publications/2014-information-security-breaches-survey.jhtml>. Cited 2015/03/08.
- InformationWeek (2005) U.S. Information Security Research Report. United Business Media, London.
- Janak P (2011) Classification of Causes and Effects of Uploading and Downloading of Pirated Film Products. *World Academy of Science, Engineering and Technology* 60: 883–887
- Jevons WS (1871) *Theory of Political Economy*. London and New York, Macmillan and Co.
- Johnston AC & Warkentin M (2010) Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly* 34(3): 549–566
- Kahneman D, Slovic P and Tversky A (1982) *Judgement under Uncertainty: Heuristics and Biases*. Cambridge and New York: Cambridge University Press.
- Kahneman D & Tversky A (1979) Prospect theory: An analysis of decision under risk. *Econometrica: Journal of the Econometric Society* 47(2): 263–292
- Kanodia, Bushman, & Dickhaut (1986) Private information and rationality in the sunk costs phenomenon. Working paper. University of Minnesota.
- Kanodia, Bushman, & Dickhaut, (1989) Escalation Errors and the Sunk Cost Effect: An Explanation Based on Reputation and Information Asymmetries. *Journal of Accounting Research* 27(1): 59–77.
- Karaganis J (2011) Copyright Infringement and Enforcement in the US: A Research Note. The American Assembly, Columbia University, New York.
- Kauffman RJ & Li X (2003) Payoff Externalities, Informational Cascades and Managerial Incentives: A Theoretical Framework for IT Adoption Herding. In: Working Paper WP 03-18, Management Information Systems Research Center, University of Minnesota.
- Kauffman RJ, McAndrews J & Wang YM (2000) Opening the ‘Black Box’ of Network Externalities in Network Adoption. *Information Systems Research* 11(1): 61–82.
- Kayworth T & Whitten D (2010) Effective IS security requires a balance of social and technology factors. *MIS Quarterly Executive* 9(3): 163–175.

- Kennedy RE (2002) Strategy Fads and Competitive Convergence: An Empirical Test for Herd Behavior in Prime-Time Television Programming. *Journal of Industrial Economics* 50(1): 43–56.
- Klepper S & Nagin D (1989) The deterrent effect of perceived certainty and severity of punishment revisited. *Criminology* 27(4): 721–746.
- Kock N (2010) WarpPLS 1.0 User Manual. Laredo, Texas, USA: ScriptWarp Systems.
- Kollock P (1999) The economies of online cooperation: Gifts and public goods in cyberspace. M. A. Smith, P. Kollock, eds. *Communities in Cyberspace*. Routledge, London, 220–239.
- Konana P & Balasubramanian S (2005) The Social– Economic–Psychological Model of Technology Adoption and Usage: An Application to Online Investing. *Decision Support Systems* 39(3): 505–524.
- Kort PM, Haunschmied JL & Feichtinger G (1999) Optimal firm investment in security. *Annals of Operations Research* 88(0): 81–98.
- Kuhn TS (1962) *The Structure of Scientific Revolutions*. U.S.A: Printed by University of Chicago. ISBN: 0-226-45803-2
- Kwan SSK, So MKP & Tam KY (2010) Applying the Randomized Response Technique to Elicit Truthful Responses to Sensitive Questions in IS Research: The Case of Software Piracy Behavior. *Information Systems Research* 21(4): 941–959.
- Kwong C (2009) *Understanding Digital Piracy Behavior of Individuals in Virtual Communities*. Doctoral thesis, City University of Hong Kong, Department of Information Systems.
- 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 YJ, Kauffman RJ & Sougstad R (2011) Profit-maximizing firm investments in customer information security. *Decision Support Systems* 51(4): 904–920.
- Li H, Zhang & Sarathy R (2010) Understanding Compliance with Internet Use Policy from the Perspective of Rational Choice Theory. *Decision Support Systems* 48: 635–645.
- Li X & Nergadze N (2009) Deterrence Effect of Four Legal and Extralegal Factors on Online Copyright Infringement. *Journal of Computer-Mediated Communication* 14(2): 307–327.
- Li X (2004) Informational Cascades in IT Adoption. *Communications of the ACM* 47(4): 93–97.
- Liang H, Saraf N, Hu Q & Xue Y (2007) Assimilation of Enterprise Systems: The Effect of Institutional Pressures and the Mediating Role of Top Management. *MIS Quarterly* 31(1): 59–87.
- Lieberman MB & Asaba S (2006) Why Do Firms Imitate Each Other? *Academy of Management Review* 31(2): 366–385.
- Lin TC, Hsu MH, Kuo FY, Sun PC & Kaohsiung T (1999) An Intention Model-based Study of Software Piracy. *Proceedings of The 32nd Hawaii International Conference on System Sciences (HICSS'99)*. IEEE Computer Society, Maui, Hawaii.
- Liska AE & Steven FM (1999) *Perspectives on Crime and Deviance* (3rd ed.). Upper Saddle River, NJ: Prentice Hall.

- Liu D, Ji Y & Mookerjee V (2005) Information Security Investment with Different Information Types: A Two- Firm Analysis. AMCIS 2005 Proceedings.
- Liu D, Ji Y & Mookerjee V (2011) Knowledge sharing and investment decisions in information security. *Decision Support Systems* 52(1): 95–107.
- Loewenstein G & Prelec D (1992) Anomalies in intertemporal choice: evidence and an interpretation. *Quarterly Journal of Economics* 107(2): 573–597.
- Lowry PB, Romano NCJ, Jenkins JL & Guthrie RW (2009) The CMC Interactivity Model: How Interactivity Enhances Communication Quality and Process Satisfaction in Lean-Media Groups. *Journal of Management Information Systems* 26(1): 155–195.
- Lowry PB, Vance A, Moody G, Beckman B, & Read A (2008) Explaining and predicting the impact of branding alliances and Web site quality on initial consumer trust of e-commerce Web sites. *Journal of Management Information Systems* 24(4): 201–227.
- Lyonski S & Durvasula S (2008) Digital Piracy of MP3s: Consumer and Ethical Predispositions. *Journal of Consumer Marketing* 25(3):167–178.
- 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.
- Mackenzie SB, Podsakoff PM & Podsakoff NP (2011) Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques, *MIS Quarterly* 35(2): 293–334.
- Malhotra N, Kim S & Patil A (2006) Common Method Variance in IS Research: A Comparison of Alternative Approaches and a Reanalysis of Past Research. *Management Science* 52(12): 1865–1883.
- Mas-Colell A, Whinston MD & Green JR (1995) *Microeconomic Theory*. Oxford University Press, New York.
- McLean K (1992) Information Security Awareness – Selling the Cause. Proceedings of the IFIP TC11, Eighth International Conference on Information Security: IT Security: The Need for International Cooperation: 179–193.
- Menger C (1871) *Principles of Economics*. AA, Ludwig von Mises Institute, 2007.
- Menkhoff L (1998) The noise trading approach—Questionnaire evidence from foreign exchange. *Journal of International Money and Finance* 17(3): 547–564.
- Milliken FJ (1987) Three Types of Perceived Uncertainty about the Environment: State, Effect, and Response Uncertainty. *The Academy of Management Review* 12(1): 133–143.
- Mizzi A (2010) Return on information security investment-the viability of an anti-spam solution in a wireless environment. *International Journal of Network Security* 10(1): 18–24.
- Moore GC & Benbasat I (1991) Developing of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation. *Information Systems Research* 2(3): 192–222.
- Mullainathan S and Thaler RH (2000) *Behavioral Economics*. National Bureau of Economic Research Working Paper 7948.

- 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.
- Nunnally JC & Bernstein IH (1994) *Psychometric Theory*, 3rd edition. New York: McGraw-Hill.
- Nunnally JC (1978) *Psychometric theory*, MacGraw-Hill.
- Okoli C & Schabram K (2010) A guide to conducting a systematic literature review of information systems research. *Sprouts: Working Papers on Information Systems*, 10(26).
- Olson M (1965) *The Logic of Collective Action*. Harvard: Harvard University Press.
- Opaluch JJ & Segerson K (1989) Rational Roots of “Irrational” Behavior: New Theories of Economic Decision-Making. *Northeastern Journal of Agricultural and Resource Economics* 18 (2): 81–95.
- Pal R & Hui P (2011) Modeling Internet Security Investments: Tackling Topological Information Uncertainty. In: *Decision and Game Theory for Security*. Springer Berlin Heidelberg: 239–257.
- Parker DB (1976) *Crime by Computer*. New York, Scribner.
- Paternoster R & Simpson S (1996) Sanction threats and appeals to morality: Testing a rational choice model of corporate crime. *Law & Society Review* 30(3): 549–583.
- Paternoster R (1989) Decision to participate in and desist from four types of common delinquency: Deterrence and the rational choice perspective. *Law & Society Review* 23(1): 7–40.
- Pavlou PA & Sawy OAE (2006) From IT leveraging competence to competitive advantage in turbulent environments: the case of new product development. *Information Systems Research* 17 (3): 198–227
- Pavlou PA, Housel TJ, Rodgers W & Jansen E (2005) Measuring the return on information technology: a knowledge-based approach for revenue allocation at the process and firm level. *Journal of the association for information systems* 6(7): 199–226.
- 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.
- Peace AG, Galletta DF & Thong JYL (2003) Software Piracy in the Workplace: A Model and Empirical Test. *Journal of Management Information Systems* 20(1): 153–177.
- Perugini M & Bagozzi RP (2001) The Role of Desires and Anticipated Emotions in Goal-Directed Behaviours: Broadening and Deepening the Theory of Planned Behaviours. *British Journal of Social Psychology* 40(1): 79–98.
- Peslak AR (2008) Current Information Technology Issues and Moral Intensity Influences. *Journal of Computer Information Systems* 48(4): 77–86.
- Petter S, Straub D & Rai A (2007) Specifying Formative Constructs in IS Research. *MIS Quarterly* 31(4): 623–656.
- Pfeffer J (1992) *Managing with power: Politics and influence in organizations*. Boston: Harvard Business School Press.

- Plowman S & Goode S (2009) Factors Affecting the Intention to Download Music: Quality Perceptions and Downloading Intensity. *Journal of Computer Information Systems* 49(4): 84–97.
- Podsakoff PM, 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.
- Pryor A, Dalenberg D, McCorkle D, Reardon J & Wicks J (2008) Buy or Burn? Empirical Tests of Models of Crime Using Data from a General Population. *The Social Science Journal* 45(1): 95–106.
- Puhakainen P & Siponen M (2010) Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly* 34(4): 757–778.
- Puhakainen P (2006) Design Theory for Information Security Awareness. Doctoral thesis. University of Oulu.
- Purser SA (2004) Improving the ROI of the security management process. *Computers & Security* 23(7): 542–546.
- Rheingold H (1994) A slice of life in my virtual community. In: L. M. Harasim, ed. *Global Networks: Computers and International Communication*. MIT Press, Cambridge, MA: 57–80.
- Ricardo D (1817) *On the Principles of Political Economy and Taxation*. Piero Sraffa (Ed.) Works and Correspondence of David Ricardo, Volume I, Cambridge University Press, 1951.
- Ringle CM, Wende S & Will S (2005) SmartPLS 2.0 (M3) Beta.
- Rittenberg L & Tregarthen T (2012) *Principles of Microeconomics*. Flat World Knowledge.
- Rowe F (2014) What literature review is not: diversity, boundaries and recommendations. *European Journal of Information Systems* 23(3): 241–255.
- Sandulli FD (2007) CD Music Purchase Behaviour of P2P Users. *Technovation* 27(6-7): 325–334.
- Sapir J (2002) Response to Gurrien's Essay. Post-autistic economics review. URI: http://www.btinternet.com/~pae_news/review/issue13.htm. Cited 2015/03/08.
- Scharfstein DS & Stein JC (1990) Herd Behavior and Investment. *The American Economic Review* 80(3): 465–479.
- Schlienger T & Teufel S (2002) IS security Culture: The Socio-Cultural Dimension in IS security Management. The IFIP TC11 17th International Conference on Information Security: Visions and Perspectives: 191-202.
- Shanahan KJ & Hyman MR (2010) Motivators and Enablers of Scouring: A Study of Online Piracy in the US and UK. *Journal of Business Research* 63(9-10): 1095–1102.
- Shen XL, Zhang KZK & Zhao SJ (2014) Understanding Information Adoption in Online Review Communities: The Role of Herd Factors. Proceedings of the 47th Hawaii International Conference on System Science, Waikoloa, Hawaii, USA, January 1-9: 604-613.

- Shim W (2011) Vulnerability & Information Security Investment Under Interdependent Risks: A Theoretical Approach. *Asia Pacific Journal of Information Systems* 21(4): 27-43.
- Shleifer A & Summers LH (1990) The Noise Trader Approach to Finance. *Journal of Economic Perspectives* 4(2): 19-33.
- Shmanske S (1991) Public Goods, Mixed Goods, and Monopolistic Competition. Texas A&M University Press, College Station, TX.
- Simmons G (1994) Cryptanalysis and protocol failures. *Communication of ACM* 37(11): 56-64.
- Simon H (1986) Rationality in Psychology and Economics. *Journal of Business* 59(4): 209-224.
- Siponen M & Vance A (2010) Neutralization: New Insight into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly* 34(3): 487-502.
- Siponen MT & Willison R (2009) Information security management standards: Problems and solutions. *Information & Management* 46(5): 267-270.
- Siponen MT (2005) An analysis of the traditional IS security approaches: implications for research and practice. *European Journal of Information Systems* 14(3): 303-315.
- Siponen MT (2006) Six Design Theories for IS Security Policies and Guidelines. *Journal of the Association for Information Systems* 7(7): 445-472.
- Siponen MT, Pahnla 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. Proceedings of the IFIP TC-11 22nd International Information Security Conference (SEC 2007)*, 14-16 May 2007, Sandton, South Africa, 232/2007: 133-144.
- Sirkeci I & Magnusdottir LB (2011) Understanding Illegal Music Downloading in the UK: A Multi-Attribute Model. *Journal of Research in Interactive Marketing* 5(1): 90-110.
- Smith A (1776) *An Inquiry into the Nature and Causes of the Wealth of Nations*. University Of Chicago Press.
- Sonnenreich W, Albanese J & Stout B (2006) Return on security investment (ROSI)-A practical quantitative model. *Journal of Research and Practice in Information Technology* 38(1): 45-56.
- Standage T (2002) The weakest link. *Economist* 365(8296): 11-16.
- Stanton JM, Caldera C, Isaac, A, Stam KR & Marcinkowski SJ (2003), Behavioral IS security: Defining the criterion space. In: Mastrangelo PM & Everton WJ (eds) *The Internet at work or not: Preventing computer deviance*. Symposium presentation at the meeting of the society for Industrial and Organizational Psychology, Orlando.
- Stiglitz JE (1985) Economics of information and the theory of economic development. NBER working paper, No. 1566.
- 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 MC & Gefen D (2004) Validation Guidelines for IS Positivist Research. *Communications of the AIS* 13(24): 380-427.

- Sun H (2013) A longitudinal study of herd behavior in the adoption and continued use of technology. *MIS Quarterly* 37(4):1013–1041.
- Swanson EB & Ramiller NC (2004) Innovating Mindfully with Information Technology. *MIS Quarterly* 28(4): 553–583.
- Taylor SA, Ishida C & Wallace DW (2009) Intention to Engage in Digital Piracy a Conceptual Model and Empirical Test. *Journal of Service Research* 11(3): 246–262.
- Tealng R & Wattal S (2007) An empirical analysis of the impact of software vulnerability announcements on firm stock price. *IEEE Transactions on Software Engineering* 33 (8): 547–557.
- Thaler R (1981) Some empirical evidence on dynamic inconsistency. *Economics Letters* 8(3): 201–207.
- Tingling P & Parent M (2002) Mimetic Isomorphism and Technology Evaluation: Does Imitation Transcend Judgment? *Journal of Association for Information Systems* 3(1): 113–143.
- Trueman B (1988) A Theory of Noise Trading in Securities Markets. *The Journal of Finance* 43(1): 83–95
- Trueman B (1994) Analyst forecasts and herding behavior. *The review of financial studies* 7(1): 97–124.
- Tversky A & Kahneman D (1986) Rational choice and the framing of decisions. *Journal of Business* 59(4): S251–0S278.
- Tversky A & Thaler RH (1990) Anomalies: Preference reversals. *Journal of Economic Perspectives* 4(2): 201–211.
- Venkatesh V, Brown SA, Maruping LM & Bala H (2008) Predicting different conceptualizations of system use: The competing roles of behavioral intention, facilitating conditions, and behavioral expectation. *MIS Quarterly* 32(3): 483–502.
- Walden EA & Browne GJ (2002) Information Cascades in the Adoption of New Technology. In: *The 23th International Conference on Information Systems*, L. Applegate, R. Galliers, and J. I. DeGross (eds.), Barcelona, Spain: 435–443.
- Walden EA & Browne GJ (2009) Sequential Adoption Theory: A Theory for Understanding Herding Behavior in Early Adoption of Novel Technologies. *Journal of the Association for Information Systems* 10(1): 31–62.
- Walras L (1874) *Elements of Pure Economics*. London, George Allen and Unwin, 1954.
- Wang J, Chaudhury A & Rao HR (2008) A Value-at-Risk Approach to Information Security Investment. *Information Systems Research* 19(1): 106–120.
- Wang P (2010) Chasing the hottest IT: Effects of IT Fashion on Organizations. *MIS Quarterly* 34(1): 63–85.
- Wang SL, Chen JD, Stirpe PA & Hong TP (2009) Risk-neutral evaluation of information security investment on data centers. *Journal of Intelligent Information Systems* 36(3): 329–345.
- Wasko MM & Faraj S (2005) Why should I share? Examining social capital and knowledge contribution in electronic networks of practice. *MIS Quarterly* 29(1):35–57.
- Webster J & Watson RT (2002) Analyzing the past to prepare for the future: writing a literature review. *MIS Quarterly* 26(2): xiii–xxiii.

- Wellman B, Gulia M (1999) Net surfers don't ride alone: Virtual communities as communities. M. Smith, P. Kollock, eds. *Communities in Cyberspace*. Routledge, London: 167–194.
- Whitman ME & Mattord H (2005) *Principles of Information Security*. Course Technology, Boston.
- Willemson J (2006) On the Gordon & Loeb model for information security investment. The Fifth Workshop on the Economics of Information Security, University of Cambridge, England.
- Willemson J (2010) Extending the Gordon and Loeb Model for Information Security Investment. In *Proceedings of International Conference on Availability, Reliability, and Security*: 258–261.
- Wiseman S (1986) A secure capability computer system. In *Proceedings of the IEEE Symposium on Security and Privacy*. IEEE Computer Society Press, Los Alamitos, California: 86–94.
- Wood CC & Parker DB (2004) Why ROI and similar financial tools are not advisable for evaluating the merits of security projects. *Computer Fraud & Security* 5: 8–10.
- Wright BRE, Caspi A, Moffitt TE & Paternoster R (2004) Does the Perceived Risk of Punishment Deter Criminally Prone Individuals? Rational Choice, Self-Control, and Crime. *Journal of Research in Crime and Delinquency* 41(2): 180–213.
- Xu Z, Hu Q & Zhang C (2013) Why computer talents become computer hackers. *Communications of the ACM* 56(4): 64.
- Zinko R, Ferris GR, Humphrey SE, Meyer CJ & Aime F (2012) Personal reputation in organizations: Two-study constructive replication and extension of antecedents and consequences. *Journal of Occupational and Organizational Psychology* 85(1): 156–180.
- Zwiebel J (1995) Corporate conservatism and relative compensation. *Journal of Political Economy* 103(1): 1–25.

Appendix 1

In Table 19, prior research is analyzed in greater detail to explain how the neoclassical economics framework for decision-making has been used in previous studies.

Table 19. Analysis of prior research

Studies	Neoclassical Framework for Decision-Making			
	Preference	Maximization of Utility	Complete Information	Optimizing Conditions
Kort (1999)	The preference is expressed as a function of the net cash flow.	The study assumes that the objective of the firm is to maximize the net cash flow stream.	Not mentioned.	A set of first order necessary conditions that equate marginal benefits and marginal costs, subject to the second order conditions.
Gordon and Loeb (2002)	The preference is expressed as a function of the expected benefits of information security investment.	The study assumes that the firm tries to maximize the expected net benefits of information security investment.	Not mentioned.	A set of first order necessary conditions that equate marginal benefits and marginal costs, subject to the second order conditions.
Huang <i>et al.</i> (2006)	The preference is expressed as a function of the net benefit of all the security investments.	The study assumes that the optimization of the security investments is to maximize the benefits.	Not mentioned.	A set of first order necessary conditions that equate marginal benefits and marginal costs, subject to the

Studies	Neoclassical Framework for Decision-Making			
	Preference	Maximization of Utility	Complete Information	Optimizing Conditions
				second order conditions.
Willemson (2006)	The preference is expressed as a function of the expected benefits of information security investment.	The study assumes that the firm tries to maximize the expected net benefits of information security investment.	Not mentioned.	A set of first order necessary conditions that equate marginal benefits and marginal costs, subject to the second order conditions.
Huang <i>et al.</i> (2008)	The preference is expressed as an expected utility function.	The study assumes that the firm maximizes the expected utility.	Not mentioned.	A set of first order necessary conditions that equate marginal benefits and marginal costs, subject to the second order conditions.
Huang and Goo (2009)	The preference is expressed as a net benefit of the security investment function.	The study assumes that the firm maximizes the net benefit of security investment.	Not mentioned.	A set of first order necessary conditions that equate marginal benefits and marginal costs, subject to the second order conditions.
Wang <i>et al.</i> (2009)	The preference is expressed as an expected net benefit	The study assumes that the firm tries to maximize the expected net	Not mentioned.	A set of first order necessary conditions that equate marginal

Studies	Neoclassical Framework for Decision-Making			
	Preference	Maximization of Utility	Complete Information	Optimizing Conditions
	of the investment function.	benefits of information security investment.		benefits and marginal costs, subject to the second order conditions.
Bohme and Felegyhazi (2010)	The preference is expressed as an expected value of total profit.	It is mentioned in this study that the optimal defense strategy for the firm can be determined by summing up the expected total profit.	Not mentioned.	A set of first order necessary conditions that equate marginal benefits and marginal costs, subject to the second order conditions.
Huang (2010)	The preference is expressed as a business value of the information security investment function.	The study assumes that the task of optimizing the security investments is to maximize business value.	Not mentioned.	A set of first order necessary conditions that equate marginal benefits and marginal costs, subject to the second order conditions.
Willemson (2010)	The preference is expressed as a function of the expected benefits of information security investment.	The study assumes that the firm tries to maximize the expected net benefits of information security investment.	Not mentioned.	A set of first order necessary conditions that equate marginal benefits and marginal costs, subject to the second order conditions.

Studies	Neoclassical Framework for Decision-Making			
	Preference	Maximization of Utility	Complete Information	Optimizing Conditions
Lee <i>et al.</i> (2011)	The preference is expressed as a function of the expected profit from security investment.	The study assumes that the firm maximizes the expected profits.	Not mentioned.	A set of first order necessary conditions that equate marginal benefits and marginal costs, subject to the second order conditions.
Shim (2011)	The preference is expressed as the function of the expected benefits from information security investment.	The study assumes that the firm maximizes the expected benefits of security investment.	Not mentioned.	A set of first order necessary conditions that equate marginal benefits and marginal costs, subject to the second order conditions.
Bojanc <i>et al.</i> (2012)	The preference is expressed as a function of the benefit of the security measure investment.	Not mentioned.	Not mentioned.	A set of first order necessary conditions that equate marginal benefits and marginal costs, subject to the second order conditions.
Huang and Behara (2013)	The preference is expressed as a function of the net benefit of all the security investments.	This study assumes that the goal of optimizing the security investments is to maximize their benefits.	Not mentioned.	A set of first order necessary conditions that equate marginal benefits and marginal costs, subject to the

Studies	Neoclassical Framework for Decision-Making			
	Preference	Maximization of Utility	Complete Information	Optimizing Conditions
				second order conditions.
Huang <i>et al.</i> (2014)	The preference is expressed as a function of the net value of security investment.	The goal of optimizing the security investments is to maximize their value.	Not mentioned.	A set of first order necessary conditions that equate marginal benefits and marginal costs, subject to the second order conditions.
Cavusoglu <i>et al.</i> (2004)	The preference (for both the firm and the hacker) is expressed as a function of the expected payoff.	The firm maximizes its expected payoff. The hacker maximizes its payoff function.	Complete information is implicitly applied in the study. The solution to the game involves maximization of a polynomial function. Therefore, the firm needs to know the hacker's payoff function, and vice versa.	A set of first order necessary conditions that equate marginal benefits and marginal costs, subject to the second order conditions.
Cavusoglu and Raghunathan (2004)	The preference is expressed as a function of the firm's expected cost of the investment in information security, and as a function of the user's expected benefit.	The firm minimizes the expected cost, and the user maximizes the expected benefit.	Complete information is implicitly applied in the study. The solution to the game involves maximization of a polynomial function. Therefore, the firm	A set of first order necessary conditions that equate marginal benefits and marginal costs, subject to the second order conditions.

Studies	Neoclassical Framework for Decision-Making			
	Preference	Maximization of Utility	Complete Information	Optimizing Conditions
			needs to know the hacker's payoff function, and vice versa.	
Bandyopadhyay <i>et al.</i> (2005)	The preference is expressed as a function of total cost of the investment in security investment.	The firms (vendors and retailers) minimize the total cost of the investment in information security.	Complete information is implicitly applied in the study. The solution to the game involves minimization of a polynomial function. Therefore, the vendor needs to know the retailer's payoff function, and vice versa.	A set of first order necessary conditions that equate marginal benefits and marginal costs, subject to the second order conditions.
Cavusoglu <i>et al.</i> (2005)	The preference is expressed as a function of the firm's expected cost of the investment in information security, and as a function of the user's expected payoff.	This study assumes that the firm minimizes the expected cost of the investment in information security, while the user maximizes the expected payoffs.	Complete information is implicitly applied in the study. The solution to the game involves a polynomial function. The firm needs to know the user's expected payoff function, and the user needs to know the firm's expected cost function.	A set of first order necessary conditions that equate marginal benefits and marginal costs, subject to the second order conditions.
Liu <i>et al.</i> (2005)	The preference is expressed as a	The firms minimize their total costs.	Complete information is	A set of first order necessary

Studies	Neoclassical Framework for Decision-Making			
	Preference	Maximization of Utility	Complete Information	Optimizing Conditions
	function of total cost of the investment in information security for information-sharing firms.		implicitly applied in the study. The solution to the game involves minimization of a polynomial function. Therefore, each firm knows information about the other firm.	conditions that equate marginal benefits and marginal costs, subject to the second order conditions.
Cremonini and Nizovtsev (2006)	The preference is expressed as the expected net payoff function.	This study assumes that attackers choose the action that gets the maximum expected net payoff.	Not mentioned.	A set of first order necessary conditions that equate marginal benefits and marginal costs, subject to the second order conditions.
Hausken (2006)	The preference is expressed as a function of the profit.	This study assumes that both firms and agents maximize profit.	The solution of the game involves maximization of a polynomial function. Therefore, each player knows information about the other.	A set of first order necessary conditions that equate marginal benefits and marginal costs, subject to the second order conditions.
Cavusoglu <i>et al.</i> (2008)	The preference is expressed as a payoff function (for both the firm and the hacker).	Both the firms and hackers are assumed to maximize their profits.	The solution of the game involves maximization of a polynomial function. Therefore, each player knows	A set of first order necessary conditions that equate marginal benefits and marginal costs,

Studies	Neoclassical Framework for Decision-Making			
	Preference	Maximization of Utility	Complete Information	Optimizing Conditions
			information about the other.	subject to the second order conditions.
Bohme and Moore (2009)	The preference is expressed as a utility function.	In this study, the firm is assumed to maximize utility.	Not mentioned.	A set of first order necessary conditions that equate marginal benefits and marginal costs, subject to the second order conditions.
Liu <i>et al.</i> (2011)	The preference is expressed as an expected cost function.	In this study, the firms are assumed to minimize the expected cost.	The solution of the game involves minimization of a polynomial function. Therefore, each firm knows information about the other.	A set of first order necessary conditions that equate marginal benefits and marginal costs, subject to the second order conditions.
Pal and Hui (2011)	The preference is expressed as the utility/payoff function.	In this study, the firms are assumed to maximize utility/payoff.	It is mentioned that the game is symmetric. The utility functions of each player are the same, and each player's belief about the degrees of its neighbors are ex-ante symmetric.	A set of first order necessary conditions that equate marginal benefits and marginal costs, subject to the second order conditions.

Studies	Neoclassical Framework for Decision-Making			
	Preference	Maximization of Utility	Complete Information	Optimizing Conditions
Gao <i>et al.</i> (2013a)	The preference is expressed as the profit function.	In this study, the firms are assumed to maximize profit.	The solution of the game involves maximization of a polynomial function. Therefore, each firm knows information about the other.	A set of first order necessary conditions that equate marginal benefits and marginal costs, subject to the second order conditions.
Gao <i>et al.</i> (2013b)	The preference is expressed as the payoff function.	In this study, the firms are assumed to maximize payoffs.	The solution of the game involves maximization of a polynomial function. Therefore, each player knows information about the other.	A set of first order necessary conditions that equate marginal benefits and marginal costs, subject to the second order conditions.

Appendix 2

Table 20. Characteristics of IS security investment in prior work

Studies	Characteristics of IS Security Investment		
	Investment Area	Intangible Benefit	Investment Goal
Kort (1999)	Security equipment. Other areas are not mentioned.	Not mentioned.	Maximize the net cash flow stream.
Gordon and Loeb (2002)	General information security investment. No specific areas are mentioned.	Not mentioned.	Maximize the expected net benefits of information security investment.
Huang <i>et al.</i> (2006)	General information security investment. No mention of the investment areas.	Not mentioned.	Maximize the benefits of information security investment.
Willemson (2006)	General information security investment. No specific areas are mentioned.	Not mentioned.	Maximize the expected net benefits of information security investment.
Huang <i>et al.</i> (2008)	General information security investment. No mention of the investment areas.	Not mentioned.	Maximizing the expected utility of information security investment.
Huang and Goo (2009)	General information security investment. No mention of the investment areas.	Not mentioned.	Maximizing the net benefit of security investment.
Wang <i>et al.</i> (2009)	General information security investment. No mention of the investment areas.	Not mentioned.	Maximizing the net benefit of security investment.
Bohme and Felegyhazi (2010)	Not mentioned.	Not mentioned.	Not mentioned.
Huang (2010)	General information security investment. No mention of the investment areas.	Not mentioned.	Maximizing business value of security investment.
Willemson (2010)	General information security investment. No specific areas are mentioned.	Not mentioned.	Maximize the expected net benefits of information security investment.

Studies	Characteristics of IS Security Investment		
	Investment Area	Intangible Benefit	Investment Goal
Lee <i>et al.</i> (2011)	General information security investment. No specific areas are mentioned.	Not mentioned.	Maximize the expected profit from security investment.
Shim (2011)	General information security investment. No specific areas are mentioned.	Not mentioned.	Maximize the expected benefit of security investment.
Bojanc <i>et al.</i> (2012)	Security technology.	Not mentioned.	Reduce risk; give a positive return on the investment; help the organization to meet the legal requirement; influence individual and organizational awareness behavior in a positive direction.
Huang and Behara (2013)	General information security investment. No specific areas are mentioned.	Not mentioned.	Maximize the benefit of security investments.
Huang <i>et al.</i> (2014)	General information security investment. No specific areas are mentioned.	Not mentioned.	The goal of optimizing the security investments is to maximize their value.
Cavusoglu <i>et al.</i> (2004)	Intrusion detection system. No other investment areas are mentioned.	Not mentioned.	To maximize the firm's expected payoff.
Cavusoglu and Raghunathan (2004)	Detection software.	Not mentioned.	Minimizes the expected cost.
Bandyopadhyay <i>et al.</i> (2005)	General information security investment. No specific areas are mentioned.	Not mentioned.	Minimize the cost associated with security breaches.
Cavusoglu <i>et al.</i> (2005)	Intrusion detection systems.	Not mentioned.	The firm is to minimize the overall expected cost.
Liu <i>et al.</i> (2005)	General information security investment. No specific areas are mentioned.	Not mentioned.	Minimize the total cost of investment in information security.
Cremonini and Nizovtsev (2006)	Not mentioned.	Not mentioned.	Not mentioned.

Studies	Characteristics of IS Security Investment		
	Investment Area	Intangible Benefit	Investment Goal
Hausken (2006)	Information security technology. No other areas are mentioned.	Not mentioned.	To maximize profit.
Cavusoglu <i>et al.</i> (2008)	General information security investment. No specific areas are mentioned.	Not mentioned.	To maximize payoff.
Bohme and Moore (2009)	General information security investment. No specific areas are mentioned.	Not mentioned.	To maximize utility.
Liu <i>et al.</i> (2011)	General information security investment. No specific areas are mentioned.	Not mentioned.	To minimize expected cost.
Pal and Hui (2011)	General information security investment. No specific areas are mentioned.	Not mentioned.	To maximize utility/payoff.
Gao <i>et al.</i> (2013a)	General information security investment. No specific areas are mentioned.	Not mentioned.	To maximize profit.
Gao <i>et al.</i> (2013b)	General information security investment. No specific areas are mentioned.	Not mentioned.	To maximize payoffs.

Appendix 3

Appendix 3 outlines the scale development process for Chapter 7. The scale development in chapter 7 follows the procedure suggested by Mackenzie *et al.* (2012). The work of Moore and Benbasat (1991) on how to perform conceptual validation was also extensively referenced.

Stage 1: Conceptualization

An extensive literature review was conducted to examine how the focal construct has been defined in prior research.

Table 21. Conceptual definition of the constructs

Constructs	Definitions	Sources
Ability	The degree to which one is able to accurately predict the issues related to using IS security management standards.	Graham (1999)
Reputation	The extent to which IS security managers are perceived by others as performing their jobs competently.	Zinko <i>et al.</i> (2012).
Signal of Prior Information	The extremeness of information that predicts the possible outcomes of using IS security management standards.	Hirshleifer (2001)
Signal Correlation	The degree of behavioral similarity in using IS security management standard X by other IS security managers.	Graham (1999)
Herding (Second-Order)	A person follows others when implementing an IS security management standard.	Sun (2012)
Imitating others	The degree to which a person will follow others' decisions when using an IS security management standard.	
Discounting one's own information	The degree to which a person disregards his/her own beliefs about a particular IS security management standard when making a decision.	

Ability

In the herding model, if the investor has the ability to accurately assess the expected value of investment, he has less intention to herd. Scharfstein and Stein (1990) assume that there are two types of managers: “smart” ones, who receive informative

signals about the value of an investment, and “dumb” ones, who receive purely noisy signals. Graham (1999) defines ability by stating, “for a given realization investment outcome, ability measures the accuracy of informative signals,” and measures ability in terms of the proportion of analysts who make the “correct” recommendation. Sun (2012) defines uncertainty as “the degree to which one is unable to accurately predict the issues related to the adoption of a technology due to imperfect information.” We argue that uncertainty has causality with ability. The higher the ability, the less the uncertainty. We summarize the definitions developed by Graham (1999) and Sun (2012) to fit our context and define ability as: **the degree to which one is able to accurately predict the issues related to using an IS security management standard.**

Reputation

Reputation in the herding model refers specifically to people’s reputation within an organization about his/her capacity to perform jobs effectively. So general reputation measurements are not suitable in our context. We adopted the definition of reputation from Zinko *et al.* (2012): the extent to which individuals are perceived by others, over time, as performing their jobs competently and being helpful towards others in the workplace. We then slightly modified this definition to: **the extent to which individuals are perceived by others, over time, as performing their jobs competently in the workplace**, since helping others is not included in our theory.

Signal of Prior Information

Scharfstein and Stein (1990) refer to prior information in the herding model as the probability of possible outcomes of an investment. In Graham (1999)’s model, prior information is referred to as the prior probability of market movement that predicts stock returns. Hirshleifer (2001) defined the strength of an information realization in terms of how “extreme” the evidence is, and indicated that the weight of evidence is its reliability or precision. For example, a large sample of conditional signals has much weight. But if the preponderance of favorable over unfavorable signals is modest, it has low strength. **In conclusion, prior information refers to all information that can predict the possible return of IS security investment. So the strength of prior information indicates the degree of extremeness of such information.**

Signal Correlation

Since information is incomplete and private information cannot be known by others, one can only estimate others' information by observing their behavior, which is referred to as informative signals (Scharfstein & Stein 1990). Signal correlation in the model developed by Graham (1999) is referred to as a positive relationship between herding behavior and the degree to which informative signals are positively correlated. To sum up, signal correlation in our paper is defined as **the degree of behavioral similarity in using IS security management standard X by other IS security managers.**

Herding

Sun (2012) studied herd behavior in the adoption and continued use of technology and indicated, with regard to herd behavior, that “a person follows others when adopting a technology.” He also discussed the differences between herd behavior, network externality, and social norms. Furthermore, Sun (2012) proposed two new concepts to describe herding behavior in the adoption of technology—imitating others and discounting one’s own information—and argued that people consider both their private information and the observations of others’ actions when making a decision, and that people subjectively determine to what extent they can prudently base their decisions on the actions/decisions of other people. **Imitating others (IO) concerns the degree to which a person will follow others’ decisions when adopting a technology; discounting one’s own information (DOI) concerns the degree to which a person disregards his/her own beliefs about a particular technology when making an adoption decision.**

Stage 2: Development of measurements

1. Generate items to represent the construct.

New items were created to ensure that the concepts were well covered by their measures.

Table 22. Original items generated

Indicator	Questions
Ability	
A1	I can accurately point out the value of using IS security management standards.
A2	I know exactly what benefit we can get from using IS security management standards.
A3	I know exactly about the outcome of using IS security management standards.

Indicator	Questions
A4	I can predict that using IS security management standards is profitable for the company.
A5	I can predict accurately the benefit that IS security management standards bring to the company.
A6	I can predict accurately the issues of using IS security management standards.
A7	My predictions of the issues related with IS security management standards are usually correct.
Reputation	
R1	I am regarded highly by others in IS security management.
R2	I have a good reputation in IS security management.
R3	I have the respect of my colleagues and associates about IS security management.
R4	As an IS security manager, I am regarded as someone who gets things done.
R5	I have a reputation for producing results in IS security management.
R6	People know I will produce only high-quality results in IS security management.
R7	I have a reputation of producing the highest quality performance in IS security management.
R8	If people have problems about IS security management, they ask me.
Strength of prior information	
SI1	Our customers appreciate a lot using IS security management standard X.
SI2	Our business partners insist on using IS security management standard X.
SI3	We suffered significantly from not using IS security management standard X.
SI4	Some companies suffered significantly from not using IS security management standard X.
SI5	We lost a lot of business partners because we didn't use IS security management standard X.
SI6	We lost a lot of customers because we didn't use IS security management standard X.
SI7	We lost much business because we didn't use IS security management standard X.
SI8	I heard successful stories of using IS security management standard X in other companies.
SI9	There are successful stories of using IS security management standard X in other companies.
Signal correlation	
SC1	There is a trend in using IS security management standard X in other organizations.
SC2	There is a trend that many organizations have a plan for using IS security management standard X.
SC3	There is a trend that many organizations make an announcement that they are going to use IS security management standard X in the next few years.
SC4	Many organizations have used IS security management standard X for a few years.
SC5	The great majority of organizations are using IS security management standard X.

Indicator	Questions
SC6	The great majority of organizations have a plan to use IS security management standard X.
SC7	The great majority of organizations have been using IS security management standard X for long.
Imitating others	
IO1	I intent to follow other companies' use of IS security management standard X.
IO2	I choose to follow other companies' use of IS security management standard X.
IO3	I would like to follow other companies' practice in using IS security management standard X.
IO4	I follow others in using IS security management standard X.
IO5	It seems that using IS security management standard X is the dominant practice; therefore, I would like to use it as well.
IO6	I would choose to use IS security management standard X because many other companies are using it.
Discounting own information	
DOI1	My use of IS security management standard X would not totally reflect my own preferences.
DOI2	My use of IS security management standard X is not totally based on my own preferences.
DOI3	I make the decision to use IS security management standard X without paying attention to my own preferences.
DOI4	My own preferences didn't play an important role in selecting the IS security management standard X.
DOI5	I didn't make the decision on using IS security management standard X totally based on my own preferences.
DOI6	I didn't use my own preferences to decide whether to use IS security management standard X.
DOI7	It is not my own preferences that make me use IS security management standard X.

The original items of Ability, Signal of prior information, Signal correlation, Asymmetric information 1 and 2, and second-order constructs of Rationality (Cognition of environment, Assessment of investment options, and Principle of choice) are created by the author. Reputation items and second-order constructs of herding (imitating others and discounting own information) are developed based on Zinko *et al.* (2012) and Sun (2012).

2. Assess the content validity of the items.

Given that the questions for measuring the constructs were adapted from various sources or developed for this study, all of the questions were assessed for content validity. First, I constructed a matrix in which definitions of constructs were listed at the top of the columns and the items were listed in the rows. Next, raters

(including graduate students and doctors) were asked to rate the extent to which each item captured the definition using a five-point Likert-type scale ranging from 1 (not at all) to 5 (completely). Then a one-way repeated measures ANOVA was then used to assess whether an item's mean rating on one definition differed from its ratings on other definitions.

Stage 3: Model specification

When formally specifying the measurement model, identification problems may occur. For first-order constructs, I fixed a path between the latent construct and one of its indicators at 1.0. For second-order constructs, I fixed a path between the second-order construct and one of its sub-dimensions at 1.0.

Since the herd behavior was conceptualized as a second-order formative construct, I followed the recommendation of Mackenzie *et al.* (2012) and included two global reflective indicators of the composite latent constructs, along with the formative indicators. The addition of these two reflective indicators produced a “multiple indicators, multiple causes” (MIMIC) model structure.

Stage 4 and 5: Scale evaluation, refinement, and validation

Stage 4 and 5 involved pretesting, scale purification and refinement, gathering data from new samples to reexamine, assessing scale validity, and cross-validating the scale.

Two pretests were conducted (N1 = 32; N2 = 22). Convergent validity, nomological validity, and discriminant validity were assessed. Items with non-significant loadings on the hypothesized construct, squared completely standardized loadings that were less than .50, large and significant measurement error co-variances with other measures, or large and significant cross-loadings on non-hypothesized subdimensions were modified or deleted.

In total, 21 items were deleted or modified (A1, A3, A7, R3, R4, R7, R8, SC1, SC2, SC5, IO5, IO6, DOI3, DOI5, DOI7, SI4–9).

Stage 6: Norm development

I developed the norm of the scale by asking IS security managers in Finnish organizations to respond to our survey. The survey was sent to Finland's 700 Fortune companies' IS security managers, together with 342 other IS security

managers in companies that are not listed in the 700 Fortune list. The organizations were offered a report of our findings as an incentive to participate. All respondents to this survey were IS security managers who were familiar with IS security management. Among the 1042 surveys distributed in these organizations, 88 responses were obtained yielding a response rate of 8.44%.

Appendix 4

Table 23. Measurement items (Chapter 7).

Construct	Indicator	Item	Source
Ability	A2	I can accurately predict the benefit that this IS security management standard brings to my organization.	New items
	A4	I know accurately about the benefit of using this IS security management standard.	
	A5	I know accurately what benefit we can get from using this IS security management standard.	
	A6	My predictions of the benefit of using IS security management standards are usually accurate.	
Reputation	R1	I am regarded highly in managing IS security in my organization.	Zinko <i>et al.</i> (2012)
	R2	I have a good reputation in managing IS security in my organization.	
	R5	I have a reputation of producing good results in IS security management.	
	R6	I have a reputation of producing high quality performance in IS security management.	
Signal correlation	SC3	A large number of organizations have used this IS security management standard.	New items
	SC4	A large number of organizations are using this IS security management standard.	
	SC6	This IS security management standard is now serving a large number of organizations.	
	SC7	This IS security management standard is accepted by a large number of organizations.	
Imitating others	IO1	I follow other companies in using this IS security management standard.	Sun (2012)
	IO2	I use the same IS security management standard as other companies.	
	IO3	I select the same IS security management standard as other companies are using.	
	IO4	I use this IS security management standard as many other companies are using.	
Discounting own information	DO11	My use of this IS security management standard would not totally reflect my own preferences.	Sun (2012)
	DO12	My use of this IS security management standard is not totally based on my own preferences.	
	DO14	I didn't make the decision on using the IS security management standard totally based on my own preferences.	

Construct	Indicator	Item	Source
	DOI6	It is not my own preferences that select this IS security management standard.	
Mandatory	Mand1	Regulation requires using the IS security management standard in my organization.	
	Mand2	Legislation requires using the IS security management standard in my organization.	
	Mand3	Our organization is required to apply the IS security management standard according to regulation.	
Use	U1	To what extent you apply IS security management standard in your current organization?	Beaudry and Pinsonneault (2010).
	U2	I apply all parts of IS security management standard in my current organization.	
	U3	To what extent you apply IS security management standard in your current organization?	
	U5	How often do you use IS security management standard in your work?	
Strength of information	SI1	I know information about this IS security management standard which is: Extremely negative Neutral Extremely positive 1 2 3 4 5 6 7	New items
	SI2	I have information about this IS security management standard which is: Extremely negative Neutral Extremely positive 1 2 3 4 5 6 7	
	SI3	There is information about this IS security management standard which is: Extremely negative Neutral Extremely positive 1 2 3 4 5 6 7	

Appendix 5

Table 24. Measurement items (Chapter 8).

Construct	Sub-dimension	Items	Questions	Source	
Warm glow	Affective feeling (WGAF)	WGAF1	Uploading unauthorized copy of digital goods to this online community makes me feel good.	Ferguson <i>et al.</i> (2012)	
		WGAF2	Uploading unauthorized copy of digital goods to this online community makes me feel happy.		
		WGAF3	Uploading unauthorized copy of digital goods to this online community is enjoyable.		
		WGAF4	Uploading unauthorized copy of digital goods to this online community makes me feel great.		
		WGAF5	Uploading unauthorized copy of digital goods to this online community makes me feel awesome.		
	Role merger (WGRM)	WGRM1	Uploading unauthorized copy of digital goods to this online community is an important part of who I am.		Ferguson <i>et al.</i> (2012)
		WGRM3	I would feel sorry if I could no longer upload digital goods to this online community.		
		WGRM4	Uploading unauthorized copy of digital goods to this online community means a lot to me.		
		WGRM5	In a sense, uploading unauthorized copy of digital goods to this online community meets my value.		
		WGRM6	In a sense, Uploading unauthorized copy of digital goods to this online community is consistent with my values.		
Subjective norm (WGSN)		WGRM7	In a sense, uploading unauthorized copy of digital goods to this online community helps me to achieve my goals.	Ferguson <i>et al.</i> (2012)	
		WGSN1	Other members of this online community think I should upload unauthorized copy of digital goods.		

Construct	Sub-dimension	Items	Questions	Source
		WGSN3	My friends think I should upload unauthorized copy of digital goods.	
		WGSN4	My parents think I should upload unauthorized copy of digital goods.	
		WGSN5	My relatives think I should upload unauthorized copy of digital goods.	
		WGSN7	People who I admire think I should upload unauthorized copy of digital goods.	
	Moral norms (WGMN)	WGMN1	If I did not upload unauthorized copy of digital goods to this online community, I would feel guilty.	Ferguson <i>et al.</i> (2012)
		WGMN2	If I did not upload unauthorized copy of digital goods to this online community, I would feel regretful.	
		WGMN3	If I did not upload unauthorized copy of digital goods to this online community, I would feel uncomfortable.	
		WGMN4	If I did not upload unauthorized copy of digital goods to this online community, I would feel upset.	
		WGMN5	If I did not upload unauthorized copy of digital goods to this online community, I would feel bad.	
Sanctions	Certainty of sanctions (CTS)	CTS2	If I upload unauthorized copy of digital goods, the likelihood of being caught is (very low...very high).	D'Arcy <i>et al.</i> (2008)
		CTS3	If I upload unauthorized copy of digital goods, it is very likely to be caught.	
		CTS4	If I upload unauthorized copy of digital goods, I would probably be caught.	
	Severity of sanctions (SS)	SS1	If caught uploading unauthorized copy of digital goods, I would be severely disciplined.	D'Arcy <i>et al.</i> (2008)
		SS2	If caught uploading unauthorized copy of digital goods, my punishment would be (not severe at all...very severe).	
		SS3	If caught uploading unauthorized copy of digital goods, severe punishment would come to me.	

Construct	Sub-dimension	Items	Questions	Source
		SS4	If caught uploading unauthorized copy of digital goods, I would be severely punished.	
	Celerity of sanctions (CS)	CS1	If caught uploading unauthorized copy of digital goods, I would be punished in a short time.	Nagin and Pogarsky (2001).
		CS2	If caught uploading unauthorized copy of digital goods, I would be punished without waiting long.	
		CS3	If caught uploading unauthorized copy of digital goods, I would receive quick punishment.	
		CS4	If caught uploading unauthorized copy of digital goods, I would be punished shortly.	
Demand for resources	N/A	DPG1	I'd like to get more shared digital goods from this online community.	Self-developed
		DPG2	I hope that more digital goods can be shared in this online community.	
		DPG3	I hope that shared digital goods in this online community will be more in the future.	

ACTA UNIVERSITATIS OULUENSIS
SERIES A SCIENTIAE RERUM NATURALIUM

634. Hyysalo, Jarkko (2014) Supporting collaborative development : cognitive challenges and solutions of developing embedded systems
635. Immonen, Ninna (2014) Glaciations and climate in the Cenozoic Arctic : evidence from microtextures of ice-rafted quartz grains
636. Kekkonen, Päivi (2014) Characterization of thermally modified wood by NMR spectroscopy : microstructure and moisture components
637. Pietilä, Heidi (2014) Development of analytical methods for ultra-trace determination of total mercury and methyl mercury in natural water and peat soil samples for environmental monitoring
638. Kortelainen, Tuomas (2014) On iteration-based security flaws in modern hash functions
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

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

S E R I E S E D I T O R S

A
SCIENTIAE RERUM NATURALIUM

Professor Esa Hohtola

B
HUMANIORA

University Lecturer Santeri Palviainen

C
TECHNICA

Postdoctoral research fellow Sanna Taskila

D
MEDICA

Professor Olli Vuolteenaho

E
SCIENTIAE RERUM SOCIALIUM

University Lecturer Veli-Matti Ulvinen

E
SCRIPTA ACADEMICA

Director Sinikka Eskelinen

G
OECONOMICA

Professor Jari Juga

H
ARCHITECTONICA

University Lecturer Anu Soikkeli

EDITOR IN CHIEF

Professor Olli Vuolteenaho

PUBLICATIONS EDITOR

Publications Editor Kirsti Nurkkala

