Mari Karjalainen

IMPROVING EMPLOYEES’ INFORMATION SYSTEMS (IS) SECURITY BEHAVIOR

TOWARD A META-THEORY OF IS SECURITY TRAINING AND A NEW FRAMEWORK FOR UNDERSTANDING EMPLOYEES’ IS SECURITY BEHAVIOR
MARI KARJALAINEN

IMPROVING EMPLOYEES’ INFORMATION SYSTEMS (IS) SECURITY BEHAVIOR
Toward a meta-theory of IS security training and a new framework for understanding employees’ IS security behavior

Academic dissertation to be presented with the assent of the Faculty of Science of the University of Oulu for public defence in OP-sali (Auditorium L10), Linnanmaa, on 28 October 2011, at 12 noon

UNIVERSITY OF OULU, OULU 2011
Karjalainen, Mari, Improving employees’ information systems (IS) security behavior. Toward a meta-theory of IS security training and a new framework for understanding employees' IS security behavior
University of Oulu, Faculty of Science, Department of Information Processing Science, P.O. Box 3000, FI-90014 University of Oulu, Finland
Oulu, Finland

Abstract
Employee non-compliance with information systems (IS) security procedures is a key concern for organizations. However, even though the importance of having effective IS security training is widely acknowledged by scholars and practitioners, the existing literature does not offer an understanding of the elementary characteristics of IS security training, nor does it explain how these elementary characteristics shape IS security training principles in practice. To this end, this thesis develops a theory that suggests that IS security training has certain elementary characteristics that separate it from other forms of training, and sets a fundamental direction for IS security training practices. Second, the theory defines four pedagogical requirements for designing IS security training approaches. Then it points out that no existing IS security training approaches meet all these requirements. To address these shortcomings, the way in which to design an IS security training approach that meets all these requirements is demonstrated.

In this thesis it is also argued that, along with an effective IS security training approach, reasons for employees’ IS security behavior need to be understood. The existing empirical research in the field of employees’ IS security behavior is dominated by theory-verification studies that test well-known theories developed in other fields in the context of IS security. Instead, it is argued that there is a need to focus the investigation on the phenomenon of employees’ compliance itself through an inductive and qualitative approach to complement the existing body of knowledge of this topic. As a result, a framework identifying reasons associated with compliance/non-compliance with security procedures is developed. A particularly interesting finding is that individuals’ violation of IS security procedures depends on the type of violation.

Besides advancing a meta-theory for IS security training and developing the theoretical framework that points out reasons for employees’ IS security behavior, the thesis provides a future research agenda for IS security training and behavior. For practitioners, this thesis points out the limitations of the previous IS security training approaches and reasons for IS security behavior and, based on these observations, offers principles for designing effective IS security training approaches in practice.

Keywords: information systems security, information systems security behavior, information systems security training, learning paradigms
Karjalainen, Mari, Työntekijöiden tietoturvakäyttäytymisen parantaminen. Kohti tietoturvavakoulutuksen meta-teoriaa ja uusi viitekehys työntekijöiden tietoturvakäyttäytymisen ymmärtämiseksi
Oulun yliopisto, Luonnontieteellinen tiedekunta, Tietojenkäsittelytieteiden laitos, PL 3000, 90014 Oulun yliopisto
Oulu

Tiivistelmä

Yhtenä keskeisenä ongelmana organisaatioissa pidetään sitä, että työntekijät laiminlyövät organisaation tietoturvakäytäntöjä. Vaikka tutkijat ja organisaatiot ovat tunnistaneet tietoturvakoulutuksen tärkeyden, olemassa oleva kirjallisuus ei tuo esio tietoturvakoulutuksen perusominaisuuksia ja niiden asettamia vaatimuksia käytännön tietoturvakoulutukselle.


Tietoturvakoulutuksen suunnittelua tukevan meta-teorian ja työntekijöiden tietoturvakäyttäytymistä selittävän teoreettisen viitekehynksen lisäksi väitöskirjassa esitetään uusia näkökulmia tietoturvakoulutuksen ja tietoturvakäyttäytymisen tutkimuksesta. Käytännön tietoturva-ammatilla on työntekijöiden selventää olemassa olevien tietoturvakoulutuksen lähdestymistapojen puutteita ja syitä työntekijöiden tietoturvakäyttäytymiselle. Näihin havaintoihin perustuen väitöskirjassa esitetään tekijöitä, joita tietoturvakoulutuksessa tulisi käytännössä ottaa huomioon.

Asiasanat: oppimisparadigmat, tietoturva, tietoturvakoulutus, tietoturvakäyttäytyminen
Acknowledgements

This doctoral thesis was undertaken at the Department of Information Processing Science at the University of Oulu during 2007–2011. When I look back at the four years during which this doctoral thesis was written, I see that I have gained great experiences and learned about an entirely new research topic and field of research. This period of my life as a Ph.D. student has also helped me to surpass myself in several ways, and I believe that the competencies I have acquired will benefit me in both my future career and my personal life. This time has been invaluable to me in several ways. First of all, during this dissertation research project, I had the great honor of working with a number of interesting and talented people, who have not only contributed to my work, but who have also supported me in my Ph.D. studies.

First of all, I am grateful to my primary supervisor, Professor Mikko Siponen, whose expertise, support, and persistent attitude enabled me to complete this doctoral thesis, who helped me through difficult periods, and who gave me faith in my work. I also want to thank my co-supervisor, Dr. Petri Puhakainen, for sharing his optimistic disposition with me, and for providing a professional perspective on this thesis.

I also want to express my gratitude to several other experts who have contributed to my thesis. I am grateful to Professor Suprateek Sarker for his co-authorship and inspiring collaboration, Dr. Riitta Hekkala for her valuable feedback on my thesis research, Minna Alasuutari for her contribution to the interview questions, and project manager, Timo Wiander, for always providing help when needed. In addition, I am greatly thankful to Dr. Tero Vartiainen and Professor Teemupekka Virtanen, who reviewed my licentiate thesis, and Professor France Bélanger and Professor Neil Doherty, who acted as reviewers of my doctoral thesis. I appreciate the time and effort they put into providing constructive feedback in order to improve my licentiate and doctoral theses. I also want to thank a company called Scribendi for proofreading my English, persons in Tutkimustie and at the University of Oulu who helped me with interview transcriptions, and anonymous reviewers of our research papers presented in the JAIS theory development workshop 2009, IFIP WG8.11/11.13 Roode Workshop 2010, and the Journal of Association for Information Systems. Although being a monograph, this thesis is largely based on my licentiate thesis (Karjalainen 2009) and the publications in journals and conferences (Karjalainen & Siponen 2009, Karjalainen & Siponen 2011, Siponen, Karjalainen & Sarker 2010).
I want to thank our company partners in the Fusion and Sepeda research projects, who have collaborated with us and provided funding for our research. I have had an exceptionally interesting research period involving travel to the US, United Arab Emirates, China, Switzerland, and India to participate in conferences, interview people, or conducting Information Systems Security training in a company. Without several contact persons in each country and voluntary interviewees, this thesis would not have been possible. In particular, I owe my deepest gratitude to information security manager, Kimmo Helaskoski, who arranged our data collection and supported our research with his expertise and work contribution. It was a pleasure and fun to collaborate with him.

I also want to thank my previous and present colleagues who have shared the everyday life at the university with me: Asheesh Nigam, Pekka Tetri, Kari Alatalo, Heli Tervo, Dr. Seppo Pahnila, Xiuyan Shao, Ying Li, Kari Nykänen, Minna Laurila, and Juhani Heikka, thank you all for interesting conversations and support also during difficult periods. I’m also grateful to the personnel of our department, and especially Marja-Liisa Liedes, Kari Pankkonen, and Professor Markku Oivo for their help and support. I also want to thank the Finnish Funding Agency for Technology and Innovation (Tekes in Finnish), European Regional Development Fund (ERDF), and the Graduate School on Software Systems and Engineering (SoSE) for financing my doctoral studies. I offer my regards to all the others who supported me in any respect during the completion of this thesis.

The constant support of my family and friends has been indispensable during my research work; thank you for bringing joy and happiness into my life, and offering a shoulder to always rely on. You are the most important people in my life. Special thanks also go to members of the Monthly Gastronomers for almost 30 years of on-going friendship. I also want to express a special word of gratitude to my dear family members — my mother Seija, father Ari and his partner Teija, my sister Minna, my brother Juha, the worlds’ dearest little nephews, Elias and Topias, and my parents-in-law Anja and Teuvo — for their presence, love, and support. My warmest thanks belong to my husband, Veikko, for his encouraging attitude, insightful feedback, love, and for just always being there for me when I need it.

Oulu, August 2011

Mari Karjalainen
Contents

Abstract
Tiivistelmä
Acknowledgements

1 Introduction

2 Toward a new meta-theory for designing IS security training approaches

11

2.1 Related work in the area of IS security training approaches

15

2.2 A meta-theory for IS security training

29

2.2.1 Meta-level thinking: The nature and the existentialistic features of IS security training

31

2.2.2 Critical-level thinking

34

2.2.3 Existing IS security training approaches and the four pedagogical requirements

47

2.2.4 Intuitive level thinking: Example of an IS security training approach meeting the four pedagogical requirements

66

3 Reasons for employees’ IS security behavior

75

3.1 Related work in the area of IS security behavior

75

3.1.1 Models of computer misuse/abuse

76

3.1.2 Models on compliance with IS security procedures

77

3.1.3 Studies of appropriate IS security behavior

79

3.1.4 A summary of the literature review

81

3.2 Data collection and analysis

82

3.2.1 Data collection

83

3.2.2 Data analysis

86

3.3 Main Categories as the Result of Data Analysis

92

3.3.1 IS security procedures

93

3.3.2 Cultural dimensions

94

3.3.3 Individual dimensions

98

3.3.4 Organizational dimensions

100

3.3.5 Rational IS security dimensions

110

3.3.6 IS security-detached dimensions

117

3.3.7 Unconscious IS security dimensions

120

3.4 Scaling Up Towards a Framework for Understanding Employees’ IS Security Behavior

122
4 Discussion

4.1 Contribution of the thesis ......................................................... 127

4.1.1 Contributions of a meta-theory for designing IS security
training approaches ................................................................. 127

4.1.2 Contributions of a framework explaining employees’ IS
security behavior ................................................................. 129

4.1.3 Overall contribution of the thesis ........................................ 142

4.2 Implications for practice ............................................................ 144

4.2.1 Practical implications of a meta-theory designing IS
security training ................................................................. 144

4.2.2 Practical implications of a framework explaining
employees’ IS security behavior ......................................... 144

4.3 Implications for research .......................................................... 149

4.3.1 Research implications of a meta-theory for designing IS
security training ................................................................. 149

4.3.2 Research implications of a framework explaining
employees’ IS security behavior ......................................... 152

4.4 Limitations of the study ............................................................ 153

5 Conclusions

References ........................................... 159

Appendices ........................................ 175
1 Introduction

No modern organization can survive without IS security. While hacking and computer viruses are frequently cited IS security hazards in the media, a number of serious IS security problems result from employees failing to comply with the basic information security procedures related to their work (Information Security Breaches Survey 2008, CSI Survey 2007, Siponen & Vance 2010). This means that if users do not comply with IS security procedures, security solutions lose their usefulness (Kruger & Kearney 2006, Thomson et al. 2006). In order to ensure that employees follow their companies’ IS security procedures, different approaches have been advanced in the literature, such as the use of sanctions and deterrences (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). Despite the fact that scholars and practitioners generally agree on the need for organizations to implement IS security training, the existing literature on IS security training does not offer an understanding of the elementary characteristics of IS security training, such as how IS security training differs from other forms of training. It is argued that in order for IS security training research and practice to develop further, there is a need not only to examine the fundamentals of IS security training (how IS security training differs from other types of training), but also to provide theory-based advice on how scholars and practitioners can design, select, and evaluate the pedagogical merit of different IS security training principles. To address these goals, it is argued that IS security training needs a theory that (i) lays down these elementary characteristics of IS security training, and (ii) explains how these elementary characteristics shape IS security training principles in practice.

As a step towards remedying this situation, a meta-theory for IS security training that addresses these issues is advanced in this thesis. First, this theory suggests that IS security training has certain elementary characteristics that separate it from other forms of training. Second, it defines four pedagogical requirements for the design and evaluation of IS security training approaches. The extant IS security training approaches are reviewed, and it is concluded that no

---

1 IS security procedures are called by various names in the literature, and multiple types of documents exist in organizations: IS security strategies, policies, instructions, guidelines, and procedures (Puhakainen & Siponen 2010). In this thesis, we use the term IS security procedures for referring to organizations’ operational-level IS security requirements for employees.
previous approach meets all these requirements. Finally, it is illustrated how an IS security training approach can meet these requirements.

In addition to an IS security training method, successful IS security training aimed at improving employees’ compliance with IS security procedures requires understanding the employees’ reasons for compliance and non-compliance with IS security procedures. Such understanding is necessary in order for employees’ IS security behavior to be effectively improved through various interventions, such as IS security training. This is the case because symptoms cannot be cured unless we know the reasons for the symptoms. Attempting to find the reasons why employees comply or do not comply with IS security procedures, IS researchers have approached this investigation under a variety of labels. These include “Computer Abuse,” “Computer Misuse,” “Employees’ compliance with information security procedures,” and the “Organization’s (IS security) culture.” In undertaking this line of research, scholars have applied theoretical models imported from criminology (e.g., Straub 1990; Siponen & Vance 2010), social psychology (e.g., Hyeun-Suk et al. 2005), and psychology (e.g., Johnston & Warkentin 2010; Myyry et al. 2009). Such a research orientation can be labeled as theory-verification. While there is no doubt that such theory-verification studies have made important contributions to the literature, it can be argued that in order to derive specific insights, there is a need to focus the investigation on the phenomenon itself, and to abstract theoretical ideas from it, rather than to test or illustrate existing theories. First, the chosen theoretical perspectives offer a biased viewpoint of the phenomenon of interest. Second, rather than investigating what is specific to a phenomenon of IS security behavior, these theory-verification studies replicate the extant theories from other disciplines such as criminology, psychology, and social psychology. As a step in overcoming this gap in the research, it is proposed in this thesis that the use of an inductive and qualitative approach will complement the existing body of knowledge of this topic.

Such a research approach is important for a number of reasons. First, the extant models in IS security are based on well-known theories developed in other disciplines, with the result that IS security researchers essentially are engaged in validating or invalidating these theories in other areas. Instead, an inductive, qualitative approach could potentially reveal new insights into the phenomena of employees’ IS security behavior. Second, such an approach could lead to new theory development in this area (see Baskerville & Myers 2002). Third, such a qualitative approach could offer a richer picture that is based on human meanings and experiences than what is obtained through “experience far” theory testing.
Finally, a qualitative approach would also allow the research of employees’ compliance with IS security procedures to move beyond “Likert scale responses,” by obtaining a deeper understanding of the reasons why people do or do not comply with IS security procedures. It is believed that such an understanding can be useful for practitioners.

The results of this thesis will be welcomed by both scholars and practitioners engaging in IS security training. For scholars, this thesis will offer a new theoretical contribution, the meta-theory for IS security training approaches, which not only provides a new understanding of the fundamental characteristics of IS security training and how it differs from other forms of training, but also suggests new principles to design IS security training approaches. In addition, the thesis contributes a conceptual understanding of the phenomenon of employees’ IS security behavior through offering some general and context-dependent reasons based on empirical data. Finally, the thesis offers directions for future research in the areas of IS security training and behavior. For practitioners, this thesis will illustrate how to put a meta-theory to practical use by offering important insights into how to improve IS security training in practice through the theoretical framework, and recognizing general and context-dependent reasons for employees’ IS security behavior.

The rest of the thesis is organized as follows: the second chapter discusses the extant IS security training approaches, and points out the need for a meta-theory of IS security training. To fill this gap in the literature, a new meta-theory is advanced, including four pedagogical requirements for IS security training approaches. The extant IS security training approaches are reviewed in section 2.2.3 in the light of these requirements with the result that no existing IS security training approach meets these requirements. Next, also in the second chapter, how an IS security training approach can meet these requirements is demonstrated. The third chapter includes the introduction of the related work of employees’ IS security behavior in the organizational context, and the empirical investigation of the reasons for employees’ IS security behavior. The fourth chapter outlines implications for practice and research, and finally, the fifth chapter concludes the findings of the thesis.

---

2 The second chapter of this thesis is based on the following publications: Karjalainen and Siponen (2009), and Karjalainen and Siponen (2011). Some part of the third chapter is published in IFIP WG8.11/11.13 Roode Workshop 2010 (Siponen, Karjalainen & Sarker 2010).
2 Toward a new meta-theory for designing IS security training approaches

This chapter includes the first part of the thesis, which introduces the extant IS security training approaches, develops a meta-theory for designing IS security training approaches, and reviews the extant IS security training approaches in the light of a theoretical framework. The chapter is organized as follows: first, based on the review of the extant IS security-training approaches, the need for a meta-theory of IS security training is pointed out in section 2.1. Second, to fill this gap in the literature, a three-level meta-theory for IS security training is advanced in a section 2.2. The meta-theory suggests that IS security training has certain elementary characteristics that separate it from other forms of training (2.2.1), defines four pedagogical requirements for the design of IS security training approaches (2.2.2), and illustrates how an IS security training approach can meet these requirements (2.2.4). In addition, the extant IS security training approaches (N = 36) are reviewed against the four pedagogical requirements in section 2.2.3.

2.1 Related work in the area of IS security training approaches

The existing IS security training approaches (N = 36) were selected for a literature review through a systematic literature search covering “all” published articles in a field, not only articles published in top journals and conferences, as suggested by Webster and Watson (2002). The selected articles include training and awareness activities for ordinary users of IS. The goal of such training is to achieve organization- and work-specific changes in employees’ attitudes and behaviors. Education for information security professionals is excluded (e.g., Goel & Pon 2006, Bishop 2000, Romney et al. 2004, Ryan 2003, Sharma & Sefchek 2007). Also, articles concentrating on evaluation of training programs (e.g., Kruger & Kearney 2006, Martins & Eloff 2001, Stanton et al. 2005, Dodge et al. 2007) are omitted, because they focus only on how to measure the effectiveness of these programs, not the actual development and implementation of training. In addition, articles referring to training as a part of an IS security awareness program are excluded if the characteristics of these training efforts are not described in detail (such studies include Bray 2002, Information Security Forum 2005, Leach 2003, Murray 1991, Olnes, 1994, Parker 1999, Sasse et al. 2001, Spurling 1995, Stacey 1996, Telders 1991). Finally, articles concentrating
on the identification of IS security training needs (e.g., Katsikas 2000) are also beyond the scope of this review.3

To increase our understanding on extant IS security training approaches, the IS security training literature is first thematically divided into following seven categories:

1. Psychological training approaches (five approaches)
2. Training approaches based on learning theories (six approaches)
3. Security awareness program approaches (twelve approaches)
4. Process approaches (nine approaches)
5. Context-specific approaches (nine approaches)
6. Computer-based training approaches (seven approaches)
7. Social engineering preventive approach (one approach)

*Psychological training approaches* are based on theoretical concepts from the fields of psychology, or social psychology. *Training approaches based on learning theories* are based on theoretical concepts from the field of education. *Security awareness program approaches* view IS security training as a method for increasing employees’ IS security awareness. Whereas for security awareness programs, training is just one tool for increasing employees’ compliance with IS security policies, *process approaches* focus solely on IS security training by introducing IS security-training principles in a stepwise manner. While other approaches can be applied in any context, *context-specific approaches* are specially designed for certain types of organizational settings, such as universities. While the previous approaches are oriented towards face-to-face learning, *computer-based training approaches* focus on e-learning approaches, and computer games. Finally, while the other IS security training approaches are designed for improving employees’ behavior in any area of IS security through training, the *social engineering preventive approach* is focused on avoiding the phenomenon of social engineering with IS security training.

Separate IS training approaches placed under one or more categories are presented in Table 1.

---

3 The selection of the articles for this review is slightly different from reviews in other articles, such as Puhakainen and Siponen (2010). This difference is due to different criteria used for reviewing the literature. There exists a number of articles in the literature (e.g., Goodhue & Straub 1991, Murray 1991, Spurling 1995, Siponen 2000b, Telders 1991, Wood 2002, Perry 1985), which mention IS security training, but do not offer detailed training program or method. Such articles are omitted in this thesis, because they can’t be reviewed in a view of the selected theoretical framework.
Table 1. IS security training approaches under seven contextual categories: 1) Psychological training approaches, 2) Training approaches based on learning theories, 3) Security awareness program approaches, 4) Process approaches, 5) Situational approaches, 6) Social engineering preventive approaches, 6) Computer-based training approaches.

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cognitive processing approach (Puhakainen 2006)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Constructive instruction approach (Heikka 2008)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Constructive scenario approach (Biros 2004)</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Andragogical approach (Herold 2005)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyber security game approach (Cone et al. 2007)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pedagogical game approach (Gretzer et al. 2007)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social psychology-oriented approach (Thomson &amp; von Solms 1998)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Motivation theory directive approach (Roper et al. 2006)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Persuasive technology approach (Forget et al. 2007)</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social psychological recommendations approach (Kabay 2002)</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Normative approach (Siponen 2000a)</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Counteractive approach (McIlwraith 2006)</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security ensuring approach (Peltier 2000)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication-oriented approach (Desman 2002)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Promotional approach (Rudolph et al. 2002)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Stakeholder approach (Kovacich &amp; Haliboe 2003)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deterrence approach (Straub &amp; Welke 1998)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Academic environment approach (Kajava &amp; Siponen 1997)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>University environment approach (McCoy &amp; Thurmond Fowler 2004)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Preventive approach (Nosworthy 2000)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strategic approach (Wilson &amp; Hash 2003)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Competence approach (Wilson et al. 1998)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operational controls approach (NIST 1995)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISD approach (Hansche 2001)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Traditional e-learning approach (Kajava et al. 2003)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hypermedia instruction approach (Shaw et al. 2009)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy creation approach (Gaunt 1998)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Healthcare environment approach (Furnell et al. 1997)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Discursive approach and online tutorial approach (Cox et al. 2001)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Briefing approach (Markey 1989)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social engineering preventive approach (Mitnick &amp; Simon 2002)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active e-learning approach (Furnell et al. 2002)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Profession–based approach (Thomson &amp; von Solms 1997)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intranet-based approach (Vroom &amp; von Solms 2002)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>An awareness campaign approach (Hadland 1998)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IS security architecture approach (Tudor 2001)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TOTAL</td>
<td>5</td>
<td>6</td>
<td>12</td>
<td>9</td>
<td>15</td>
<td>1</td>
<td>7</td>
</tr>
</tbody>
</table>
As can be seen in Table 1, twenty-two of thirty-six approaches are placed under only one of the seven categories. However, nine approaches are situated under two categories, and five approaches belong to three categories. Table 1 shows the number of separate IS security-training approaches in each category. The extant IS security training approaches are introduced in more detail in Table 2.

Table 2. Extant IS security training approaches, their key findings, and underlying theories.

<table>
<thead>
<tr>
<th>ISS training approaches</th>
<th>Category</th>
<th>Key findings</th>
<th>Underlying Theory</th>
</tr>
</thead>
</table>
| Cognitive processing approach        | Training approaches based on learning theories, process approaches, and situational approaches | 1. Stresses changes in IS security-related attitudes through cognitive processing (recognizing, understanding, and evaluating persuasive arguments).  
2. Offers concrete guidance on how to achieve behavior changes.  
| Constructive instruction approach    | Training approaches based on learning theories, process approaches, and situational approaches | 1. Emphasizes participants' thinking, interpretations, knowledge construction, and interaction with the environment.  
2. The impact of the IS security training on managers' security behaviors is evaluated and reviewed. | The systematic approach to training (Buckley & Cable 1990) and constructivist learning principles (Fosnot & Perry 2005). |
| Constructive scenario approach       | Training approaches based on learning theories, psychological training approaches, and situational approaches | 1. Introduces scenario-based IS security training for teaching deception detection.  
2. Users' experiences and active construction of knowledge were mentioned as essential factors in learning. | Signal detection theory (Klein et al. 1997) and constructivism. |
| Andragogical approach                | Training approaches based on learning theories, security awareness program approaches, and process approaches | 1. Emphasizes learners' needs, former experiences, involving users, and improvement in employees’ job performance as the main goal of learning.  
2. Offers guidelines and practical examples to develop, implement, deliver, and evaluate IS security awareness and training. | Four basic principles of adult learning: readiness, experience, autonomy, and action (Knowles 1950). |
<table>
<thead>
<tr>
<th>ISS training approaches</th>
<th>Category</th>
<th>Key findings</th>
<th>Underlying Theory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber security game approach (Cone et al. 2007)</td>
<td>Training approaches based on learning theories, situational approaches, and computer-based training approaches</td>
<td>1. Actions, experiences, problem-solving skills, and critical thinking are essential factors in learning.  2. Introduces the use of a video game tool in training.  3. Provides an examination of IS security training and awareness policies in the target organization.</td>
<td>Learning principles in the area of games and simulations (e.g., Gee 2005).</td>
</tr>
<tr>
<td>Pedagogical game approach (Greitzer et al. 2007)</td>
<td>Training approaches based on learning theories, situational approaches, and computer-based training approaches</td>
<td>1. Incorporation of cognitive and pedagogical principles for IS security training: well-connected knowledge structures, personally significant learning experiences, and reconstruction of knowledge.  2. Offers usability and training effectiveness assessments.  3. Presents suggestions for addressing deficiencies in the prevailing gaming context.</td>
<td>Discovery learning (Bruner 1966, Herman 1969), active or autonomous learning (e.g., Johnson et al. 1991), and constructionist learning theory.</td>
</tr>
<tr>
<td>Social psychology-oriented approach (Thomson &amp; von Solms 1998)</td>
<td>Psychological training approaches</td>
<td>1. Applies concepts of social psychology to create training that is more effective by influencing people’s behaviors and/or attitudes.  2. Presents three methods for understanding and changing human behavior: a) directly change users’ behavior regardless of their attitudes, knowledge, or feelings (e.g., instrumental learning), b) change attitudes through changes in behavior (e.g., self-persuasion), and c) change attitudes through persuasion.</td>
<td>A typical attitude system (Zimbardo &amp; Leippe 1991).</td>
</tr>
<tr>
<td>ISS training approaches</td>
<td>Category</td>
<td>Key findings</td>
<td>Underlying Theory</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------</td>
<td>--------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Persuasive technology approach (Forget et al. 2007)</td>
<td>Psychological training approaches and computer-based training approaches</td>
<td>1. Introduces an e-learning system based on persuasive technology to influence people’s attitudes and behavior, to educate users of IS on the safe use of security measures.&lt;br&gt;2. Examines the effectiveness of the persuasive authentication framework.</td>
<td>A psychological framework on interactive computing systems (Fogg 2003).</td>
</tr>
<tr>
<td>Social psychological approach (Kabay 2002)</td>
<td>Psychological training approaches and security awareness program approaches</td>
<td>1. Applies social psychology to improve employees’ information security beliefs, attitudes, and behavior.&lt;br&gt;2. Presents practical recommendations for IS security training to encourage people to be more inclined to approve of information security policies and features of effective communication and day-to-day security practices.</td>
<td>Schema, theories of personality, explanations of behavior, errors of attribution, intercultural differences, framing the reality, beliefs and attitudes, persuasion, encouraging initiatives, and group behavior.</td>
</tr>
<tr>
<td>Normative approach (Siponen 2000a)</td>
<td>Psychological training approaches</td>
<td>1. Addresses the need for normative approaches and motivation/behavioral theories in organizational IS security training.&lt;br&gt;2. An approach aimed at making users internalize and commit to the organization’s security guidelines.</td>
<td>The theory of intrinsic motivation (e.g., Deci 1975) and TRA.</td>
</tr>
<tr>
<td>Counteractive approach (McIlwraith 2006)</td>
<td>Security awareness program approaches</td>
<td>1. Considers IS security training as an effective tool as part of the awareness program to reduce human error.&lt;br&gt;2. Offers practical strategies and techniques, measuring awareness, and delivery media for implementing security awareness.&lt;br&gt;3. Considers a change in behavior as the result of a decision-making process.&lt;br&gt;4. An approach to the awareness process includes five phases: managing by fact, goals and objectives, planning, implementation, and feedback.</td>
<td>-</td>
</tr>
<tr>
<td>ISS training approaches</td>
<td>Category</td>
<td>Key findings</td>
<td>Underlying Theory</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------</td>
<td>--------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Security ensuring approach (Peltier 2000)</td>
<td>Security awareness program approaches</td>
<td>1. Considers the IS security awareness program as an element of an overall security program in an organization. 2. The purpose is to make employees aware of security policies, standards, procedures, and guidelines. 3. Discusses security awareness program goals, IS security training needs identification, program developments, methods for IS security training, and program presentations.</td>
<td>-</td>
</tr>
<tr>
<td>Communication oriented approach (Desman 2002)</td>
<td>Security awareness program approaches</td>
<td>1. Presents instructions for building and evaluating an IS security awareness program in a step-by-step manner. 2. The purpose of the program is to make employees aware of the value of the information, their responsibilities, and protection activities.</td>
<td>-</td>
</tr>
<tr>
<td>Promotional approach (Rudolph et al. 2002)</td>
<td>Security awareness program approaches</td>
<td>1. IS security training is considered a comprehensive and detailed action to teach employees knowledge and skills to perform effectively. 2. The purpose is to reinforce the desired behavior and attitudes toward security, and change undesired ones through repetition. 3. Offers practical principles for establishing IS security training that resemble commercial advertising and campaigns.</td>
<td>-</td>
</tr>
<tr>
<td>Stakeholder approach (Kovacich &amp; Haliboze 2003)</td>
<td>Security awareness program approaches</td>
<td>1. Introduces guidelines for developing and maintaining a corporate information security program and implementing security procedures. 2. The IS security training program is considered an important corporate security function to make all relevant actors responsible for the organization’s information assets, be aware of the ways to protect them, and comply with corporate practices.</td>
<td>-</td>
</tr>
<tr>
<td>ISS training approaches</td>
<td>Category</td>
<td>Key findings</td>
<td>Underlying Theory</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------</td>
<td>--------------</td>
<td>-------------------</td>
</tr>
</tbody>
</table>
| Deterrence approach     | Security awareness program approaches and situational approaches | 1. IS security awareness and training is considered a part of their security program.  
2. A deterrent countermeasure is used to increase employees' knowledge of risks, policies, and sanctions in the organizational environment, and to provide a baseline for security planning and prevention activities. | Deterrence theory (Straub 1990) and the model of managerial decision making (Simon 1960). |
| Academic environment approach | Security awareness program approaches and situational approaches | 1. Discusses the need for IS security awareness to create behavioral changes in the academic context.  
2. Considers training, student education, and campaigning methods to increase IS security awareness and the level of security. | - |
| University environment approach | Security awareness program approaches, and situational approaches | 1. Introduces an IS security awareness program to educate students and employees in the academic environment.  
2. The purpose of the training is to change people’s attitudes and actions dealing with information security issues and develop metrics to measure the audience’s knowledge level before and after the program implementation.  
3. Concentrates on describing the planning process that includes determination of content, audience identification, selection of correct methods of delivery, and branding as well as monthly activities. | - |
<table>
<thead>
<tr>
<th>ISS training approaches</th>
<th>Category</th>
<th>Key findings</th>
<th>Underlying Theory</th>
</tr>
</thead>
</table>
| Preventive approach     | Process approaches  | 1. The purpose is to make employees aware, trained, and motivated with respect to their security responsibilities and countermeasures in their daily work.  
2. Offers practical instruction for the phases of the IS security-training program: defining objectives, identifying requirements and training sources, developing and implementing the program, and monitoring and testing its effectiveness. | -                 |
| (Nosworthy 2000)        |                     |                                                                                                                                                                                                             |                   |
| Strategic approach      | Process approaches  | 1. Presents guidelines for the IS security training program at a strategic level for federal agencies and other organizations.  
2. The purpose of awareness is to change or reinforce users’ security behavior. In turn, training aims at developing essential security skills and competencies for ordinary users. | -                 |
| (Wilson & Hash 2003)    |                     |                                                                                                                                                                                                             |                   |
| Competence approach     | Process approaches  | 1. Addresses role- and performance-based IS security training, which emphasizes actual roles, responsibilities, and the individual needs of employees.  
2. The awareness program aims to change employees’ attitudes and the organizational culture concerning security and training with information security knowledge and skills to all employees involved with IS.  
3. The purpose of the publication is to support the training needs identification, course development, and evaluation of learning effectiveness. | -                 |
<p>| (Wilson et al. 1998)    |                     |                                                                                                                                                                                                             |                   |</p>
<table>
<thead>
<tr>
<th>ISS training approaches</th>
<th>Category</th>
<th>Key findings</th>
<th>Underlying Theory</th>
</tr>
</thead>
</table>
2. IS security awareness, training, and education are considered as operational controls to improve employees’ security attitudes and behavior.  
3. Presents seven phases: a) identifying the scope, goals, and objectives, b) identifying the training staff, c) identifying the target audience, d) motivating the management and employees, e) administering the program, f) maintaining the program, and g) evaluating the program. | - |
| **ISD approach** (Hansche 2001) | Process approaches | 1. An IS security training curriculum is provided to meet job duties and roles.  
2. Study reviews phases of the traditional instructional system design (ISD) model: a) needs analysis and goal formation, b) design, c) development, d) implementation, and e) evaluation. | - |
| **Traditional e-learning approach** (Kajava et al. 2003) | Situational approaches and computer-based training approaches | 1. Introduces a generic intranet-based e-learning approach for technically oriented specialists in the case organization.  
2. Introduces technical, content-related, and pedagogical requirements for the learning environment, and handles presentation issues. | - |
| **Hypermedia instruction approach** (Shaw et al. 2009) | Situational approaches and computer-based training approaches | 1. Examines organizational security awareness training in three types of online environments: hypermedia, multimedia, and hypertext environments.  
2. Considers security awareness as three sequenced levels of abilities: users’ perception, comprehension, and projection of information security risks.  
3. Investigates the impact of information richness on the effectiveness of online IS security training approaches through statistical analysis of the collected data. | - |
<table>
<thead>
<tr>
<th>ISS training approaches</th>
<th>Category</th>
<th>Key findings</th>
<th>Underlying Theory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy creation approach</td>
<td>Situational approaches</td>
<td>1. Discusses IS security training as part of the development and implementation of an IS security policy in the healthcare environment.</td>
<td>-</td>
</tr>
<tr>
<td>(Gaunt 1998)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Healthcare environment approach</td>
<td>Situational approaches</td>
<td>1. Introduces basic definitions of measures to establish the training and awareness framework with respect to specific training needs and actions within the healthcare environment.  2. The purpose is to make all the employees of the organization know, understand, and accept security basics and procedures as part of their responsibilities and roles in the work environment.</td>
<td>-</td>
</tr>
<tr>
<td>(Furnell et al. 1997)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Discursive approach and online tutorial approach</td>
<td>Situational approaches</td>
<td>1. Introduces three approaches for IS security awareness in the university environment: a discussion session, a checklist, and a web-based tutorial.  2. The objective of these approaches is to increase users’ understanding of security and motivate users to act in a secure manner.  3. A discussion session as a discursive approach and a web-based tutorial as an online tutorial approach can be considered in terms of IS security training, while a checklist represents written communication with respect to security issues.</td>
<td>-</td>
</tr>
<tr>
<td>(Cox et al. 2001)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Briefing approach</td>
<td>Situational approaches</td>
<td>1. Introduces IS security training and awareness program including briefings for new employees, seminars for security officers, and briefings for directors.</td>
<td>-</td>
</tr>
<tr>
<td>(Markey 1989)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISS training approaches</td>
<td>Category</td>
<td>Key findings</td>
<td>Underlying Theory</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td>-------------------</td>
</tr>
</tbody>
</table>
| Social engineering preventive approach (Mitnick & Simon 2002) | Social engineering preventive approaches | 1. Presents guidelines for the IS security training program and the implementation of customized security policies as prevention activities for social engineering.  
2. Employees’ awareness of security policies is considered as the most effective issue to prevent social engineering.  
2. Focuses on policies and procedures as well as a continuous awareness program that is imperative for IS security to create changes in employees’ behavior and attitudes. | - |
| Active e-learning approach (Furnell et al. 2002) | Computer-based training approaches | 1. Introduce a prototype software tool for self-paced IS security training, including three modes of operation: exploration mode (investigation of security measures and different types of security), evaluation mode (scenario-based testing), and author mode (creation of new scenarios). | - |
2. Suggest three different IS security training approaches for top management, IT personnel, and end-users with different contents and techniques. | - |
2. Separate general and HR department specialized IS security training.  
3. Suggest intranet-based website as the efficient way to deliver information to all personnel. | - |
| Awareness campaign approach (Hadland 1998) | Situational approaches | 1. Present an information security awareness program including ten topics of a good IS security practice. | - |
To summarize the literature review of the extant IS security training approaches, while previous studies have echoed the importance of IS security training at organizations, no studies have attempted to lay down the fundamentals of IS security training, starting with issues such as identifying the fundamental nature of IS security training, and how it differs from other types of training. This is not a surprise, since only 12 out of the 36 security-training approaches summarized in Table 2 include any kind of theory, or theoretical concepts. Of these twelve theory-based approaches, six approaches apply learning theories (Biros 2004, Cone et al. 2007, Greitzer et al. 2007, Heikka 2008, Herold 2005, Puhakainen 2006); six approaches employ theories from the field of psychology or social psychology (Biros 2004, Forget et al. 2007, Kabay 2002, Roper et al. 2006, Siponen 2000a, Thomson & von Solms 1998); and one approach uses criminology (Straub & Welke 1998). The other IS security training approaches (n = 24) do not include any theoretical foundations (Table 2).

Similar findings are echoed by Puhakainen and Siponen (2010), who report the lack of pedagogical theories in the IS security training literature, and highlight the need for IS security training studies, based on proper pedagogical theories. There are specific reasons why theories play an important role in IS security training. Indeed, we argue that IS security training approaches must be based on

4 In a more broad sense, theories have an important role in the scientific research and IS in general. First, it is reported in the literature that theory development in the field of IS is scarce, emphasizing the role of IS as reference-theory discipline without independent identity (Weber 2003). Because of this concern, there has been calls for theory-development in IS (Baskerville & Myers 2002). While this thesis do not fill the vacuum of theory-development in IS, it is a first step in remedying the situation in the specific context of IS security training. Second, in social sciences and IS, theories are useful for predicting or increasing our understanding of the phenomenon in question (Dubin 1969). Similarly, theory-development on IS security training is useful for increasing our understanding of this
an explicit understanding of pedagogical theories for two reasons. First, the proper pedagogical theories offer tried-and-tested frameworks for IS security training. Therefore, their use guarantees the quality of the training program. Second, the underlying pedagogical theory of the IS security training approach – whether implicit or explicit – also sets fundamental limitations on the IS security training program. Therefore, it is of the utmost importance for practitioners and researchers to be aware of these underlying limitations of the existing approaches and other possible pedagogical theories.

In this thesis it is also argued that before any pedagogical theory can be selected on which to base an IS security training approach, a meta-level theory of the fundamental nature of IS security training is needed. It is maintained that only when we have a theory offering an understanding of such fundamentals of IS security training are we in a position to select proper pedagogical theories on which to base IS security-training approaches.

Thus, for offering understanding of the phenomenon of IS security training and guidance for organizations, this thesis develops a meta-theory that (i) lays down the elementary characteristics of IS security training, (ii) explains how these elementary characteristics shape IS security training principles in practice, and (iii) provides models on how IS security training practices can be executed. The meta-theory stems from the concept of three levels of thinking (Hare 1952, 1963, 1981) from the field of philosophy. The concept of three levels of thinking is used for sketching the structure of a new meta-theory for designing new IS security training approaches within IS. In addition, a social constructivist learning paradigm and experiential learning theory (Kolb 1984) from the discipline of education is applied for formulating pedagogical principles for a phenomenon under IS, and illustrating the meaning of these principles in practice. Such a theory is presented next.
2.2 A meta-theory for IS security training

For distinguishing the different purposes of a theory, Gregor (2006) presents five theory types in IS research: (1) analysis, (2) explanation, (3) prediction, (4) explanation and prediction, and (5) design and action. Niiniluoto (1993) calls the first four of these types descriptive (they explain, understand or predict the world, humans, culture, etc.), while he labels the latter type of scientific enquiry as design sciences, which focus on how things ought to be in order to meet a certain goal (the technical norm in terms of von Wright 1972). The descriptive theories are therefore interested in knowledge, and the accuracy of the information about the world, culture, man, society, etc. The correctness of the knowledge is typically estimated in terms of truth or truthlikeness (Niiniluoto 1999). In the case of “design and action” (Gregor 2006) or “design science” (Niiniluoto 1993), success is not defined in terms of true or false, but the effectiveness related to the intended use (Niiniluoto 1993, von Wright 1972).

Against this backdrop, it is argued that the ultimate objective of IS security training (theory) is “design and action” (Gregor 2006) or “design science” (Niiniluoto 1993), since its objective is goal oriented. That is, the aim of IS security training theory is not only to analyze the nature of IS security training, but also to produce theoretically informed guidance on how to design effective training approaches; “effective” meaning herein that employees would comply with IS security procedures. However, before such approaches can be developed, the fundamental nature of IS security training needs to be understood, provided that it sets the fundamental direction to IS security training. Hence, in order to find a framework that allows us to define the fundamental characteristics of IS security training and explains how these characteristics have an effect on IS security-training practices, a framework that is both descriptive and action guiding (“design and action”) is needed. To this end, Hare’s (1952, 1963, 1981) concept of three levels of thinking is ideal. This concept is descriptive and prescriptive. As for the former, it describes maturity levels in relation to how people form action-guiding principles. Hare’s concept is applied to sketch the structure of a new meta-theory for designing IS security training approaches (Figure 1).
Fig. 1. A Framework for the meta-theory of designing IS security training approaches based on Hare's concept of three levels of thinking (1952, 1963, 1981).

The meta-level refers to fundamental questions, such as “What is IS security training?” and “How does IS security training differ from other types of training?” (Figure 1). In turn, the intuitive thinking level means conventional activities in practice. The critical thinking level, lying between the meta- and intuitive thinking levels, is needed to test the validity of our conventional activities, and form new guidance in novel situations when needed (Hare 1981). When applied to IS security training, people at the intuitive level apply their conventional activities in terms of learned principles to IS security training. These intuitive level conventional activities are obtained, for example, through education, upbringing, and personal experience. People who simply follow their intuitive-level conventional activities, without ever questioning them, reside at the conventional level throughout their lives. For example, a practitioner engaging in IS security training, who uses the same training method that his supervisor used when educating him, without ever questioning the validity of these methods, stays

---

5 The term “conventional activities” in this context means that a person’s ways of conducting IS security training in an organization is based on customs usually formed by his/her previous experiences without critically considering their validity.
at the level of intuitive thinking. However, when people critically ponder the validity and effectiveness of their conventional activities, they move to “Critical-level Thinking.” Such moves may be prompted by feedback from other people, self-critique, feedback from learners, or hints that the IS security training does not work as desired. At the critical level, people can form new imperatives and ways of acting with respect to IS security training, which they then implement at the level of intuitive thinking. This means that the principles at the intuitive level are overridable; they can be modified, refined, or omitted (see Hare 1981). Or, in a case where two of the principles are in conflict, we can override (follow) one. Next, these levels of thinking, starting from the meta-level, are described.

2.2.1 Meta-level thinking: The nature and the existentialistic features of IS security training

Meta-level thinking encompasses issues such as the meaning of learning in the context of IS security training, or the fundamental characteristic of IS security training. Issues at this level are important because they help us to understand how IS security training differs from other types of training. In this thesis, it is argued that IS security training differs because it has certain specific characteristics, namely its fundamental nature and existentialistic features. These will be discussed next.

The Fundamental Nature of IS Security Training

Based on non-cognitivism (Hare 1963) and the theory of persuasion (Stevenson 1944), it is argued in this thesis that the nature of IS security training is non-cognitive and persuasive. This nature contrasts with other types of training, such as university education, which is descriptive (hence, cognitive), provides scientific facts, and does not seek to influence learners’ attitudes and behavior in the manner of persuasive training. IS security training is persuasive and non-cognitive because IS security procedures, similar to moral norms, require more normative training approaches than learning facts (Siponen 2000a). Indeed, compared to fact-telling educative strategies (presentation of the facts), persuasive approaches are more effective in situations where the level of commitment to change is low (Hayes 2010). This low level of employees’ commitment to complying with IS security policies is widely mentioned in the literature (Siponen & Vance 2010). IS security procedures are also non-cognitive
because they are created within an organizational context, and not necessarily based on scientific or moral inquiry (as are the creation of facts and moral norms, respectively). Following non-cognitivism as a philosophical doctrine, IS security procedures are utterances expressing organizations’ non-cognitive attitudes regarding how employees ought to behave in a secure manner. At first sight, the expressional side of IS security procedures resembles cognitivism, in that this procedure seems to have a true value, although it does not. This is the case since IS security procedures are incapable of being objectively true or false; hence, they are non-cognitive because they do not describe any factual features. For example, “This computer is red” is a cognitive statement, for which a truth-value can be resolved through scientific scrutiny. However, an IS security procedure, such as “Do not share your passwords with peers,” is not a fact; it does not have an objective truth-value.

In addition to a non-cognitive and persuasive nature, other factors are characteristic of IS security training. While other types of organizational training for white-collar employees can be persuasive and non-cognitive, such as firefighting, IS security training is related to daily and exceptional work situations; that is, the emphasis of IS security training is usually on daily work situations (Siponen & Vance 2010). For example, firefighting training for white-collar employees typically focuses on exceptional work situations, such as how to evacuate the building when there is a fire, but most IS security training focuses on routine work situations, and hence, employees’ daily activities, such as logging out of the computer every time the employees leave their computer (Siponen & Vance 2010; Puhakainen & Siponen 2010). While IS security training can also cover exceptional work situations (e.g., how to recover after an earthquake), such situations concern a limited number of employees, such as IT and IT security staff. Hence, IS security training of ordinary white-collar employees focuses on routine activities, and thus, should have relevance to employees’ daily work (Puhakainen & Siponen 2010).

Existentialistic Features of IS Security Training

Along with this persuasive and non-cognitive nature of IS security training, three existentialistic features are characteristic of IS security training: (1) the existence of security-sensitive organizational assets; (2) threats towards them; and (3) different technical, social, and organizational mechanisms for protecting the organization’s assets (protection mechanisms) (modified from Siponen et al.)
2006). Without these features, IS security training is not needed, hence, the label of existentialistic features. For example, if there are no assets of value in the organization, or if there are no threats to the organization, there is no need for IS security or for IS security training. The first feature, the existence of security-sensitive organizational assets, means that IS security training should ensure that the employees understand these assets. If employees lack this understanding, the IS security training is meaningless and arbitrary from the viewpoint of the substance. The second feature means that there has to be a threat to those assets. Again, it is argued that IS security training needs to introduce the relevant threats to employees in a pedagogically meaningful manner. Finally, the third feature means that IS security training assumes that mechanisms are in place that are able to protect security-sensitive organizational assets from threats, and that this training must be focused on achieving this objective. These three existentialistic features set the fundamental direction (general aim) of IS security training.

Related to these existentialistic features, and in comparison many other types of organizational training IS security training has two characteristics: voluntariness vs. mandatoriness in the use of protection mechanisms and the intangible nature of the information security threats and assets. The first characteristic (voluntariness vs. mandatoriness) means that while the use of some protection mechanisms can be forced through some technical solutions (e.g., restricting Internet access), and compliance with IS security procedures is typically mandatory (i.e., required in IS security policies), employees can bypass most protection mechanisms (e.g., leave their computer unlocked, send confidential e-mail without encryption, open links to infected websites). This is different from training in the use of the system, for example. If a new IS is taken into account in an organization, the employees may have to use the system, because that may be the only way to perform their work. For instance, a travel agent may have been forced to use a new travel system, whether she or he liked it or not.

The second point is the intangible nature of IS security threats and assets, meaning that the consequences of IT and the lack of information security may be difficult for employees to see. This is different from firefighting, for example. Most people have seen a fire, but who has seen password cracking? In other words, compared to the IS security risks of an organization’s information assets, firefighting training, for example, concentrates on more concrete risks that can threaten organizations’ facilities, employees’ health, or even their lives. If employees do not understand the consequences of their actions, say, the negative
consequences for selecting an easy-to-guess password, then why would they comply with IS security policies requiring passwords that are difficult to guess. Therefore, it is no surprise that IS security researchers have observed the difficulty employees have in understanding IS security assets and threats (Shaw et al. 2009).

From the discussion of the nature of IS security training, and the existentialistic features, which differentiate IS security training from other types of training, the following meta-level requirements are formulated:

The first meta-level requirement is for IS security training approaches: An IS security training approach must be based on the understanding that the nature of IS security training is persuasive and non-cognitive.

The second meta-level requirement is for IS security-training approaches: An IS security training approach must focus on the existentialistic features of IS security training.

Next, the preferred pedagogical requirements to be used in order to meet these two meta-level requirements for designing IS security-training approaches are focused on.

2.2.2 Critical-level thinking

Applied to this context, critical-level thinking (Hare 1981) concerns the selection of the proper pedagogical principles for carrying out IS security training in practice. This thesis suggests that a framework based on paradigms of learning contributes to understanding IS security training as an educational practice. After all, the goal of IS security training is to educate employees to comply with the IS security procedures. This thesis introduces and uses paradigms of learning as an analytical framework because principles of learning and learning processes contribute to effective educational practices (e.g., Hergenhahn & Olson 2001). Given that this thesis examines the preferred pedagogical principles for IS security training, it scrutinizes paradigms of learning—behaviorism, cognitivism, constructivism, and social constructivism (Hung 2001)—to find the most appropriate paradigm for this context. In order to select the most suitable paradigm of learning for IS security training, it is helpful to apply the concept of
meta-orientations. In terms of Hare (1981), these theories help us to determine the most appropriate critical level requirements for IS security training approaches. Next, this framework (learning paradigms and meta-orientations) is illustrated, and four pedagogical requirements at the critical level are derived from it. Then, the extent to which the existing IS security training approaches meet these pedagogical requirements is analyzed in section 2.2.3.

Compared to the paradigms of learning, meta-orientations allow us to more concretely examine IS security training approaches. Meta-orientations refer to fundamental educational philosophy underlying any intentional interaction designed to facilitate learning and achieving educational goals (Miller & Seller 1985, Cheung and Wong 2002). Paradigms of learning and meta-orientations are interrelated; paradigms of learning form a theoretical basis for meta-orientations, which are used to analyze IS security-training approaches. Table 3 summarizes the learning paradigms and features of meta-orientations.

---

6 In the literature, meta-orientations are also called educational approaches or positions (Miller 2001), orientations to teaching (Smith 1999), or epistemological orientations (Brody 1998). Here, the term meta-orientation is used consistently.
Three meta-orientations—transmission, transaction, and transformation—have five dimensions. The first of these is the psychological context of learning. As can be seen from Table 3, different meta-orientations are linked with the three paradigms of learning (behaviorism, cognitivism, and constructivism, and social constructivism): transmission meta-orientation favors behaviorist principles, transaction meta-orientation is influenced by cognitivism, and transformation meta-orientation is linked with constructivism and social constructivism. The other dimensions are general aims (2), content (3), teaching methods (4), and evaluation of learning (5) – Table 3. Next, these dimensions are discussed, starting from the general aim of IS security, because the dimension of “general aim” (Table 3) sets the overall direction for the development of the training approach, including another four dimensions of meta-orientations.
General aim of IS security training

Recognizing the persuasive and non-cognitive nature of IS security training, and the existentialistic features of IS security training (training must be connected to protection of valuable assets from threats through protection means), it is argued that communal transformation meta-orientation is the preferred choice for IS security training.

In transmission-oriented training, the general aims are to convey certain predefined contents or objective knowledge, facts, skills, concepts, and values to learners (Miller & Seller 1985). When characterizing transmission, Miller (2007) used the concept of a one-way flow of skills and knowledge usually through reading or listening, without opportunities to analyze or reflect on the information. While it is necessary that employees understand IS security procedures, the aim of IS security training is not to simply help them to remember and understand IS security procedures through delivering them to learners without giving them an opportunity to analyze or reflect on information, as in transmission-oriented training. An example of such IS security training is the one-way spread of information to the employees—“here are the IS security rules”—without any feedback, discussion, or activation of thinking processes. The transmission-oriented approach would be ideal for helping employees to remember and understand pre-determined contents (facts, concepts, or values) through one-way communication. However, given that IS security training is persuasive, as discussed in section 2.2.1, it requires a more discursive approach than just spreading the facts, as in the case of transmission-oriented training. Hence, the general aim of transmission-oriented training is not suitable for IS security training.

The general aims of transaction-oriented training are to obtain problem-solving skills through inquiring, analyzing, synthesizing, evaluating, or applying knowledge (Miller & Seller 1985). This cognitive interaction emphasizes analyses and thinking rather than syntheses and feeling (Miller 2007). Thus, the general aims of training are clearly connected with the cognitive adaptation and application of knowledge; that is, cognitive problem solving. To give an example of this, a lecture could first present the IS security procedures to employees, and then ask them to apply them to predefined situations given by the lecturer. While such transaction-oriented training can be persuasive, it is not connected to employees’ own working experiences (because the examples are predefined by the educator). Hence, the employees lose their connection to their own work tasks.
Hence, the general aim of transaction-oriented training is not suitable for IS security training.

In transformation-oriented training, the general aims are expressed in relation to personal experiences, and according to this position, learning is pursued to transform predominant beliefs and actions (Miller & Seller 1985). Hence, it strives for students’ personal development and integration of affective (emotions, attitudes, and values) and cognitive (intellectual knowledge) domains (Cheung & Wong 2002). Accordingly, the most obvious purpose of IS security training is to change employees’ IS security attitudes and behavior in order for them to become a natural part of the employees’ daily activities (Siponen 2000a, Thomson et al. 2006). In other words, the nature of IS security training is non-cognitive and persuasive. Even if IS security training can include transmission- and transaction-oriented aims, such as delivering knowledge to employees or developing their cognitive abilities or problem-solving skills, these cannot be seen as an overall direction for training. In transformation orientation, this issue is addressed by connecting the learning issues, such as compliance with IS security procedures, to the employees’ own work tasks and experiences. Hence, learning is based on learners’ previous experience (Miller & Seller 1985). This is important since previous research shows that new knowledge is best constructed through previous experiences; hence, IS security learning must be reflected through the work experiences of the employees. Through transformation-oriented training, employees can be allowed to figure out with reference to their own work tasks why the assets they handle in their work need to be protected, what are the threats to those assets, and how the assets can be protected (existentialistic features of the IS security training).

Finally, transformation orientation includes two different directions for designing training: individual and communal (Miller & Seller 1985). In this thesis, the importance of the latter in IS security training is emphasized, because it is argued that IS security training is primarily directed towards creating a communal change in employees’ IS security behavior, rather than only an individual change (see Table 3). This means that IS security training is directed not only towards influencing individuals’ IS security behavior but also changing the work communities’ prevailing organizational work practices, and developing the organization’s security culture (Dhillon 2007). It is argued that employees’ IS security behavior consists of such shared organizational work practices, which, along with formal IS security policies, depend on organizations’ unwritten culture, which defines what kinds of behavior are seen as acceptable and unacceptable.
(see Robbins 1993). To influence such shared working practices, it is argued that group-oriented training approaches are better than individual approaches, because group approaches help employees obtain richer knowledge and increased acceptance of the prescribed changes to their behavior (Robbins 1993). For example, educators can organize a discussion section where learners present their own views on, say, why they should encrypt sensitive e-mails. Presentation of the different views of group members not only helps their peers to obtain richer knowledge in terms of understanding the different reasons why they should encrypt their e-mails, and correct their own misconceptions in the context of their work (e.g., “My e-mails do not contain sensitive information”), but also mutually to achieve higher acceptance of using e-mail encryption in their work. Keeping these issues in mind, it is argued that communal transformation meta-orientation is preferred for IS security training.

The general aim of communal transformation meta-orientation sets the direction of selection of other features of meta-orientations: psychological context, content, teaching method, and evaluation of learning (see Table 3). Next, the features of meta-orientations are discussed. Also, the corresponding pedagogical requirements for IS security training at the critical level derived from communal transformation orientation are put forward as part of a meta-theory for designing IS security training.

Pedagogical requirements for IS security training

First pedagogical requirement for IS security training: Psychological context

As the first pedagogical requirement for IS security training approaches derived from communal transformation meta-orientation, the explicit psychological context—the learning paradigm behind the training approach—must be based upon a group-oriented theoretical approach to teaching and learning, which will guide training activities (see Fardanesh 2006, Gibson 2001, Hinsz et al. 1997). Such a group-oriented learning theory is needed for IS security training because it is primarily directed towards creating communal rather than personal change (see Table 3).

The transmission meta-orientation does not meet this requirement as it emphasizes the stimulus-response system of learning in terms of behaviorism (see Miller and Seller, 1985). This meta-orientation represents mechanistic and natural science thinking, and its educational form stems from behaviorist psychology
Thus, behaviorism is considered as a clear psychological context in educational practices that represents the transmission orientation. Behaviorism presupposes that a change in the context or outcome can change the behavior. Teaching is expected to shape the learner’s responses through instructional procedures, such as modeling and reinforcement (Palincsar 1998). However, the basic concepts of behaviorism are criticized for being misleading ideas of learning compared to recent learning theories, especially concerning the use of knowledge and ignoring the affective domain of learning (emotions, attitudes, and values). Behaviorism is usually related to lower levels of learning (e.g., information recall and basic skills), not high-order analytical and conceptual skills (e.g., reasoning and problem solving) (Miller & Seller 1985, Palincsar 1998).

In turn, transaction meta-orientation is psychologically oriented to developmental and cognitive psychology (see Kohlberg & Mayer 1972, Piaget 1963, Miller & Seller 1985). Common to all cognitive approaches of learning is the emphasis on the individual development of cognition, which is the focus of cognitive theories. Cognition refers to the individual construction of knowledge and the learner’s ability to control own achievements concerning a learning task or problem (Poikela & Poikela 1997). Thus, cognitivism is the corresponding psychological context in transaction-oriented educational practices. This differs from behaviorism in that psychological mechanisms in human learning are taken into consideration when establishing educational practices (see Palincsar 1998).

In more detail, a conceptualization of students’ learning processes and issues concerning receiving, organizing, storing, and retrieving information is the essence of cognitive theories (Ertmer & Newby 1993). Cognitive psychology offers conceptions to understand individual information processing, problem solving, decision making, and learning. Cognitive theories help to design instructional designs, which facilitate students’ growth and specific intellectual competencies. In cognitive instructional practices, it is essential to use advance organizers, mnemonic devices, and metaphors, chunk instructional materials into meaningful parts, and organize the materials from simple to complex (Bednar, Cunningham, Duffy, & Perry 1995). However, in most cases, cognitivism emphasizes logical and analytical problem solving, and ignores intuitive or creative problem solving. This intuitive element stresses novel solutions instead of attempts to identify a clear set of alternatives. The approach has also been criticized for ignoring real social problems by focusing only on cognitive analysis (Miller & Seller 1985). Consequently, within cognitive theories, learning is
mainly restricted to text-based and subjective information-processing tasks without clear connections to actual practices and actions outside the learning situation (e.g., Tuomi-Gröhn, Engeström, & Young 2003). Because psychological contexts of transmission and transaction meta-orientations consider learning only as an individual process, they do not represent a suitable learning paradigm for IS security training, which requires a group-oriented learning paradigm.

The transformation meta-orientation covers a diverse body of literature and assumptions (e.g., see Meyer 2003). However, it has psychological roots in humanistic psychology (e.g., Maslow 1970, Rogers 1969, Miller & Seller 1985). The humanistic approach to learning has much in common with the constructivist approach to learning, as both theoretical approaches emphasize an active role for the learner. A humanistic approach to learning emphasizes the learners’ self-directedness and the interactive and communal character of learning (Poikela & Poikela 1997). Constructivism or reflection orientation is based on the individual’s cognitive reflection on concrete experiences to construct new knowledge (Fenwick 2001). The purpose of the humanistic approach to learning is self-actualization and self-transcendence (Miller & Seller 1985), or growth and personal integrity (McNeil 1981). Constructivism (and social constructivism) is a more appropriate learning paradigm to construct meanings of events and ideas, transform understandings (Ross 2002), and build a connection between the learner’s former knowledge and what he or she is expected to learn (Gagnon & Collay 2006).

In constructivism, instead of knowing particular facts or retrieving intact knowledge structures, the goal of instruction is to make students elaborate on and interpret information and create new understandings. Representations of experiences are not structured into declarative knowledge and stored in the head. Thus, memory is always under construction, developing through task engagement and context-dependent processes. According to constructivism, learning is always situated, which means that it is dependent on the goals, needs, and engagement of the learner, tasks, resources available, expectations, etc. Hence, authentic learning environments are preferred. In constructivism, learning also depends upon seeing a learning problem as important and personally relevant, and involves feeling the value of actions in the learning situation, and having decision-making responsibilities. Learning is social because interacting with others is one of the most effective ways to test one’s views (Jonassen 1991, Ertmer & Newby 1993). Social interaction is considered effective from the viewpoint of individual learning. A concrete experience at the starting point of learning could be
simulated and developed specially for a learning situation (e.g., role play), an exercise where a learner practices the skills to be learned, or a real-life or workplace experience that the learner has encountered (Fenwick 2001). However, this psychological context within transformation meta-orientation also emphasizes individual learning and thus, is not a suitable learning paradigm for IS security training.

However, since social constructivism, as a second corresponding psychological context of transformation orientation, emphasizes the social viewpoint in the learning process (Palinscar 1998), it meets this requirement. Social constructivism stresses the social viewpoint of learning processes, interactions, and knowledge. While Piaget’s (1985) socio-cognitive conflict theory explains the role of social interaction in the learning process from the viewpoint of individual learning, Vygotsky’s (1978) socio-cultural theory considers individual thinking to be secondary to and a derivative of social interaction (Palinscar 1998). Social constructivism emphasizes the effects of the social context on learning and interaction in cognitive development. Instead of seeing cognition as an individual activity, it stresses socially constructed knowledge and multiple interpretations through the social context (Hung 2001). Learning is considered to require interaction, negotiation, and collaboration (Palinscar 1998). For instance, collaborative learning implements social constructivist learning theory (Barkley et al. 2005). Because such a learning paradigm offers a group-oriented theoretical approach for learning, it is argued that social constructivism is the most suitable learning paradigm for IS security training.

In addition to communal change being a general aim of IS security training rather than individual change (see General aim of IS security training, subhead of section 2.2.2), there are other justifications for considering social constructivism as the preferred approach for IS security training. First, studies in other areas have found that social learning influences the change of individuals’ risk perceptions, and further, protective behavior (e.g., Helleringer & Kohler 2005, Douglas & Wildavsky 1982), which is also an essential goal in IS security training. Based on that, social learning is also a potential approach for influencing employees’ IS security risk perceptions; for instance, risks related to selecting easy-to-guess passwords, which can be expected to lead employees to protect the valuable documents saved in their computers through complying with the organization’s password procedures. Social learning in IS security training means that the learning content includes employees’ collective experiences (e.g., employees’
shared experiences in IS security risks related to password use), and collaborative
teaching and evaluation methods (e.g., discussion of the relevance of IS security
risks related to password use in employees’ work, and achieving mutual
agreement to minimize the occurrence of these risks by adhering to password
policies). (Content, teaching method, and evaluation of learning are discussed in
more detail in the next sections.)

Second, in the change management literature, social constructivism includes
several characteristics useful for motivating employees to change: user
participation, involvement, and negotiated agreements (Nadler 1993, Lines 2004,
Hayes 2010). Empirical evidence of the effectiveness of such participatory
approaches can also be found in the field of IS development (e.g., Ives & Olson
1984), IS security risk management (e.g., Spears & Barki 2010), and IS security
awareness programs (Albrechtsen & Hovden 2010). For example, Markus and
Mao (2004) explain the success of participatory IS development through making
IS development more personally relevant and important for users, with a positive
influence on their attitudes, system usage, and relationship with IS professionals,
as well as making developers better informed about business needs.

Third, previous research reports that employees’ IS security behavior is
influenced by other people, which is consistent with the principles of social
constructivism. For example, employees’ compliance intentions or behavior are
influenced by management and co-workers’ attitudes and behavioral expectations
(Pahnila et al. 2007, Herath & Rao 2009), peers’ behavior (Herath & Rao 2009),

Second pedagogical requirement for IS security training: Content

As the second pedagogical requirement for IS security training derived from
communal transformation meta-orientation, the content of the training must be
based on the collective experiences and meaning perspectives of the learners (see
Hmelo-Silver & Barrows 2008). This is required because to make IS security
procedures community centered, understood, accepted, and implemented
collectively (not just individually), training must include learners’ shared
perceptions of these procedures in their own work.

Transmission-oriented content is not ideal for IS security training because it
does not involve the learners’ collective experiences and meaning perspectives
(hence, it does not meet the second pedagogical requirement). Rather, knowledge
(content) is seen to be objective, unrelated to human subjectivity (Brody 1998),
and static (Miller 2007). The content of transmission-oriented training is subject centered (Miller & Seller 1985, Miller 2007). In the context of IS security training, transmission-centered content could be predefined standards or best practices. Because the content with transmission orientation is predefined and generic, training it is not connected to the unique experiences of each learner with the result that learning is not maximized.

Transaction orientation emphasizes problem-centered content mainly selected by the teacher, but also takes into account the students’ interests (Miller & Seller 1985). In addition, this cognitive process orientation stresses the learning process and cognitive process skills rather than curriculum content and the acquisition of factual knowledge (Cheung & Wong 2002). As an example in the context of IS security training, learners can complete assignments to analyze information security procedures, or create classifications of information security threats and prevention activities provided in the literature. Also, with transaction orientation, the instructor uses concrete examples or questions in the training session to activate the learners’ cognitive processing of knowledge. However, a transaction-oriented content of training does not emphasize communal and experiential characteristics, which were required from effective IS security training.

Learner-centered transformation-oriented training stresses the learners’ experiences and involvement in the community (Miller & Seller 1985). Further, as new knowledge emerges from the community through collaborative knowledge building (Hmelo-Silver & Barrows 2008), it is community centered. Thus, the content of transformation meta-orientation is based on the collective experiences and meaning perspectives of the learners, which meets the second requirement for IS security training. Using the example of IS security training (rules in the area of IS security), in the case of transformation-oriented training, the meaning and relevance of the rules are discussed in the company’s actual work situations. In addition, employees’ experiences in this area are taken into account, because the substance of the training—in this case, rules—needs to be based on learners’ previous understanding according to transformation orientation. Finally, such employee experiences are shared and communicated during the training.

Third pedagogical requirement for IS security training: Teaching methods

As the third pedagogical requirement for IS security training derived from communal transformation meta-orientation, teaching methods must focus on collaborative learning in order to reveal and produce collective knowledge (see
Mezirow 1991, Palincsar 1998, Dillenbourg et al. 1996, Rochelle & Teacley 1995). Such teaching methods are needed in IS security training because they enable the creation of communal change in the employees’ IS security attitudes and behavior (see Table 3).

This requirement is not met in transmission-oriented training, where the teaching method is the educator’s approach to spreading knowledge. Thus, the teacher’s role is directive, and learners are passive participants (Miller 2007). Teaching shapes the learner’s responses through instructional procedures, such as modeling and reinforcement (Palincsar 1998). In the context of IS security training, teaching methods characterized with transmission orientation emphasize instructor-led activities, techniques to deliver security messages, and rewards. The teacher presents IS security procedures to learners through different audio-visual means (e.g., face-to-face presentations and computer-based presentations) without paying attention to the learning processes, problem-solving assignments (transaction), or individual or communal reflection of experiences (transformation). Thus, the content is presented to employees through their reading or listening to formal presentations.

Also in transaction orientation, teaching methods are not focused on collaborative learning in order to reveal and produce collective knowledge as required from IS security training. Instead, teaching methods focus on cognitive problem solving through applications, analyses, and syntheses of the learning material (Bloom 1956, Miller & Seller 1985). In these cases, training includes cognitive problem-solving activities that are mainly defined by the teacher, and which demand active information processing from the learners. As an example in the context of IS security training, students can complete assignments on information security issues based on written materials. The assignment could be to recognize and classify threats and prevention activities related to information security in imaginary scenarios created by the teacher in relation to general definitions in the IS security literature.

Transformation-oriented teaching methods, in contrast, make connections between students and the real world, while making students aware of their thinking processes (Miller & Seller 1985). Thus, these methods maintain that learning occurs through the critical reflection of information through authentic problem solving or communication. In critical reflection, a person or a group ponders the validity of his or her actions, thoughts, and feelings in order to change these meaning perspectives (Mezirow 1991). In the context of IS security training, teaching methods that create communal experiences must be executed
through discussions concerning experiences, attitudes, and behaviors towards security issues. The communal creation of experiences includes collaboration (which must engage each member of the group) in order to collectively solve the common problem or reach an agreement (Dillenbourg et al. 1996, Rochelle and Teacley 1995). In this sense, differentiating personal teaching methods from communal ones is closely related to the general aims of training. For example, a discussion to support individual understanding can be considered a personal teaching method. However, if the goal of the discussion is to reflect on collective experiences and to achieve mutual understanding and agreements, it can be considered a communal teaching method, which meets the third requirement for IS security training.

Fourth pedagogical requirement for IS security training: Evaluation of learning

As the fourth pedagogical requirement for IS security training derived from communal transformative meta-orientation, evaluation of learning should emphasize experiential and communication-based methods from the viewpoint of the learning community (see Miller & Seller 1985; Birenbaum 1996). These methods are preferred in IS security training because the goal of training is to construct collaborative knowledge (in other words, to mutually understand new IS security procedures).

Transmission-oriented training does not meet this goal, as the evaluation concentrates on an objective measurement of training goals with pre-defined responses. Examples of evaluations representing the transmission orientation in the context of IS security training are formal exams, tests, or competence-based evaluations in authentic situations typically conducted after a training session. For example, a web-based training evaluation asking learners about IS security procedures (e.g., a good password has more than 12 characters, “yes” or “no”) with multiple-choice-style answers is an example of a transmission-oriented evaluation of training.

As for transaction-oriented training, evaluation focuses on examining learners’ information processing through cognitive problem-solving tasks. Examples of transaction-oriented evaluation tasks in the context of IS security training include verbal or written exercises to analyze information or apply learned issues in a similar context. Thus, learning assignments and evaluation tasks are highly similar in nature (see “Third pedagogical requirement for IS security training: Teaching method,” above). An example of this is case-based training, where a
number of cases are introduced to the employees. Then the employees are asked to point out how many IS security violations each case contains, and the teacher’s task is to assess whether the employees’ results are relevant according to some predefined criteria.

Evaluation in transformative training includes various conversational models, such as informal, experimental, and open-ended forms of evaluation for individuals or groups (Miller & Seller 1985). Learners are active participants who share responsibility in the evaluation process through self-evaluation, reflection, collaboration, and continuous dialogue with the trainer during the IS security training sessions. Evaluation methods include feedback during work or assignments, group projects, peer evaluations, and interviews (Birenbaum 1996).

An example of an assignment could be one where the employees are asked to indicate how the training has improved their skills, knowledge, or behavior. Ideally, in transformative training, these are also discussed among the learners and IS security trainers, and this communal sharing of knowledge may result in new learning experiences. In that way, the evaluation is a key part of the continuous learning process, not an end in itself. These evaluation methods are experiential and communication based, and thus fulfill the fourth requirement for IS security training.

Next, before introducing the third level of a meta-theory (see Figure 1), the extent to which the existing IS security training approaches meet these four requirements is pointed out.

2.2.3 Existing IS security training approaches and the four pedagogical requirements

All existing IS security training approaches (N = 36) (see section 2.1) were systematically reviewed. The aim of this literature review is to describe the extent to which the extant IS security training approaches fulfill the four pedagogical requirement formulated in the previous section 2.2.2. In the literature review of this thesis, IS security training approaches are examined in light of meta-orientations, transmission, transaction, and transformation, in order to analyze their (1) explicit psychological contexts and reveal the practical features of educational practices: (2) content, (3) teaching methods, and (4) evaluation of learning. Explicit psychological contexts refer to the IS security training approaches based on learning theories (see Table 1). In this section, each feature of meta-orientation is illustrated with five randomly selected IS security
approaches that contain exclusively one kind of meta-orientation and its corresponding learning paradigm. In case there are not enough illustrations, five exemplars are randomly selected from all IS security approaches representing the handled feature of the meta-orientation. In this case, the selection of IS security approaches is executed through selecting every fifth approach from the list arranged in alphabetical order according to the author. However, only one approach is selected once inside every feature of meta-orientation, and for avoiding a selection of a certain approach twice, next free approach from the list is selected.

Selected articles have been analyzed through content analysis. As a research technique, content analysis means analyzing texts in order to find reliable, replicable, and valid inferences. Texts are dependent on the reader’s perspective and interpretations in the process of his or her conceptual engagement with them (Krippendorff 2004). A qualitative processing is based on logical reasoning and interpretation, where the material (IS security training approaches) is first broken down according to the research objective (data reduction), then conceptualized based on the conceptual framework (data display), and finally assembled into a new logical entity (conclusion drawing) (Miles & Huberman 1994).

Next, IS security training approaches are reviewed through meta-orientations in order to recognize their underlying paradigms of learning and to see how they meet the four requirements.

First pedagogical requirement for IS security training: Psychological context

Only six of 36 IS security approaches apply any learning theories, and one of them applies an instructional design approach. This means that the majority of IS security training approaches are lacking any explicit psychological context. While none of the six approaches represents transmission orientation and behaviorism, one approach is placed exclusively under the transaction orientation, and

---

7 For example, from the list arranged in alphabetical order including ten approaches, five exemplars are selected as follows: fifth approach, tenth approach, sixth approach, first approach, and seventh approach. However, four IS security training approaches were analyzed after this selection of the exemplars was made (Hadland 1998, Thomson & von Solms 1997, Tudor 2001, Vroom & von Solms 1997).

8 The word theory is used here in the broad sense: if the IS security training approach includes any references towards applying a particular type of learning research (e.g., models, frameworks, or concepts), then we classify it as including a theory.
cognitivism category. This is the cognitive processing approach of Puhakainen (2006: 70–73\(^7\)), which is based on the requirements derived from the elaboration likelihood model (ELM) (Petty & Cacioppo 1981, 1986), and stresses changes in attitude through recognizing, understanding, and evaluating persuasive arguments. Accordingly, IS security training should take into account working memory (i.e., cognitive load) and the learner’s previous knowledge and should encourage systematic cognitive processing of information. Through providing guidelines for IS security training in practice, ELM, combined with universal constructive instructional theory (Schott & Driscoll 1997), functions as an instructional design approach for IS security training.

The following five approaches are placed exclusively under transformation orientation and constructivism: 1) the constructive scenario approach of Biros (2004: 33) applies constructivism, while the active construction of knowledge and users’ experiences are essential factors in learning. 2) The cyber security game approach of Cone \textit{et al.} (2007: 64) introduces the learning principles behind games and simulations, which refer to constructivist learning: actions, experiences, problem solving, and critical thinking. 3) The pedagogical game approach of Greitzer \textit{et al.} (2007: 2–3) is rooted in research on cognitive processing, and constructionist learning theory, which emphasizes the involvement of personally significant learning experiences in training. 4) The constructive instruction approach of Heikka (2008: 4) is based on constructivist learning principles and training methods (Fosnot & Perry: 2005), and emphasizes participants’ thinking, interpretations, knowledge construction, and interaction. 5) The andragogical approach of Herold (2005: 101–104) is based on Knowles’s andragogy, which emphasizes learners’ readiness, experience, autonomy, and action. Within the learning research, this approach is associated with the humanistic theories of learning (e.g., Finger & Asún 2001), which are also considered theoretical foundations of transformation orientation (Miller & Seller 1985). Like constructivism, humanistic theories of learning emphasize participants’ thinking, experiences, and interactions with the environment.

None of the IS security training approaches is based on preferred social constructivist learning theory within transformation orientation. As has been observed, learning theories within IS security training are built on the individual viewpoint, cognitivism, or constructivism, and consequently, the social (or

---

\(^7\)Besides the year of publication, numbers in brackets after every author refer to the page numbers where evidence for the analysis can be found.
communal) viewpoint of learning is not taken into account. In addition, none of
the IS security training approaches applies the social constructivist instructional
design approach for training design. In this thesis, this means that IS security-
training approaches are not effective and pedagogically meaningful educational
practices. Therefore, none of the IS security training approaches meet the first
requirement for future IS security training: the explicit psychological context, the
learning theory behind the training approach, must be based upon the group-
oriented learning paradigm and instructional design approach (Fardanesh 2006,
Gibson 2001, Hinsz et al. 1997). The results of analyzing the psychological
contexts in existing IS security training approaches are presented in Table 4. In
Table 4 (as well as 5–7), the term inclusive means that such IS security training
approaches represent all the meta-orientations and corresponding learning
paradigms with respect to the handled feature of the meta-orientation. In turn, the
term exclusive indicates that those approaches contain only one kind of meta-
orientation and a corresponding learning paradigm with respect to the handled
feature of the meta-orientation.
Table 4. The psychological context of learning in the existing IS security training approaches.

<table>
<thead>
<tr>
<th>Transmission</th>
<th>Transaction</th>
<th>Transformation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Behaviorism (0)</td>
<td>Cognitivism (1)</td>
<td>Constructivism (5)</td>
</tr>
<tr>
<td>Inclusive (0)</td>
<td>-</td>
<td>Exclusive (5)</td>
</tr>
<tr>
<td>-</td>
<td>Exclusive (1)</td>
<td>-</td>
</tr>
<tr>
<td>Exclusive (0)</td>
<td>-</td>
<td>Constructive instruction approach (Helkka 2008), Constructive scenario approach (Biros 2004), Andragogical approach (Herold 2005), Cyber security game approach (Cone et al. 2007), Pedagogical game approach (Greitzer et al. 2007)</td>
</tr>
</tbody>
</table>

Missing (30)

Social psychology-oriented approach (Thomson & von Solms 1998), Motivation theory directive approach (Roper et al. 2006), Social psychological recommendations approach (Kabay 2002), Normative approach (Siponen 2000a), Deterrence approach (Straub & Welke 1998), ISD approach (Hansche 2001), Counteractive approach (McIlwraith 2006), University environment approach (McCoy & Thurmond Fowler 2004), Security-ensuring approach (Peltier 2000), Academic environment approach (Kajava & Siponen 1997), Communication-oriented approach (Desman 2002), Promotional approach (Rudolph et al. 2002), Preventive approach (Nosworthy 2000), Stakeholder approach (Kovacich & Halibozek 2003), Strategic approach (Wilson & Hash 2003), Competence approach (Wilson et al. 1998), Policy creation approach (Gaunt 1998), Healthcare environment approach (Furnell et al. 1997), Social engineering preventive approach (Mitnick & Simon 2002), Discursive approach and online tutorial approach (Cox et al. 2001), Briefing approach (Markey 1989), Operational controls approach (NIST 1995), Active e-learning approach (Furnel et al. 2002), Traditional e-learning approach (Kajava et al. 2003), Persuasive technology approach (Forget et al. 2007), Hypermedia instruction approach (Shaw et al. 2009), Profession-based approach (Thomson & von Solms 1997), Intranet-based approach (Vroom & von Solms 2002), Awareness campaign approach (Hadland 1998), IS security architecture approach (Tudor 2001)\(^{10}\)

\(^{10}\) Items 1 and 3 in the list of 28 studies that are missing a clear “psychological context” include the term “psychology” or “psychological” in their titles. These two IS security training approaches belong to psychological training approaches that are based on theoretical concepts from the fields of psychology, or social psychology (see table 1). However, the term “psychological context” here refers to the possible learning theory behind the training approach.
Second pedagogical requirement for IS security training: Content

The transmission-oriented content of training is presented without connection to learning processes, problem solving, or the experiences of the learners in the training situation. The following five of eight approaches solely include such transmission-oriented content: 1) The healthcare environment approach of Furnell et al. (1997: 708–710) outlines static content areas such as security procedures and security duties of employees without taking into account learners’ thinking during the training. 2) The academic environment-focused approach of Kajava and Siponen (1997: 108, 110–111) consists of general information on IS and the responsibilities of the organization’s members ranging from corporate information security procedures to the consequences of risky behavior, without recognizing the learners’ own experiences of these topics. 3) The stakeholder approach of Kovacich and Halibozek (2003: 255) consists of various predetermined topics, such as asset protection practices and unauthorized actions, which are presented to learners without any attempt to have them modify this knowledge based on their own experience. 4) The university environment approach of McCoy and Thurmond Fowler (2004: 346–347) is based on statistical information and perceived problems in the case organization and opinions of industry experts including both static and annually evaluated topics such as the Internet and e-mail security, social engineering, new password requirements, and the university’s procedures. Although this approach recognizes both organization-specific and industrial viewpoints in the selection of IS security training topics, it does not include learners’ experiences towards these topics. 5) Similarly, Nosworthy’s (2000: 344) preventive approach completely comprises predetermined topics (e.g., the company’s IS security procedures and basics of information security) without any connections to learners’ thinking.

Further, 20 of the approaches include process- and/or problem-centered training content, which are typical of transaction orientation and also cognitivism, which emphasizes integration of new knowledge with existing knowledge or cognitive problem solving and analysis (e.g., Palincsar 1998). Process-centered contents take into account the cognitive processing of information. Problem-centered contents emphasize cognitive problem-solving tasks as a part of training. None of the IS security approaches (N = 36) introduces content, which is typical only of transaction orientation. However, the following five randomly selected approaches include transaction-oriented features as a part of the training: 1) The constructive scenario approach of Biros (2004: 35) uses videotaped scenarios as
examples to support learners’ cognitive understanding. 2) According to the pedagogical game approach of Greitzer et al. (2007: 3–4), new information presented in a training situation needs to be connected with the former knowledge of the learner, and the learner’s cognitive load needs to be managed by organizing the material. 3) In the traditional e-learning approach of Kajava et al. (2003: 33), enabling learners to assimilate new knowledge with their previous knowledge structures and taking account of different learning strategies and styles (e.g., learning through different senses) are mentioned as pedagogical principles of the learning environment. 4) The motivation theory directive approach of Roper et al. (2006: 111) employs concrete examples in similar contexts, stories, and problem-solving activities as a part of training. 5) Similarly, the competence approach of Wilson et al. (1998: 18, 20) recommends case studies, simulations, and problem solving.

Finally, 25 approaches include learner-centered contents. In these approaches, the content of training is partly created during a training session according to the learners’ experiences and choices, which is typical of the transformation orientation and constructivism. The following four exclusive and one randomly selected approaches represent transformation orientation: 1) The cyber security game approach of Cone et al. (2007: 63–64) suggests the application of security concepts to the simulated environment. 2) The purpose of the discursive approach and online tutorial approach of Cox et al. (2001: 12) is to reveal experiences of the learners as the main content of the session. 3) The active e-learning approach of Furnell et al. (2002: 354) uses simulated case-study scenarios with problem-solving activities. 4) In the policy creation approach of Gaunt (1998: 134), users’ opinions and participation are emphasized in the process of planning and implementing security. 5) In the normative approach of Siponen (2000a: 33–34, 37), active participation is seen as a way of changing human behavior by stressing users’ choices, interaction, attitudes, and involvement in the decision making.

Two of twenty-five transformation-oriented approaches also include community-centered contents typical to social constructivism, which stress communal knowledge formulated during training: 1) The social psychological recommendation approach of Kabay (2002: 8–9) includes features of the existing corporate culture, expectations, and social schemata (views of reality) through making them apparent and alterable. 2) The cognitive processing approach of Puhakainen (2006: 75–76) seeks to reveal the communal relevance of the learning task. Therefore, only two IS security training approaches meet the second requirement for future IS security training: the content of training must be
community centered, *i.e.*, based on the collective experiences and perspectives of the learners (*e.g.*, Kolb 1984, Gibson 2001). The results of analyzing training content in existing IS security-training approaches are presented in Table 5.

**Table 5. The training content in existing IS security training approaches.**

<table>
<thead>
<tr>
<th>Transmission</th>
<th>Transaction</th>
<th>Transformation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Behaviorism (28)</td>
<td>Cognitivism (20)</td>
<td>Constructivism (25)</td>
</tr>
<tr>
<td>Exclusive (8)</td>
<td>Exclusive (0)</td>
<td>Exclusive (4)</td>
</tr>
<tr>
<td>Deterrence approach (Straub &amp; Welke 1998)</td>
<td>Normative approach (Siponen 2000)</td>
<td>Cyber security game approach (Cone et al. 2007)</td>
</tr>
<tr>
<td>Academic environment focused approach (Kajava &amp; Siponen 1997)</td>
<td>Policy creation approach (Gaunt 1998)</td>
<td>Active e-learning approach (Furnell et al. 2002)</td>
</tr>
<tr>
<td>Transmission</td>
<td>Transaction</td>
<td>Transformation</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Behaviorism + cognitivism (3)</td>
<td>Communication-oriented approach</td>
<td></td>
</tr>
<tr>
<td>(Desman 2002)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Promotional approach (Rudolph et al. 2002)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IS security architecture approach (Tudor 2001)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cognitive-processing approach (Puhakainen 2006)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pedagogical game approach (Greitzer et al. 2007)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Persuasive technology approach (Forget et al. 2007)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hypermedia instruction approach (Shaw et al. 2009)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cognitive-processing approach (Puhakainen 2006)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pedagogical game approach (Greitzer et al. 2007)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Persuasive technology approach (Forget et al. 2007)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hypermedia instruction approach (Shaw et al. 2009)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Behaviorism + constructivism (4)</td>
<td>Operational controls approach (NIST 1995)</td>
<td></td>
</tr>
<tr>
<td>Constructive instruction approach (Heikka 2008)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operational controls approach (NIST 1995)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strategic approach (Wilson &amp; Hash 2003)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intranet-based approach (Vroom &amp; von Solms 2002)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social constructivism (2)</td>
<td>Cognitive-processing approach (Puhakainen 2006)</td>
<td></td>
</tr>
<tr>
<td>Social psychological recommendations approach (Kabay, 2002)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Third pedagogical requirement for IS security training: Teaching methods

With respect to teaching methods, 28 approaches represent transmission orientation and behaviorism. These learning activities facilitate teachers in transmitting knowledge and learners in receiving knowledge or external reinforcement of their behavior. The following five of eight approaches include solely transmission-oriented content: 1) In the communication-oriented approach of Desman (2002: 136–138, 143–144), despite an opportunity for questioning, learners simply receive information presented through a formal presentation. External reinforcement of users’ learning is also done through providing FAQ sheets and trinkets after training. 2) In the healthcare environment approach of Furnell et al. (1997: 708–710), delivery of information is executed through security guidelines, training seminars, and Internet-based services. 3) In the stakeholder approach of Kovacich and Halibozek (2003: 248, 260), understanding, motivation, and knowledge are acquired through regular briefings in person, online, and through videos and consulting. 4) In the university environment approach of McCoy and Thurmond Fowler (2004: 348–349), the delivering of information by presentations, in-person training, and web-based training is proposed. 5) The preventive approach of Nosworthy (2000: 345) suggests using consultants, conferences, and videos.

Twelve approaches employ transaction-oriented teaching methods and cognitivism, which use cognitive processing of information, implementation activities of cognitive problem solving and analysis, or both. None of the IS
security approaches introduces an exclusively transaction-oriented teaching method. The following five randomly selected approaches include transaction-oriented features as a part of the training: 1) The **Discursive approach and online tutorial approach** of Cox et al. (2001: 13) includes role-based scenarios and alternatives for users to select. 2) The **academic environment-focused approach** of Kajava and Siponen (1997: 111) includes projects and master’s theses. 3) and 4) The **counteractive approach** of McIlwraith (2006: 95) and the **competence approach** of Wilson et al. (1998: 20) recommend problem-solving activities. 5) The **strategic approach** of Wilson and Hash (2003: 34) emphasizes instructor-led training including peer presentations and lectures complemented with case study workshops.

Finally, 25 approaches include teaching methods that represent transformation orientation and constructivism. Such teaching methods employ reflection of the content through exercises, authentic problem solving, and/or communication. Through these activities, learners can reflect on their own reasons behind their security behaviors and attitudes and, through this reflection, become more security conscious. In these IS security training approaches, collaborative teaching methods (i.e., discussion) are employed to promote individual learning (e.g., reflection of own actions) to achieve personal changes. The following five of eight approaches solely include transformation-oriented teaching methods: 1) The **cyber security game approach** of Cone et al. (2007: 63–64) suggests the application of security concepts to the simulated environment, thus involving authentic problem solving. 2) Similarly, the **active learning approach** of Furnell et al. (2002: 354) uses simulated case-study scenarios with problem-solving activities. 3) The **policy creation approach** of Gaunt (1998: 134) includes a discussion of security principles in which users’ opinions and participation are emphasized. 4) The **constructive instruction approach** of Heikka (2008: 4–5) emphasizes individual reflection on information and concrete experiences through discussion in order to formulate questions and interpretations. 5) The **hypermedia instruction approach** of Shaw et al. (2009: 3–4), includes the selection of relevant information and forming new mental models. Virtual realities also allow authentic problem solving.

Two approaches also include collaborative teaching methods that emphasize the communal character of learning: 1) The **social psychological recommendations approach** of Kabay (2002: 8–9), which tries to reveal corporate culture and social views of the reality through discourse; and 2) the **cognitive processing approach** of Puhakainen (2006: 75–76), which seeks the communal
relevance of a learning task through a team rehearsal. Therefore, only two IS security approaches meet the third requirement for IS security training: teaching methods need to focus on critical reflection of collective knowledge and experiences through authentic problem solving or communication; i.e., they must include collaborative learning techniques in order to reveal and produce collective knowledge (e.g., Barkley et al. 2005). The results of analyzing teaching methods in existing IS security-training approaches are presented in Table 6. 

Table 6. Teaching methods in the existing IS security training approaches.

<table>
<thead>
<tr>
<th>Transmission</th>
<th>Transaction</th>
<th>Transformation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Behaviorism (28)</td>
<td>Cognitivism (12)</td>
<td>Constructivism (25)</td>
</tr>
<tr>
<td>Exclusive (8)</td>
<td>Exclusive (0)</td>
<td>Exclusive (8)</td>
</tr>
<tr>
<td>Deterrence approach (Straub &amp; Welke 1998)</td>
<td>Normative approach (Siponen 2000a)</td>
<td>Cognitive processing approach (Puhakainen 2006)</td>
</tr>
<tr>
<td>University environment approach (McCoy &amp; Thurmond Fowler 2004)</td>
<td>Preventive approach (Nosworthy 2000)</td>
<td>Cyber security game approach (Cone et al. 2007)</td>
</tr>
<tr>
<td>(Kajava &amp; Siponen 1997)</td>
<td>Briefing approach (Furnell et al. 1997)</td>
<td>Hypermedia instruction approach (Shaw et al. 2009)</td>
</tr>
<tr>
<td>Pedagogical game approach (Siponen 2000a)</td>
<td>Cyber security game approach (Cone et al. 2007)</td>
<td>Active learning approach (Furnell et al. 2002)</td>
</tr>
<tr>
<td>(Rudolph et al. 2002)</td>
<td>Active learning approach (Furnell et al. 2002)</td>
<td>Hypermedia instruction approach (Shaw et al. 2009)</td>
</tr>
<tr>
<td>Behaviorism + cognitivism (3)</td>
<td>Academic environment approach (Kajava &amp; Siponen 1997)</td>
<td>Active learning approach (Furnell et al. 2002)</td>
</tr>
<tr>
<td>IS security architecture approach (Tudor 2001)</td>
<td>Pedagogical game approach (Siponen 2000a)</td>
<td>Hypermedia instruction approach (Shaw et al. 2009)</td>
</tr>
<tr>
<td>Transmission</td>
<td>Transaction</td>
<td>Transformation</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Behaviorism + constructivism (8)</td>
<td>Social psychological recommendations approach (Kabay 2002)</td>
<td>Social psychological recommendations approach (Kabay 2002)</td>
</tr>
<tr>
<td></td>
<td>Constructive scenario approach (Biros 2004)</td>
<td>Constructive scenario approach (Biros 2004)</td>
</tr>
<tr>
<td></td>
<td>Social engineering preventive approach (Mitnick &amp; Simon 2002)</td>
<td>Social engineering preventive approach (Mitnick &amp; Simon 2002)</td>
</tr>
<tr>
<td></td>
<td>Persuasive technology approach (Forget et al. 2007)</td>
<td>Persuasive technology approach (Forget et al. 2007)</td>
</tr>
<tr>
<td></td>
<td>Traditional e-learning approach (Kajava et al. 2003)</td>
<td>Traditional e-learning approach (Kajava et al. 2003)</td>
</tr>
</tbody>
</table>

Social constructivism (2)
Social psychological recommendations approach (Kabay 2002)
Cognitive-processing approach (Puhakainen 2006)
Transmission Transaction Transformation

Inclusive (9)
- Motivation theory-directed approach (Roper et al. 2006)
- Andragogical approach (Herold 2005)
- Counteractive approach (McIlwraith 2006)
- ISD approach (Hansche 2001)
- Strategic approach (Wilson & Hash 2003)
- Operational controls approach (NIST 1995)
- Discursive approach and online tutorial approach (Cox et al. 2001)
- Competence approach (Wilson et al. 1998)
- Awareness campaign approach (Hadland 1998)

**Fourth pedagogical requirement for IS security training: Evaluation of learning**

Eighteen approaches contain transmission-oriented evaluation practices. These behaviorist evaluation practices measure the effectiveness of IS security training with formal written measures before and after training, including various evaluation methods with predetermined responses. Measuring learners’ actual performance and the effectiveness of training through performance-based assessments without the participants’ knowledge (e.g., observation) also represents a transmission-oriented evaluation of learning. The following five approaches include examples solely of the transmission-oriented evaluation of learning: 1) The communication-oriented approach of Desman (2002: 138, 182, 173–174) employs multiple-choice tests and objective evaluation of an entire IS security awareness program including statistics of break-in incidents. 2) The traditional e-learning approach of Kajava et al. (2003: 37) brings forward electronic questionnaires. 3) The stakeholder approach of Kovacich and Halibozez (2003: 268) advocates surveys. 4) The social engineering preventive approach of Mitnick and Simon (2002: 255–256) suggests evaluation of learning through direct observations (penetration testing) and knowledge testing. 5) The security-ensuring approach of Peltier (2000: 29–30) suggests the use of information security assessment questionnaires.

A typical evaluation of transaction and cognitivism is performed in five approaches, where the object of evaluation is the adaptation of learned knowledge and problem solving through interactive exercises, case studies, or essay questions. None of the IS security approaches introduces an exclusively transaction-oriented evaluation of learning. The following five approaches...
include transaction-oriented features as a part of the training: 1) The constructive scenario approach of Biros (2004: 35) tests the effectiveness of scenarios through judgment tests (identifying deceptive behaviors) conducted before and after scenario-based training. 2) The pedagogical game approach of Greitzer et al. (2007: 3) suggests quizzes and interactive exercises as a means to provide opportunities for learning through exploration and discovery. 3) Problem-solving exercises are considered as a method to evaluate learning in the operational controls approach of NIST (1995: 147). 4) In order to assess learning performance, the recognition of harmful e-mail titles and explanations in an essay format are used in the hypermedia instruction approach of Shaw et al. (2009: 5). 5) The competence approach of Wilson et al. (1998: 161, 171) employs solvable case studies and essay questions.

In 15 approaches, features of the transformation orientation and constructivism are identified in the suggestions to conduct evaluation practices. Hence, these conversational evaluation practices are characterized as informal, experimental, and/or open-ended. In addition, experimental evaluation of learning based on action and feedback provided during the computer-based instruction is implemented. The following five approaches represent transformation orientation: 1) The cyber security game approach of Cone et al. (2007: 67, 70) includes game state conditions, active triggers, and awareness messages in order to assess the achievement of objectives, change environments to the next phase, and relate actions taken with real-life circumstances. 2) In the persuasive technology approach of Forget et al. (2007: 825), monitoring the user’s actions and accordant reports with respect to more secure behaviors can be considered as a method to evaluate learning. At the same time, explanations for desired behaviors can be presented. 3) The purpose of the active learning approach of Furnell et al. (2002: 354–356) is to test one’s understanding of security before real actions take place within an organization. The system both evaluates the suggested security strategy (e.g., selection of protection for identified problems) and identifies weak areas or problems in users’ activities. Users’ solutions are also rated against the ideal solution defined by the teacher or security expert. In addition, the system provides additional information (e.g., narrative descriptions) in order to enhance learners’ understanding. 4) The constructive instruction approach of Heikka (2008: 5) employs participants’ reports concerning the implementation of the topics of a previous education session and follow-up interviews. 5) The counteractive approach of McIlwraith (2006: 104) uses retrospective feedback, which forces students to reflect on the content of training.
Along with the evaluation of individual learners, three approaches represent transformation orientation and social constructivism while they stress communication as the purpose of evaluation, which is viewed as a feature of effective educational practice: 1) corrective feedback during group assignment in the cognitive processing approach of Puhakainen (2006: 76), 2) role-play scenarios and focus groups in the andragogical approach of Herold (2005: 246), and 3) group interviews in the strategic approach of Wilson and Hash (2003: 37–38). Therefore, only three IS security-training approaches meet the fourth requirement for IS security training: informal, experimental, and open-ended forms of evaluation for groups need to be applied. This means that assessment of learning must emphasize experiential and communication-based methods that reveal the groups’ viewpoint of the training results (Birenbaum, 1996). The results of analyzing the evaluation of learning in existing IS security-training approaches are presented in Table 7.

Table 7. Evaluation of learning in the existing IS security training approaches.

<table>
<thead>
<tr>
<th>Transmission</th>
<th>Transaction</th>
<th>Transformation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Behaviorism (18)</td>
<td>Cognitivism (5)</td>
<td>Constructivism (15)</td>
</tr>
<tr>
<td>Exclusive (6)</td>
<td>Exclusive (0)</td>
<td>Exclusive (4)</td>
</tr>
<tr>
<td>Security-ensuring approach (Peltier 2000)</td>
<td>Constructive instruction approach (Heikka 2008)</td>
<td>Cyber security game approach (Cone et al., 2007)</td>
</tr>
<tr>
<td>Communication-oriented approach (Desman 2002)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stakeholder approach (Kovacich &amp; Halibozek 2003)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social engineering preventive approach (Mitnick &amp; Simon 2002)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Traditional e-learning approach (Kajava et al. 2003)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intranet-based approach (Vroom &amp; von Solms 2002)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Behaviorism + cognitivism (2)</td>
<td>Constructive scenario approach (Biros 2004)</td>
<td>Persuasive technology approach (Forget et al. 2007)</td>
</tr>
<tr>
<td>Operational controls approach (NIST 1995)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transmission</td>
<td>Transaction</td>
<td>Transformation</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Cognitivism + constructivism (1)</td>
<td>Pedagogical game approach</td>
<td>(Greitzer et al. 2007)</td>
</tr>
<tr>
<td></td>
<td>Motivation theory directive approach</td>
<td>Motivation theory directive approach (Roper et al. 2006)</td>
</tr>
<tr>
<td></td>
<td>Cognitive processing approach (Puhakainen 2006)</td>
<td>Cognitive processing approach (Puhakainen 2006)</td>
</tr>
<tr>
<td></td>
<td>Andragogical approach (Herold 2005)</td>
<td>Andragogical approach (Herold 2005)</td>
</tr>
<tr>
<td></td>
<td>Counteractive approach (McIlwraith 2006)</td>
<td>Counteractive approach (McIlwraith 2006)</td>
</tr>
<tr>
<td></td>
<td>Promotional approach (Rudolph et al. 2002)</td>
<td>Promotional approach (Rudolph et al. 2002)</td>
</tr>
<tr>
<td></td>
<td>Preventive approach (Nosworthy 2000)</td>
<td>Preventive approach (Nosworthy 2000)</td>
</tr>
<tr>
<td>Social constructivism (3)</td>
<td>Cognitive processing approach (Puhakainen 2006)</td>
<td>Andragogical approach (Herold 2005)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Strategic approach (Wilson &amp; Hash 2003)</td>
</tr>
<tr>
<td>Inclusive (2)</td>
<td>Competence approach (Wilson et al. 1998)</td>
<td>Hypermedia instruction approach (Shaw et al. 2009)</td>
</tr>
</tbody>
</table>
To summarize, none of the IS security approaches meets all four requirements (see Table 8).
Table 8. The degree to which the extant IS security training approaches meet the four pedagogical requirements for IS security training approaches. (1) Fulfils the requirement for the explicit psychological context. (2) Fulfils the requirement for the content. (3) Fulfils the requirement for teaching method. (4) Fulfils the requirement for evaluation of learning.

<table>
<thead>
<tr>
<th>IS security training approaches</th>
<th>(1)</th>
<th>(2)</th>
<th>(3)</th>
<th>(4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cognitive processing approach (Puhakainen 2006)</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Social psychological recommendations approach (Kabay 2002)</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td>Andragogical approach (Herold 2005)</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>X</td>
</tr>
<tr>
<td>Strategic approach (Wilson and Hash 2003)</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>X</td>
</tr>
</tbody>
</table>

Pedagogical requirements:

1. The explicit psychological context must be based upon the group-oriented theoretical approach of teaching and learning.
2. The content of training must be based on the collective experiences of the learners.
3. Teaching methods must focus on collaborative learning in order to reveal and produce collective knowledge.
4. Evaluation of learning should emphasize the experiential and communication-based methods from the viewpoint of the learning community.

Analyzed IS security training approaches, which do not fulfill any of the pedagogical requirements:

Constructive instruction approach (Heikka 2008); Constructive scenario approach (Biros 2004); Cyber security game approach (Cone et al. 2007); Pedagogical game approach (Greitzer et al. 2007); Social psychology-oriented approach (Thomson & von Solms 1998); Motivation theory directive approach (Roper et al. 2006); Persuasive technology approach (Forget et al., 2007); Normative approach (Siponen, 2000a); Counteractive approach (McIlwraith 2006); Security-ensuring approach (Pettila 2000); Communication-oriented approach (Desman 2002); Promotional approach (Rudolph et al. 2002); Stakeholder approach, (Kovacich & Halibozek 2003); Deterrence approach, (Straub & Welke 1998); Academic environment approach (Kajava & Siponen 1997); University environment approach (McCoy & Thurmond Fowler 2004); Preventive approach (Nosworthy 2000); Competence approach (Wilson et al. 1998); Operational controls approach (NIST 1995); ISD approach (Hansche, 2001); Traditional e-learning approach (Kajava et al. 2003); Hypermedia instruction approach (Shaw et al. 2009); Policy creation approach (Gaunt 1998); Healthcare environment approach (Furnell et al. 1997); Discursive approach and online tutorial approach (Cox et al. 2001); Briefing approach (Markey 1989); Social engineering preventive approach (Mitnick & Simon 2002); and Active e-learning approach (Furnell et al. 2002); Profession-based approach (Thomson & von Solms 1997); Intranet-based approach (Vroom & von Solms 2002); Awareness campaign approach (Haddad 1998); IS security architecture approach (Tudor 2001).

One study (Puhakainen 2006) meets the last three requirements; another (Kabay 2002) meets the second and third requirements; and two (Herold 2005, Wilson & Hash 2003) meet the last requirement. However, the features of the existing IS security training approaches that fulfill these pedagogical requirements are not guided by the social constructivist learning paradigm or instructional design approach. Therefore, they are considered to be only single features and not in the
essence of the IS security training practice. This means that instead of an active communal production of knowledge and work practices, IS security training is directed towards adopting stable work practices (see Tuomi-Gröhn & Engeström 2003). Given that no existing IS security-training approaches meet all four pedagogical requirements, the following section advances an example of a new training approach that meets these four requirements.

**2.2.4 Intuitive level thinking: Example of an IS security training approach meeting the four pedagogical requirements**

In the previous sections, a meta-theory for IS security training approach is advanced, mirroring Hare’s concept of three levels of thinking. Accordingly, two meta-level requirements are put forth, as follows: 1. An IS security training approach must be based on the understanding that the nature of IS security training is persuasive and non-cognitive. 2. An IS security training approach must focus on the existentialistic features of IS security training. These two requirements informed the search for pedagogical requirements at the critical thinking level. As a result, four pedagogical requirements for IS security training approaches were laid down. This section demonstrates a potential pedagogical approach to IS security training, which meets these four pedagogical requirements.

*Searching for a Proper Instructional Design Approach fulfilling the pedagogical requirements for IS security training: The Experiential and Collaborative IS Security Training Approach*

The first pedagogical requirement for IS security training argues that the explicit psychological context of IS security training must be based upon the group-oriented theoretical approach to teaching and learning. In seeking such candidate approaches that meet the first pedagogical requirement for IS security training, constructivist instructional design theories are found to constitute ideal theoretical bases for designing IS security training. This is due to two reasons. First, a constructivist instructional design theory is beneficial in training design because it expresses concrete instructions for training, unlike the four high-level pedagogical requirements derived from the social constructivist learning
paradigm (Yilmaz 2008, Wasson 1996). Second, constructivist instructional design approaches are also relevant for social constructivist instructional design. The key difference between them is that constructivism has a viewpoint of the individual learner and social constructivism emphasizes a social viewpoint towards learning with respect to general aims, content, teaching methods, and evaluation (see Table 3).

Of the alternative constructivist instructional design approaches (see Fardanesh 2006 Kirschner et al. 2006), experiential learning is used here as an example to illustrate how to meet the four requirements; because it is the preferred learning approach in the organizational context (Pavlica et al. 1998, Backström 2004, Dixon 1999), it is work-based learning (Honey and Mumford 1992), and it has achieved the raising of group consciousness, community action, and social change (Weil and McGill 1989). Thus, it is also deemed the experiential learning approach to be a suitable approach for changing employees’ IS security attitudes and behaviors.

A leading experiential learning approach is the theory of experiential learning by Kolb (1984) (see Tennant 1997). Hence, it is selected to form the instructional design part of the IS security training approach (which should meet the four pedagogical requirements). Because Kolb’s theory of experiential learning does not address the social aspects of learning (Pavlica et al. 1998, Holman et al. 1997), collaborative learning techniques are added (Barkley et al. 2005) to the IS security training approach, in order to achieve effective learning in groups. Collaborative learning has been reported to be effective; for example, for conceptual change (Rochelle 1992), promoting achievement and productivity (Johnson et al. 1981), and improving attitudes towards the subject matter (Springer et al. 1999). Next, the IS security training approach, combining experiential learning and collaborative learning techniques, is introduced.

The Experiential and Collaborative IS Security Training Approach

The learning approach involves four prescriptive guidelines based on Kolb’s four-stage cycle (1984): (1) Involve Learners’ Concrete Experiences, (2) Engage Reflective Observation, (3) Support Formation of Abstract Concepts and Generalizations, and (4) Enable Active Experimentation. These phases of the

---

11 This is the case since the four pedagogical requirements at the critical level were meta-requirements, i.e., high-level requirements for IS security training approaches.
Complemented by collaborative learning techniques (Barkley et al. 2005), the theory of experiential learning offers an instructional design approach analogous to collective cognition, which refers to the processing of information in groups (Gibson 2001, Hinsz et al. 1997). Then, these four phases include certain processes to make changes in collective thinking and develop effective group decisions and actions. It is argued that such a training approach stresses the experiences and collective activities of learners in order to achieve communal change. This approach resembles the features of transformation orientation and of social constructivism (previously presented in this thesis). Thus, this training approach fulfils the first pedagogical requirement for IS security training: the explicit psychological context of IS security training must be based upon the group-oriented theoretical approach to teaching and learning. Next, each of the four phases of experiential learning is described in order to demonstrate how the experiential and collaborative IS security training approach meets the other three pedagogical requirements for IS security training.
1) Involve Learners’ Concrete Experiences

The learning cycle begins with concrete experiences (Kolb 1984; Gibson 2001), which form the basis for learning. In IS security training, the concrete experiences at the initial phase of learning are former experiences that the learner has encountered (see Fenwick 2001, Dixon 1999) with respect to the existentialistic features of IS security training—security-sensitive organizational assets, threats towards them, and protection mechanisms. To illustrate this, let us presume that an organization finds insecure e-mail use by employees to be a problem. In this case, the employees’ concrete experience with the security-sensitive organizational assets (e.g., confidential documents), threats towards them (e.g., e-mail eavesdropping) and protection mechanisms (e.g., e-mail encryption) with regard to secure e-mail use, will constitute the starting point for IS security training.

2) Engage Reflective Observation

The second phase, reflective observation, occurs via the retrieving, exchanging, and structuring of groups’ shared experiences (Kolb 1984, Gibson 2001). Then, concrete experiences can be reflected through group discussions in order to react to others’ perspectives and practices (Honey & Mumford 1992), and to map a causal relationship between their work practices and respective organizational consequences (Pavlica et al. 1998). In collaborative activities, learners generate rich descriptions and analyses through systematic and intentional conversations with others, which take into account learners’ personal and interpersonal perspectives, former knowledge, and attitudes (Pavlica et al. 1998).

In practice, in the context of IS security training, learners work in small groups to generate interpersonal experiences regarding the existentialistic features of IS security training, in order to define their meanings and implications for the organization. For instance, if the topic of the training is to make employees’ e-mail use more secure, their task is to consider what kinds of security-sensitive e-mails require protection, what protection mechanisms constitute secure e-mail use in general, which of these practices are valid in their own work and why, and what threats exist if these protection mechanisms are not followed. Thus, while this phase implements collective experiences as a content of training, it also involves groups’ interpersonal perspectives towards the existentialistic features of IS security training. Hence, it meets the second pedagogical requirement.
Reflective observation of these collective experiences can be accomplished, for example, through the collaborative learning technique called Think-Pair-Share (Barkley et al. 2005), which is implemented as follows. First, learners think of existentialistic features with respect to secure e-mail use individually, and then share their ideas with a colleague to create a joint response. Next, pairs share their ideas in a group of four to expand common viewpoints (Lyman 1981). Finally, the results are visually presented to the whole group by amalgamating them on the blackboard, a method that supports learners’ understanding of different aspects and enhances their ability to build group consensus on the secure use of e-mail. Hence, the teaching methods are focused on collaborative learning in the form of group discussions (i.e., Think-Pair-Share) in order to reveal and produce collective knowledge. Hence, this phase meets the third pedagogical requirement for IS security training: teaching methods must focus on collaborative learning in order to reveal and produce collective knowledge.

3) Support Formation of Abstract Concepts and Generalizations

The third phase, the formation of abstract concepts and generalizations, involves processes of negotiation, interpretation, and evaluation (Kolb 1984, Gibson 2001). In this phase, the meanings of collective experiences are interpreted in the organizational context by comparing them to the organizational viewpoints (Honey & Mumford 1992), as stated in the organization’s written IS security procedures. The instructor needs to introduce the organization’s e-mail procedures, related security-sensitive organizational assets, threats towards them, and protection mechanisms. Building on the aforementioned exercises in the previous phase (e.g., Think-Pair-Share), the learners analyze the similarities and differences between group experiences and the presented organizational viewpoint. This phase is an examination of the overlap between organizational regulations and employees’ communal experiences. Some variations are possible in cases where the existing IS security procedures and instructions do not reconcile with actual work practices.

Similarly to the previous phase, this phase involves collective experiences as a content of training, thereby fulfilling the second pedagogical requirement: the content of training must be based on the collective experiences of the learners. It also involves collaborative learning in the form of group discussion in order to reveal and produce collective knowledge; hence, it fulfills the third pedagogical requirement: teaching methods must focus on collaborative learning in order to
reveal and produce collective knowledge. However, compared to the previous phase, collective experiences are now expanded from the group to the organizational level involving reflection of the organization’s formal e-mail procedures.

4) Enable Active Experimentation

The last phase, active experimentation, refers to the integration of collective experiences in order to reach decisions and actions (Kolb 1984, Gibson 2001). In this phase, employees’ experiences (which were previously described and analyzed) are now used to develop new organizational practices (Pavlica et al. 1998). To put this into the context of IS security training, and to take secure use of e-mail as an example, concrete e-mail use instructions are established in a manner that solves the original problem of insecure e-mail use by employees—by combining individual (first phase), interpersonal (second phase), and organizational (third phase) viewpoints with respect to the existentialistic features of secure e-mail use.

The ultimate purpose of the fourth phase is to define how formal e-mail procedures and instructions are actually experienced by employees, and how they can be applied by the learners. For example, the instructor can deliver written procedures to learners with open spaces for learners’ possible correctives, supplements, and/or corrections. This document can also function as a “learning contract” that supports the transfer of learned knowledge and attitudes of employees (for example, to secure e-mail practices) (Kirkpatrick 2006, Knowles 1986).

As part of the last phase to ensure effective collective learning, learners need to be able to test their new understanding in practice (Backström 2004). In addition to describing, analyzing, and creating organizational practices, learners are required to implement changes in their work (Pavlica et al. 1998). In order to validate a new practice in an organization, potential changes in the IS security procedures and instruction must be accepted by management. Employees need to consciously observe their e-mail use practices, and must execute applicable changes based on what has been learned in training. Finally, these new experiences are evaluated through group interviews, which are then used to evaluate the effectiveness of the training from the learners’ perspective. If required, these new experiences can function as a starting point for a second learning cycle (Dixon 1999).
A function of this phase is to put together the collective experiences of the learners with respect to existentialistic features in the area of secure use of e-mail, which formed the content of the training in the presented example. A “learning contract” as a concrete form of this collective knowledge can again be created through collaborative learning techniques (e.g., Think-Pair-Share). This fourth phase of the experiential learning cycle also meets the second and third requirements for IS security training. At the same time, after employees have changed and observed their IS security practices with respect to the topic of the training (for example, e-mail use), evaluation of learning is conducted using the group interview. Then, the fourth pedagogical requirement for IS security training is also fulfilled: evaluation of learning should emphasize experiential and communication-based methods from the viewpoint of the learning community. Table 9 illustrates the four phases of the experiential learning cycle in the context of IS security training.

Table 9. Phases of experiential learning cycle (Kolb 1984; Gibson 2001) in the context of IS security training.

<table>
<thead>
<tr>
<th>Phase</th>
<th>Description of the phase</th>
<th>Example in IS security training on the use of strong passwords</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase 1: Concrete experiences</td>
<td>Employees’ individual experiences regarding the following features in their work form the basis of learning:</td>
<td>Employees’ experiences of secure passwords, which will be changed during the training, form the basis of learning:</td>
</tr>
<tr>
<td></td>
<td>1. Sensitive information (e.g., personnel data, business and strategic decisions, financial, customer, and R&amp;D information).</td>
<td>1. What security-sensitive information in the employees’ work environment requires password protection?</td>
</tr>
<tr>
<td></td>
<td>2. IS security threats (e.g., loss of sensitive information due to unintentional information leak, IS security breach, virus infections).</td>
<td>2. Which protection mechanisms constitute secure password use, and which of these practices are valid in employees’ own work (and why)?</td>
</tr>
<tr>
<td></td>
<td>3. Means to protect sensitive information from IS security threats (e.g., selecting strong passwords, encrypting e-mails, making regular backups).</td>
<td>3. What threats exist if these protection mechanisms are not followed? For example, an HR secretary may think that only personnel information (1) needs to be secured with passwords to prevent other employees from seeing it (3), but does not recognize other areas of sensitive information or IS security threats in his work. In addition, he may not recognize why passwords need to be changed frequently or why selecting strong passwords is important (2).</td>
</tr>
</tbody>
</table>
Phase Description of the phase Example in IS security training on the use of strong passwords

Phase 2: Reflective observation
Learners work in small groups to share their experiences regarding secure working practices (see Phase 1). To be more precise, they describe and analyze employees' collective experiences of sensitive information, IS security threats, and ways to protect sensitive information from threats (see phase 1) in their work through a certain systematic discussion procedure called Think-Pair-Share.

1. Learners think about secure password practices individually (see Phase 1).
2. They share their ideas with colleagues.
3. Pairs share their ideas in a group of four to expand common viewpoints.
4. These viewpoints are discussed and visually presented to all learners, e.g., via the blackboard.

For example, through discussing their password experiences with a co-worker, a HR secretary may realize that she has also customer-related data in her laptop requiring password protection (2). In addition, in the group of four, she realizes that to prevent information theft, it might be necessary to use password protection also for confidential e-mails (3). Finally, because almost all groups stated that it is important not to share passwords with other people, the HR assistant becomes more convinced to follow this practice (4).

Phase 3: Formation of abstract concepts and generations
Analyzing the possible differences between groups' collective experiences (formulated in phase 2) and organizations' written IS security policies, which provide guidelines for using different ways to protect sensitive information from IS security threats through the systematic discussion method.

First, the instructor introduces the company's password procedures and justifies the protection of security-sensitive organizational assets from threats. Second, learners analyze the similarities and differences between group experiences and the password procedures through a discussion method described in phase 2.

For example, in contrast with the organization's IS procedures, an HR assistant did not find it necessary to use strong passwords, which was required by the company's IS security policies. After an illustration of the importance of using strong passwords, employees become aware why they should use stronger passwords, and why they should be changed frequently.
| Phase 4: Active experimentation | Establishing new procedures to protect sensitive information from IS security threats, using them in practice, and evaluating their practical suitability through group interviews. | First, the instructor delivers password use procedures to learners with open spaces for feedback. Original procedures supplemented with employees' comments function as a concrete form of the employees' collective knowledge, and can again be created through a discussion method (e.g., Think-Pair-Share). All IS security policies need to be discussed, and their use should be supported, in order for them to be applicable by employees. For example, as a result of the discussion, it is found that, although employees understand the rationale behind most password procedures, and are willing to comply with them, they think that it is inconvenient to remember multiple passwords and select strong passwords, which need to be changed frequently. For that reason, the ease of selecting strong passwords should be supported, for example, through password mnemonics. After training, employees need to observe their password use, and execute changes based on what has been decided in the training. These new user experiences are evaluated through group interviews, and if required, these can form a starting point for a second learning cycle. |
3 Reasons for employees’ IS security behavior

Besides a training method, successful IS security training aimed at improving employees’ compliance with IS security procedures requires understanding the employees’ reasons for compliance and non-compliance with IS security procedures. Such understanding is necessary in order that employees’ IS security behavior can be effectively improved through various interventions, such as IS security training. This is the case because symptoms cannot be cured, unless we know the reasons for the symptoms. Accordingly, this chapter includes the second part of the thesis, which introduces the extant studies in the area of employees’ IS security behavior, and presents a theoretical framework for understanding employees’ IS security behavior based on an empirical study. The chapter is organized as follows: first, the extant studies in the area of employees’ IS security behavior are reviewed in terms of the purpose of research, theoretical background, methods, and the main results are presented in section 3.1. Second, empirical data collection and analysis methods—semi-structured qualitative interviews and inductive data analysis method for developing a theoretical framework—are introduced in section 3.2. Third, the main categories and their relationships as a result of a data analysis are elaborated on and illustrated in section 3.3. Finally, a framework based on the main categories, and their relationships formulated in the previous coding phases, is formulated in section 3.4.

3.1 Related work in the area of IS security behavior

Besides IS security training approaches (see section 2.1), the extant research in the area of IS security behavior in an organizational context is focused on three research areas: (1) models on computer misuse/abuse, (2) models on compliance with IS security procedures, and (3) studies of appropriate IS security behavior. All three of these research streams offer understanding as to why employees comply with the IS security procedures in an organizational context based on an empirical research. In Table 15 (Appendix 1), research articles are introduced in more detailed explicating the purpose of research, theoretical background, methods, and the main results.
3.1.1 Models of computer misuse/abuse

Computer abuse studies can be traced back to the research of Parker (1976), who introduced the term “computer abuse.” While Parker did not apply a theory in his studies, later studies on computer abuse have utilized the Deterrence Theory. In the first of these, Straub (1990) applied the Deterrence Theory to examine whether information security investments deter computer abuse. Straub applied formal sanctions by linking the number of reported incidents to different information security countermeasures and found that these countermeasures reduced the number of computer abuse incidents in organizations. While Straub (1990) did not measure computer abuse at the individual level, subsequent studies have addressed this point, and these studies have also included other variables to their models, in addition to the Deterrence Theory. To start with these, Harrington (1996) found that codes of ethics act as deterrents because they induce a fear of punishment in the sense of the Deterrence Theory. Another interpretation that operationalizes the Deterrence Theory in the context of IS security is by Lee et al. (2004). The authors examined whether a number of deterrents, such as IS security procedures, awareness programs, and physical security systems deter computer abuse. In addition, based on social control theory, Lee et al. (2004) explained the phenomenon of computer abuse through an influence of organizational trust, which means attachment (e.g., co-workers’ views and opinions), commitment (e.g., importance of success of the company), involvement (e.g., loyalty to the company), and moral norms (e.g., obedience with laws). In turn, D’Arcy et al. (2008) extended the Deterrence Theory to include preceding factors, such as computer awareness and training as well as the formulation of security procedures and computer monitoring. Similarly, D’Arcy and Hovav (2007) empirically examined the relationship between misuse intentions and awareness of IS security procedures, security awareness programs, preventive security software, and computer monitoring. Of these studies, D’Arcy et al. (2008) and D’Arcy and Hovav (2007) investigate employees’ misuse intentions generally without connecting their results to the specific misuse intentions. Instead, Harrington (1996) and Lee et al. (2004) have a connection to specific misuse procedures: the former investigates intentional misuse of IS in terms of virus, fraud, sabotage, software copying, and cracking, and the latter investigates the influence of intentions to install access control and intrusion protection software, controlling others’ identification, and illegal software use on actual computer abuse.
frequency (i.e., data loss, hardware loss, unauthorized IS use, illegal software copying, virus infection via e-mail and hacking).

### 3.1.2 Models on compliance with IS security procedures

In addition to studies on computer abuse, employees’ compliance with IS security procedures has recently received attention by IS scholars. These studies investigate employees’ intentions to comply with IS security procedures (Bulgurcy et al. 2010a, Johnston & Warkentin 2010, Herath & Rao 2009a, 2009b, Li et al. 2010, Siponen & Vance 2010), their actual behavior (Beaument et al. 2010, Chan et al. 2005, Ng et al. 2008), or both (Pahnila et al. 2007, Siponen et al. 2006, 2007, Myyry et al. 2009, Bulgurcy et al. 2010b). Like computer abuse studies, these studies (except Beaument et al. 2010) also tested theories and models derived from reference theories through surveys. Of these thirteen theory-verification studies of compliance with IS security procedures, Myyry et al. (2009) investigated password sharing with co-workers, Ng. et al. (2008) explained IS security procedure compliance-related with e-mail, Johnston and Warkentin (2010) accounted for compliance with IS security procedures with respect to spyware, and Li et al. (2010) investigated compliance with Internet use procedures, while others were concentrated on general compliance with IS security procedures.12

Five studies applied protection motivation theory (PMT) (Herath & Rao 2009a, Johnston & Warkentin 2010, Pahnila et al. 2007, Siponen et al. 2006, 2007). In these studies, employees’ motivation towards compliance with IS security procedures was examined related with their perceptions of probability and the consequences of IS security threats in their organization, perceptions of efficacy of the response and individuals’ ability to perform it, and/or perceptions of a hindrance caused by complying with IS security procedures. In addition, derived from PMT or theory of planned behavior (TPB), four of these studies also explored the impact of normative beliefs and/or other people’s behavior on employees’ compliance with IS security procedures (Pahnila et al. 2007, Siponen et al. 2006, Herath & Rao 2009a, Johnston & Warkentin 2010). Besides PMT, four of these five studies have also included other than PMT variables with the models. First, the deterrence theory was applied in three studies (Pahnila et al.

---

12 General compliance with IS security procedures means that these surveys use general statements such as “I intend to comply with my company’s IS security policies in the future” instead of specifying the type of IS security procedures or policies in question through using statements such as “I intend to encrypt my confidential e-mails in the future.”
2007, Siponen et al. 2007, Herath & Rao 2009a). In addition, Pahnila et al. (2007) applied Information Systems Success and Triandi’s Behavioral Framework, and explained compliance with IS security procedures through perceived quality and the usefulness of IS security procedures, organizational and technical support, and habits. Siponen et al. (2006) studied the visibility of IS security on employees’ compliance with IS security procedures, and Herath and Rao (2009a) investigated whether compliance is influenced by the influence on organizational commitment on IS security behavior.

Similarly with the concepts of PMT (i.e., threat perceptions, response efficacy, self-efficacy, response costs, and/or normative beliefs), Bulgurcy (2010a) combined Theory of Planned Behavior (TPB) with Rational Choice Theory (RCT), and investigated the influence of attitudes formed by balancing costs and benefits of compliance, normative beliefs, and self-efficacy with employees’ intentions to comply with IS security procedures. Further, as a foundation of cost-benefit assessments, the following factors were examined: intrinsic benefit, safety, rewards, work impediment, intrinsic cost, vulnerability, and sanctions. In turn, based on Rational Choice Theory, Li et al. (2010) also investigated the influence of cost-benefit assessment (i.e., the influence of security threats and perceived benefits, formal sanctions, expectations of influential people), moral norms, and organizational context factors (i.e., organizational norms and organizational identification) on employees’ intention to comply with procedures regarding secure use of the Internet.

Also, studies of Ng et al. (2006), Herath and Rao (2009b), and Chan et al. (2005) have common features with concepts of protection motivation theory: threat appraisal and coping appraisal. Ng et al. (2006) employ the Health Belief Model (HBM) to investigate the connection between e-mail security behaviors in terms of reading e-mail attachments and perceived severity and susceptibility to security incidents and self-efficacy, as well as perceived benefits and barriers of practicing e-mail security. In addition, the influence of organizational support and employees’ general security orientation on IS security behavior was studied. Similarly with self-efficacy and normative beliefs derived from PMT and also punishments and monitoring derived from the deterrence theory, Herath and Rao (2009b) studied the influence of intrinsic motivation (i.e., perceived effectiveness of own actions), and extrinsic motivation (i.e., managers and peers’ expectations, behavior of peers, severity of punishments, and certainty of detection) on employees’ policy compliance intention. Chan et al. (2005) developed and examined a theoretical model built on the safety climate literature and the social
information processing approach, explaining the effects of managerial action and co-worker socialization on information security climate, and further on employees’ compliance with IS security procedures. Also, the influence of self-efficacy on compliant IS security behavior (Bandura, 1977) was examined by Chan et al. (2005).

In turn, Siponen and Vance (2010) employed Neutralization Theory and pointed out that employees use several neutralization techniques (e.g., denial of injury and responsibility) for rationalizing their IS security procedure violations. In addition, they studied the impact of sanctions derived from the deterrence theory, informal sanctions, and shame on employees’ IS policy compliance.

While Li et al. (2010) studied the influence of moral norms on employees’ compliance intentions based on RCT as one aspect of their study, Myyry et al. (2009) exclusively investigated the influence of values and moral reasoning on employees’ compliance with IS security procedures. They applied the Theory of Cognitive Moral Development and Theory of Motivational Types of Values.

Having common characteristics with the study of Pahnila et al. (2007), which studied the influence of perceived quality and usefulness of IS security procedures based on the concept of information quality, Bulgurcu et al. (2010b) also explain compliance with IS security procedures through characteristics of these procedures: fairness and quality (i.e., clarity, completeness, and consistency) based on the concept of quality, as well as the group engagement model.

While other studies investigating IS security policy compliance use theory verification approaches through the quantitative research methodology, Beautement et al. (2010) study this phenomenon through the qualitative research approach. They apply techniques of economic management and optimization for modeling employees’ costs (i.e., increased physical and cognitive load, embarrassment, missed opportunities, the hassle factor such as pressure) and benefits (i.e., avoiding the consequences of a security breach, protection from sanctions) associated with IS security procedures. Based on these issues, they present a theoretical approach for explaining employees’ compliance with organizations’ IS security procedures generally without any connection with specific IS security procedures.

3.1.3 Studies of appropriate IS security behavior

Along with computer abuse and employees’ compliance with IS security procedures, ten studies exist that investigate employees’ appropriate IS security
behavior from various perspectives. Four of these studies employed various theories/models, which emphasize the role of employees’ social environment in IS security behavior. First, D’Arcy and Greene (2009) applied social exchange theory to explain the impact of security culture on both compliance with IS security procedures and supererogatory actions, i.e., voluntary IS security actions not required by the company’s IS security policy. In turn, relying on social comparison theory, Hyeun-Suk et al. (2005) explained employees’ IS security behavior through their risk perception, and its relation to perceived control and other people. Dinev and Hu (2007) used the theory of planned behavior to use (intention) anti-spyware technology, and examined the influence of technology awareness on behavioral intentions, as well as subjective norms and attitudes. Dinev et al. (2009) expanded this model with the integrated model of user acceptance of e-commerce (Pavlou & Fygenson 2006), and cultural dimensions and indices (Hofstede 1993, 2001), and investigated the impact of national cultural factors between South Korea and the United States. Of these four studies, Dinev et al. (2009) and Dinev and Hu (2007) investigate employees’ intentions to use anti-spyware software, while D’Arcy and Greene (2009) and Hyeun-Suk et al. (2005) do not specify any particular IS security procedures. In addition, also using the theory-testing research setting, Stanton et al. (2003) used surveys to examine the influence of psychological concepts of organizational commitment on users’ security behavior (i.e., good password practices, voluntary IS security training participation, obeying IS security procedures, and discussing IS security procedures in the workplace). Similarly, Stanton et al. (2005) used surveys to focus on explaining password-related behavior (i.e., password changing, password selection, writing down passwords, and sharing passwords) related to training, awareness, monitoring, and motivation.

Under the category of appropriate IS security behavior, three studies also exist explaining employees’ IS security behavior without theory-testing research setting. Sasse et al. (2001) and Adams and Sasse (1999) conducted interviews to explore why people exhibit good password behavior (17 users and 30 users, respectively). In turn, Albrechtsen (2007) explored users’ experiences and personal roles in organizations’ information security work through qualitative interviews.
3.1.4 A summary of the literature review

To summarize the extant literature, the empirical studies on employees' IS security behavior can be divided into three research areas: (1) models on computer abuse/misuse, (2) models on compliance with IS security procedures, and (3) studies on appropriate IS security behavior.

The first research area, computer abuse/misuse, applied existing criminological theories, such as the Deterrence Theory or the Social Control Theory. In other words, these studies basically tested well-known and generic criminological theories in a new context — that of IS security. In turn, second and third research areas, models on compliance with IS security procedures and studies on appropriate IS security behavior, test not only criminological, but also socio-psychological, organizational, and psychological theories or constructs in the context of IS security (see theoretical background column in Table 15). In addition, in the second research area, Beautement et al. (2008) developed a theoretical model on employees’ IS security policy compliance based on qualitative interviews and techniques of economic management and optimization. Instead of validating existing theories or constructs originating from various research disciplines, there is a need to focus the investigation on the phenomenon of compliance with IS security procedures itself through inductive theory development, rather than test or illustrate existing theories for two reasons. First, the chosen theoretical perspectives may be forming blinders, which prevent researchers and readers from seeing issues that may be salient to the phenomenon of interest. Second, theory-verification studies carried out in IS rely on the adaptation of theoretical perspectives from reference disciplines, having no particular relationship with the information security compliance phenomenon. Hence, rather than investigating what is specific to IS security behavior, such studies are replicating the extant theories from criminology, psychology, and social psychology.

In the third research area, appropriate IS security behavior, three studies exist that are not focused on theory verification. Instead, these studies investigate employees’ password behavior (Sasse et al. 2001, Adams & Sasse 1999), or on general descriptions of users’ experiences of information security in their work (Albrechtsen 2007). However, these three studies are not focused on employees' compliance with organizational IS security procedures. Instead of extracting individual reasons for either password practices or general IS security behavior,
there is a need for qualitative research approaches to compliance with IS security procedures.

As a step in overcoming this gap in the research, it is proposed in this thesis that the use of an inductive and qualitative approach will complement the existing body of knowledge of employees’ compliance with IS security procedures. Such a research approach is important for a number of reasons. First, the majority of extant models in IS security are based on well-known theories developed in other areas, with the result that IS security researchers essentially are engaged in validating or invalidating these theories in other areas. Rather than validating the relevance of generic criminological or (social) psychological theories, an inductive, qualitative approach could potentially reveal new insights into the specific phenomena of employees’ compliance. Second, such an approach could lead to new theory development in this area (see Baskerville & Myers 2002). Third, because such a qualitative approach would not be limited by an extant theory, it could offer a richer picture that is based on human meanings and experiences than what is obtained through “experience far” theory testing. Indeed, owing to the focus on the operationalization of theoretical constructs, and in an effort to keep the survey length manageable, only a few theories/constructs can be studied for the same population. Finally, a qualitative approach would also allow the research of employees’ compliance with IS security procedures to move to the next level, beyond “Likert scale responses,” by obtaining a deeper understanding of the reasons why people do or do not comply with IS security procedures. It is believed that such an understanding can be useful to practitioners.

3.2 Data collection and analysis

In this thesis, empirical data is collected through interviewing employees belonging to an industrial company. The thesis can be situated under the interpretive research tradition (Walsham 1995, Charmaz 2000), which is focused on human interpretations of information security in the work surroundings. Consistent with the interpretive research tradition, instead of seeking objective knowledge and universal truth, or discovering a reality, the study is pursued to construct an interpretation of a perceived reality, and considers scientific knowledge to be based upon the inseparable perspective of researchers and interviewees (Charmaz 2000, Lincoln & Cuba 1985, Schulze & Avital 2011). Thus, both the credibility and the generalizability of the results are context dependent, which emphasizes the importance of the accurate documentation of
the data collection and analysis processes (Walsham 1995). Therefore, the applicability of the research results can be evaluated by a reader, based on the well-grounded documentation of the researchers’ reasoning and the research environment. Thus, before presenting the empirical results, data collection and the analysis methods are described.

3.2.1 Data collection

The purpose of the research was to understand and explain people’s attitudes and experiences related to information security in their working environment. Empirical data collection was executed in multiple locations of a global company (Company X, a pseudonym), which operates in the field of the marine industry and the energy market. In 2009, the company had over 18,000 employees in 70 countries. The selected locations were Switzerland, UAE, and China. While the offices in Switzerland, UAE, and China formally belong to the same organization, they can be seen as different organizations, because they operate independently, and have independent economic responsibilities. Finally, they were all previously owned by other companies and were bought by the multinational company they now formally belong to. In fact, these three locations in different countries were selected as representative of different cultural settings with the assistance of the information security manager of the organization.

Empirical data was collected through semi-structured qualitative interviews. The literature advises interviewers to pay attention to a number of issues when conducting interviews. To start with, Myers and Newman (2007) suggest that researchers should avoid a situation in which only certain groups of employees in an organization are interviewed, with the result that the interview results do not represent the views of the whole organization. In order to avoid this issue, interviewees were selected in different organizational positions.

Another thing is to ensure that interviewees are randomly selected as much as possible. Keeping this in mind, based on the list of employees and their titles we received from the Managing Directors and Executive Assistants in each of the three locations, we randomly selected the interviewees so that they would represent various positions, each of which involve handling valuable information within the organization in each organizational location (in Switzerland, UAE, and China). Altogether, 72 face-to-face interviews were conducted between June and November of 2009. The average interview lasted 47 minutes. Table 10 presents the number of interviews in different organizational positions and countries.
Table 10. Number of interviews in different positions and countries.

<table>
<thead>
<tr>
<th>Position</th>
<th>UAE</th>
<th>China</th>
<th>Switzerland</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager</td>
<td>10</td>
<td>7</td>
<td>6</td>
<td>23</td>
</tr>
<tr>
<td>Officer</td>
<td>15</td>
<td>13</td>
<td>9</td>
<td>37</td>
</tr>
<tr>
<td>Engineer</td>
<td>2</td>
<td>3</td>
<td>5</td>
<td>10</td>
</tr>
<tr>
<td>Unclear</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Total</td>
<td>29</td>
<td>23</td>
<td>20</td>
<td>72</td>
</tr>
</tbody>
</table>

It is also important to make sure that interviewees feel that the information they reveal will not be used against them (Myers & Newman 2007). To address this issue, the purpose of introductions and general discussions at the beginning of the interviews was to inform interviewees about the research and researchers and to make interviewees’ feel comfortable while emphasizing the importance of their own viewpoint regarding information security in their daily work. In addition, in each interview, we carefully explained to the participant that the interview was confidential, and that only the researchers were able to access the interview data. We made special mention of the fact that we would not provide the original interviews to the employer under any circumstances. We also pointed out that what each individual answered wouldn’t be reported. Furthermore, to avoid representing our own opinions of the research topic, it was emphasized that there were no right or wrong responses. Rather, eliciting interviewees’ own experiences was important, and we used neutral language in asking the questions. We asked the interviewees’ permission to record the interviews using a digital recorder, saying also that if they preferred, we could use field notes instead. This practice is consistent with Walsham (2006) and Mårtensson and Lee (2004). Seventy-one interviews were recorded and transcribed in text form. Only one interviewee preferred the use of field notes.

Finally, it is important that scholars’ theoretical perceptions and perspectives or “pet” theories should not drive the interview questions (Stinger 1999, Myers and Newman 2007), and that the interviewees and interviewers understand each other. For the development of the interview questions, we followed Spradley (1979), who suggests that the researcher first ask questions that are general and neutral, to enable participants to describe their situation in their own terms. The use of interviewees’ own words and phrases in the formulation of interview questions, a mirroring technique, was also used to enable interviewees to explain their experiences in their own words (Meyers & Newman 2007). When more information is needed, more directed probing questions can be presented,
focusing on issues that need further elaboration. In cases where the researchers did not get a clear sense of the meaning of an interviewee’s statements, they requested clarification immediately during the interview. Thus, the interviews had strongly conversational nature involving active listening, and activation of interviewees’ construction of meaning rather than the elicitation of facts (Schulze & Avital 2011). Because two interviewers conducted the interviews, the following two issues were accomplished in order to maximize the consistency of interviews. First, the structure of the interview was planned by the interviewers. Second, two interviewers executed the first seven interviews together.

The interviews began with the interviewers asking what Information Security (IS) means to the employees in general, and specifically for the respondents themselves. The idea was to discover the terminology they used. Then we asked what kind of confidential information they handle in their work, and what means, if any, they use to protect it. We asked if they comply with these means, and we also asked if their peers comply with them. Later, we asked them if they comply with specific information security instructions. Based on previous studies on the most common IS security policy violations (Siponen & Vance 2010), awareness of practices in other organizations we had studied in the past, and the IS security policy of the organization, we also asked about the most frequently occurring security instructions. These related to the secure use of the Internet, writing passwords down on paper, selecting appropriate passwords, and locking the workstation when leaving the workstation.

“Secure use of the Internet” includes Internet browsing habits, the sending of confidential e-mails, the use of e-mail encryption, installing software or loading files from the Internet, and avoiding viruses. “Writing passwords down” refers to an activity in which people write passwords down on paper. “Password selection” refers to the ways in which employees select their passwords, and whether the password is easy to guess. “Locking the workstation” refers to the practice of employees turning their workstations off when leaving their computers unattended (as a result, the computer is protected by a password). Other issues discussed in the interviews were awareness of information security, information security competence, communications, information security policies, and management’s role. Even if these broad research themes were planned to be discussed beforehand according to the researchers’ experiences of the topic and the company’s research needs, the interviews progressed flexibly in terms of the interviewees. This way, we avoided limiting the employees’ responses only to the
pre-determined themes (Fontana & Frey 2000), which brought both deeper understanding of the pre-determined themes and opened up new ones.

3.2.2 Data analysis

The purpose of the analysis was to develop a theoretical understanding of the phenomenon of IS security behavior embedded in the experiences of human subjects (Sarker et al. 2001) who are involved with the information systems in their work on a daily basis. In other words, the analysis developed a theoretical framework that explains the collected data (Charmaz 2000). Thus, transcribed interviews were analyzed through systematic inductive analysis in order to draw reliable and valid inferences from the phenomenon. However, inductive analysis of the data is dependent on the researcher’s perspective and interpretations in the process of his or her conceptual engagement with it (Krippendorff 2004). This means that the existing literature, particularly in the form of hypothesis falsification, and the researcher’s personal experiences and conceptual structures of the phenomenon, cannot be ignored, even if these pre-conceptions need to be consciously avoided, while remaining true to the interviewees and data (Traut 1997, Sarker et al. 2001, Suddaby 2006) during both data collection and analysis. This means that predetermined themes used in data collection (see section 3.2.1) were used only for support, not as a framework for analyzing the collected data. Based on the purpose to increase inductive understanding of the phenomenon of IS security behavior in the organizational context, and basic assumptions of the interactive nature of social reality, and, thus, data collection and analysis, a modified grounded theory approach is employed in this thesis.

The selected inductive data analysis method resembles a coding procedure adopted from grounded theory tradition, which includes the identifying and refining of concepts and the relationships between them and constructing a theoretical framework (Charmaz 2000). First, the transcribed interviews were examined at the sentence or paragraph level using an initial or open-coding process (Charmaz 2000, Glaser 1978). Open coding means “breaking down, examining, comparing, conceptualizing, and categorizing data” (Strauss & Corbin 1990, 61). In this thesis, all interviewees’ ideas, which included their viewpoints about IS security attitudes and behavior of their own, other employees, or people’s behavior in general, was first separated from the interview transcripts. These statements, including codes for every interviewee, were separated into a new text document. Next, from that new text document consisting of direct
quotations from the original interview transcripts, open codes were created through combining quotations with similar meaning, and conceptualizing them under reasonably understandable codes. Each new quotation was compared with existing open codes, and new open codes were created if no existing one fit with the meaning of a quotation. In addition, some original open codes were merged into a single more general one. For example, restrictiveness, difficulty, time-consumption, and memorability became a new code termed “Inconvenience.” After several iterations of the created text document, altogether, 59 open codes emerged from the data (see Appendix 2).

Of these 59 open codes, 18 explained both compliant and non-compliant IS security behavior, referred to in Appendix 2 as (+/-). In turn, 23 open codes explained only non-compliance, referred to in Appendix 2 as (-), and 18 compliance only, referred to in Appendix 2 as (+). Table 11 presents some examples of text quotations and the open codes generated from them.

Table 11. Examples of open codes generated from interview transcripts.

<table>
<thead>
<tr>
<th>Quotation from Interview transcript</th>
<th>Open code</th>
</tr>
</thead>
<tbody>
<tr>
<td>I act upon the company guidelines; whatever company guidelines are, we have to follow.</td>
<td>Policy obedience</td>
</tr>
<tr>
<td>If people will know that someone is being rewarded for taking care of those information, it would be a good motivation for them.</td>
<td>Rewards</td>
</tr>
<tr>
<td>Humans are not only individuals. They are living in a group. And if the majority of the group is doing certain things, then the others will follow.</td>
<td>Social conformity</td>
</tr>
<tr>
<td>We’re hard driven to update our files. Every week we are doing that. So I think it’s to protect them because sometimes the systems are not working here. And so the laptop will crash, the system. So at least we, still we could do something, not to lose those information.</td>
<td>IS security threats</td>
</tr>
</tbody>
</table>

Next, the phase of selective or focused coding means that categories identified in the open-coding phase are organized into a coherent framework, thus offering a more abstract and comprehensive conceptual framework of the data (Glaser 1978, Charmaz 2000, Charmaz & Mitchell 2001). This means that open codes become the properties of the low-level categories, and these categories become the properties of the higher-level, more abstract categories (Glaser 2002). In addition, in this study some of the open codes directly become low-level categories. Accordingly, fifty-nine open codes defined in the previous phase were further condensed into nineteen low-level categories, and seven higher-level categories (i.e., cultural dimensions, individual dimensions, organizational dimensions,
rational IS security dimensions, IS security-detached dimensions, unconscious IS security dimensions, and IS security procedures). These open codes and selective codes are presented in Table 12.
Table 12. Major higher level categories, and their associated lower-level categories.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a) Cultural mentality</td>
<td>a) Previous experiences</td>
<td>a) Communications</td>
<td>a) Balancing IS security threats and value of information</td>
<td>a) Policy obedience</td>
<td>a) Habitual enactment</td>
<td>a) General ISS procedures</td>
</tr>
<tr>
<td>Religion</td>
<td>Experienced</td>
<td>Quality of ISS procedures</td>
<td>IS security threats</td>
<td>IS as a part of habitual behavior</td>
<td>Automatic/ convenient security practices</td>
<td></td>
</tr>
<tr>
<td>Upbringing</td>
<td>IS security accidents</td>
<td>Oral communication</td>
<td>Value of information</td>
<td>Automatic/ convenient security practices</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Habits of the country</td>
<td>Activity on IS security issues</td>
<td>Role model Involvement</td>
<td>Biased thrusting of technical security</td>
<td>Automatic/ convenient security practices</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Language</td>
<td>Work experience</td>
<td></td>
<td>Rapid change of the work environment</td>
<td>Automatic/ convenient security practices</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>False thrust for IS security procedures</td>
<td>Automatic/ convenient security practices</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Hurry / workload / stress</td>
<td>Automatic/ convenient security practices</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Attending to interruption</td>
<td>Automatic/ convenient security practices</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Trust in other people</td>
<td>Automatic/ convenient security practices</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Trust in work environment</td>
<td>Automatic/ convenient security practices</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------</td>
<td>-----------------------------</td>
<td>---------------------------</td>
<td>---------------------------</td>
<td>-------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>b) Company's culture</td>
<td>b) Personality qualities</td>
<td>b) Extrinsic control</td>
<td>b) Inconvenience</td>
<td>b) Authority</td>
<td>b) Mistakes</td>
<td>b) Violation types</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Monitoring/control</td>
<td></td>
<td></td>
<td></td>
<td>Internet and e-mail</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Coercion</td>
<td></td>
<td></td>
<td></td>
<td>Password selection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Punishments</td>
<td></td>
<td></td>
<td></td>
<td>Writing down passwords</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rewards</td>
<td></td>
<td></td>
<td></td>
<td>Logging out of workstation</td>
</tr>
<tr>
<td></td>
<td>Carefulness</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Laziness</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Curiosity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Self-discipline</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c) Work ethics</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Trustworthiness</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>honesty</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>loyalty</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>sincerity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Intentional abuse</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>personal benefit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Motives to harm</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>the company</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------</td>
<td>-----------------------------</td>
<td>--------------------------</td>
<td>---------------------------</td>
<td>-----------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>d) A lack of trust for IS security procedures</td>
<td>d) Pressure</td>
<td>Inability to say no</td>
<td>Experiencing fear</td>
<td>Avoiding embarrassment</td>
<td>Maintaining good relationships</td>
<td>Willingness to help</td>
</tr>
<tr>
<td>e) Professionalism</td>
<td>IS as a part of profession</td>
<td>Sense of duty/responsibility</td>
<td>Common sense</td>
<td>Responsibility denial</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Theoretical coding involves the process of examining the relationships between the categories that had been created in the previous phases (Glaser 1978). In practice, relationships between the 19 low-level codes were identified through identifying how interviewees see them to be connected. This identification was executed through the drawing of diagrams representing connections with each category with other categories, which helps in the consideration of relationships between categories in a systematic manner (Strauss 1987, Urquhart 2007). In this thesis, these connections mean that certain categories act as conditions that give rise to some categories, or as consequences for other categories (Charmaz 2000). This means that antecedent and corollary relationships between categories were identified. This procedure is illustrated in Figure 3.

![Diagram](image)

**Fig. 3. An example of a procedure of identifying relationships between categories.**

In Figure 3, there is an “antecedent relationship” between communications and the awareness of IS security threats and a “corollary relationship” between the awareness of an IS security threat and habitual enactment. Thus, communications explain the nature of employees’ awareness of IS security threats, and further, the awareness of the IS security threat—category influences on the formation of habitual enactment. All the relevant categories and relationships between them that are supported by interviews are elaborated on in the next section.

### 3.3 Main Categories as the Result of Data Analysis

This section describes the seven main categories: IS security procedures, cultural dimensions, individual dimensions, organizational dimensions, rational IS security dimensions, IS security detached dimensions, and unconscious IS security dimensions, respectively, and their relationships are found in section 3.2 (see Table 12). Based on these main categories and their relationships, a
framework is formulated in the next section, 3.4. For increasing the credibility and transparency of an analysis process, all categories and their relationships are illustrated with authentic quotations from the interviews. In the quotations, text in not italized represents the questions asked by the interviewer, and the code at the end of the each quotation indicates the country and the number of each individual. In addition, a work position of each quoted interviewee is added at the end of the code: manager, officer, or engineer. In order to protect interviewees’ identity, only these broad work positions are mentioned instead of titles. To provide more details, interviewees’ titles under these three broad categories are listed in Table 13.

Table 13. A list of interviewees’ titles.

<table>
<thead>
<tr>
<th>Officers</th>
<th>Managers</th>
<th>Engineers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Marketing coordinator (1)</td>
<td>Engineering manager (1)</td>
<td>R&amp;D/Engine performance (1)</td>
</tr>
<tr>
<td>HR officer/assistant (8)</td>
<td>IM manager (4)</td>
<td>Sales support engineer (3)</td>
</tr>
<tr>
<td>Business controller (2)</td>
<td>Reconditioning manager (1)</td>
<td>Design engineer (1)</td>
</tr>
<tr>
<td>Spare parts coordinator (1)</td>
<td>Environment, health, safety and security</td>
<td>Project engineer (1)</td>
</tr>
<tr>
<td>Sales coordinator/Service sales (5)</td>
<td>Sales account manager (2)</td>
<td>R&amp;D/Automation &amp; Control (2)</td>
</tr>
<tr>
<td>SP merchant (3)</td>
<td>Facility manager (1)</td>
<td>R&amp;D/ Fuel injection (2)</td>
</tr>
<tr>
<td>Order processor (4)</td>
<td>Contract manager (1)</td>
<td></td>
</tr>
<tr>
<td>Accountant (1)</td>
<td>Quality Control/Assurance manager (2)</td>
<td></td>
</tr>
<tr>
<td>Purchase officer / Material specialist (3)</td>
<td>Account manager (2)</td>
<td></td>
</tr>
<tr>
<td>Credit controller (1)</td>
<td>HR manager (1)</td>
<td></td>
</tr>
<tr>
<td>Service coordinator (2)</td>
<td>Regional support manager (1)</td>
<td></td>
</tr>
<tr>
<td>Cost analyst (1)</td>
<td>Business development manager (2)</td>
<td></td>
</tr>
<tr>
<td>Assistant (5)</td>
<td>Sales support manager (1)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Manager (1)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Service sales manager (1)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Design &amp; development manager (1)</td>
<td></td>
</tr>
</tbody>
</table>

3.3.1 IS security procedures

First, one category of IS security procedures consists of employees’ conceptions regarding general requirements for the company’s IS security procedures related with their work. Particularly, employees need to be aware of an organization’s IS security practices (guidelines for prevention, guidelines for recovery, IS security procedures, rules, and instructions), which is illustrated below:
What kind of training would you like to receive? How to really enhance information security and of course, inform me, whatever I do will be some leak or what can we do or how to prevent that. (...) what are the details, how can we be able to take care of it, how can we be able to really practice it (...) So there should be some policies how to handle it, how to really... what is that... like to... how to see that. Take care. (UAE2, officer)

Second, IS security procedures are also referred to as different violation types, which mean compliance with certain IS security procedures: secure use of the Internet, writing passwords down, password selection, and locking the workstation. “Secure use of the Internet” refers to Internet browsing habits, the sending of confidential e-mail, the use of e-mail encryption, installing software from the Internet, and avoiding malware. “Writing passwords down” refers to an activity in which people write passwords down on a piece of paper. “Password selection” refers to the ways in which employees select their passwords; that is, is the password easy to guess. “Locking the workstation” refers to the practice of employees turning their workstation off when leaving their computers unattended (as a result, the computer is protected by a password).

The following sections present categories that explain compliance with IS security procedures: cultural dimensions, individual dimensions, organizational dimensions, rational IS security dimensions, IS security-detached dimensions, and unconscious IS security dimensions, as well as connections between these categories. In addition, while the three former categories were not found to be connected with different violation types, the possible connections to different violation types and the latter three categories (i.e., rational IS security dimensions, IS security-detached dimensions, and unconscious IS security dimensions) are presented. These violation types are secure use of the Internet, writing down passwords, password selection, and locking one’s computer.

3.3.2 Cultural dimensions

Cultural dimensions include the impact of cultural mentality and the company’s culture on employees’ thinking towards IS security in their work. These dimensions explain both employees’ compliance and non-compliance with IS security procedures (+/-) through certain other categories. Cultural dimensions were not related with certain violation types.
Cultural mentality

First, interviewees see that cultural mentality has an influence on employees’ IS security behavior, for example through the different religions, upbringing, and habits of a country. This cultural mentality is realized through the IS security-detached dimensions described in section 3.3.6 (authority, pressure), and the rational IS security dimensions described in section 3.3.5 (balancing threats and the value of information, professionalism, work ethics), which were viewed as culturally related explanations for IS security behavior. In addition, cultural mentality influences the nature of a company’s culture (see section 3.3.2), and also explains the success of applying organizational dimensions in terms of extrinsic control (see section 3.3.4).

As an example, the following quotations illustrate the connection between cultural mentality and balancing the threats and the value of information, which is considered to be low in Chinese culture:

You said that almost nobody does that (lock their computers)? I think it's just the perception. People don't realize the potential harm. And I think here, locally, and again in Chinese culture, I don't see any sense of risk. People don't perceive risk. Even if you, well, look in the traffic. People don't see risk. So I think the whole concept is also lost in the sense of the information protection. (...) What I see here is that due to the cultural differences between Europe and Asia, let's say, the perception of sensitivity and intellectual property is simply different. For example, it is very normal here to copy products. There's absolutely no respect for intellectual property in that respect. (...) as long as we have this cultural aspect, then there will be differences in way of working due to that. Just interpretation of information and its classification. (ChinaC7, manager)

Also another rational IS security dimension, professionalism in the form of responsibility denial, was considered to be a (Chinese) culture-related explanation for employees’ IS security behavior, as illustrated below:

Do you think that people consider that it is their responsibility to protect information? Hmm, for some countries I have to say no, for example in China. Also people think it is IM’s responsibility, not theirs. For example, last time I met a case, the person, they tried to have more powerful rights on their computer, for them (now) they can install software by themselves. But it's not allowed by the IM policy. There was a, “okay, why you don’t give me these
rights”; I say “Okay, if we give the rights maybe you abuse,” but you don’t
know, sometimes you abuse but you don’t know, so virus will attack to your
computer. But he says, “It’s okay, if virus attacks my computer it’s your
business, your responsibility to remove those viruses, not me.” (...) I believe
most of the people know the policy, know the guideline. Yes, but the problem
is they don’t think it’s their responsibility, that’s a major problem. (ChinaC5,
manager)

The following quotation illustrates that it is also considered to be a part of
(Chinese) cultural mentality that the organizational dimensions in terms of
extrinsic control in the form of punishments and rewards improve employees’
motivation to change their IS security behavior:

When you manage people in China, you must set out a test. And the test, the
result is related to his salary or bonus or some [laughs] gifts. Then we can
make the information exactly in his mind, otherwise he’s only “oh, listen,”
then out of the class, nothing new was in his mind. (...) we must have the
award and penalty. (ChinaA14, manager)

Also, the IS security-detached dimensions in the form of pressure is seen as a
(Chinese) cultural mentality-related issue, which has an influence on IS security
behavior. This means that it is a culturally related issue to violate IS security
procedures in terms of revealing confidential information under pressure, as
shown in the following example:

How to answer, how to say no. How to answer if other people challenge you:
you should tell me or I want to know more information. I don't know how to
say, I don't know. So do you think it is a cultural thing? In your culture that
you should tell everything and... In China culture? If you do not tell, it means
you don't like this person. It's very bad culture. (ChinaC3, officer)

The following quotation illustrates the connection between the IS security-
detached dimensions of authority and (Chinese) cultural mentality, which is
relevant for explaining employees’ IS security behavior. This means that in
Chinese culture, authority may be required to make people comply with IS
security procedures:

In China, you have also to learn: it is only working from up to down. Not like
in Europe where you have a real breadth, long site where many people are on
the same level. They can communicate with each other and they can also
make decisions. They only inform to upstairs and he is happy, he had nothing, so much to do with these cases. Here in China it's different. Nobody's doing anything if the advice is coming from upstairs. And you have to argue first, (us) the experienced expert from Europe. And if the Lau Ban accept, he can advise. This is the way. And you lose a lot of time. Maybe also a lot of sensitive informations. (ChinaA16, manager)

Finally, cultural mentality has an influence on the characteristics of the company's culture with respect of information security, which is illustrated below:

Like an American company or state (China) own the company, maybe they have different, the culture about information security in (think leak can). Usually to discuss the different departments’ internal information, and even there are the person out from the company, so I think the degree then it’s the different culture, including company culture and native culture. (ChinaC4, officer)

**Company’s culture**

The influence of a second cultural dimension, the company’s culture, on the employees’ IS security behavior is realized through organizational dimensions in the sense of communications (see section 3.3.4), rational IS security dimensions in the sense of balancing threats and the value of information (see section 3.3.5), and IS security-detached dimensions in the sense of authority and social conformity (see section 3.3.6). In addition, a company’s culture is formed by the country’s cultural mentality (see section 3.3.2).

As an example, a company’s culture has an influence on IS security behavior in the form of the organizational dimensions of communications, and also in the IS security-detached dimension of social conformity. This means that if a company does not have proper communication channels for discussing IS security issues, people will behave according to informal knowledge or common laws of the work community, as illustrated below:

And this company's culture. I think this company is not very confidential (open). A little (open). Why, what do you think is the reason? I think the communication is not very good. The communication. Because your line manager will not talk to you about the company's (-- [18:03], so people were on the lunch, were talk (many). And our, what we get information is from the
chatting, from the talking. While this talking will be coming to truth. So next time we will believe on the chatting. Why do you think people talk? What is the reason? Because they haven't the good channel to get the correct information. If they couldn't get, they will find other channel. (ChinaC3, officer)

With respect to IS security behavior, a relevant connection is also seen between a company’s culture and the IS security-detached dimension of authority, which means that in different organizational settings, different authority structures may be required to ensure the compliance with IS security procedures, as illustrated below:

What kind of support do you think you would use in order to improve information security, if you…? We need a manager to do the job. A manager to tell the subordinates specifically. A manager, first a manager, and standard rule. A manager follows the rule, a manager asks that people follow the rules. (…) I think there's a gap. So what do you think would be the best way to improve that? I do not know, you know, different companies have different culture. Some company manager is taking care of everything, but maybe some company they choose to ask specific people, maybe for me, I'm the safety person, I should manage all the safety-related issues. Do you think that it's because they don't understand their responsibilities over, or…? I do not know, is, I think maybe it's a company tradition. (ChinaC11, manager)

The following quotation illustrates the connection between the company’s culture and the rational IS security dimension of balancing threats and the value of information, which means that a lack of threat awareness as a characteristic of the company’s culture explains non-compliance with IS security procedures:

What do you think, why are you not destroying them [confidential work documents] properly? Yeah, because it's not, there are not any rules I think, it's not a practice in our company. I think nobody's doing it, so... Just kind of based on trust in everyone who's here. (SwitzerlandC3, engineer)

3.3.3 Individual dimensions

Individual dimensions include personality qualities (carefulness/carelessness, laziness, curiosity, self-discipline) and employees’ previous experiences (experienced IS security accidents, work experience, and activity on IS security
issues), and explain both compliant and non-compliant IS security behavior (+/-) through a certain number of other categories. Individual dimensions were not related with certain violation types.

**Personality qualities**

As an example, the following quotation illustrates the impact of personality qualities in terms of carelessness on non-compliance with IS security procedures:

> Those people who don’t follow this good USB practice, why you think, what is the reason why they don’t follow? Simply, you can say that they are careless. That's it. After sending one e-mail you are facing some problem in your laptop and you are not bothered, again I'm sending e-mail and again you are not bothered, it means that you are careless. (UAE1, manager)

Even if personality qualities were often viewed as an explanation for employees’ IS security behavior, no connections were found with it between other categories.

**Previous experiences**

Employees’ previous experiences have an impact on their thinking towards compliance with IS security procedures. These include experienced IS security accidents, work experience, and individual activity on IS security issues. Next, these dimensions are elaborated on through introducing the meaning of these categories and illustrating connections between categories.

First, IS security accidents that employees have experienced in their former or present work environment influence the rational IS security dimension of balancing the threats and the value of information (see section 3.3.5). Besides IS security awareness and knowledge, these kinds of experiences increase the relevance of the IS security procedures to them personally. The influence of experienced IS security accidents to employees’ threat awareness is illustrated below:

> So I think it's to protect them because sometimes the systems are not working here. And so the laptop will crash, the system. So at least we, still we could do something, not to lose those information. So every week, we are updating our files with laptops. (UAEC11, officer)
Second, activity on IS security issues explains an employee’s attitudes towards IS security, as the following quotation illustrates:

How have you acquired your knowledge about information security? (…) I keep myself updated by things. I read a lot. (…) on the Internet. And basically I get more information about information systems from my brother-in-law. He is an IT guy. ... most of the time I keep on discussing these things, like... he keeps on, informing me new technologies and new things and new techniques and things. (…) You really need to have ... willingness to learn about it or know about it. Or else nobody cares about it. (UAE5, officer)

Even if activity on IS security issues was often viewed as an explanation for employees’ IS security behavior, no connections were found with it between other categories.

Finally, employees’ work experience, or lack of it, explains the rational IS security dimension of professionalism (see section 3.3.5) and the unconscious IS security dimension of habitual enactment (see section 3.3.7) in the field of IS security, as the following quotation illustrates:

I worked in an American law firm before and here. So I think I know in a certain extent what is the professional way to handle information confidentially. This is really during the work experience and different working positions. And what kind of training or experience you have received. That you will implement that kind of habit in your daily working. (ChinaC6, officer)

3.3.4 Organizational dimensions

The organizational dimensions include two types of interviewees’ expressions that have an influence on employees regarding compliance with IS security procedures: (a) communications and (b) extrinsic control. Communications and extrinsic control have an influence on employees leading to both compliance with IS security procedures and also to non-compliance (+/-). Common to these organizational dimensions is that they are ways to maintain IS security issues visible in the organization, and usually their execution is experienced as part of management’s role: how management is concerned with IS security issues and how they support employees in establishing and maintaining their understanding and role within the organization. This means that information security procedures
do not belong to the daily work automatically. However, this doesn’t necessitate a passive role for the employees in IS security. Instead, they expect to be supported through these organizational dimensions ordered by the management of the organization. Next, both of these dimensions are elaborated on through introducing the meaning of these categories and their sub-categories and illustrating connections between other categories.

Communications

*Communications* are considered to be a necessary organizational dimension to create and maintain employees’ thinking towards IS security. Communications consist of the quality of IS security procedures, oral communications, training, reminders, management’s role model, and involvement.

First, the quality of IS security procedures means that these procedures in any form (e-mails, intranet, paper documents) need to be sufficient, clear, and customized for the particular demands of the organization, the business unit, and work tasks of the employees, as the following quotation illustrates:

> Frankly speaking, that depends on if you really think that policy is right and reasonable. (…) So the policy has to be reasonable and easy to follow and understandable. What do you think is the reason, why the policies are too… Different? Of course there are the cultural differences. And “the company” is dealing with a different business. That every office is different. And your position, your working characters are different. And of course superior bosses are different. (ChinaC6, officer)

Second, oral communications refers to the visibility of IS issues in the daily practices of the organization in the form of personal coaching, management’s requests and explanations, formal discussions with management, and informal discussions with co-workers. An example of this is presented below:

> I think so in our department, people will have knowledge. So, how do they have knowledge, are they well-educated or how have they acquired this? It's mainly basically because of our interaction and mutual sharing of experiences. (UAEA1a, manager)

Third, also training is considered to have a direct influence on improving IS security awareness and knowledge, as is illustrated in the following quotation:
What do you think, what is the reason for more awareness? Why do people have it now more than before? Yeah, because it came from top management, because we have had bribery cases, in Scandinavia, so the company decided to counteract and avoid this in future. So it has been communicated, or…? Yes, it was, yes, and there was training as well, at least for the sales people who are directly in that front position. (SwitzerlandD1, manager)

Fourth, changing employees’ thinking towards IS security is considered to require regular reminding through different means, as the following quotation illustrates:

You do a things quite a long time, it will become this, the common sense for you to, for the security. But before that, you have got to be reminded occasionally, so for a long time if you work to get this (feeling). So I think this is what the IT, quality, and maybe other department should ... Remind people about security? Yeah, in a different way. Yeah. They finally become this, feeling. (ChinaC4, officer)

Fifth, management acting as a role model has an effect on interviewees’ thinking towards IS security. Then, experiencing an influence on a role model on employees’ thinking towards IS security is connected to the IS security-detached dimension of authority, as the following quotation illustrates:

because obviously when your manager is not complying to things, then people, the subordinates below you, would, take it, so likely that okay, he is not too keen about that, why should we. Kind of attitude can come in. (UAE5, officer)

Finally, a possibility for employees to participate in information security is likely to have a positive effect on their thinking. Such involvement is seen to create more diverse ideas for IS security management from the users’ point of view, and thus, making them learn and commit themselves to the IS security more effectively. In addition, involvement was also considered to be related to the company’s culture (see section 3.3.2). An example of an effect of involvement, and its connection with the company’s culture, is illustrated below:

Do you see any other sources that might have an influence on one's protection of his confidential or sensitive information? Yeah, there's a, already we discussed that we need to build one environment like this. And for the environment, we need to work all together with each of the co-workers, manager, management, everybody's involved there. So we can build an
environment. When anybody enters in this environment, he feels like, and he tries to improve his self also. And when I enter here in “the company,” also I feel little improving environment here. So also I try to make myself more improved. So these are things. This is also influence. (UAEA3b, engineer)

Interestingly, while most of the interviewees considered communications to be an effective means for developing IS security awareness, and were aware of the existence of IS security-related information in the company’s intranet, at the same time, they were rarely aware of the content of these documents (e.g., IS security procedures and instructions). Typically, employees hope to receive more communications, and also suggested several characteristics for effective IS security-related communications. Improving communications in the organization is especially important, because the interviewees consider it to have an influence on the most rational IS security dimensions (balancing the threats and the value of information, inconvenience, and professionalism, as described in section 3.3.5), IS security-detached dimensions of policy obedience (see section 3.3.6), and unconscious IS security dimension of habitual enactment (see section 3.3.7), which explain employees’ IS security behavior.

The following quotations illustrate the influence of effective communications on three rational IS security dimensions: balancing the threats and the value of information, inconvenience, and professionalism. First, communication potentially makes employees aware of IS security threats and the value of information, as illustrated in the following two quotations, respectively:

Sometimes it's also just the understanding, that we don't understand why we shall do certain things. Perhaps it makes no sense for us, but if the IT department or management explains what the risks are. If we are not doing it, then we understand better. And then it's why we can follow it easier. (SwitzerlandD4, officer)

I don't know if everybody knows that information is really important (...) But I'm not so sure if everybody's aware, not to leak all those information. We should have trainings or we should have information that we need to, to inform everybody, that this is really important that they should be aware of all these things. (UAEA1b, officer)

Second, according to the following example, communication can also decrease the inconvenience experienced with IS security procedures:
Could be, the people are not aware, and it's quite sometimes easily, to make it easily but attaching the file, and not to create a link, maybe this could be helpful when it's quite easy to create the link or to inform the people how they can do that. So people are not doing it, it's because they are not aware? Do they know how to do that… They are not really aware is one point, on the other side there are not really information how to do that in an efficient way. They are not trained to act as such. (SwitzerlandA1b, manager)

Third, communication also has a role of making employees more professional in terms of becoming aware of their responsibilities regarding IS security, as illustrated below:

So do you think that people are aware of the responsibility? No, they are definitely not aware. What could be done? What is your…? To train them, and give them a short checklist how to work with that, for the daily business. (SwitzerlandA1b, manager)

The following quotations illustrate the influence of effective communications on the unconscious IS security dimension of habitual enactment:

What kind of training should there be? You said that there could be more training here in “the company.”. …They have already set up a... information security instructions they maybe can share in the... because we have... our traditional training for new employees. They can share this kind of instructions to new employees. For all the employees maybe they can organize some training day and share this kind of information. Also in public under we have internal magazine (...). So they also can put this kind of information into magazine. You can always expect that employees have this kind of sense immediately today but I think right away they will have... this kind of sense has a good habit. (ChinaA10, officer)

The following quotation illustrates that communication can also have an impact on the IS security-detached dimension of policy obedience:

Like if IT needs to take suggestions and what is your main role or main responsibility? That I follow those rules and I follow those suggestions. And perhaps then it should not be a suggestion, but it should be a clear rule, that you have to do it. That everybody has to do it. And that you have to follow those rules. (...) But of course you have to have clear rules. And they have to be understood from everybody. But I think the main thing is really that they
must be important, or that they must be clear and followed. (...) But of course on the other hand clear rules and clear communication to make it understandable for everybody. (SwitzerlandD4, officer)

Extrinsic control

As a second organizational dimension, some interviewees think that extrinsic control has an effect on employees’ thinking, which leads to compliance with IS security procedures. This category includes the four following sub-categories as related to controlling employees’ work in relation to compliance with IS security procedures: monitoring, rewards, punishments, and coercion. While the first three subcategories explain employees’ thinking leading to compliance with IS security procedures (+), coercion also can lead to non-compliance (+/-). Next, each of these dimensions is elaborated on through introducing the meaning of these categories and illustrating connections between other categories.

First, monitoring means electronic monitoring (e.g., monitoring employees’ Internet usage) and managerial monitoring (i.e., manager’s observation of subordinates’ working habits and personal feedback). Monitoring employees’ IS security behavior was considered to have an influence on employees’ IS security-detached dimension of pressure in terms of fear of getting caught not complying with rules (see section 3.3.6). Correspondingly, a lack of monitoring and management’s feedback was seen as one of the reasons for neglecting safe IS security tasks. The following quotation illustrates the impact of managerial monitoring:

There are two groups. One is that kind of group where everybody locks their PCs, always…. And the other group, no one is doing that. What do you think could be the explanations, why are these groups so different? Perhaps [it] might be that the superior is checking it ...The rule came out and then everybody had to follow...So it's on the one hand a control thing (...) That perhaps it's not checked and nobody cares. And that's why they should do. (SwitzerlandD4, officer)

In addition, the following quotation illustrates that an effect of monitoring on employees’ IS security behavior can be explained through pressure in terms of avoiding negative feelings (see section 3.3.6):
Two months ago, our system is very low so that we cannot receive e-mails, we cannot send e-mails on our outbox, so find. Then they’ve, the headquarters; they send an e-mail to HR or one of our managers that this person, they’re sending e-mails with the big files may be, 5MB, 10 MB, so now, nobody is doing that anymore. They’re afraid that headquarters so. And even it can also check, who is sending files and who is using Internet with this site. (UAEC11, officer)

Second, some of the employees mention rewarding as an effective motivation for a good performance in the IS security tasks in terms of both material (money, gifts) and symbolic rewards (public praise). This means that extrinsic pressure motivates employees’ IS security behavior (see section 3.3.6). In addition, such rewards were seen as useful for increasing the rational IS security dimension of professionalism in terms of feelings of responsibility (see section 3.3.5), as illustrated below:

Because if the people doing good job, everything. We need to give rewards, some rewards also. Have the regular intervals, people will be happy and work happily. And they will be more responsible for their jobs also. But for a good practice, people will get reward. When management for example gives me something, they have in general my view. How I am. So as for me, they give me some reward. (UAEA3b, engineer)

Such rewards were also seen as useful for directing the influence of the IS security-detached dimension of social conformity (see section 3.3.6) towards compliant IS security behavior. This means that while employees tend to behave according to common laws of the work community (i.e., social conformity), rewards may be useful in showing the desired IS security behaviors congruent with the company’s IS security procedures. This connection between extrinsic control and social conformity is illustrated in the following quotation:

If there are some policies, some measurable system for this much information secure, and that person is this much only, then of course, there should be some rewards for that. There should be, he is complying with the company policy, he is very well, he is very loyal to the company, and he is working for the company. Then he should be rewarded. Then that will motivate others also. (UAE4, manager)
Third, some interviewees consider punishments to be useful for directing employees’ IS security behavior through creating pressure in terms of fear of punishments (see 3.3.6.4). Also, in the disciplinary sense (e.g., termination, monetary sanctions, warnings), the following quotation illustrates that some interviewees consider punishments to be useful ways for creating a balance between threats and the value of information in a sense of personal accountability for IS security action:

This means that you receive some kind of sanction. Do you think that it would be a good thing or not? Yeah, I think that that can be useful thing. If IM controls what you do in the Internet, and they can come to you and say, you don't have to do this... And it would have an effect on people's behavior, do you think? Yeah, I think so. Because if nothing can happen to me, then I listen what you tell to me, but goes in and out. Not by everyone, but somebody. (SwitzerlandC2a, manager)

Fourth, some interviewees think that coercion with respect to the installation of software, password changing, Internet browsing, and e-mail encryption work as a good reminder for such an activity, as illustrated below in the case of changing passwords:

if there is not such a remind system would you still change your password, what do you think? Say we are supposed to change once in a month, we are told to do that to keep the things on a safer side but I guess it's the prompt switchers, which are waking us to do it often. (UAEC14, officer)

In addition, coercion was considered necessary for changing employees’ IS security behavior, as the following quotation illustrates:

Do you think that also attitudes towards those kinds of devices, how would people usually accept them here? So difficult question to answer. I think, I assume that in the beginning the people will refuse to use them. So this can't be put into force on to whoever wants to use it is allowed or has the possibility to use. This only can be set into force by making it mandatory and obligatory to everyone. So you have disk encryption, you have e-mail encryption and you can't switch this off. So did you say that it needs to be forced or did you think that it is not a good thing to force people to do that? I think it's a good thing. To force them? To force people, because I also think
that if you don't do this, the people won't use it probably. (SwitzerlandC5, manager)

In addition, coercion was also considered to cause inconvenience while creating a hindrance for efficient working practices (see section 3.3.5), and thus, sets the scene for non-compliant IS security behavior. For example, the following quotation illustrates that system-generated requests to change passwords frequently was experienced as an cause for a need to write passwords down, or use very simple passwords:

I know that it should be combined with numbers and letters, but, 'cause, we have to change it very frequently, so I don't use very complicated password now. First, when I just come into this company I used complicated password. But if I use the one that I can't remember, then I can't log in. (...) Otherwise, I have to record this password on my notebook or some place I can see, then it also cannot protect my information. (ChinaA13, officer)

However, the research results of this thesis show that the role of extrinsic control is highly controversial, while the interviewees’ opinions of its influence vary significantly. First, it was found that cultural mentality explains the success of applying punishments and rewards in the organization (see section 3.3.2). Second, some people see that they do not have an influence on employees' IS security behavior, as illustrated below:

Do you think that if there are not any punishments or rewards, do you think your behavior will be different? No. My confidentiality, and it will not be changed, even if when there is no punishment there, but still I have my role as, my role is mostly confidential, so it will not change. (UAEC10, officer)

Third, the following quotation shows that punishments and rewards were considered as inappropriate means for creating professional behavior:

What do you think about rewarding people? Does it motivate for good information security behavior? I think that's a motivation, but I'm not sure if it's a motivation in this particular area. Because this security, this should be there somehow automatically, that you have some rules which you have to keep, and this is something, not you might do if you want and then you get some reward for this, this should be something, (really which has) to the policy of the company. So I think either punishment or reward is not a good way in this case. (SwitzerlandC3, engineer)
Fourth, monitoring and punishments were even seen to have a negative influence on the company’s business and employees’ work motivation, as is illustrated below, respectively:

I don’t like monitoring, it’s too much workload [laughs], and maybe people will feel unhappy, but in the current state, for example in China, we are still doing this because even we have reminded people many times about this policy, still we find a lot of cases about abuse of Internet. So, I don’t know, maybe it’s the culture of China, we have to monitor and catch out something, abuse, some bad guys and punish, maybe people will say “okay, it’s very serious, then we will follow up.” But I don’t think it’s a good way for “the company X” business. (ChinaC5, manager)

In China, there the people are often watched, I think. It’s a controlled regime, or like earlier in Czech Republic with the Russian communism. I don’t like this kind of policy. What do you think are the consequences there, for example in China if people are monitored? They are working with fear. Maybe they work a little bit faster, but maybe they also get sick and tired. (SwitzerlandA4, officer)

Fifth, the following quotation illustrates the rationale behind extrinsic control in terms of when monitoring was not always attached to information security, people didn’t understand the real reasons behind such activity:

I think most of people may only be aware that the company’s controlling that you are visiting a Internet website. They are not linking that to information security. They are only linking that to that the company is monitoring: have you done your job. Or have you visited unnecessary websites (...) Because currently there’s no communication saying that the company monitoring of Internet visiting is because of information security. (ChinaC6, officer)

In addition, control dimensions were associated with the intentional abuse situations, and thus, these were considered to be contradictory procedures for organizations, which are based on mutual trust and on employees having good intentions in their work. Finally, even if some interviewees consider rewards to be good for increasing such motivation for proper IS security behavior, some feel it is too complicated to define criteria for such an activity.
3.3.5 Rational IS security dimensions

Rational IS security dimensions include five types of reasons that involve deliberate consideration of advantages and disadvantages before engaging in a particular behavior with respect to IS security: balancing threats and the value of information, inconvenience, lack of trust in the IS security procedures, professionalism, and work ethics. While inconvenience and lack of trust in the IS security procedures explains only employees’ non-compliance with IS security procedures (-), balancing threats and the value of information, professionalism, and work ethics can lead to both compliance and non-compliance (+/-).

Balancing IS security threats and the value of information

First, balancing threats and the value of information awareness is one of the key dimension through which employees comply (or don’t comply) with IS security procedures. Interviewees explained that they comply with the IS security procedures in their work in order to protect valuable company property, personal work, personal data, confidential data, or maintain the position of their organization or department to the competition. Accordingly, the results herein suggest that IS security guidelines are not adhered to if employees do not see any value in the extra effort necessary for compliance. Especially, protecting information of a confidential nature (e.g., personnel and salary information) is strongly connected to ones’ professional competence, as illustrated below:

How does this awareness of these threats affect your actions here in your departmental daily job? It’s always there. It’s always there with us that we work in HR and information picture is highly confidential. It’s not a threat like but it’s always. When you work for the HR department, you are aware you are dealing with humans and human behavior and contracts, all these are very sensitive matters and have to be very careful with this. It’s not a threat but we have to be highly aware that we shouldn’t talk about this loosely with anybody or mention it even within our families. (UAEC9, officer)

In addition, protecting information of a confidential nature (e.g., personnel and salary information) is also strongly attached to IS security-detached dimensions of pressure (see section 3.3.6), when the leaking of such information is believed to cause feelings of inequality amongst the work community, as the following quotation illustrates:
So why do you think it’s important to protect information? So why is it important? *It’s like if someone is getting increment or something, and maybe if someone knows, then he’ll demand or he will leave the job or whatever. It leads to so many problems (…) If the information is not protected, OK, if somebody is getting increment or somebody is getting promotion, OK, so if other persons come, so OK, maybe he will fight the manager and he gets the increment and I didn’t get it and I am going to leave the company. (UAEC10, officer)*

Besides being aware of the value of information, the IS security behavior of the employees is strongly attached to their conceptions of IS security threats in their work environment. For example, when IS security procedures are followed when employees experience threats of an information leak, threats from the Internet, or technical and physical threats in their work. Consistently, employees’ deliberate choices to partake in risky IS security behavior are dependent on how likely they assume the potential threats are to occur. Under this category, a typical reason that contributes to non-compliance in many instances is when employees recognize the potential threats, but do not seem to realize their possibility because they have high trust towards technical security (secured servers, access rights, firewalls, virus protection), or other people and the working environment, as is illustrated below:

So do you think it is lack of awareness of the threats or what is the actual reason why they don’t (lock their PCs)? They trust the other people. (…) they don’t lock the PC, they lock the door so I think everything is safe. (…) And also they trust to others, they trust the system of the security…safety guard of company… (ChinaA10, officer)

Another typical example of employees’ lack of threat awareness is that they often believe easy passwords to be strong enough to protect their valuable information. This case is illustrated below:

*What kind of passwords do you select usually?… My name, company’s name, plus a few digital numbers. Do you think those passwords are safe? Yes. (ChinaA9, officer)*

Further, when employees had to attend to interruptions—breaking of their normal routines to attend to something immediate and out of the ordinary—they tend to consciously choose not to comply with IS security procedures. For example,
interviewees saw that interruptions caused them to non-comply with the IS security procedures in the case of locking the workstation when leaving it unattended. Finally, a rapid change of the work environment was considered to be a reason for not seeing threats relevant in the employees’ current work, as is illustrated below:

If you were going to processes in the past, if you look into one or two generations before us, the people had a position to grow with modern technology. So they took some manual, let’s say (...), then it becomes automatic and they have still in mind the process what she wants to have, right. Nowadays, youngsters, they are missing this part, what is actually the process. So a lot of people is not anymore thinking in process. So they know things are going, if you can follow. It means that they are not looking in what is coming from, as I mentioned. (...) And every process, every way of handling has a certain risk. And those risks must be talked about. (UAE3, manager)

An impact of balancing threats and the value of information on employees’ IS security behavior was also considered to be related to cultural dimensionss (see section 3.3.2). In addition, the organizational dimension of communications and extrinsic control (see section 3.3.4.1) and the individual dimension of previous experiences (see section 3.3.3) were thought to have an influence on it. Further, these dimensions were thought to have an effect on the unconscious IS security dimension of habitual enactment (see section 3.3.7). Finally, balancing threats and the value of information was associated with all four IS security procedures: the secure use of the Internet, writing passwords down on paper, selecting passwords, and locking the workstation when absent from the workstation.

Inconvenience

As a second rational IS security dimension, employees often deliberately consider the extent of inconvenience associated with all four security procedures, and this sometimes leads to non-compliance with IS security procedures. For example, interviewees stated that IS security procedures, with respect to the secure use of the Internet (e.g., e-mail encryption, remote connection, using PDF-formats, link creation) are too restrictive, inconvenient, or difficult, as illustrated below:
What do you think is the reason why they don’t encrypt? *It’s not easy, it’s not convenient. You need to take some steps before you send the e-mail out, so it’s not convenient to (…) They have enough technical, they have enough knowledge, but just lazy.* (SwitzerlandC5, manager)

In the case of locking the workstation, the inconvenience was visible in the sense that the activity of locking one’s computer was viewed as too time-consuming, as the following quotation illustrates:

*Maybe they think they will leave only a few seconds and will be back later and if they lock the PC they have to import a keyword again. It will take a little time for some.* (ChinaA11, engineer)

In addition, the selection of good, difficult-to-guess passwords was considered too hard to comply with in practice, because the respondents felt that good passwords are too difficult to remember. The next quotation on the selection of the passwords illustrates this:

*… for my case I would go for a date or abbreviation, if I am familiar with it, then I don’t get to forget it, like my favorite password, always, even in my other accounts, like [the] special birth date of my family members, I don’t miss it.* (UAEC15, officer)

Similarly to the selection of passwords, writing down the password was done in order to increase the convenience of handling the passwords, as the following quotation illustrates:

*I sometimes even write down the password, because you have got password even in our banking, if we have to do transfers, for that also there are passwords, so there are so many passwords nowadays with this modern age, that I need a diary to keep writing down all of my passwords. (…) we are three users in the payables departments, two passwords are already locked, so it’s just my password that is still valid. Maybe it’s because I’m writing it down in case I forget, so with God’s grace I’ve not forgotten, so that is the reason I, it’s just a backup for me, it is not that, this is my prime area of “how would you go about changing my behavior,” I need to write it somewhere, if I don’t I write it in the diary [laughing] and I need to write it on the PC, I need to write it somewhere.* (UAEA2b, officer)

Inconvenience was thought to be influenced by organizational dimensions of communications and extrinsic control (see section 3.3.4), and it was thought to
have an impact on the unconscious IS security dimension of habitual enactment (see section 3.3.7). Like balancing threats and the value of information, inconvenience was associated with all four IS security procedures.

A lack of employees’ trust in IS security procedures

As a third rational IS security dimension, another interesting pattern that emerged is that non-compliance emerges due to a lack of employees’ trust in IS security procedures (-). This means that when interviewees saw that there was no significant (positive) consequence of using (or not using) these IS security procedures, they tended not to comply, as the following quotation illustrates:

Do you think it is important to have a strong password that is difficult to break? If somebody wants to really get something from your computer and if he's competent, he always get it. It doesn't matter if you protect it with that long password or that long password. (UAEAS5b, manager)

Lack of trust for IS security procedures is connected to certain IS security procedures. Particularly, this relates to the secure use of the Internet and password selection.

Professionalism

Fourthly, under the rational IS security dimensions, employees’ compliance with the IS security procedures is explained through professionalism, which means that IS security is seen as an aspect of work responsibility, common sense, or work duty. Professionalism was seen as a property of an individual employee, working teams, or a whole department with strong connection to the nature of the information that people are handling in their work. Professionalism at the individual level is illustrated below:

Why do you lock it, either the door or the computer? It’s my duty to do that, for me. (…) Maybe somebody told me, but it’s also personally thinking. I’m responsible for these data. (SwitzerlandA4, officer)

On the other hand, considering information security activities to be common sense does not necessarily indicate that this IS security-related thinking is in accordance with the actual IS security demands of the work environment. Because most of the interviewees’ were unfamiliar with the organization’s written
communications (IS security procedures and instructions), it can be expected that an employee may overestimate his/her own IS security knowledge and abilities, or underestimate the significance of using information security procedures. Such a case is illustrated below:

Do you think that you comply with all the policies, which “the company X” has? I expect so. But what I mainly stick to is what I find acceptable for myself. And assuming that my own good practice falls within “the company X’s” policy, which I expect so, then I would comply, yes. (ChinaC7, manager)

Under the category of professionalism also belong expressions, which explain non-compliance with IS security procedures: responsibility denial. In this case, IS security procedures are not complied with, because employees believe that it is not their responsibility to comply with these IS security procedures. For example, regarding the secure use of the Internet, employees expect that information security and technical safeguards, such as secured servers, firewalls, and virus protection, are being taken care of by the IT department, and hence are not their responsibility. Usually in these cases, employees experience a conflict between efficient work practices and IS security procedures. The following quotation illustrates a case of responsibility denial:

Sometimes people in their workplace behave other like they would do in the personal environment. For example, using the Internet in the workplace. Some programs or some issues, which they perhaps don’t use in their private environment due to being afraid of getting a virus or something like this. (…) What I was saying is that the people might lose the awareness for these issues, when they are at work, in their working environment. And when they are sitting in front of the personal computer, which they are the only person who is responsible or who has to look after the security of this computer. And the company, there’s always the IT department, which is looking for these issues like virus scanning and firewall blocking and so on. So therefore people are perhaps not so aware of these issues. (SwitzerlandC5, manager)

An impact of professionalism on employees’ IS security behaviors was also considered to be related to cultural dimensions in the sense of cultural mentality (see section 3.3.2). In addition, professionalism was thought to be influenced by organizational dimensions of communications and extrinsic control (see section 3.3.4.1), individual dimensions of work experience (see section 3.3.3), which explain the formation of the unconscious IS security dimension of habitual
enactment (see section 3.3.7), as well as balancing threats and the value of information (see earlier in this section). Besides offering a general explanation for IS security behavior, professionalism was connected with secure use of the Internet and locking of computers.

**Work ethics**

Finally, individual’s work ethics were also found as an explanation for IS security behavior. This means that a person with a high sense of loyalty, honesty, and trustworthiness is more likely to comply with safe IS security practices. In contrast, intentional abuse in the sense of gaining personal benefit or causing harm to the company are motivations for non-compliance. Interestingly, some people connected non-compliant IS security behavior only to a person’s work ethics in the sense of intentional purpose to reveal sensitive information to unauthorized persons. This may indicate a lack of awareness and knowledge of the IS security-related requirements and threats in their work environment, if work ethics are the only possible reason why people choose to comply or violate IS security procedures. This case is illustrated below:

> What do you think are the reasons for not behaving safely? They generally do behave safely, but in certain cases wherein they would like to get some information about somebody else or something, then they may disclose some facts, means they might try to behave unsafely so that they can get some information by doing this, so by doing this, you give me this I give you this. Give as take policy like. Otherwise generally people do behave safely I suppose. (...) I think that I can imagine only this reason because I cannot imagine anything else. Because once we behave, then people don’t approach, they know that they won’t disclose anything. (UAEC9, officer)

Work ethics were considered to be relatively stable by nature, while they are influenced by a cultural mentality (see section 3.3.2), as is illustrated below:

> What do you think, let's presume that there are two persons, one is honest and one is not, what do you think, what makes someone sincere or honest? This depends on the people. We are here from the many countries and we have different environments also. All, if we have good education, everything, we have good environment in our country, our before, where we worked. So we develop our personality. (UAEA3b, engineer)
Thus, interviewees considered it to be difficult for work ethics to have an influence through any efforts aimed at improving IS security behavior, as the following quotation illustrates:

> What kind of changes or improvements would you like to make in your company’s information security practices? ...the most important is that, that people must have, must be chosen by HR on a certain attitude. (...) So if you bring the wrong people, it’s very hard to control that (...). That means that when the basis is wrong, it is a complete story to get that gone. So when you bring people in who are not trustful, it is almost impossible to make them trustful. So if you choose trustful people, if you can do that, if the attitude is right, then it is not so difficult. Right. So that is I think the biggest part. (UAE3, manager)

Work ethics were not associated with different IS security procedures.

3.3.6 IS security-detached dimensions

The IS security-detached dimensions mean reasons for employees’ IS security behavior, which are not based on security-conscious decisions: policy obedience, authority, social conformity, and pressure. These reasons explain both compliant and non-compliant IS security behavior (+/-).

**Policy obedience**

The first IS security-detached dimension is policy obedience for its own sake, which offers an explanation for employees’ IS security behavior. Also, people obey IS security procedures, rules or instructions or other agreements without necessarily understanding the rationale behind their behavior, as illustrated below:

> For example, if I [look] (around), I found that 90 percent of people did not lock the computer, then I sent an e-mail and I told them it's a company rule to lock your computer. All people said, oh, that's a company rule, I should do that. (ChinaC11, manager)

Policy obedience is considered to be influenced by organizational dimensions in terms of communications (see section 3.3.4), and explain the formation of the unconscious IS security dimension of habitual enactment (see section 3.3.7). Besides offering a general reason for employees’ IS security behavior, policy
obedience offers an explanation for the secure use of the Internet and for locking one’s computer, but not for writing down passwords, or password selection.

Authority

Second, people obey the IS security procedures if they are ordered to do so by a person with authority, which usually means the management of the organization. Interestingly, no was found evidence that authority explains the compliance with other IS security procedures expect for locking the computer. Also, authority does not necessitate that people need to understand why they are ordered to behave according to certain rules. The following quotation illustrates this case:

Because if the company, if your boss gives you the lock, I think his purpose is to ask you to lock your computer. I will lock it still. (ChinaC2, engineer)

An impact of authority on employees’ IS security behavior was also considered to be related to cultural dimensions (see section 3.3.2) and organizational dimensions of communications (see section 3.3.4). Besides offering a general reason for employees’ IS security behavior, authority was seen as a reason for locking the computer.

Social conformity

Third, the IS security-detached dimension means that people tend to behave according to how they think others will behave. Also, if employees perceive that their co-workers are using, or not using, particular IS security practices, they tend to copy that behavior. This pattern of social conformity means that people consciously or unconsciously behave according to the common laws of the work community. The influence of social conformity on employees’ IS security behavior is illustrated by the following quotation:

The people or the humans are not only individuals. They are living in a group. And if the majority of the group is doing certain things, then the others will follow. So I think if all of the majority is doing it, then the minority should follow. Of course there are always people who think: we don't want to do it. But I would say if mainly all the people are doing it, then it's a common thing and everybody will do it. (SwitzerlandD4, officer)
An impact of social conformity on employees’ IS security behavior was also considered to be related to a cultural dimension in terms of the company’s culture (see section 3.3.2). In addition, there was a connection between social conformity and extrinsic control in terms of rewards (see section 3.3.4). Social conformity is dependent on the IS security procedures to some extent while it has an effect on the interviewees’ computer locking practices, but not on the secure use of the Internet, writing down a password, and password selection.

**Pressure**

Under the IS security-detached dimensions also belong IS security behavior that is motivated through intrinsic pressure (e.g., avoiding negative feelings) or extrinsic pressure (e.g., experiencing fear). As an example of intrinsic pressure, employees do not ask to see employee badges, do not browse the Internet for personal reasons in their work laptop, or lock their computers because they feel embarrassed to act in an opposite way, as illustrated below:

> Do you lock your computer? Before is one hundred percent. Now it is 90 percent, because of the environment I think (...) it’s atmosphere. If every person was doing it, then nobody will disobey. If every person was not doing that, you will feel that, am I idiot to do that. (ChinaC11, manager)

In addition, they may reveal sensitive information because they want to help others, or maintain good relationships under pressure. This influence of intrinsic pressure on employees’ IS security behavior is illustrated below:

> As if my manager ask me everything, I will tell everything. Why? I think if I don’t, he will feel very strange: Why you not told me? I have this authority. This is my manager. The second is colleagues. Colleagues: Oh, we know you knew this information. Why didn’t you tell me? I shouldn’t have told but in order to the good relation, maybe in China the people’s relations is very important. (ChinaC3, officer)

As an example of the extrinsic pressure, employees may lock their computers or refrain from browsing unsafe Internet sites because they fear getting caught due to monitoring, or to be punished. Further, people may reveal sensitive information personally or through e-mail because they feel threatened, as illustrated below:
Yeah, could be different reasons why, or maybe if someone puts enough pressure on it and says you really need now urgently that they give the access because they feel pressured, that they may be a bit scared and then they give the access although they should not, that's also possible, of course. (SwitzerlandC1, officer)

An impact of pressure on employees’ IS security behavior was considered to be related to cultural dimensions in the sense of cultural mentality (see section 3.3.2) and balancing threats and the value of information (see section 3.3.5). Pressure is dependent on the IS security procedures to some extent while it has an effect on the interviewees’ practices of locking the computer, and on the secure use of the Internet, but not on writing down a password and password selection.

### 3.3.7 Unconscious IS security dimensions

The unconscious IS security dimension means such reasons for employees’ IS security behavior, which are not based on conscious thinking: habitual enactment and mistakes. Habitual enactment explains both compliant and non-compliant IS security behavior (+/-), while mistakes account for only non-compliant behavior (-).

#### Habitual Enactment

The unconscious IS security dimension of habitual enactment means that the interviewees state IS security procedures are used if they are a part of the employees’ habitual behavior, where he/she does not consciously make a decision to comply or not comply. The following extract illustrates this:

> I don't know for the other people but I always lock my computer when I go. Why? I don't know. Has to be a reason. No, that's sometimes because it's a habit. Habit? Yeah, just, lock and go, that's all. (...) It just, also if I leave my computer open, in one minute it go by itself to lock down. I really don't know why I'm locking that. (UAEA5h, manager)

In turn, non-compliance with IS security procedures with respect to the secure use of the Internet was explained through “bad” working habits (-). The influence of bad habits on IS security behavior is illustrated below:
Do you think that people are usually aware of the dangers? Not everyone. (...) Because some people need, let's say Facebook very often, and it's... It's too usual, they don't think what is behind them, and ... which information they give out every time... Because they grow up with that kind of stuff and, yeah, it's normal, it's usual. (...) I think the problem is that you can go into the Internet from everywhere, and then, over the cell phones and, you can be online everywhere. Maybe that's a big part, that somebody lose[s] the natural sensitive mind... Do you mean that because it's too common to use the Internet, so they are not thinking about it thoroughly? Yes. (SwitzerlandC2a, manager)

The results of the thesis also explain the factors that have an influence on the formation of habitual enactment. According to the interviewees, the rational IS security dimensions of professionalism (see section 3.3.5) and balancing threats and the value of information (see section 3.3.5), plus the IS security-detached dimensions of policy obedience (see section 3.3.6) explain employees' IS security behavior, and also the development of the unconscious IS security dimension of habitual enactment. This means that if a person recognizes the potential risk of losing sensitive information due to neglecting IS security procedures, has a high sense of responsibility in the work, and obeys the compulsory rules, they tend to actively develop certain automatic working procedures. In addition, if the IS security procedure is experienced to be convenient to execute (see the rational IS security dimension of inconvenience in section 3.3.5), the decision to engage the formation of the unconscious IS security dimension is more likely to occur. All of these reasons for explaining the formation of the unconscious IS security dimension of habitual enactment are illustrated below:

There are many people who do not ever lock their laptops or (...). But at least I can talk about my department, each and every person, it has become habit now, that automatically when they get up the seat to go to the next person, next cubicle, they Control-Alt-Delete and then go. Why you think it has become a habit for your department? What do you think is the reason? (...) We cannot leave the laptops unattended. (...) Because we have a lot of interaction with other companies, other department managers, other employees. So everything that we do, (98%) relates to employment matters. So we need to prevent others from looking at what is happening on our tables. We do not want anyone to peek into what we are doing. That's the reason we always lock it. We have had a, at least two or three cases, probably three
years back when we had get some information, very confidential, but then that leaked out. And then we found out the source of the leak. We questioned that person thoroughly and he said, he confessed that he saw it on the laptop of ours. So then it has been made mandatory thereafter that we lock our computers (...) and then people have realized that okay, we have to do something. And that’s why it has become a habit. Yes. (UAEA3a, manager)

In addition, the unconscious IS security dimension of habitual enactment was considered to be influenced by organizational dimensions of communications (see section 3.3.4), and by individual dimension of previous experiences (see section 3.3.3). The unconscious IS security dimension was partly connected with certain IS security procedures, while of the types of IS security procedures, only password selection was not associated with habitual enactment.

Mistakes

A typical argument for explaining unsafe working procedures was also that of human mistakes, which increase particularly when a person is experiencing work pressure (hurry, high workload, or stress). Besides causing deliberate decisions not to comply with IS security practices (see balancing threats and the value of information in section 3.3.5), such situations increase the possibility of making mistakes unintentionally, which can compromise the information security, as is illustrated below:

What do you think, what could be the reason if somebody is not locking the PC? Oh, just not thinking about it, if a lot of things are happening simultaneously or you’re under stress and you just don’t think about doing it. (SwitzerlandA5, officer)

Mistakes offer an explanation for neglecting the secure use of the Internet and for locking one’s computer, but not for writing down passwords, or password selection.

3.4 Scaling Up Towards a Framework for Understanding Employees’ IS Security Behavior

Finally, for scaling up towards an emerging theory, based on the seven main categories and their relationships formulated in the previous coding phases, a
Theoretical framework was formulated through grouping and relabeling these categories into three broader themes or core categories (Urquhart et al. 2010): (1) formative elements, which potentially influence on the formation of employees’ IS security behavior, termed (2) behavioral contingencies, which can be explained through (3) cognitive mechanisms. These core categories and the relationships between them as supported by interviews (arrows) are presented in Figure 4.

Fig. 4. A theoretical framework that explains employees’ IS security behavior.

The idea behind the theoretical framework presented in Figure 4 is similar to analytical approaches aimed at explicating the social mechanisms (M) that explain the observed relationships between two entities (A) and (B) (Hedström & Swedberg 1998). According to Elster (1998), such explanation by mechanisms represents an intermediate between scientific laws and descriptions. This means that instead of presenting deterministic scientific laws aimed at predicting the phenomenon in question, or only describing the variation of different views of the phenomenon (e.g., Kaapu et al. 2006), mechanisms-based explanation presents plausible, frequently observed causal patterns that open the black-box between the two entities (Elster 1998). Then, a causal pattern here is not the form of a
scientific law, such as entity (A) (the cause) will always produce entity (B) (the effect). Instead, an explanation by mechanisms says that (A) will sometimes produce (B), and offers an potential explanation (M) of why (A) sometimes produces (B), thus offering reasons for certain behavior (Elster 1998). Accordingly, the framework represents a mechanism-based explanation of two types of entities termed formative elements (A) and behavioral contingencies (B). The way in which these two categories are linked to one another is expressed with the cognitive mechanisms (M)\(^{13}\), which explain how individual beliefs and desires generate a specific action (Hedström & Swedberg 1998; Schelling 1998). These cognitive mechanisms can be seen as different kinds of human processes by which certain kinds of IS security violations occur or are prevented.

As a first main theme, the formative elements (A) combine three main categories formulated as a result of the data analysis (see sections 3.3.2–3.3.4): cultural dimensions (i.e., cultural mentality and company’s culture), organizational dimensions (i.e., communications, extrinsic control), and experience-based dimensions (i.e., IS security accidents, and work experience)\(^{14}\). According to the causal pattern specific to the mechanism-based explanation, the main idea of the framework is that these formative elements (A), through their subcategories, sometimes have an influence on employees’ IS security behavior (i.e., behavioral contingencies (B)), and this causal pattern can be explained through employees’ individual thinking (i.e., cognitive mechanisms (M)). In other words, the framework is based on the idea that it is important to understand how (M) certain formative elements (A) can have an impact on IS security behavior (B), rather than only conclude that such a connection between these two entities (A) and (B) exists. For example, instead of pointing out a direct connection between communications (i.e., oral communications, training, role model, and involvement) and IS security behavior, or extrinsic control (i.e., monitoring, punishments, rewards, and coercion) and IS security behavior, it is argued here that such potential influences need to be explained through cognitive mechanisms (M) between formative elements (A) and behavioral contingencies (B) (i.e., IS security behavior). The connections between formative elements (A) and

\(^{13}\) Hedström and Swedberg (1998) use the term “action-formation mechanism.” For the sake of consistency, here the term “action-formation” is replaced with “cognitive,” because the main purpose is to find conscious or unconscious mental reasons for explaining employees’ IS security behavior.

\(^{14}\) The individual dimensions presented in the previous section (3.3.3) are here re-labeled as experience-based dimensions because no connections between personality qualities and other categories (i.e., cognitive mechanism) were found. For the same reasons, activity on IS security issues was left out of the model.
cognitive mechanisms (M) elaborated on and illustrated in section 3.3 are not presented in detail in this figure because the emphasis in the framework is to show that different cognitive mechanisms (M) potentially lead to different behavioral contingencies (B). Apart from section 3.3, found connections between formative elements and cognitive mechanisms are graphically presented in Appendix 3.

A second theme labeled as the cognitive mechanisms (M) combines three main categories formulated as a result of the data analysis (see sections 3.3.5–3.3.7), which can have a direct effect on explaining employees’ IS security behavior (B): (1) Rational IS security dimensions include five types of reasons involving deliberate consideration of advantages and disadvantages before engaging in a particular behavior with respect to IS security: balancing threats and the value of information awareness, inconvenience, trust in IS security procedures, professionalism, and work ethics. (2) IS security-detached decisions mean reasons for employees’ IS security behavior, which are not based on security-conscious decisions, but certain other motivations: obedience, authority, social conformity, and pressure. (3) Unconscious IS security dimensions means such reasons for employees’ IS security behavior, which are not based on conscious thinking: habitual enactment and mistakes.

In turn, the theme of behavioral contingencies (B) equals a category of IS security procedures (see section 3.1) including employees’ general IS security behavior without any references to specific IS security procedures, and different violation types. In the latter case, the data suggests that different rationales (i.e., cognitive mechanisms M) “motivate” employees to comply or violate different IS security procedures termed violation types: secure use of the Internet, writing passwords down, password selection, and locking the computer. For that reason, both of these conceptualizations of employees’ IS security behavior are included in the theoretical framework under the main category of behavioral contingencies.

Accordingly, Figure 4 shows that from the rational IS security dimensions, balancing threats and the value of information and inconvenience were associated with explaining all violation types, and work ethics were not associated with specific violation types, but instead, merely offer a general explanation for IS security behavior. In turn, besides offering a general explanation, lack of trust for IS security procedures was connected with secure use of the Internet and password selection, and professionalism was connected with secure use of the Internet and locking of computers. Figure 4 also illustrates that all IS security-detached dimensions offer an explanation for locking one’s computer. In addition,
policy obedience and pressure explain secure use of the Internet. Finally, the unconscious IS security dimensions explain secure use of the Internet and locking the computer, and of these, habitual enactment also explains writing down passwords.
4 Discussion

The key results of this thesis are discussed in this chapter. First, section 4.1 discusses the contribution of this thesis with respect to the existing research on IS security training and employees’ IS security behavior. Second, section 4.2 covers the thesis’s implications for practice, and section 4.3 shows its implications for research within both the theoretical perspectives of this thesis: a meta-theory of IS security training and a framework for understanding employees’ IS security behavior. Finally, limitations of this thesis are discussed in section 4.4.

4.1 Contribution of the thesis

4.1.1 Contributions of a meta-theory for designing IS security training approaches

This thesis advanced a meta-theory for designing IS security training with three levels of thinking: the meta-level, critical level, and intuitive level. Theories have various purposes, (see Gregor 2006), and the purpose of the meta-theory in this context is to analyze the nature of IS security training at the first level and produce respective guidance on how to design effective training approaches at the second and third levels. Through this theory, three contributions are highlighted. First, at the meta-level, this theory advances fundamental features of IS security training, which clarify how IS security training is different from other training (non-cognitive and persuasive nature, existentialistic features, emphasis on daily work situations, voluntariness vs. mandatoryness in using protection mechanisms, and the intangible nature of IS security threats and assets), and formulates respective meta-level requirements. This is an important contribution because decisions regarding suitable pedagogical requirements for effective IS security training at a critical thinking level is based on these fundamental features and corresponding meta-level requirements. Even if some of the existing studies in the area of IS security training apply learning theories (see training approaches based on learning theories in Table 1), none of them has considered these features as a basis for a selection of suitable learning theory and respective pedagogical requirements.

As the second contribution of the thesis, previous IS security training approaches are systematically reviewed from the viewpoint of learning paradigms
and corresponding meta-orientations. In this manner, the thesis points out the limitations of the existing IS security training approaches as regards their educational practices. Similar reviews already exist in the area of IS security awareness. Puhakainen (2006) used an analytical framework to examine the organizational role of IS security, research objectives, and research approaches and their theoretical background. In turn, Puhakainen and Siponen (2010) used key findings, a basis of findings, academic/practical, underlying theory and theoretical orientation, and empirical evidence for analyzing IS security training literature. However, we have found no review of IS security training that shows the strengths and weaknesses of the existing IS security training approaches in regard to the theories of learning. Results of the literature review indicate that only one study (Puhakainen 2006) meets the last three requirements; another one (Kabay 2002) meets the second and third requirements; and two (Herold 2005, Wilson & Hash 2003) meet the last requirement. This means that even if some practical features of effective training can be found in these four IS security training approaches (i.e., content, teaching method and/or evaluation of learning), none of the existing IS security studies is focused on and directed towards theoretical bases of social constructivism i.e., fulfill all four pedagogical requirements formulated at the critical thinking level.

As the third contribution of the thesis, new theoretical and practical insights are advanced into how the domain of IS security training can be brought forward. At the critical thinking level of the meta-theory, this means that the thesis presents four pedagogical requirements for effective IS security training, and at the intuitive thinking level, it outlines guidelines for IS security training that illustrate these four requirements by incorporating experiential and collaborative learning. Even if 36 approaches for IS security training exist in the literature, none of the existing IS security training approaches offers either theoretical of practical guidance based upon pedagogical requirements formulated at the critical thinking level of the meta-theory. As a new contribution, this thesis illustrates how to execute IS security training based on experiential, and particularly communal and communicative, characters of the psychological context, content, teaching methods, and evaluation of learning.
4.1.2 Contributions of a framework explaining employees' IS security behavior

A theoretical framework including two main categories (i.e., formative elements and cognitive mechanisms) explaining employees' IS security behavior (i.e., behavioral contingencies) was also developed in this thesis. The previous IS security literature with similar results for each individual component of the framework is presented in Table 14. A connection between constructs of the previous literature and sub-categories of cognitive mechanisms found in this thesis is presented through the following numbering: (1) Balancing threats and the value of information, (2) Inconvenience, (3) Lack of trust in IS security procedures, (4) Professionalism, (5) Work ethics, (6) Policy obedience, (7) Authority, (8) Social conformity, and (9) Pressure.
Table 14. A comparison between previous IS security behavior literature and constructs of the theoretical framework explaining employees’ IS security behavior.

<table>
<thead>
<tr>
<th>Formative elements</th>
<th>Cognitive mechanisms</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Rational*</td>
</tr>
<tr>
<td></td>
<td>Communicative</td>
</tr>
<tr>
<td><strong>Beaumont et al.</strong> 2009</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Increased physical and cognitive load (2)</td>
</tr>
<tr>
<td></td>
<td>Missed opportunities (2)</td>
</tr>
<tr>
<td></td>
<td>The “Hassle Factor” (1)</td>
</tr>
<tr>
<td></td>
<td>Avoiding the consequences of a security breach (1)</td>
</tr>
<tr>
<td><strong>Bulgurcy et al.</strong> 2010a</td>
<td>Rewards as a benefit of compliance</td>
</tr>
<tr>
<td></td>
<td>Sanctions as a cost of non-compliance</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Bulgurcy et al.** 2010b

Information security policy quality and fairness
<table>
<thead>
<tr>
<th>Formative elements</th>
<th>Communicative</th>
<th>Control</th>
<th>Experience</th>
<th>Cultural</th>
<th>Rational*</th>
<th>ISS detached</th>
<th>Unconscious</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chan et al. 2005</td>
<td>Upper management practices: safety policy and training and awareness programs</td>
<td>Supervisory practices are related with information security climate</td>
<td>Self-efficacy (2)</td>
<td>Co-worker socialization (8)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D'Arcy et al. 2008</td>
<td>Security policies, security education, training, and awareness program</td>
<td>Perceived severity of sanctions</td>
<td>Computer monitoring</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D'Arcy &amp; Greene 2009</td>
<td>Security communications</td>
<td>Top management's commitment and communications are related to security culture</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D'Arcy &amp; Hovav 2007</td>
<td>Security policies, security awareness program</td>
<td>Technology awareness</td>
<td>The influence of technology awareness, and subjective norm is moderated on cultural effects</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dinev et al. 2009</td>
<td>Technology awareness</td>
<td></td>
<td></td>
<td>Subjective norm (8)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Formative elements</td>
<td>Cognitive mechanisms</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communicative</td>
<td>Control</td>
<td>Experience</td>
<td>Cultural</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dinev &amp; Hu 2007</td>
<td>Technology awareness</td>
<td>Perception usefulness and ease of use (2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Controllability (2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Perceived behavioral control (2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Harrington 1996</td>
<td>Company's codes of ethics</td>
<td>Denial of responsibility (4)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Herath &amp; Rao 2009a</td>
<td>Resource availability Detection certainty</td>
<td>Organizational commitment (4) Subjective norm (8)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Response efficacy (3) Descriptive norm (8)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Response costs (2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security breach concern level (1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Self-efficacy (2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Herath &amp; Rao 2009b</td>
<td>Certainty of detection</td>
<td>Perceived effectiveness (3) Normative beliefs (8)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hyeun-Suk et al. 2005</td>
<td></td>
<td>Optimistic bias in risk perception (1) Peer behavior (8)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Johnston &amp; Warkentin 2010</td>
<td></td>
<td>Response efficacy (3) Social influence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lee et al. 2004</td>
<td>Involvement</td>
<td>Perceived threat severity (1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Self-efficacy (2) Norms (5)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Formative elements</td>
<td>Cognitive mechanisms</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-----------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication</td>
<td>Rational* ISS detached Unconscious</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control</td>
<td>Detection probability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Experience</td>
<td>The effect of sanction</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cultural</td>
<td>severity is conditioned on personal norms</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Perceived security risks (1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Perceived benefits (5)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Personal norms (5)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Li et al. 2010</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Myyry et al. 2009</td>
<td>Fear of punishments</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(preconventional moral reasoning)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Posing a personal risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(preconventional moral reasoning) (1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Values: openness to change and conservation (5)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ng et al. 2009</td>
<td>Perceived benefits (3)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Perceived susceptibility and severity of security incidents (1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Self-efficacy (2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pahnila et al. 2007</td>
<td>Information quality</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Facilitating conditions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sanctions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Siponen et al. 2007</td>
<td>Threat appraisal (1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Normative beliefs (8)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Siponen et al. 2006</td>
<td>Response efficacy (3)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Threat appraisal (1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Self-efficacy (2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Self-efficacy (2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Normative beliefs (8)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Threat appraisal (1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Formative elements</td>
<td>Cognitive mechanisms</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communicative</td>
<td>Control</td>
<td>Experience</td>
<td>Cultural</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Siponen &amp; Vance 2010</td>
<td>User involvements is related with awareness campaigns and written rules User-involvement</td>
<td>Conflict of priority between information security and usability, and functionality (2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Albrechtsen 2007</td>
<td>Adams &amp; Sasse 1999</td>
<td>Multiple passwords (2) Password content (2) Perceptions of organizational security and information sensitivity (1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sasse et al. 2001</td>
<td>Stanton et al. 2003</td>
<td>Accountability (1) Identity issues (8) Usability issues (2) Social issues (8) Nobody-will-target-me thinking (1) Professional reputation (9) They-could-not-do-much-harm-anyway thinking (1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stanton et al. 2005</td>
<td></td>
<td>Organizational commitment (4)</td>
<td>Rewards Training Monitoring</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Through this framework, the following contributions are highlighted. First, in reviewing the previous empirical studies of reasons for employees’ IS security behavior cited in Table 14, it is clear that none of them includes all seven categories presented in this thesis: seven used concepts in only one category, twelve used two, three used three, and three used reasons from four categories. In addition, one study that explains non-compliance with IS security procedures through neutralization techniques (Siponen & Vance 2010) couldn’t be placed under any of the categories. Thus, to understand the phenomenon of IS security behavior and to create a coherent basis for improving an organization’s IS security management approaches, these individual dimensions were incorporated into a holistic theoretical framework explaining employees’ IS security behavior (see Figure 5.) A framework offers a categorization that reduces a broad range of concepts to a more manageable framework, and thus, makes it easier to compare existing research results.

In terms used by the thesis, the existing formative elements and employees’ cognitive mechanisms should been taken into account for creating positive changes in employees’ IS security behavior (i.e., behavioral contingencies) effectively. In contrast with the existing research, this framework stresses the difference between these two main categories explaining employees’ IS security behavior: formative elements (A) sometimes have an influence on employees’ IS security behavior (i.e., behavioral contingencies (B)), and this causal pattern can be explained through employees’ individual thinking (i.e., cognitive mechanisms (M)). In other words, formative elements are possible causes or organizational tools for creating or changing employees’ cognitive mechanisms that motivate their IS security behavior. Therefore, the framework (see Figure 5) is based on the idea that it is important to understand why certain formative elements can have an impact on IS security behavior, rather than only to conclude that different formative elements have an influence on IS security behavior. In addition, the results of this thesis imply that employees’ reasons for compliance with IS security procedures can be partly dependent on the type of compliance, which is not recognized in the previous literature. Next, a contribution of each category of the framework is discussed in relation to the previous literature.

**Formative elements**

Formative elements include three subcategories: (1) Organizational dimensions (i.e., communications and extrinsic control), (2) Cultural dimensions (i.e., cultural
mentality and company’s culture), and (3) Experience-based dimensions (i.e., IS security accidents and work experience). Regarding organizational dimensions (1), the results emphasize the importance of having effective communications for creating, maintaining, and improving employees’ IS security behavior, because these have an influence on employees’ rational IS security dimensions (balancing threats and the value of information, professionalism, inconvenience) the IS security-detached dimensions (policy obedience, authority), and the unconscious IS security dimension (habitual enactment). In the previous literature, IS security-related communications, such as IS security policies and training programs, have shown to have an influence on employees’ IS security behavior (Bulgurcy et al. 2010b, Chan et al. 2005, D’Arcy et al. 2008, D’Arcy & Hovav 2007, D’Arcy & Greene 2009, Harrington 1996, Herath & Rao 2009a, Pahnila et al. 2007, Stanton et al. 2005). However, an explanation for this influence is mentioned only in Herath and Rao (2009a), who state that training improves employees’ self-efficacy, which, in turn, leads to the intention to comply with IS security procedures. This finding is consistent with the results of this thesis. In addition, this thesis showed the factors that can influence the success of the communication efforts, namely authority, extrinsic control, and personal involvement during IS security communication. Similarly, D’Arcy et al. (2008) concluded that the influence of IS security policies and IS security training can also be realized through increased sanction perceptions (severity). In addition, Albrechtsen (2007) reported that involving users has been considered a requisite for effective IS security training, and Chan et al. (2005), and D’Arcy and Greene (2009) concluded that management’s support has proven to have an effect on employees’ IS security behavior. The importance of employees’ involvement in their organization’s IS security issues is also recognized in Lee et al. (2004).

Regarding organizational dimensions (1), this thesis also explains the impact of the use of extrinsic control, which means monitoring, rewards, punishments, and coercion for improving employees’ IS security behavior through cultural dimensions related to cultural mentality, rational IS security dimensions of

---

15 In more detail, existing studies investigate employees’ intentions to comply with or violate IS security procedures (Johnston & Warkentin 2010, Herath & Rao 2009, Siponen & Vance 2010, Peace et al. 2003, Harrington 1996, D’Arcy et al. 2008, D’Arcy & Hovav 2009), their actual behavior (e.g., Albrechtsen 2007, Chan et al. 2005, Ng et al. 2008, D’Arcy & Greene 2009, Stanton et al. 2003, 2005, Sasse et al. 2001, Adams & Sasse 1999), or both (e.g., Pahnila et al. 2007, Siponen et al. 2007, Myyry et al. 2009, Lee et al. 2004). However, we don’t differentiate these concepts in this study, but rather use the term ‘IS security behavior’ in terms of both intentional and actual compliance with IS security policies.
balancing threats and the value of information, professionalism, and inconvenience, and the IS security-detached dimensions of social conformity and pressure. In the previous IS security literature, the influence of sanctions, rewards, or monitoring has shown to have a direct effect on employees’ IS security behavior, but the rationale behind this influence has not been considered in more detail (Beautement et al., 2009; Bulgurcy et al., 2010a; D’Arcy et al., 2008; Herath & Rao, 2009a; 2009b; Li et al., 2010; Siponen et al., 2007; Stanton et al., 2005). However, while some research reports an insignificant effect between monitoring, sanctions, and/or rewards, and IS security behavior (Siponen & Vance, 2010; Pahnila et al., 2007; Herath & Rao, 2009a, 2009b; D’Arcy & Hovav, 2007; Li et al., 2010) the thesis also shows some contradictions related to their use. While the previous IS security literature explains this inconsistency through individuals’ level of moral reasoning (Myyry et al., 2009; Li et al., 2010), the thesis showed a more diverse viewpoint on why extrinsic control may not be effective. At worst, it was associated to have a negative effect on creating professional behavior, to have a negative influence on a company’s business and employees’ work motivation, and to be a procedure that is contradictory with mutual trust and employees’ good intentions in their work.

Regarding cultural dimensions, (2) the thesis shows that IS security behavior (herein referred to as behavioral contingencies) is also influenced by cultural mentality through rational IS security dimensions of balancing threats and the value of information, professionalism and work ethics, and the IS security-detached dimensions of authority, social conformity, and pressure. In addition, cultural mentality influences the nature of a company’s culture, and also explains the success of applying organizational dimensions in terms of extrinsic control, and a company’s culture is related to an organizational dimension of communications. Similarly, the results of the thesis of Dinev et al. (2009) reveal that national culture has an influence on the effects between social conformity (i.e., subjective norm) and IS security behavior, as well as activity on IS security issues (i.e., technology awareness) and IS security behavior. However, other studies (and reasons) explaining this influence of cultural mentality on employees’ IS security behavior were not found. The effect of a second cultural dimension (2) of a company’s IS security culture on employees’ IS security behavior is also supported by the previous IS security literature through communications (i.e., supervisory practices) and social conformity (i.e., co-worker socialization) in Chan et al. 2005, and through communications (i.e., management’s commitment to security and security communication) in D’Arcy and Greene (2009). These
results are similar to the results of this study, while a company’s culture was found to be connected and the IS security-detached dimensions of social conformity and authority, as well as the formative dimensions of communications and extrinsic control. However, a connection between the rational IS security dimension of balancing threats and the value of information and a company’s culture was not found by previous research.

Regarding experience-based dimensions (3), employees’ former experiences in the form of experienced IS security accidents, work experience, and activity on IS security issues have an influence on employees’ IS security behavior through the rational IS security dimensions of balancing threats and the value of information, as well as professionalism and the unconscious IS security dimension of habitual enactment. None of the existing studies investigate the influence of experience-based dimensions in terms of experienced IS security accidents and work experience on employees’ IS security behavior. However, the impact of an individual’s activity on IS security issues is also recognized in Dinev and Hu (2007) and Dinev et al. (2009), who report that technology awareness, in terms of being concerned with security issues, has an influence on employees’ IS security behavior. While Dinev et al. (2009) did not elaborate on this influence further, Dinev and Hu (2007) explain this connection with employees’ moral attitudes towards IS security behavior.

Cognitive mechanisms

Cognitive mechanisms include three sub-categories: (1) Rational IS security dimensions (i.e., balancing threat and value of information, inconvenience, lack of trust for IS security procedures, professionalism, and work ethics), (2) IS security detached dimensions (i.e., policy obedience, authority, social conformity, and pressure), and (3) Unconscious IS security dimensions (i.e., habitual enactment and mistakes). The key contribution of the thesis is that these reasons for employees’ violation of and compliance with IS security procedures (i.e., cognitive mechanisms) may depend on the type of IS security procedures (i.e., violation type). The previous studies in the area of employees’ compliance with IS security procedures do not assume such a difference. Although the previous literature does not systematically report a dependence between violation types and reasons for users’ IS security behavior (i.e., cognitive mechanisms), some individual violation type-related explanations for employees’ IS security behavior can be found in the previous studies, which limits their studies to particular forms
of IS security behavior. Next, the dependency between violation types and reasons for users’ IS security behavior (i.e., cognitive mechanisms) and their connections with existing studies are discussed.

First, the results show that the rational IS security dimensions (1) in terms of balancing threats and the value of information can be the key dimension that has an influence on employees’ IS security behavior, while it explains all four IS security procedures. One of the violation types was secure use of the Internet, with a sub-category of avoiding viruses. Regarding this, Ng et al. (2009) found that the perceived susceptibility of an IS security risk explained the IS security behavior of employees in terms of opening suspicious e-mail attachments, Johnston and Warkentin (2010) reported that perceived threat severity has an influence on intentions to use anti-spyware software (through improved self-efficacy and response efficacy), and Li et al. (2010) found that perceived IS security risks have an influence on employees’ compliance with intern use policy in terms of visiting non-work-related websites. In addition, threat awareness and user’s identification of sensitive information in their work were related to the explanation of password practices (e.g., password selection and writing down passwords) in Adams and Sasse (1999) and Sasse et al. (2001), which is also consistent with the results of this thesis. IS security threat awareness is considered to be one of the key factors explaining IS security behavior also in the previous IS security literature without linking it with certain IS security procedures (Beautement et al. 2009, Pahnila et al. 2007, Siponen et al. 2007, Herath & Rao 2009a, Bulgurcy et al. 2010a, Siponen et al. 2006). However, it is also argued that the possibility that users risk recognition itself does not have an influence on users’ risky behavior, because of their high trust in their own working environment or themselves (Hyeun-Suk et al. 2005). Finally, Myyry et al. (2009) report the influence of experiencing only a personal risk to be effective in making employees to avoid password sharing with others. However, password sharing is not elaborated on in this thesis.

The second rational IS security dimension (1), inconvenience, also explains all four IS security procedures. Regarding the two violation types of writing passwords down and the selection of good passwords, explained through inconvenience (i.e., the second type of the rational IS security dimensions), the findings of this thesis are consistent with Adams and Sasse (2001) and Sasse et al. (2001). Similarly, it was also stated in the previous IS security literature that employees need safe IS security procedures to be both convenient to use in their daily working practice (Albrechtsen 2007’ Beautement et al. 2009, Bulgurcy et al. 2010a, Pahnila et al. 2007, Siponen et al. 2007, Herath & Rao 2009a, Siponen et al. 2006). However, it is also argued that the possibility that users risk recognition itself does not have an influence on users’ risky behavior, because of their high trust in their own working environment or themselves (Hyeun-Suk et al. 2005). Finally, Myyry et al. (2009) report the influence of experiencing only a personal risk to be effective in making employees to avoid password sharing with others. However, password sharing is not elaborated on in this thesis.
2010a, Dinev & Hu 2007, Herath & Rao 2009a) and feel competent enough to use these procedures (Bulgurcy et al. 2010a, Chan et al. 2005, Herath & Rao 2009a, Siponen et al. 2007, 2006). It was also found that employees do not experience a conflict between individual security duties and work efficiency (Beautement et al. 2009, Bulgurcy et al. 2010a) and, in particular, have a need to feel confident of recognizing suspicious e-mails or doing so conveniently (Ng et al. 2009), as well as being able to use anti-spyware software (Johnston & Warkentin 2010, Dinev & Hu 2007).

As a third IS security-detached dimension (1), lack of trust for IS security procedures explains secure use of the Internet and password selection, but not locking the computer and writing down passwords. Previous studies also show that employees need to trust the effectiveness of IS security procedures (Bulgurcy et al. 2010, Herath & Rao 2009a, 2009b, Siponen et al. 2007, 2006). In Ng et al. (2009), besides explaining general IS security behavior, this reason is also connected with secure use of the Internet in terms of opening e-mail attachments, using anti-spyware software (Johnston & Warkentin 2010), and good password practices (Sasse et al. 2001), which is consistent with the results of this thesis. Finally, no previous studies were found that report a connection between the violation type of locking one’s computer and any of these three rational IS security dimensions: balancing threats and the value of information, inconvenience, and lack of trust in IS security procedures.

The fourth rational IS security dimension (1) of professionalism (i.e., responsibility, common sense, duty, and responsibility denial) explains secure use of the Internet and locking one’s computer, but not writing down passwords or a password selection. Harrington (1996) concluded that responsibility denial was related to five “computer abuse” intentions of employees: virus, fraud, sabotage, software copying, and cracking. While this is consistent with the results of this thesis, it is important to point out that Harrington (1996) utilized scenarios where the situation was predefined and hence, may not exactly match the situations described by the interviewees of this thesis. Further, Stanton et al. (2003) reported that employees with a high organizational commitment are less likely to use their companies’ computers for personal web-surfing and e-mail. The results shown by Stanton et al. (2003) can be interpreted as being consistent with the findings of this thesis, holding that professionalism in terms of responsibility denial and organizational commitment explains employees’ secure use of the Internet, at least when this is related to avoiding viruses and Internet browsing habits.
Professionalism was found as a reason for general compliance with IS security procedures, also in Herath and Rao (2009a) and Bulgurcy et al. (2010a).

Finally, as the fifth rational IS security dimension (1), an individual’s work ethics in terms of a high sense of loyalty, honesty, and trustworthiness and intentional abuse was found to be one explanation for IS security behavior without associating it with different IS security procedures. Similarly, the previous literature also reports that moral considerations towards IS security procedures have an effect on employees’ compliance with them: Lee at al. (2004) show that norms explain computer abuse, Li et al. (2010) report that perceived benefits of Internet abuse and personal norms have an influence on employees’ Internet use for non-work-related purposes, Dinev and Hu (2007) conclude that moral attitudes towards IS security behavior explain the use of anti-spyware tools, and Myyry et al. (2009) conclude that values have an impact on password sharing with co-workers.

Second, in this thesis it was found that the IS security-detached dimensions (2), IS security policy obedience, authority, pressure, and social conformity explain employees’ IS security behavior. In addition, these all explain locking one’s computer and IS security policy obedience and pressure also explains secure use of the Internet, but not writing down passwords or a password selection. In the existing literature, no violation type-related explanations exist for the first two IS security-detached dimensions: policy obedience and authority. Regarding the violation of secure use of the Internet, it is found in the thesis that avoidance of viruses (a sub-category of secure use of the Internet) was not influenced by other IS security-detached dimensions, but by policy obedience. Interestingly, Johnston and Warkentin (2010) and Dinev et al. (2005) reported that the third IS security-detached dimension, social conformity in terms of perceptions of peers and managers’ expectations and attitudes, has an influence on employees’ behavioral intentions to use anti-spyware software. These findings could be interpreted as contradictory with the results of this thesis, because findings show that social conformity is relevant only in the case of locking one’s computer, but not in the case of secure use of the Internet. Another reason that explains the different findings between the present thesis and that of Johnston and Warkentin (2010) and Dinev et al. (2005) is that both studies focused on a different phenomenon because the use of anti-spyware tools was not an issue in this thesis; the employees we interviewed in the three locations have no privileges to install anti-spyware software. In addition, Johnston and Warkentin (2010) focused on a different population—use of anti-spyware software by home
computer users in terms of students and faculty members. Similarly with social conformity, management and/or co-workers’ attitudes and behavioral expectations or peer behavior (Bulgurcy et al. 2010a, Chan et al. 2005, Herath & Rao 2009a, 2009b, Pahnila et al. 2007; Siponen et al. 2006) have been shown to have an influence on employees’ IS security behavior.

In addition, an IS security detached dimension in terms of pressure (i.e., negative feelings associated with non-compliance with IS security procedures) is considered as a key factor for influencing employees’ password practices and locking the computer in Sasse et al. (2001) and compliance with IS security procedures in Beautement et al. (2009) and Bulgurcy et al. (2010a). While these findings are mostly consistent with the results of this thesis, as an exception, the findings of Sasse et al. (2001) could be partly interpreted as contradictory with the results, because pressure is found relevant only in the case of locking one’s computer and secure use of the Internet, but not in the cases of writing down passwords or a password selection. One explanation for this contradiction could be that Sasse et al. (2001) report this pressure to be related to good password behavior generally, also including password sharing with colleagues. Therefore, pressure is not necessarily related to the password procedures investigated in this thesis.

Third, it was found that users’ IS security behavior is also explained through unconscious IS security dimension (3), namely habitual enactment. This was also discovered by Pahnila et al. (2007). In addition, habitual enactment explains the secure use of the Internet, writing down passwords, and locking one’s computer, but not password selection. In addition, as regards developing IS security-supportive working habits, the thesis offers explanations for habit development, while, based on the results, professionalism, balancing threats and the value of information, policy obedience, inconvenience, communication, and previous experiences can explain the habit formation. No previous research reporting similar findings was found.

4.1.3 Overall contribution of the thesis

This thesis is composed of two studies in the field of employees’ IS security behavior; a meta-theory for designing corporate IS security training in chapter 2 and a framework for explaining employees IS security behavior in chapter 3. While first part of the thesis is targeted to developing well-founded and effective IS security training approach for improving employees’ IS security behavior, the
second part aims at understanding the rationale behind such behavior through explaining why certain kinds of IS security procedures are complied with or neglected by employees. Both of these viewpoints are needed because, besides a training method, successful IS security training aimed at improving employees’ compliance with IS security procedures requires understanding the employees’ reasons for compliance and non-compliance with IS security procedures. Such understanding is necessary in order for employees’ IS security behavior to be effectively improved through various interventions, such as IS security training.

A meta-theory for IS security training offers valuable contribution for IS security research and practice in three sense. First, former studies do not discuss the features of how IS security training is different from other trainings and formulate respective requirements based on learning theories. Even if some of the existing studies in the area of IS security training apply learning theories, none of them have considered these features and respective requirements that characterize IS security training. Second, the thesis points out the limitations of the existing IS security training approaches as regards their educational practices. We have found no review of IS security training approaches that shows the strengths and weaknesses of the existing IS security training approaches in regards to the theories of learning. Third, this thesis advances new theoretical and practical insights through a social constructivist learning paradigm and experiential and collaborative learning as to how the domain of IS security training can be brought forward. There exist no similar IS security training approaches based on experiential and collaborative learning in the extant literature.

Through a theoretical framework explaining employees’ IS security behavior, four main contributions are highlighted. First, this framework offers a holistic perspective of the phenomenon of employees’ IS security behavior, which reduces a broad range of concepts under a more manageable framework, and thus, makes it easier to compare existing research results. Second, the thesis offers new insights into the influence of organizational, cultural, and experience-based dimensions on employees’ IS security behavior through certain cognitive mechanisms. Particularly, none of the existing studies investigates the influence of experience-based dimensions on employees’ IS security behavior. Third, for developing IS security-supportive working habits, the thesis offers explanations for habit development, which was not reported by previous research. Finally, the results imply that employees’ reasons for compliance with IS security procedures depend on the type of IS security procedure violation, which is not recognized by the previous literature.
4.2 Implications for practice

4.2.1 Practical implications of a meta-theory designing IS security training

Two practical implications of the meta-theory for designing IS security training approaches need to be highlighted. First, based on meta-level requirements (i.e., how IS security training differs from other types of training) and learning theories, four pedagogical requirements for effective IS security training were formulated: 1) the explicit psychological context, the learning theory behind the training approach, must be based upon the group-oriented theoretical approach to teaching and learning, which directs the training activities; 2) the content of training must be based on collective experiences and the meaning perspectives of the learners; 3) teaching methods must include collaborative learning techniques in order to reveal and produce collective knowledge; and 4) evaluation of learning should emphasize experiential and communication-based methods from the viewpoint of the learning community.

As none of the existing IS security training approaches meets all four pedagogical requirements, as the second contribution, an example of IS security training is advanced, the experiential and collaborative IS security training approach, which meets these requirements and provides overridable guidelines for IS security training at the intuitive level. This learning approach involves four prescriptive guidelines based on the four-stage cycle of Kolb (1984): (1) Involve Learners’ Concrete Experiences; (2) Engage Reflective Observation; (3) Support Formation of Abstract Concepts and Generalizations; and (4) Enable Active Experimentation. These phases in the case of IS security training aimed at improving employees’ insecure e-mail use was illustrated.

4.2.2 Practical implications of a framework explaining employees’ IS security behavior

Based on the results of this thesis, the following eight practical implications of the investigation of the reasons for IS security behavior are highlighted.

First, while the results of this thesis emphasize the importance of communications as a foundation of employees’ IS security behavior, an organization’s IS security procedures, the value of information in their work, IS security threats, and IS security responsibilities need to be communicated
effectively. In addition, the thesis showed the factors that can influence the success of the communication efforts. For example, addressing authority and extrinsic control issues as a part of a communication was seen to be essential in making communication more effective (with certain limitations). On the other hand, personal involvement during IS security communication was seen as a way for improving understanding and the relevance of IS security-related communications. The results imply also that making employees’ IS security attitudes and behavior visible through discussion can be a possible way to exploit the positive effects of role modeling and involvement in IS security management. While the former aspect stresses the importance of the visibility of managements’ activity in IS security, the latter highlights the active role of the learners themselves. In addition, this can be a way to correct employees’ false conceptions, and provide concrete means for situations in which they may feel pressured to behave against IS security procedures.

Second, the results show that the impact of the use of extrinsic control (i.e., monitoring, rewards, punishments, and coercion) for improving employees’ IS security behavior can be controversial. Despite their potential positive influence, they were also associated with having a negative effect on creating professional behavior and a negative influence on a company’s business and employees’ work motivation, as well as being a procedure contradictory to employees having mutual trust and good intentions in their work. For these reasons, the role of the activities under extrinsic control as a part of the organization’s IS security management should be seriously considered, and perhaps alternative ways to achieve the positive changes should be found, such as strengthening employees’ IS security behavior, motivation, feelings of responsibility, and personal accountability and reducing bad habits. For this purpose, other formative elements, (i.e., communicative dimensions), should be preferred instead of extrinsic control.

Third, in different cultural settings, cultural dimensions should be taken into account in the designing of IS security training approaches, because IS security behavior was seen to be related to national culture through the rational IS security dimensions of balancing threats and the value of information, professionalism, work ethics, and the IS security-detached dimensions of authority and pressure. In addition, cultural mentality also explains the success of applying organizational dimensions in terms of extrinsic control. Recognizing the importance of these factors can contribute to a better understanding of the employees’ IS security attitudes (e.g., how they perceive the risk or value of information in their
surroundings), and how to influence them more effectively. In turn, in terms of this thesis, a company’s IS security culture includes the following three factors: the organizational dimensions (communications), rational IS security dimensions (balancing threats and the value of information), and IS security-detached dimensions (authority, social conformity). Similarly with cultural dimensions, the dimensions related to a company’s culture found in this thesis can be taken into account, for instance, in the evaluation and development of the IS security culture of organizations.

Fourth, the results of the thesis show that experience-based dimensions in terms of experienced IS security accidents and work experience improve employees’ IS security behavior through the rational IS security dimensions of balancing threats and the value of information and professionalism, as well as the unconscious IS security dimension of habitual enactment. However, the importance of a long working history for the employees’ IS security behavior can also be criticized. A long working experience does not necessarily assure the application of IS security procedures in the work, while employees’ former experiences can also function as a hindrance for learning new issues, with respect to working environment demands for IS security. To overcome this hindrance, proper communications for offering new insights as regards IS security threats need to exist.

Fifth, because the results of this thesis show that the rational IS security dimension of balancing threats and the value of information can be the key mechanism that influences employees’ behavioral contingencies, addressing these issues in the IS security training can be of significant importance for creating positive changes in employees’ IS security behavior. This means that for adopting new working practices, employees need to understand IS security threats and the value of information in their work environment and personal situation, as well as the vulnerability of existing security measures.

Sixth, the rational IS security dimension of experiencing inconvenience with IS security procedures can have an influence on employees’ IS security behavior. Accordingly, employees may need some guidance in order to decrease the experienced inconvenience with IS security procedures. Because most of the interviewees felt inconvenienced using IS security procedures, even though the procedures are actually very simple and fast to execute, employees could be informed and taught how to use them effectively. This can both lower their negative attitudes towards these practices and improve their skills to use them in practice. Particularly, supporting the employees’ selection and remembering of
passwords seems an essential target for improvement. This can be done, for instance, through introducing password mnemonics for employees.

Seventh, it was learned that users’ IS security behavior is also explained through the unconscious IS security dimension of habitual enactment. In addition, based on the results, the rational IS security dimensions of professionalism, balancing threats and the value of information and inconvenience, as well as the IS security-detached dimension of policy obedience can explain the dimension of habitual enactment. This means that if a person recognizes the potential risk of losing sensitive information due to the neglect of IS security procedures, has a high sense of responsibility in the work, and experiences IS security procedures as being convenient and mandatory to execute, certain IS security procedures may eventually become habitual activities.

Finally, while the reasons for employees’ violation of and compliance with IS security procedures depend on the type of violation, the training sessions can use different argumentation or persuasive messages according to the different types of violation: secure use of the Internet, locking one’s computer, writing down passwords, and password selection.

With respect to secure use of the Internet, the results regarding IS security-detached dimensions of policy obedience imply that a strong message, which clearly states what types of Internet uses constitute a procedure violation, are needed. This may also encourage employees not to reveal sensitive information under the IS security-detached dimension of pressure. In addition, regarding secure use of the Internet, the results suggest that persuasion with rational arguments can be an effective approach in four sense. First, the IS security staff can carefully explain to their employees and make them to understand that the information they have access to is valuable. At the same time, it should also be explained that there are active threats related to these assets. The results suggest that regarding the secure use of the Internet, if the employees see the related threat and understand the value of the information (i.e., the rational IS security dimension of balancing threats and the value of information), they may be motivated to protect the information by more secure use of the Internet. Second, regarding the rational IS security dimension of professionalism, supervisors can tell their employees that compliance with procedures on secure use of the Internet is part and parcel of their work duties. Third, to prevent the influence of the rational IS security dimensions from generating a lack of trust in IS security procedures, it is necessary to explain to employees that IS security procedures are useful, and indeed, if they are correctly used, they help to prevent threat from
occurring. Finally, even though activities to carry out secure use of the Internet may take some time and cause inconvenience, it is important to point out to the employees that securing their work documents is also an important work task.

With respect to locking one’s computer, the IS security awareness activities need to pay attention to the following. First, as with the secure use of the Internet, regarding the rational IS security dimension of balancing threats and the value of information and professionalism, it is important to make employees understand that there is sensitive information on their computers, and locking one’s computer is a good way of protecting this information; also, doing this is the responsibility of every employee. For example, given that it was found that suddenly arising interruptions cause employees to leave their desk without locking their computers, organizations need to explain to their employees that even in the case of an urgent need to leave their desks, the employees need to lock their workstations. Second, locking computers is strongly related with all IS security-detached dimensions: policy obedience, authority, social conformity, and pressure. Regarding policy obedience, there is a need to clearly demonstrate to the employees that locking one’s computer is the official procedure of their organization, and procedures need to be followed. Assuming that argument based on authority is seen as important reason for locking one’s workstation, it is necessary to ensure that top management, or someone from the senior management, announces the importance of locking one’s computer, and to make sure that employees do as required. This is especially important, given that the findings suggest that a lack of authority may have an influence on making employees lock their computers. Also, given that social conformity and pressure have an influence, it is necessary to ensure that all employees lock their computer, so the influence of social conformity spreads, and locking the computer is not attached with negative feelings, such as embarrassment. Similarly, given that habitual enactment functioned in both ways, it is important to ensure that employees do not develop the habit of not locking their computers.

With respect to writing down passwords, IS security awareness activities need to exert an influence on the rational IS security dimensions of balancing threats and the value of information and inconvenience. In practice, IS security staff need to explain to the employees as to what kind of threats writing down the password entails. Also, the employees must understand that difficult-to-guess passwords are effective for protecting the information on their computers. Given that inconvenience was associated with writing down passwords, the IS security staff needs to educate their employees as to how to select passwords that are easy
to remember and difficult to guess. Finally, given that writing down passwords easily becomes a habitual activity, it is necessary to constantly remind employees to memorize their passwords rather than write them down. Also, regarding password selection, besides having an influence on the rational IS security dimensions of balancing threats and the value of information and inconvenience, IS security awareness activities need to decrease the impact of the rational IS security dimension of a lack of trust in IS security procedures. This means that employees need to be aware of the fact that a good password, which is difficult to guess, is a key protection mechanism, and very effective in protecting the assets in their computers.

4.3 Implications for research

4.3.1 Research implications of a meta-theory for designing IS security training

Based on the findings of the thesis, three directions for future research are suggested. As a first research direction for the field of IS security training research, this thesis suggests research methodologies to validate IS Security Training approaches. Given the lack of empirical research on IS security training programs (Puhakainen & Siponen 2010), it is called for four levels of evaluations (Kirkpatrick 2006) to validate the IS security training approaches (these are also used to empirically study the second and third research directions): 1) user reactions; 2) learning (changes in attitudes, knowledge, thinking, or skills); 3) behavior (e.g., how learning is implemented in the organization); and 4) results (e.g., decreased frequency of accidents and improved productivity). To study users’ reactions, (1) learning, (2) behavior, and (3) interviews, observations, and surveys can be used. Also, to study behavior, objective measures can be used. For example, users’ objective Internet use behavior can be studied before and after training on the non-work-related use of the Internet from log files. Objective measures, if available, can be used to study results (4), as well. To give an example, the number of malware infections can be analyzed in the long term before and after the IS security training on protection against malware. To study changes in thinking (2), the use of integrative complexity (Suedfeld et al. 1992) can be suggested. It measures the complexity of mental abilities in terms of differentiation and integration: differentiation refers to the perception of different
perspectives, and integration to the conceptual connections among differentiated perspectives (e.g., trade-offs between alternatives). Integrative complexity has been successfully applied to investigate attitude changes and social perceptions and solve organizational problems (Suedfeld et al. 1992). This assumes that the level of the complexity of thoughts can be changed by discussion, information gathering, or training (Myyry 2002, Suedfeld et al. 1992). Thus, it offers an opportunity to see if IS security training increases the integrative complexity of thoughts regarding IS security behavior. As a result of IS security training, learners are expected to analyze and solve information security-related problems in their work using more diverse perspectives.

Evaluation of the impact of IS security training at levels 2–4 (Kirkpatrick 2006) requires a pre- and post-research design. This calls for a post- then pre-research design with a control group. In the post- then pre-research design, in addition to pre- and post-measurements being taken, participants would be asked immediately after training how they judged their earlier behavior. The post- then pre-research design should correct participants’ previously incorrect views because, after training, they are expected to better understand the training issues (Robinson and Robinson 1989, Mezoff 1981).

A second research direction involves the development of the critical-level principles of IS security training. The meta-theory presented in this thesis explains why 36 IS security training approaches have been developed, but only a few are based on pedagogical theories and offer empirical evidence on their practical usefulness (Puhakainen & Siponen 2010). This is explained through three levels of thinking. It is normal for practitioners dealing with a phenomenon—here, IS security training—to have their own beliefs, based on practical experiences and education. These beliefs reside at the intuitive level. When people realize that these beliefs may not be valid (in some situations) or they are not optimal, their thinking matures beyond those thoughts, towards the critical level where the validity of these principles are questioned (Hare, 1981). While method engineering (Brinkkember 1996; Kumar & Welke 1992) and advocates of the contingency view in management science (Weill & Olson 1989) realized that there cannot be a universal “fit-one-fit all” principle, the IS security training literature has not paid attention to this aspect. Hence, scholars need to develop critical-level principles for the selection of intuitive-level principles. There are three situations in which critical thinking is needed (Hare 1981). First, the validity of the intuitive level principles (a) needs to be known. The second situation is when the intuitive general principles conflict in particular cases (b).
The third situation when critical thinking is necessary is for selecting the intuitive principles that we will use in a given IS security training (c). Hence, the aim of this research direction is the development of critical-level principles. These principles can be inferred by studying the validity of IS security training practices (at intuitive-level thinking), at the organizations (a), through the research setting described in the first research direction. When developing and testing such principles, it would be important to pay attention to the context and the conditions under which the principles may be valid. Another research issue is how to make a selection when the intuitive principles conflict in particular cases (b). Given that the aim of the critical level is to (b) develop principles to solve situations where intuitive-level principles are in conflict, critical-level principles of this type should be developed. An authentic example of such a conflict is when there is a recognized need to implement IS security training, but strict deadlines to finalize the software products in due time block the training (Puhakainen & Siponen 2010). This also calls for research on how to develop a computer-supported learning environment in the organizational context, which offers an interesting viewpoint for effective and cost-effective learning and provides a comparison between face-to-face and e-learning-based IS security training.

As a third research direction, future research should develop intuitive thinking-level IS security training approaches that meet the four pedagogical requirements, which were further based on the meta-level requirements and the social constructivist learning paradigm. This thesis suggested that an experiential learning approach can be used to satisfy the four critical-level requirements. In addition, IS security training approaches with different constructivist instructional design approaches (e.g., Fardanesh 2006) should be developed and tested for different training topics and contexts. It is expected that the implementation of the four pedagogical requirements for IS security training should improve learners’ understanding of security-sensitive organizational assets, impending threats, and protection mechanisms (i.e., the existentialistic feature of IS security training). Against this backdrop, there is a need to study how IS security training practices can be developed based on the practices of existentialistic features. For example, regarding the three main existentialistic features—1. the existence of security-sensitive organizational assets, 2. threats towards them, and 3. protection mechanisms—scholars could develop different exercises that attempt to increase employees’ understanding of the assets with which they deal in their daily work (1), threats towards these assets (2), and a protection mechanism to use with the
assets (3). The effect of these techniques should be studied using the research setting described in the first research direction.

4.3.2 Research implications of a framework explaining employees’ IS security behavior

Because in this thesis a holistic framework of the reasons for employees’ IS security behavior is developed inductively through interpreting the user’s observations and experiences of information security in the particular organization, future research should examine the validity of this framework in other organizations. If that were to occur, then the results of the thesis could be used in the form of hypotheses that future researches can use and refine in similar research settings. Both qualitative and quantitative studies can be suggested for this purpose.

Second, theoretical sampling as a distinctive characteristic of a grounded theory approach means that the constructed categories and concepts are used for directing further data collection, and thus, the development of a solid grounded theory (Urquhart et al. 2009, Charmaz 2000). For further developing the preliminary categories and their relationships towards theoretical constructs and formal theory, there is a need to gather precise information on the inductively derived categories and concepts that explain employees’ IS security behavior. Then, it would be possible to concentrate on one category at a time for improving their relevance and providing in-depth information of “when, how, and to what extent they are pertinent and useful” (Charmaz 2000). For example, instead of creating a holistic framework of the phenomenon, a study could concentrate on investigating it from the viewpoint of the categories of cultural mentality or the company’s culture. Then, for guiding the theory development, theoretical frameworks from the fields of cultural identity of organizational culture could be selected to “scaffold” a coding process (see Sarker et al. 2001, Walsham 1995).

Third, the results suggest that the reasons that employees comply with IS security procedures are partly context-dependent, i.e., dependent on the type of violation. This means that future studies on employees’ compliance with IS security procedures need to take the type of violation into account. Thus, research is needed to compare how employees’ responses differ when asked why they comply with IS security procedures in general, versus when the type of violation is specified. This is important, given that there are a number of previous studies, and hence an active research stream, based on the use of such generic
measurements (e.g., “I comply with IS security procedures of my organization”). Given the findings, future research needs to determine if such generic measurements are a reliable and meaningful way of carrying out research on employees’ compliance with IS security compliance.

In addition, future research issues need to relate to the rationalizations people use to justify their level of compliance with the IS security procedures. Siponen and Vance (2009) suggested that neutralization techniques, which are different types of excuses, predict the employees’ compliance with IS security procedures. Given the findings, it is suggested that future research should determine if employees use different neutralization techniques to justify the violation of different types of IS security procedures. For this research stream, the Grounded Theory approach aimed at trying to find IS security-specific neutralizations (the opposite strategy would be theory verification, where one would find out if the original Neutralization Techniques by Sykes and Matzda can be found in this area) is especially welcomed. The existence of such Neutralization Techniques would open new possibilities for IS security training research and practice. The research and practice could use this information for the development of techniques to counter Neutralization Techniques. Subsequent research could test the impact of these techniques using pre and post and control group research settings.

Finally, it is suggested that future research should explore if the employee’s conceptions and thinking on the reasons for compliance with IS security procedures constitute a qualitatively different developmental stage of thinking in the sense of Kohlberg’s (1984) theory of Cognitive Moral Development.

4.4 Limitations of the study

This thesis is subjected a number of limitations. To start with the meta-theory part (the first part of the thesis), one limitation of the development of the meta-theory for designing IS security training is that it is based on conceptual-analytical work without empirical evaluation of its validity and usefulness in practice. Also, the theory may not be universally applicable; for example, to all national or organizational cultures, employees’ IS security competence, or learning styles. The success of the presented collaborative and experiential IS security training approach, relying highly on user participation and group dynamics, is also dependent on employees’ willingness to collaborate and take an active role in the training.
Limitations of the latter part of the thesis are typical for qualitative studies. First, care should be taken in generalizing the findings of the thesis. This framework for employees’ compliance with IS security procedures (Figure 4) is advanced as the initial formulation of a framework explaining employees’ compliance with IS security procedures. While the number of employees interviewed is relatively high for a qualitative study (N = 72), it is not claimed that the rationales found for the employees’ compliance with IS security procedures are exhaustive, and further research, especially in different organizations, might find alternative reasons for, and different connections with, certain violation types. However, although interviews were conducted in the three organizations, which formally form one company, it was seen by the managers of the company and the authors that due to the independent nature of the three separate locations (UAE, Switzerland, China), the results do not necessarily reflect only the experiences of one coherent organization with common management, business areas, and organizational culture.

Based on the investigation of authentic users’ experiences, this thesis offers some suggestions to understand the rationale behind IS security behavior, and thus its improvement, even though it is impossible to create one fit for all solutions for all organizations. This means that any intervention (e.g., IS security training) aimed at increasing employees’ IS security procedure compliance would need to be customized. Even if some general patterns for development can be stated, the decisions made must always be based on thorough investigation and recognition of the nature of the existing formative elements and cognitive mechanisms. Nonetheless, as is typical with interpretive research, both the credibility and the generalizability of the results of the thesis are context dependent, and generalizations are more like tendencies rather than predictions (Walsham 1995). Therefore, the applicability of the results can be evaluated by readers based on the documentation of the data collection and analysis processes, as well as the quotations illustrating the findings.

Finally, it can be questioned whether interviews can report honestly in respect to such matters as employees’ compliance with IS security procedures, especially if those employees fear that their employer may be able to trace the respondents who provided the answers. To address this concern, it was clearly communicated to the employees (interviewees) that we do not show the individual results to their employer, and that we are interested, not in what any individual respondent says, but in the general patterns stemming from the data. Finally, they were also
provided the option of having us write down their interview as field notes rather than recording them digitally.
5 Conclusions

Employee non-compliance with IS security procedures is considered to be one of the biggest threats to IS security. To solve this problem, several training approaches have been introduced in the IS security literature. Despite the recognized importance of having effective training, IS security training is largely a theoretically underdeveloped area. To fill this gap in research, a new meta-theory was established to design IS security training approaches, based on Hare’s concept of three levels of thinking. This meta-theory suggests that IS security training differs from other types of training, and needs to be understood before pedagogical principles for IS security training can be selected. In addition, the meta-theory proposed four pedagogical requirements that must be satisfied by any IS security training approach. The existing IS security training approaches were then reviewed in the light of these four requirements. This review pointed out that no previous IS security training approach meets all these requirements. Finally, it was demonstrated how an IS security training approach can indeed meet these requirements.

In addition, besides a training method, successful IS security training aimed at improving employees’ compliance with IS security procedures requires understanding of reasons why employees comply or don’t comply with IS security procedures. To address this concern, a number of empirical studies have also been conducted in the IS security literature, using a variety of labels such as “Computer Abuse,” “Computer Misuse,” “Employees’ compliance with information security procedures,” and “Organization’s (security) culture” in examining this phenomenon. While studies on computer abuse and employees’ compliance with IS security procedures have increased our understanding of what factors explain employees’ violations of IS security procedures, these studies basically test well-known and generic theories in a new context — that of IS security compliance. It is argued here that IS research needs to go beyond instantiating these generic theories taken from other fields and explore, grounded in data, why and how employees comply (or don’t comply) with IS security procedures. In this thesis, a first step in this direction is taken. To be more precise, 72 employees were interviewed in multiple locations of a global company. The locations were: China, UAE, and Switzerland. The results suggest that the reasons for violating IS security procedures depend on the type of violation. Previous research in the area has not reported such a difference.
The key contribution of the thesis was the introduction of a new meta-theory for IS security training, including understanding of the fundamental nature of IS security training, four pedagogical requirements for designing IS security training approaches, and illustration of these requirements in practice. A research agenda including three directions for future research was also advanced based on the meta-theory for IS security training. Besides a training method aimed at improving employees’ compliance with IS security procedures, a theoretical framework for explaining employees’ IS security behavior was developed. As a key contribution to future research on employees’ IS security behavior, it was suggested here that scholars should study the specific types of violations. For practitioners, it was noted that any intervention (e.g., IS security training aimed at increasing employees’ IS security procedure compliance) would need to be customized. That is, the training sessions need to use different argumentation or persuasive messages, according to the different types of violations. Accordingly, a number of strategies on how to do this were outlined in this thesis.
References

New York, David McKay Co. Inc.
11–15.
280.
Brody CM (1998) The Significance of Teacher Beliefs for Professional Development and
Development for Cooperative Learning. Albany, State University of New York Press:
Bulgurcy B, Cavusoglu H & Benbasat I (2010a) Information Security Policy Compliance:
An Empirical Study of Rationality-Based Beliefs and Information Security Awareness.
Bulgurcy B, Cavusoglu H & Benbasat I (2010b) Quality and Fairness of an Information
Security Policy as Antecedents of Employees’ Security Engagement in the Workplace:
An Empirical Investigation. Proceedings of the 43rd Hawaii International Conference
on System Sciences.
Workplace: Linking Information Security Climate to Compliant Behavior. Journal of
NK & Lincoln YS (eds) Handbook of Qualitative Research (2nd Edition). London,
Coffey A, Delamont S & Lofland J (eds) Handbook of Ethnography, London,
Cheung D & Wong H (2002). Measuring Teacher Beliefs About Alternative Curriculum
Cohen J & Cohen P (1975) Applied Multiple Regression/Correlation Analysis for the
Setting. VINE, 123(1): 11–16.


168


Stevenson C (1944) Ethics and Language. New Haven CT, Yale University Press.
Thorndike EL (1911) Animal Intelligence. New York, Macmillan.

171


Appendix 1

The extant research in the area of IS security behavior in an organizational context is focused on three research areas: (1) models on computer misuse/abuse, (2) models on compliance with IS security procedures, and (3) studies of appropriate IS security behavior. All three of these research streams offer understanding as to why employees comply with the IS security procedures in an organizational context based on an empirical research. In Table 15, research articles are introduced in more detailed explicating the purpose of research, theoretical background, methods, and the main results.

Table 15. Previous research on employees’ IS security behavior.

<table>
<thead>
<tr>
<th>Authors</th>
<th>Purpose of research</th>
<th>Theoretical background</th>
<th>Methods</th>
<th>Main Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Straub (1990)</td>
<td>Investigates if computer abuse in terms of number of incidents, monetary losses, and seriousness of a breach can be lowered through deterrent certainty (qualities of IS security staff/work), deterrent severity (disciplinary actions and availability of information about penalties and acceptable system use), use of preventives (number of operating system and database, security software), motivational factors (qualities of an offender), and environmental factors (tightness and visibility of security)</td>
<td>Theory of general deterrence</td>
<td>Data collection: Survey questionnaire for information technology professionals (N = 1211)</td>
<td>1) Certainty and severity of IS security deterrents (weekly hours dedicated to data security and security, existence and multiple sources of information about penalties and acceptable system usage) and preventives in terms of using security software reduce computer abuse</td>
</tr>
<tr>
<td>Authors</td>
<td>Purpose of research</td>
<td>Theoretical background</td>
<td>Methods</td>
<td>Main Results</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Harrington (1996)</td>
<td>Investigates the deterrent influence of organizations' written ethical statements (IS specific and generic), and proclivity to responsibility denial on employees' computer abuse judgments and intentions (i.e., intentional misuse of IS in terms of virus, fraud, sabotage, software copying, and cracking)</td>
<td>Literature on codes of ethics, ethical decision making, deterrence, and denial of responsibility</td>
<td>Data collection: A scenario-based questionnaire including potential rationalizations for the computer abuses, and Schwartz's Responsibility Denial scale for employees in nine organizations (N = 219)</td>
<td>1) Generic ethical statements improve virus, fraud, and sabotage-related computer abuse judgments and intentions of employees who tend to deny responsibility 2) IS specific ethical statements have an effect on sabotage judgments and intentions 3) Responsibility denial is related to all studied computer abuse judgments and intentions: virus, fraud, sabotage, software copying, and cracking</td>
</tr>
<tr>
<td>Authors</td>
<td>Purpose of research</td>
<td>Theoretical background</td>
<td>Methods</td>
<td>Main Results</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Lee, Lee, &amp; Yoo (2004)</td>
<td>Develop and empirically validate a model for explaining and preventing employees' defence and control intentions (i.e., to installing access control and intrusion protection software, controlling others' identification, and illegal software use) related to computer abuse frequency (e.g., data loss, illegal software copying, virus infection, hacking) through organizational trust (attachment, commitment, involvement, and norms) and general deterrence (IS security procedure, security awareness, and physical security system)</td>
<td>Social control theory, general deterrence theory, theory of planned behavior (Ajzen 1991), and theory of reasoned action (Ajzen, &amp; Fishbein 1980; Fishbein &amp; Ajzen 1975)</td>
<td>1) Data collection: Survey questionnaires for MBA students and managers in six companies (N = 182)</td>
<td>1) From the general deterrence factors, the physical security system predicts employees' defence intention (e.g., to install protective software) more than IS security procedure and awareness</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2) Data analysis: standardized path coefficients and t-values</td>
<td>2) High defence intention (to install protective software) predicts the high rate of computer abuse</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3) From the organizational thrust factors, involvement in terms of meetings participation, personal relationship, and loyalty, as well as norms, affect employees' intention to control others identification and illegal software use</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4) Intention to control others decreases insiders' computer abuse</td>
</tr>
<tr>
<td>Authors</td>
<td>Purpose of research</td>
<td>Theoretical background</td>
<td>Methods</td>
<td>Main Results</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>D'Arcy, Hovav, &amp; Galletta (2008)</td>
<td>Develop and empirically validate a model for explaining the relationship between security countermeasures, sanction perceptions, and IS misuse intentions for understanding, how to reduce employees' intentional IS misuse in organizations.</td>
<td>General deterrence theory</td>
<td>1) Data collection: Survey based on misuse scenarios for employees of eight companies (N = 269)</td>
<td>1) Employees’ awareness of security procedures, security education, training, and awareness (SETA) programs, and computer monitoring deter IS misuse.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2) Data analysis: Partial Least Squares Structural Model Analysis</td>
<td>2) Perceived severity of sanctions is more effective in reducing IS misuse than certainty of sanctions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3) The impact of sanction perceptions vary based on the individual's morality level.</td>
</tr>
<tr>
<td>D'Arcy &amp; Hovav (2007)</td>
<td>Examine the relationship between employees’ misuse intentions (password sharing, inappropriate use of e-mail, software piracy, unauthorized access and modification to company data) and awareness of security countermeasures (IS security procedures, security awareness program, computer monitoring, preventive security software)</td>
<td>-</td>
<td>Data collection: Scenario-based survey for employees and university students (N = 579)</td>
<td>1) Security awareness programs, awareness of IS security procedures, and preventive security software, respectively, reduce IS misuse intentions</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Data analysis: Regression analysis</td>
<td>2) Employees’ awareness of computer monitoring does not appear to reduce IS misuse intentions</td>
</tr>
<tr>
<td>Authors</td>
<td>Purpose of research</td>
<td>Theoretical background</td>
<td>Methods</td>
<td>Main Results</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Pahnila, Siponen, & Mahmood (2007) | Develop and empirically validate a model for explaining employees’ attitudes, intentions, and actual compliance with IS security procedures | General deterrence theory, protection motivation theory, the theory of reasoned action, information systems success, behavioral framework (Triandis 1979), and rewards | Data collection: Survey questionnaire for employees of a company (N = 245)  Data analysis: Factor analysis | 1) Actual compliance with IS security procedures: - is influenced by the perceived characteristics of IS security procedures (information quality) - is influenced by intention to comply - is not influenced by rewards  
2) Intentions to comply with IS security procedures: - are influenced by attitudes towards complying, expectations of others (normative beliefs) and habits - are not influenced by sanctions  
3) Attitudes towards compliance with IS security procedures: - are influenced by threat perceptions (threat appraisal) and organizational and technical support (facilitating conditions) - are not influenced by perceived effects and abilities on compliance with IS security procedures (coping appraisal) |
<table>
<thead>
<tr>
<th>Authors</th>
<th>Purpose of research</th>
<th>Theoretical background</th>
<th>Methods</th>
<th>Main Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Siponen, Pahnila, &amp; Mahmood</td>
<td>Advances a model that explains employees’ intentional and actual compliance with IS security procedures</td>
<td>Protection motivation theory</td>
<td>Data collection: Model testing through survey for employees of five organization (N = 919)</td>
<td>1) Preceding factors (visibility, normative beliefs) have significant effect on threat appraisal (perceived vulnerability and severity), and coping appraisal (self-efficacy, response efficacy) 2) Threat appraisal have significant effect on intention to comply 3) Intention to comply has significant effect on actual compliance</td>
</tr>
<tr>
<td>(2006)</td>
<td></td>
<td></td>
<td>Data analysis: Factor analysis and principal component extraction method</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Siponen, Pahnila, &amp; Mahmood</td>
<td>Develop and empirically validate a model that explains employees’ intentional and actual compliance with IS security procedures</td>
<td>Protection motivation theory</td>
<td>Data collection: Survey questionnaire for employees of four organizations (N = 917)</td>
<td>1) Intention to comply with IS security procedures is influenced by threat awareness (threat appraisal), perceived effects and abilities on compliance with IS security procedures (response efficacy and self-efficacy) 2) Actual compliance with IS security procedures: - is influenced by sanctions (legal sanctions and social pressure with relation to top-management, immediate supervisors, peers, and information security staff) and intention to comply with IS security procedures</td>
</tr>
<tr>
<td>(2007)</td>
<td></td>
<td></td>
<td>Data analysis: Structural equation modeling</td>
<td></td>
</tr>
<tr>
<td>Authors</td>
<td>Purpose of research</td>
<td>Theoretical background</td>
<td>Methods</td>
<td>Main Results</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Herath & Rao     | Develop and empirically test a model explaining employees’ intentions IS security policy compliance, attitudes towards IS security policies and security breach concerns | Protection-motivation theory, general deterrence theory, organizational commitment, theory of planned behavior, and decomposed theory of planned behavior (Taylor-Todd 1995) | Data collection: Survey questionnaire (N = 312) for employees in 78 organizations Data analysis: Partial Least Square for measurement validation and to test the structural model | 1) Attitudes towards IS security policies are:  
- positively influenced by high security breach concerns and perceptions of response efficacy and self-efficacy  
- negatively influenced by high response costs perceptions  
2) Intention to comply with IS security policies:  
- is positively influenced by organisational commitment, others’ behavior and expectations (subjective and descriptive norms), certainty of detection, severity of penalty, and response perception (self-efficacy)  
- is not positively influenced by attitudes toward IS security policies  
3) Security breach concerns are positively influenced by perceived severity, but not perceived probability  
4) Response perceptions:  
- availability of recourses increases self-efficacy  
- organizational commitment increases response efficacy  

181
<table>
<thead>
<tr>
<th>Authors</th>
<th>Purpose of research</th>
<th>Theoretical background</th>
<th>Methods</th>
<th>Main Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Johnston &amp; Warkentin</td>
<td>Examine the influence of fear appeals on behavioral intentions to comply with recommended computer security actions with respect to spyware</td>
<td>Protection motivation theory (Rogers 1975)</td>
<td>Data collection: Survey instrument with experimental research design for university employees and students (N = 311)</td>
<td>1) Fear appeals have an influence on end-users’ behavioral intentions to comply with recommended computing practices 2) The influence is affected by individual respondents’ perceptions of self-efficacy, response efficacy, threat severity, and social influence</td>
</tr>
<tr>
<td>Ng, Kankanhalli, &amp; Xu</td>
<td>Validate a model that explains users’ computer security behavior related with e-mail use.</td>
<td>Health belief model</td>
<td>Data collection: Survey questionnaire for employees of three IT organizations and part-time (working) students of a university (N = 134)</td>
<td>- Perceived susceptibility, perceived benefits, and self-efficacy are determinants of e-mail-related security behavior - perceived severity moderates the effects of perceived benefits, general security orientation, cues to action, and self-efficacy on IS security behavior</td>
</tr>
<tr>
<td>Herath &amp; Rao (2009b)</td>
<td>Develop and test theoretical model for understanding employees’ intentional compliance with IS security procedures</td>
<td>Literature in agency theory</td>
<td>Data collection: Survey for employees from 77 organizations (N = 312)</td>
<td>Security behavior intentions are influenced by intrinsic and extrinsic motivators - Subjective norms and peer behaviors - Perceived effectiveness of own actions - Certainty of detection - Severity of punishment was not found to have an effect</td>
</tr>
<tr>
<td>Authors</td>
<td>Purpose of research</td>
<td>Theoretical background</td>
<td>Methods</td>
<td>Main Results</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------------------------------------------------------------</td>
<td>-----------------------------------------</td>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Li, Zhang, &amp; Sarathy (2010)</td>
<td>Examine the influence of cost-benefit assessment, personal norms, and organizational context on employees’ intention to comply with Internet use procedure</td>
<td>Rational choice theory</td>
<td>Data collection: Online survey for online panel consisting of organizational employees (N = 246)</td>
<td>- Employees’ intention to comply with Internet procedure is influenced by perceived benefits, personal norms and perceived security risks</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Data analysis: Partial least squares analysis (PLS)</td>
<td>- The influence of sanction severity is moderated by personal norms</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Organizational norms and organizational identification have an influence on personal norms</td>
</tr>
<tr>
<td>Myyry, Siponen, Pahnila, Vartiainen, &amp; Vance (2009)</td>
<td>Examine the influence of moral reasoning on hypothetical and actual compliance with IS security procedures, and propose a theoretical model that explains non-compliance in terms of moral reasoning and values in the situations where a password is shared with co-workers.</td>
<td>Theories of moral reasoning: Theory of cognitive moral development (Kohlberg 1969), and the theory of motivational types of values (Schwartz 1992)</td>
<td>Data collection: Questionnaire for employees of an organization and part-time students (with work experience) based on hypothetical scenario method (N = 163)</td>
<td>- Preconventional moral reasoning (fear of sanctions, what’s in it for me-thinking) is positively related to both hypothetical and actual compliance with the IS security procedure.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Data analysis: Multivariate regression analysis</td>
<td>- Openness to change (following their own intellectual and emotional interests) is negatively related to both hypothetical and actual compliance with the IS security procedure.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Hypothetical and actual behavioral choices are very significantly related to each other, at least in the case of giving one’s password to others.</td>
</tr>
<tr>
<td>Authors</td>
<td>Purpose of research</td>
<td>Theoretical background</td>
<td>Methods</td>
<td>Main Results</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Bulgurcu, Cavusogly, G Benbasat (2010a) | Identification of the antecedents of employees' attitudes and intention to comply with IS security procedures (ISP) | Theory of planned behavior                   | Data collection: A Web-based questionnaire survey for employees' (N = 464)                        | - Intention to comply with ISP is influenced by attitude, normative beliefs, and self-efficacy  
- Outcome beliefs  
- Data analysis: Structural equation modeling, and component-based partial least squares (PLS)  
- Intention to comply with ISP is influenced by attitude, normative beliefs, and self-efficacy  
- Outcome beliefs  
- Data analysis: Structural equation modeling, and component-based partial least squares (PLS)  
- Intention to comply with ISP is influenced by attitude, normative beliefs, and self-efficacy  
- Outcome beliefs  
- Data analysis: Structural equation modeling, and component-based partial least squares (PLS) |
| Bulgurcu, Cavusoglu, & Benbasat (2010b) | Investigate the influence on features of IS security procedures (ISP) on employees' security compliance in terms of intention to comply and current compliance in the workplace | The group engagement model, literature showing the link between quality and behavioral intention | Data collection: Online survey for employees (N = 464)                                            | - ISP fairness (i.e., employees' belief in the justice of the IS security rules) has an influence on employees' compliance  
- ISP quality (clarity, completeness, and consistency) has an influence on employees' compliance and perceived ISP fairness |
<table>
<thead>
<tr>
<th>Authors</th>
<th>Purpose of research</th>
<th>Theoretical background</th>
<th>Methods</th>
<th>Main Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chan, Woon, &amp; Kankanhalli (2005)</td>
<td>Develop and examine theoretical model explaining the effects of social contextual factors on employees’ compliance with organizational security policies</td>
<td>Safety climate literature, the social information processing approach</td>
<td>Data collection: Survey instrument for employees of two IT intensive organizations (N = 140)</td>
<td>- Management practices, supervisory practices, and co-worker’s socialization are positively related to employees’ perceptions of the information security climate</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Data analysis: Structural equation modeling</td>
<td>- Perceptions of security climate and self-efficacy have positive impacts on compliant behavior</td>
</tr>
<tr>
<td>Authors</td>
<td>Purpose of research</td>
<td>Theoretical background</td>
<td>Methods</td>
<td>Main Results</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Siponen &amp; Vance (2010)</td>
<td>Develop and empirically validate a model for explaining employees’ intention to violate organizations’ IS security procedures through neutralization techniques and deterrents</td>
<td>Neutralization theory (Sykes &amp; Matza 1957) and Deterrence theory (Paternoster &amp; Simpson 1996)</td>
<td>1) Data collection: Survey based on hypothetical scenario method (Weber 1992) for employees of a university and two organization (N = 1449) 2) Data analysis: Partial least squares using SmartPLS (Ringle et al., 2005), structural equation modeling technique (MacKenzie et al., 2005)</td>
<td>1) Neutralization explains employees’ intention to violate IS security procedures. This means that IS security procedures are violated if violation was viewed to be a) necessary action, b) an individual right based on past good performance, c) irrelevant to cause significant harm, IS security procedures were seen as e) unreasonable, f) in conflict to other work duties, or d) consequences of action were seen beyond one’s responsibilities and control 2) None of the deterrents: formal sanctions, informal sanctions, and shame, have an influence on intention to violate IS security procedures</td>
</tr>
<tr>
<td>Authors</td>
<td>Purpose of research</td>
<td>Theoretical background</td>
<td>Methods</td>
<td>Main Results</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>-------------------------</td>
<td>----------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Beautement, Sasse, &amp; Wonham (2008)</td>
<td>Propose a new approach for understanding and influencing employees' IS security behavior: The Compliance Budget</td>
<td>Research on usable security and economics of security</td>
<td>Data collection: Interviews with employees of two organizations (N = 17) Data analysis: Grounded theory</td>
<td>Employees' compliance with IS security procedures can be explained through the following: 1) The actual and anticipated costs and benefits for an employee and perceived costs to the organization - Increased physical load, increased cognitive load, embarrassment, missed opportunities, the hassle factor, avoiding the consequences of a security breach, protection from sanctions 2) External factors - system design, awareness, training, and education, the culture of the organization, monitoring, and sanctions</td>
</tr>
</tbody>
</table>
### 3. Research area: Studies on appropriate IS security behavior

<table>
<thead>
<tr>
<th>Authors</th>
<th>Purpose of research</th>
<th>Theoretical background</th>
<th>Methods</th>
<th>Main Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>D’Arcy &amp; Greene (2009)</td>
<td>Investigate the relationship between organizations’ security culture (managements’ support for information security and ongoing training and communication efforts) and employees’ IS security behavior (compliance with IS security procedures and voluntary IS security behavior)</td>
<td>Social exchange theory (Blau 1964; Chan et al. 2005)</td>
<td>Data collection: Surveys for computer using professionals in several organizations (N = 105) Data analysis: Partial least squares structural equation modeling technique</td>
<td>1) Top management commitment to security and security communication are key dimensions of a security culture 2) Security culture has an effect on employees’ compliance and voluntary security behavior</td>
</tr>
<tr>
<td>Hyeun-Suk, Young, &amp; Cheong-Tag (2005)</td>
<td>Explaining users’ IS security behavior through optimistic bias in their risk perception on information security and explicating the factors influencing the extent of the optimistic bias (perceived controllability and comparison target)</td>
<td>Social comparison theory (Festinger 1954), literature on psychology and information systems</td>
<td>Data collection: Survey questionnaire for university students with part- or full-time job (N = 248) Data analysis: an exploratory factor analysis, maximum likelihood method, an oblique rotation method</td>
<td>1) Users have an optimistic bias in their perception of vulnerability related to information security 2) Optimistic bias increases as social/psychological distance with a comparison target increases 3) Users show self-serving tendency in their perceptions of controllability related to information security 4) Self-serving bias increases a social/psychological distance with a comparison target increases 5) There is negative relationship between perceived controllability and risk perception</td>
</tr>
<tr>
<td>Authors</td>
<td>Purpose of research</td>
<td>Theoretical background</td>
<td>Methods</td>
<td>Main Results</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Dinev, Goo, Hu, &amp; Nam (2009)</td>
<td>Empirically validate a model of user behavior towards protective IT in terms of anti-spyware technology for cross-cultural comparison between South Korea (SK) and the United States (US)</td>
<td>Theory of planned behavior (Ajzen 1988; Ajzen, 2002), integrated model of user acceptance of e-commerce (Pavlou &amp; Fygenson 2006), and cultural dimensions and indices (Hofstede 1993)</td>
<td>Data collection: Surveys for IS professionals and student of two universities (N = 227) Data analysis: Equation modeling techniques and multi-group analysis</td>
<td>National cultural factors moderate the strength of most of the relationships in the behavioral model in the case of anti-spyware technology:&lt;br&gt;1) Relationship between subjective norm (social pressure) and behavioral intention is stronger in SK than in the US, which is explained through the high priority of group norms, high power distance, strong uncertainty avoidance, and weak masculinity&lt;br&gt;2) Relationship between technology awareness and both attitude toward behavior (ethics) and behavioral intention is weaker in SK than in the US, which is explained through high collectivism and low masculinity&lt;br&gt;3) There was no statistical difference in relationships between behavioral intention and both attitude towards behavior and perceived behavioral control</td>
</tr>
<tr>
<td>Authors</td>
<td>Purpose of research</td>
<td>Theoretical background</td>
<td>Methods</td>
<td>Main Results</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------------------------------------------------</td>
<td>------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Dinev &amp; Hu</td>
<td>Investigate users’ behavioral intentions towards using anti-spyware</td>
<td>Theory of planned behavior</td>
<td>Data collection: A survey for IS professionals and students of a university (N = 332) Data analysis: Structural equation modeling (SEM)</td>
<td>- Awareness of the threats’ influences on intention to use protective technologies - Subjective norm influences on behavioral intention to use protective technologies more in the case of advanced technology users compared to basic users - Perceived ease of use and computer self-efficacy do not have an influence on behavioral intentions</td>
</tr>
<tr>
<td>Authors</td>
<td>Purpose of research</td>
<td>Theoretical background</td>
<td>Methods</td>
<td>Main Results</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Stanton, Stam, Guzman, &amp; Caldera (2003)</td>
<td>Examine the influence of organizational commitment on IS security behavior including counterproductive computer usage (personal web surfing, e-mail, and gaming), password management practices (revealing password, writing password, password training), taking offered IS security training, discussing IS security procedures with co-workers and compliance with IS security procedures</td>
<td>- Data collection: interviews (N = 110) and survey questionnaire (N = 298) for IT users in organizations</td>
<td>- In the case of respondents’ views of co-workers’ IS security behavior, organizational commitment influence on writing password, password training, personal web surfing, personal e-mail, personal gaming, taking offered security training, and compliance with IS security procedures. - In the case of respondents’ views of their own behavior, organizational commitment influences on personal gaming, discussing IS security procedures with co-workers, and compliance with IS security procedures. - Organizational commitment was not attached to revealing passwords. - Respondents’ high level of organizational commitment was seen related with avoidance of using the company’s computers for personal web surfing, personal e-mail, and personal gaming - Employees’ low level of organizational commitment was seen related with high levels of compliance with IS security policies</td>
<td></td>
</tr>
<tr>
<td>Authors</td>
<td>Purpose of research</td>
<td>Theoretical background</td>
<td>Methods</td>
<td>Main Results</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Stanton, Stam, Mastrangelo, &amp; Jolton (2005)</td>
<td>Develop a taxonomy of employees' IS security behavior, and examine the impact of training, awareness, monitoring, and rewards on password-related behavior in terms of frequency of changing passwords, formulating passwords, writing down passwords, and sharing them with workgroup, in the company and outside the company</td>
<td>-</td>
<td>Data collection: Interviews (N = 110), a behavior rating exercise (N = 49), and survey (N = 1167) for IT professionals, managers, and employees</td>
<td>- Good password practices in terms of changing passwords frequently and formulating better passwords were related to training, awareness, monitoring and rewards, but not to sharing passwords. Simultaneously, the likelihood of writing down passwords increases</td>
</tr>
<tr>
<td>Sasse, Brostoff, &amp; Weirich (2001)</td>
<td>Investigate the reasons for undesirable user behavior</td>
<td>Research on human / computer interaction design approach</td>
<td>Data collection: Questionnaire for employees (N = 144), password reset logs, in-depth interviews for employees of a organization and PHD students of a university (N = 17)</td>
<td>Undesirable user behavior with passwords can be caused by failure to recognize the characteristics of human memory, unattainable or conflicting task demands, and lack of support, training, and motivation.</td>
</tr>
<tr>
<td>Adams &amp; Sasse (1999)</td>
<td>Explore the reasons for users' compromising of computer security mechanisms and ways to improve user behaviors</td>
<td>-</td>
<td>Data collection: A web-based questionnaire for employees of one organization (N = 139) and semi-structured in-depth interviews for employees from two organizations (N = 30)</td>
<td>Factors influencing effective password usage: - multiple passwords - password content - perceived compatibility with work practices - users' perceptions of organizational security and information sensitivity</td>
</tr>
</tbody>
</table>

Data analysis: Grounded theory
<table>
<thead>
<tr>
<th>Authors</th>
<th>Purpose of research</th>
<th>Theoretical background</th>
<th>Methods</th>
<th>Main Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Albrechtsen</td>
<td>Explore users’ experience of information security and their personal role in the information security work</td>
<td>-</td>
<td>Data collection: Qualitative interviews for the users at an IT company and a bank (N = 9)</td>
<td>(1) Users report to be motivated for information security work, but do not perform many individual security actions; (2) high information security workload creates a conflict of interest between functionality and information security; (3) documented requirements of expected information security behavior and general awareness campaigns have little effect alone on user behavior and awareness; and (4) the users consider a user-involving approach to be much more effective for influencing user awareness and behavior.</td>
</tr>
</tbody>
</table>


Appendix 2

This appendix 2 includes a list of 59 open codes generated from interview transcripts. A list includes also original open codes (sub-codes inside 59 open codes) that were merged into a single more general one. Of these 59 open codes, 18 explained both compliant and non-compliant IS security behavior, referred to (+/-). In turn, 23 open codes explained only non-compliance, referred to (-), and 18 compliance only, referred to (+).

1. INCONVENIENCE (-)
   - Restrictiveness
   - Difficulty
   - Time-consuming
   - Memorability

2. MISTAKES (-)

3. TRUSTFULNESS/HONESTY/LOYALTY/SINCERITY (+/-)

4. ACTIVITY ON IS SECURITY ISSUES (+/-)

5. WORK EXPERIENCE (+/-)

6. EXPERIENCING IS SECURITY ACCIDENTS (+)

7. IS SECURITY THREATS (+/-)
   - Information leak
   - General threat awareness
   - Threats of the Internet
   - Technical / physical threats / necessity

8. BIASED TRUSTING OF TECHNICAL SECURITY (-)
   - Secured servers
   - Access rights
   - Firewalls
   - Virus protection software

9. COMMON SENSE (+)

10. FALSE TRUST FOR IS SECURITY PROCEDURES (-)

11. RAPID CHANGE OF THE WORK ENVIRONMENT (-)

12. HURRY/WORKLOAD/STRESS (-)

13. ATTENDING TO INTERRUPTIONS (-)

14. INABILITY TO SAY NO (-)
15. SENSE OF DUTY/RESPONSIBILITY (+)
16. THE VALUE OF INFORMATION (+)
   - The valuable property of the company
   - Competitiveness
   - Personal work
   - Personal data
   - Confidential data
17. IS AS A PART OF HABITUAL BEHAVIOR (+)
18. MOTIVES TO HARM THE COMPANY (-)
19. INTENTIONAL ABUSE /PERSONAL BENEFIT (-)
20. AUTHORITY (+)
21. ROLE MODEL (+/-)
22. INVOLVEMENT (+)
23. PASSWORD SELECTION (+/-)
24. SOCIAL CONFORMITY (+/-)
25. INTERNET AND EMAIL USE (+/-)
26. EXPERIENCING FEAR (-)
27. AVOIDING EMBARRASSMENT (+)
28. POLICY OBEDIENCE (+)
   - Policy /guidelines /rules /instructions obedience
   - Agreement / contract obedience
29. MONITORING /CONTROL (+/-)
   - Electronic monitoring
   - Managerial monitoring
   - Unspecified monitoring
   - Lack of monitoring /control
30. FORCE/TECHNICAL RESTRICTIONS (+/-)
   - Installations
   - Passwords changing
   - Internet browsing
   - Email encryption
31. PUNISHMENTS (+)
   - Termination

195
– Warning letter
– Talking-to
– Reducing salary
– Stopping a bad habit
– Showing the consequences of actions
– Feeling of personal accountability

32. RESPONSIBILITY DENIAL (-)
33. COMPANY’S CULTURE (+/-)
34. TRUST FOR OTHER PEOPLE (-)
35. REWARDS (+)
– Good motivation
– Profitable regulations
– Public praise
– Increase happiness
– Increase responsibility
– Money /bonus / allowance
– Gifts

36. ORAL COMMUNICATION (+)
– Personal coaching
– Managements’ requests and explanations
– Formal discussions with management
– Informal discussion with co-workers
– Training
– Reminders

37. CAREFULNESS/CARELESSNESS (+/-)
38. LANGUAGE (-)
39. RELIGION (+)
40. MAINTAINING GOOD RELATIONSHIPS (-)
41. WILLINGNESS TO HELP (-)
42. LACK OF THRUST FOR IS SECURITY PROCEDURES (-)
43. BAD HABITS (-)
44. AUTOMATIC / CONVENIENT IS SECURITY PRACTICES (+)
45. WRITING DOWN PASSWORDS (-)
46. LOGGING OUT THE WORKSTATION (+/-)
47. GUIDELINES FOR RECOVERY (+/-)
48. GUIDELINES FOR PREVENTION (+/-)
49. POLICIES/RULES/INSTRUCTIONS (+/-)
50. UPBRINGING (+)
51. IS AS A PART OF PROFESSION (+)
   – Individual level
   – Team level
   – Department level
52. TRUST FOR WORK ENVIRONMENT (-)
53. AVOIDING FEELINGS OF INEQUALITY (+)
54. QUALITY OF IS SECURITY PROCEDURES (+/-)
   – Sufficiency
   – Clarity
   – Adjustment
55. CURIOSITY (-)
56. LACK OF COURAGE/WILL TO CONTROL (-)
57. LAZINESS (-)
58. SELF-DICIIPLINE (+)
59. HABITS OT THE COUNTRY (+/-)
Appendix 3

The main idea of the theoretical framework explaining employees’ IS security behavior in section 3.4 is that formative elements (A), through their subcategories, sometimes have an influence on employees’ IS security behavior (i.e., behavioral contingencies (B)), and this causal pattern can be explained through employees’ individual thinking (i.e., cognitive mechanisms (M)). The formative elements combine three main categories described in sections 3.3.2–3.3.4: cultural dimensions (i.e., cultural mentality and company’s culture), organizational dimensions (e.g., communications, extrinsic control), and experience-based dimensions (e.g., IS security accidents, and work experience). The connections between formative elements and cognitive mechanisms are not presented in detail in the theoretical framework because the emphasis in the framework is to show that different cognitive mechanisms lead to different behavioral contingencies. However, the connections between formative elements and cognitive mechanisms are elaborated on and illustrated in section 3.3 and graphically presented in this Appendix 3.

First, the connections between cultural formative elements (i.e., cultural dimensions) and cognitive mechanisms elaborated on in section 3.3.2 are presented in Figure 5. Cultural dimensions include the impact of cultural mentality and the company’s culture on employees’ thinking on IS security in their work. These dimensions explain employees’ IS security behavior through rational IS security dimensions, and IS security detached dimensions as shown in Figure 5. In addition, cultural mentality influences the nature of a company’s culture (see section 3.3.2), and also explains the success of applying organizational dimensions in terms of extrinsic control (see section 3.3.4).
Second, the connections between experience-based formative elements (i.e., experience-based dimensions) and cognitive mechanisms elaborated on in section 3.3.3 are presented in Figure 6. Experience-based dimensions include the impact of IS security accidents, and work experience on employees’ thinking towards IS security in their work. These dimensions explain employees’ IS security behavior through rational IS security dimensions, and unconscious IS security dimensions as shown in Figure 6.
Third, the connections between organizational formative elements (*i.e.*, organizational dimensions) and cognitive mechanisms elaborated on in section 3.3.4 are presented in Figure 7. Organizational dimensions include the impact of communications (*i.e.*, the quality of IS security procedures, oral communications, training, reminders, management’s role model, and involvement), and extrinsic control (*i.e.*, monitoring, rewards, punishments, and coercion) on employees’ thinking towards IS security in their work. These dimensions explain employees’ IS security behavior through rational IS security dimensions, IS security detached dimensions, and unconscious IS security dimensions as shown in Figure 7. In addition, cultural dimensions explain the success of applying organizational dimensions.
Fig. 7. The connections between organizational formative elements and cognitive mechanisms.

564. Karppinen, Katja (2010) Biosynthesis of hypericins and hyperforins in Hypericum perforatum L. (St. John’s wort) – precursors and genes involved

565. Louhi, Pauliina (2010) Responses of brown trout and benthic invertebrates to catchment-scale disturbance and in-stream restoration measures in boreal river systems

566. Hekkala, Ritta (2011) The many facets of an inter-organisational information system project as perceived by the actors

567. Niittyvuopio, Anne (2011) Adaptation to northern conditions at flowering time genes in Arabidopsis lyrata and Arabidopsis thaliana


570. Kaartinen, Salla (2011) Space use and habitat selection of the wolf (Canis lupus) in human-altered environment in Finland


574. Petsalo, Aleksandri (2011) Development of LC/MS techniques for plant and drug metabolism studies

575. Leppälä, Mirva (2011) Successional changes in vegetation and carbon dynamics during boreal mire development


577. Alahuhta, Janne (2011) Patterns of aquatic macrophytes in the boreal region: implications for spatial scale issues and ecological assessment

578. Moody, Gregory (2011) A multi-theoretical perspective on IS security behaviors

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

IMPROVING EMPLOYEES’ INFORMATION SYSTEMS (IS) SECURITY BEHAVIOR

TOWARD A META-THEORY OF IS SECURITY TRAINING AND A NEW FRAMEWORK FOR UNDERSTANDING EMPLOYEES’ IS SECURITY BEHAVIOR