Information Security Management and Employees' Security Awareness: An Analysis of Behavioral Determinants

Von der Wirtschaftswissenschaftlichen Fakultät der

Gottfried Wilhelm Leibniz Universität Hannover

zur Erlangung des akademischen Grades

Doktor der Wirtschaftswissenschaften

- Doktor rerum politicarum –

genehmigte Dissertation

von

Diplom-Ökonom Jörg Uffen

geboren am 16. April 1983 in Aurich

2014

Betreuer und Gutachter:	Prof. Dr. Michael H. Breitner
Weiterer Gutachter:	Prof. Dr. Stefan Wielenberg
Vorsitzender der Prüfungskommission:	Jun.-Prof. Dr. Hans-Jörg von Mettenheim
Weiteres Mitglied (beratend):	Dr. Ute Lohse
Tag der Promotion:	19. Dezember 2013

Meiner Familie.

I. Abstract/ Abstrakt

Organizations and companies are heavily reliant on information systems (IS) to carry out their business strategies and processes. This leads to an emerging discussion on how to increase information security and assure security-compliant behavior. This cumulative doctoral thesis is rooted in the investigation of behavioral aspects within an information security context. Since the human factor is still seen as the weakest link in the entire information security environment, this thesis takes behavioral aspects of two perspectives into account – the management level represented through information security executives and the employee level represented through end-users. Regarding both perspectives, the following research objectives have been determined:

A. Determination of attitudes towards holistic information security management (ISM) by examining information security executives' personality traits (Part A)
B. Development and implementation of an organization specific needs assessment process model for SETA programs based on end-user's actual behavior (Part B)

To address these research objectives, this thesis makes use of both IS research paradigms, behavioral science and design science, by applying different research methods. This thesis relies on the application of various models from different research disciplines in order to identify, explain and predict individual's behavior in the context of information security. The investigation of the research objectives from the two perspectives allows an active interaction between research and practice. The research results are summarized in four research papers regarding the management level and three research papers regarding employees' or end-users' security awareness and behavioral compliance.

Keywords: Information Security, Personality Traits, Holistic ISM, Security Awareness, Information Security Policy, Compliant Behavior, TPB, Theory of Planned Behavior, Action Design Research, Process Model

Durch die zunehmende Integration von Kunden, Lieferanten und Partnern in die Geschäftsprozesse und Strategien von Unternehmen und Organisationen, werden die Informationssysteme zunehmend komplexer und somit risikobehafteter. Dies führt zu einer Diskussion, wie die Informationssicherheit gesteigert und sicherheitsrelevantes Verhalten generiert und aufrecht gehalten werden kann. Die vorliegende kumulative Dissertation hat ihre Wurzeln in den Verhaltenswissenschaftlichen Ansätzen im Kontext der Informationssicherheit. Da der Faktor Mensch nach wie vor als das schwächste Glied im Informationssicherheitsumfeld gesehen wird, greift die vorliegende Arbeit verschiedene Verhaltensaspekte aus zweierlei Perspektiven auf – die Management Ebene repräsentiert durch die Zielgruppe der IT-Sicherheitsführungskräfte und die Mitarbeiter- bzw. Endanwenderebene. Hieraus wurden folgende Forschungsziele entwickelt:

A. Determinierung der Einstellungskomponenten gegenüber eines ganzheitlichem Informationssicherheitsmanagementsystems durch die Betrachtung der individuellen Unterschiede von IT-Sicherheitsführungskräften (Teil A)
B. Entwicklung und Umsetzung eines untenehmensspezifischen Bedarfsanalyse-Prozessmodells für SETA-Programme auf Basis des tatsächlichen Verhaltens der Endanwender (Teil B).

Zur Erreichung dieser Forschungsziele wurden verschiedene wissenschaftliche Ansätze aus beiden Forschungsparadigmen der Wirtschaftsinformatik, Behavioral Science und Design Science Research, angewandt. Die Arbeit stützt sich auf die Anwendung verschiedener Modelle aus interdisziplinären Forschungsdisziplinen, um das Verhalten im Rahmen der Informationssicherheit erklären und vorhersagen zu können. Die aufgeführten Ergebnisse stammen aus Forschungsbeiträgen zu den Perspektiven der Management Ebene (vier Publikationen) sowie der Endanwender Ebene (drei Publikationen).

Schlagworte: Informationssicherheit, Persönlichkeitsmerkmale, ganzheitliches Informationssicherheitsmanagement, Sicherheitsbewusstsein, Informationssicherheitspolicy, sicherheitsrelevantes Verhalten, Theorie des geplanten Verhaltens, konstrultionsorientierte Aktionsforschung, Prozessmodell

II. Management summary

Problem formulation and research objectives

Organizations and companies are heavily reliant on information systems (IS) to carry out their business strategies and processes. The extent of the organizational IS environment is for example driven by globalization, increasing customer and supplier expectations, rapidly changing technology and the pressure to increase the efficiency. Due to that dependency, IS researchers emphasized management's increasing concern about the protection of organizational information assets (Straub and Welke, 1998; Taylor, 2006). Empirical studies noted an increasing number of security incidents (e.g. KPMG e-Crime Report 2011) even as organizations and companies invest more and more in security-related solutions. The proliferation of complex, sophisticated and multinational information security risks lead into major challenges for information security management (ISM). Security incidents can have dire consequences, including loss of prestige and credibility, corporate liability, and monetary damage (Bulgurcu et al., 2010). As a result, ISM that depends on the management of technology, processes and people has been established as an integrated organizational IS function.

In information security literature, researchers are in consent that information security is obtained by ensuring the semantic dimensions comprising the confidentiality, integrity and availability (CIA) of information (see e.g. Eloff and Eloff, 2005; Saleh et al., 2006; Torres et al., 2006). In detail, confidentiality represents the prevention of unauthorized disclosure; integrity ensures that information cannot be modified by unauthorized individuals; and availability makes sure that information are available to authorized individuals when needed (Siponen and Oinas-Kukkonen, 2007). But implementing air-tight security technologies without focusing other dimensions of information security is neither attainable nor efficient. Organizations and companies need to reconsider their risk strategies and reassess how to establish efficient and sustainable protection of their information assets. These information security objectives can be achieved when focusing on both – the technical and socio-organizational resources (Bulgurucu et al., 2010).

Since the human factor has been shown to be the weakest link in the entire information security environment (Bulgurucu et al., 2010; Hu et al., 2008), recent studies focus the human challenge from different perspectives: end-users/ employees, information security managers/ executives, or senior managers/ board members (Ashenden, 2008). For example, from an end-user perspective, D'Arcy et al. (2009) demonstrated that information security policies, security education, training and awareness (SETA) programs, and monitoring activities have a deterrent effect on the behavioral intention (BI) to misuse IS, while Johnston and Warkentin (2010) showed that fear appeals significantly impact BI to comply with information security, but the impact is not uniform to all kind of end-users. From information security executives perspective, Karahanna and Watson (2006) pointed out, IS leadership requires a complex mix of competencies and traits to successfully manage an IS environment; and from a higher management level focus, there is evidence that management´s sensitivity towards security activities and advanced security software are associated with higher perceived information security effectiveness (Straub and Welke 1998; Krankanhalli et al. 2003). In order to explain and predict a specific security-related behavior, these studies implicate that the human challenge in information security needs to be focused by including the individual’s unique behavioral facets such as attitudes, beliefs, perceptions, and other cognitive processes.

This cumulative doctoral thesis focuses on the investigation of behavioral factors, cognitive processes and the roots of both within the information security context. The human factor is regarded from two perspectives – the employee or end-user perspective (hereafter end-user) and the IS management level represented by information security executives. Regarding both perspectives, this thesis follows two main research objectives:

- Determination of attitudes towards holistic ISM by examining information security executives’ personality traits (Part A)
- Development and implementation of an organization specific needs assessment process model for SETA programs based on end-user’s actual behavior (Part B)

Summarized publications within this thesis

This cumulative doctoral thesis consists of two independent parts. In part A four research papers are summarized that contribute to the above mentioned research area from information security executives’ perspective. These research papers are building upon one another. The following topics and publications are addressed within part A of this thesis:

- Determination of a holistic ISM approach; published in the proceedings of the Multikonferenz Wirtschaftsinformatik (MKWI) 2012,
- Explanation of the influence of personality traits on attitudes towards holistic ISM; published in the proceedings of the International Conference on Information Systems (ICIS) 2012,
- Demonstration of the complexity of the relationship between personality traits and attitudes; published in the proceedings of the Hawaii Conference on System Science (HICSS) and in the International Journal of Social and Organizational Dynamics in Information Technology (IJSODIT) 2013.

In part B three research papers are summarized that address the above mentioned research area from end-user perspective:

- Determination of the state of the art in security awareness and compliant behavior literature; published in the proceedings of the Hawaii Conference on System Science (HICSS) 2013 and accepted for publication in the international IS journal “Management Research Review” 2014.

- Development and evaluation of a needs assessment process model for SETA programs; published in the proceedings of the European Conference on Information Systems (ECIS) 2013.

Research background and methodological overview

Hevner et al. (2004) have shown that IS research "is the scientific analysis of the interplay of people, organizations, and technology (Silver et al., 1995) and therefore contributes to and relies on various disciplines such as organizational theory, management sciences, cognitive sciences, and computer sciences". To address the above mentioned research objectives, this thesis makes use of both IS research paradigms, behavioral science and design science (see e.g. Hevner et al., 2004). The main focus of this thesis lies in the former.

In part A, behavioral models from interdisciplinary areas are applied in order to explain and predict target individuals behavior. While researchers focused behavioral, educational and psychological approaches of IS and executives, only few studies combined these approaches to an integrated model. More in detail, the purpose of part A in this thesis is to investigate how individual differences between information security executives are related to holistic ISM within organizations and companies. Holistic ISM is measured by an information security executive's beliefs or attitudes towards information security. These attitudinal constructs are rooted in the Theory of Planned Behavior (TPB) as proposed by Ajzen (1991) (Figure 1).

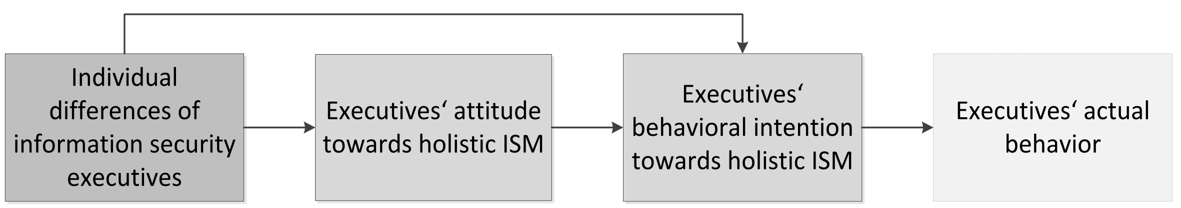

Individual differences of information security executives
Executives' attitude towards holistic ISM
Executives' behavioral intention towards holistic ISM
Executives' actual behavior

Figure 1: General research model part A

The first summarized publication (Uffen et al., 2012a) starts with the presentation of a comprehensive literature review that aims to identify academic publications in the topic of holistic, multidimensional information security management approaches. A lack of generally accepted models or frameworks with coherent information security dimensions or labels were found (Kritzinger and Smith, 2008; May and Dhillon, 2010). Based on a qualitative content analysis and a consolidation process as well as the testing of empirical data using principle component analysis (PCA), seven broad dimensions of holistic ISM were picked out and discussed. These are labeled to the technical, human, organizational, economic, strategic, cultural, and compliance dimension of information security. The way an information security executive considers and valuates each dimension of holistic ISM depends on individual differences in personality. This was the main topic of the second publications (Uffen et al., 2012b). Individual differences are measured by applying the Five Factor Model (FFM) with the personality constructs of conscientiousness, openness, neuroticism, agreeableness and extraversion (Costa and McCrae, 1991). Since a (behavioral) theory defines constructs, specifies the research domain, explains and predicts internally consistent relationships (Wacker, 1998), hypotheses were developed to relate personality traits to attitude towards holistic ISM. Hypotheses rely on assumptions derived from existing research results and considered theories that can be empirically tested (Weiber and Mühlhaus, 2010). The resulting integrated research model was tested with empirical data from 174 information security executives. As underlying data analyzing technique, structural equation modeling (SEM) was applied, without and in a second (and third) study (Uffen et al., 2013a; Uffen et al., 2013b) including the influence of potential moderators and control variables. Variance-based partial least squares (PLS) was applied as the underlying SEM technique, because the emphasis lies on theory development, prediction of latent constructs and identify relationships between them (Reinartz et al., 2009).

In part B, since researchers and practitioners realized that end-users are one of the weakest link in information security (Bulgurucu et al., 2010), the discussion about how to implement efficient SETA programs have become more and more important. The purpose of part B in this thesis is to develop and test a needs assessment process model for SETA programs that is based on end-users actual behavior. Researchers incorporated multidisciplinary behavioral theories, including theories from psychology, pedagogy and criminology, into integrated behavioral information security models (Karjaleinen and Siponen, 2011) in order to increase security awareness and assure security-compliant behavior. To comprehensively identify applied behavioral theories in the research area of end-users' information security awareness and behavioral compliance within the past decade, a structured literature review was conducted (see Lebek et al., 2013a; Lebek et al., 2014). Based on 113 publications, the four mainly applied behavioral theories, namely TPB, protection motivation theory (PMT), general deterrence theory (GDT) and technology acceptance model (TAM) were analyzed on the basis of the number of constructs, their relationships, and the statistical significance level. A lack of actual behavior measurement and general procedure models addressing SETA programs were identified. According to Roseman and Vessey (2008), research should provide relevance for practitioners in order to prevent research from becoming an end unto it-self. To fulfill this requirement the third summarized publication in this part deals with the development of a process model for a needs assessment of SETA programs that is based on end-users actual behavior. At this point, there is a shift to the design science research paradigm. To close the gap of methodological rigor and practical relevance, a research approach was chosen in which researchers and practitioners continuously interact with each other, namely Action Design Research (ADR). This ADR approach was applied in a German engineering company and reflects a combination of two research approaches, design science research and action research, with the objective to develop and evaluate an IS artifact. In four stages, (1) problem formulation, (2) building, intervention and evaluation, (3) reflection and learning, and (4) formalization of learning, the needs assessment process model for SETA programs is developed and evaluated. Stage 2 consists of five cycles in which the researchers continuously interact with IT managers (in an early stage) and end-users (in a later stage). During these cycles, different research methods are applied in order to concretize the process model: literature analysis, semi-structured interviews, online questionnaires, analytical hierarchy process, and goal question metrics.

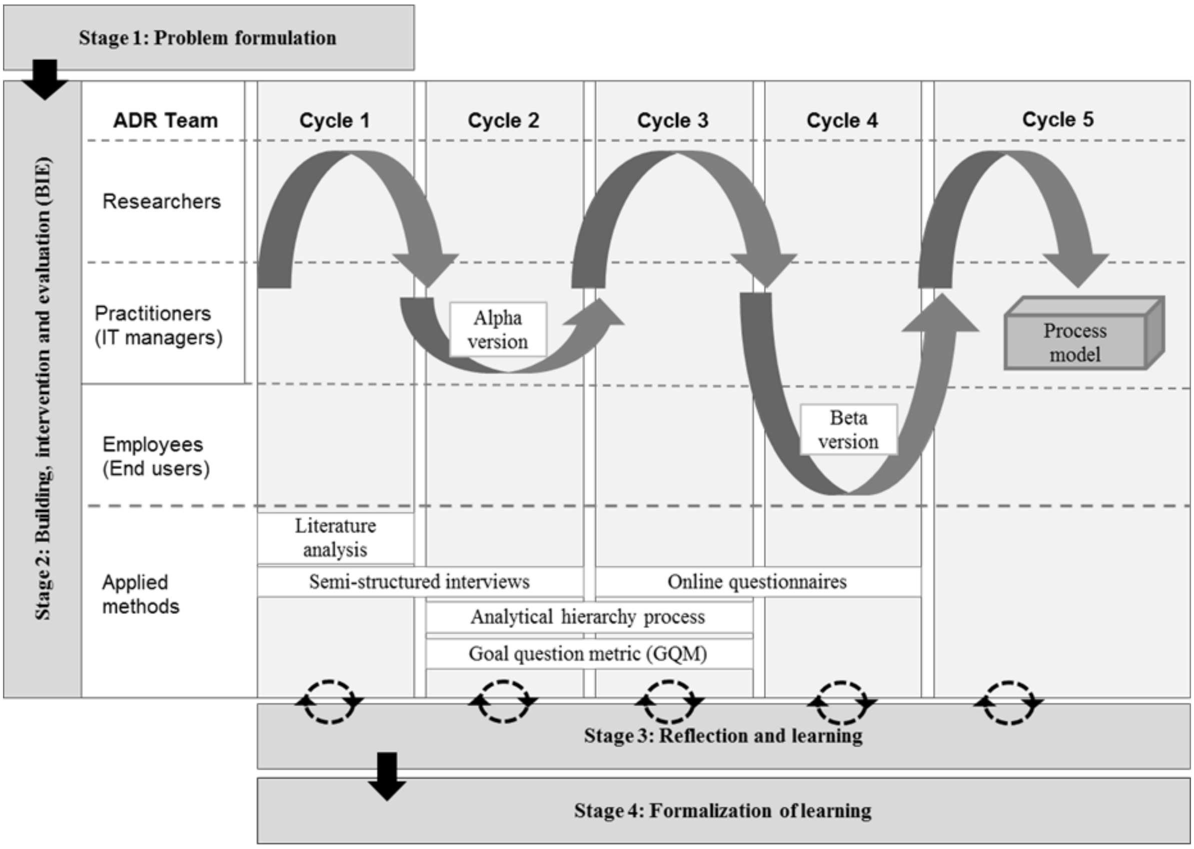

Stage 1: Problem formulation
Stage 2: Building, intervention and evaluation (BIE)
ADR Team
Cycle 1
Cycle 2
Cycle 3
Cycle 4
Cycle 5
Researchers
Practitioners (IT managers)
Employees (End users)
Applied methods
Alpha version
Beta version
Process model
Literature analysis
Semi-structured interviews
Online questionnaires
Analytical hierarchy process
Goal question metric (GQM)
Stage 3: Reflection and learning
Stage 4: Formalization of learning

Figure 2: Applied ADR method

Summary of results and contribution

This cumulative doctoral thesis follows two separate research objectives in two research areas. Based on the identified research gaps, different research methods adapted from both IS research paradigms (see Hevner et al., 2004) were applied.

In part A, a state of the art overview on the topics of holistic ISM, personality traits and TPB in IS research is given. The main objective was to develop and test a research model that integrates information security executives' personality traits and the attitudinal constructs of holistic ISM. Personality research has shown that personality traits vary in their respective relevance but are resistant to transformation (Junglas et al. 2008). In addition, prior meta-analytic studies have demonstrated that some FFM traits are more relevant in explaining different factors of behavior than others (Barrick et al. 2001). Therefore, a hypothesized relationship between a specific personality trait and attitude is relevant when it is appropriate, and is grounded in and supported by theoretical and empirical research studies. Figure 3 provides the estimates and a summary of results of the hypothesized relationships.

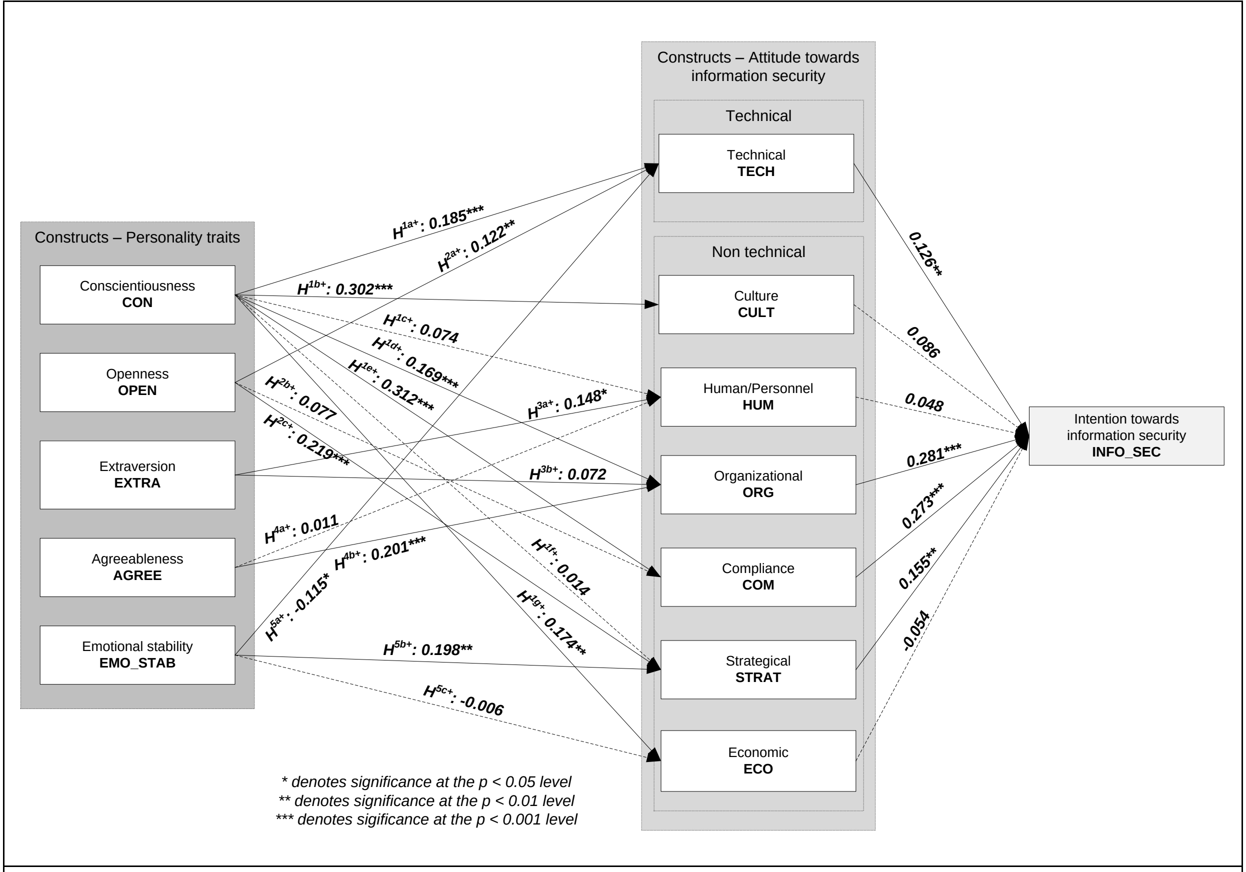


Figure 3: Research model and results

The results show that personality traits are influential in determining information security executives' attitudes towards holistic ISM but the influence varies, depending on the different personality traits. Conscientiousness is a valid predictor in job performance (Barrick et al. 2001). Due to rapidly changing requirements and challenges in ISM, information security executives require a high level of attention and professionalism in complex situations (Torres et al. 2006). Conscientiousness with its traits such as dutifulness, persistence, and self-discipline is an important characteristic that supports an information security executive in his or her attempts to completely understand complex situations (Barrick et al. 2001). Openness contains an individual's ability to face multiple challenges simultaneously and be receptive to new - but also to critically examine existing - ideas and information. These facets lead to more efficient actions and decisions if there is a security incident. As a result, such awareness and openness to innovations has been shown to affect an information security executive's attitude towards the technical and strategic ISM dimension. Given the importance of interpersonal interaction in the context of the end-user information security dimension and since extraversion is associated with being outgoing, social, active, and talkative, information security executives who are highly extraverted are shown to be more likely to have a positive attitude towards the dimensions with social and interpersonal interaction. On the other side, the required skills for information security executives, soft skills, the ability to sell security, and the management of relationships (Ashenden 2008) are aligned with agreeableness. Since the organizational ISM dimension contains tasks such as leadership and coordination of teams or communication with a higher management level, information security executives with a high degree of agreeableness are shown to form positive attitudes towards this dimension. Turning to emotional stability, research studies have demonstrated that emotionally stable individuals are likely to view innovative technical advances in their job as helpful and important (Devaraj et al. 2008). Information security executives with a high degree of emotional stability are shown to identify changing security conditions and skeptically examine the current technical information security implementation and stability status and therefore form positive attitudes towards the technical and strategic dimension of ISM.

The results in Figure 3 demonstrate that some relationships between personality traits and the attitudinal constructs towards holistic ISM are not significantly influential. Because the relationships between personality traits and attitudes do not occur in a vacuum, this leads to the assumption that the relationships are more complex than a simple linear relationship. Information security executives' beliefs or attitudes are influenced by external factors such as information security standards or guidelines if these beliefs match their attitude and behavioral intention. Dependent on the individual personality, these compliance factors shape the attitude towards managing technical security measures. For this purpose, an integrated research model that incorporates compliance factors as potential moderators and control variables has been developed. To get a more detailed view, attitude is regarded from the technical dimension of ISM (Figure 4).

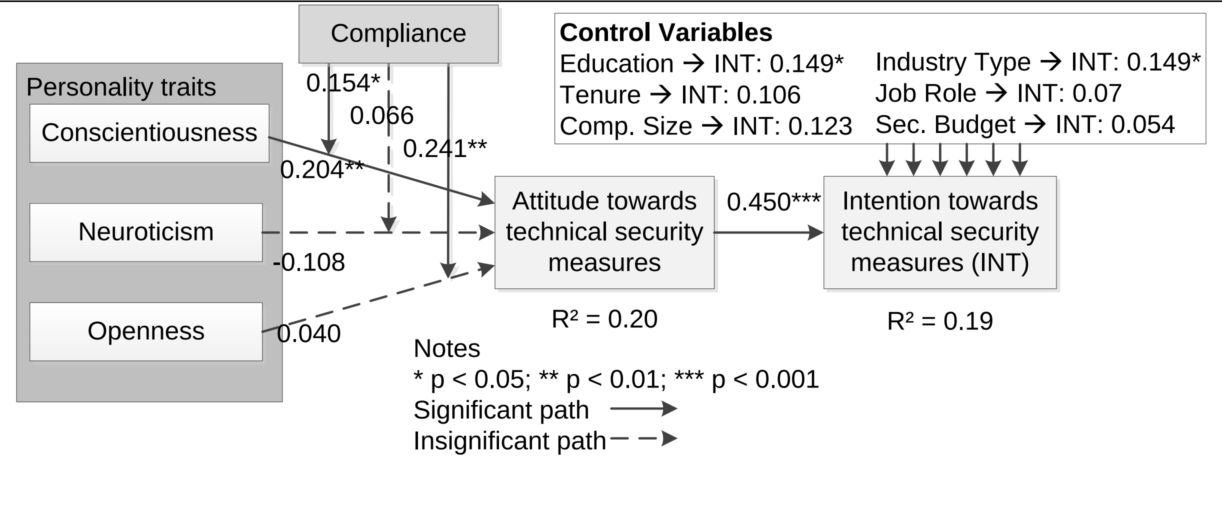


Figure 4: Extended research model and results

Besides the direct relationship of conscientiousness and attitude, the results show that compliance has a moderating effect on the relationship between the personality traits of conscientiousness and openness and attitude towards the management of technical security measures. In both cases, compliance is an external variable that moderates the relationships. Personality traits are stable in a long-term view (Costa & McCrae, 1992), thus other external factors such as compliance are more likely to moderate the affect of these traits on attitudes towards management of security measures. Turning to the four control variables, beside industry type no significant impact on explaining an executive’s behavioral intention towards technical security measures could be identified. This suggests that an information security executive’s behavioral intention towards the management of technical security measures varies based on the industry type of an organization.

Part A of this thesis contributes to the understanding of the influence of personality traits on a holistic ISM approach. Together with other behavioral patterns, this research can open an area for the development of a comprehensive model for assessing holistic ISM in organizations or companies. In addition, the results indicated that the personality – attitude relationship is more complex than a simple linear one. This can lead to a rethinking in the applied research field. From a practical perspective, the results have demonstrated that there is no “one size fits all” approach. An information security executive’s personality traits affect his or her attitude towards information security management dimensions, and it could be shown that his or her focus towards these dimensions would also be different. Consequently, if an organization or company reflects the behavior traits of its information security executives, it can improve the information protection level.

In part B, the current state of behavioral research that deals with end-users security awareness and behavioral compliance is analyzed. By referring to the four most frequently applied behavioral theories, a meta-model is specified. Results suggest that the core construct relationships from each theory were adopted by most identified publications that apply the respective theory. Since factors like end-users’ behavioral intentions, attitudes or subjective norms are not verifiable by means other than self reporting (Podsakoff and Organ, 1986), the majority of reviewed literature applying TPB, TAM, GDT or PMT use quantitative methods to test their hypotheses. This represents a shortcoming in information security literature, because self-reports are prone to the problems of common method variance, consistency motif and social desirability (Podsakoff and Organ, 1986) and are not sufficient predictors of end-users actual behavior (Workmann et al., 2008). Even if it is impossible to observe all factors of security related behavior (e. g. password strength, encrypting sensitive e-mails, etc.) for a large amount of employees, other research methods such as experimental studies or case studies might serve as indicators for actual behavior. Other shortcomings that could be identified were research studies with low response rates, the use of student samples, and different labels for the same constructs. Regarding the relationships between constructs, only few studies examined the relationship between the self-reported construct of behavioral intensions and actual behavior in real-life situations. Others postulate a strong and consistent relationship between BI and actual behavior by referring to Venkatesh et al. (2003). Since the authors also used self reported data and did not deal with security-related behavior, the assignability of the results has to be challenged. Consequently, the question whether end-users' BI is a reliable predictor for actual behavior in an information security context remains unanswered. There may be external or environmental factors mitigating the influence of BI and actual behavior. To give an example, end-users that are faced with heavy workload and complex security measures might intend to behave in compliance with the organization's information security policy, but is not able to transform the intentions into actual behavior.

The results of this literature review demonstrated that in the context of end-users' security awareness and behavioral compliance, generally accepted models and approaches that are applicable for practitioners are still lacking. Practical relevant information security research is still in its beginnings and practitioners face the problem of how empirically validated constructs can be adopted in real life situations. To close this gap, a needs assessment process model for SETA programs is developed and tested within a German engineering company (Figure 5). The main objective lies in the determination of a risk and priority measurement method that assists organizations in capturing, evaluating, and depicting the current state of end-users' security awareness and behavior. To allow an organization specific consideration of end-users' security awareness and behavioral compliance, it is necessary to integrate different end-user perspectives into the needs assessment process. The areas of focus need to be defined organization specific in dependence of the role and responsibility of the end-user to meet the objectives of a SETA program. The awareness target value definitions as well as the development of a reliable and valid measurement process were emphasized as major challenges to conduct a SETA needs assessment. On this basis, the initial process model was developed and refined during several cycles of feedback loops between researchers and practitioners, after general design principles were set up. End-users' actual behavior was measured with system data, however, the experience of this study showed that the use of self-reported data were also necessary in order to gain full coverage of employees' security awareness and behavior compliance. The resulting presentation of the degree of target achievement was proposed in an awareness map that enables a quick initial overview of the gap between organizational objectives and the current state of end-users' security awareness and behavioral compliance.

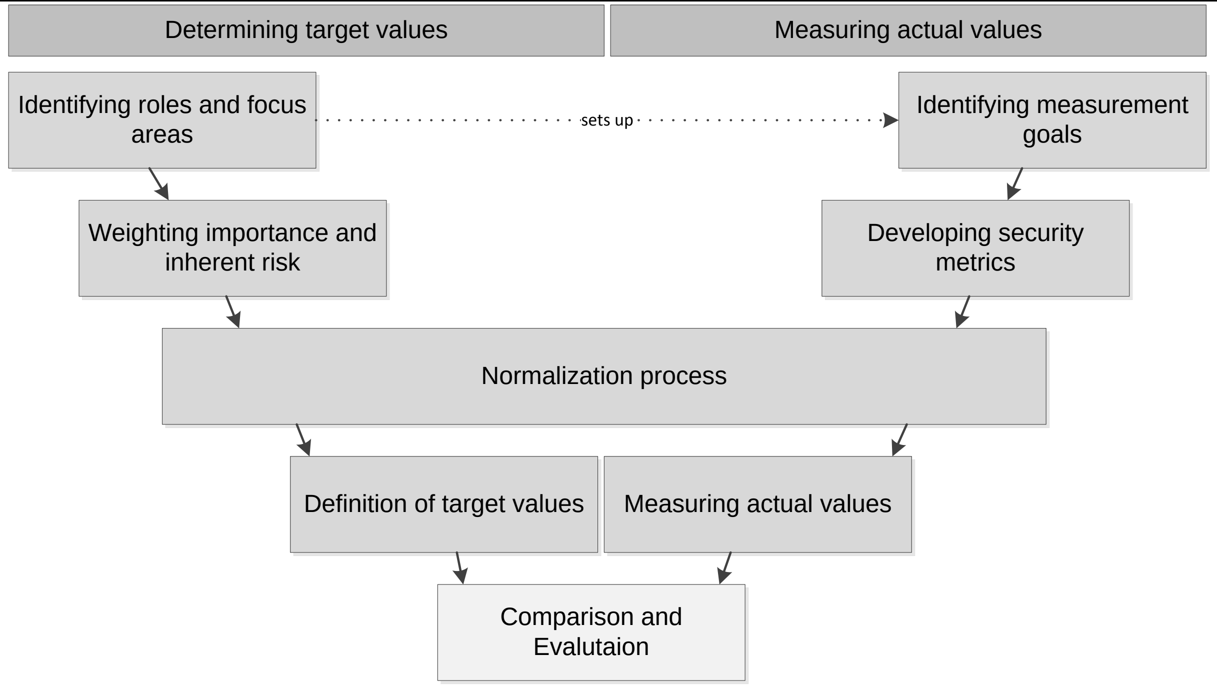

Determining target values
Measuring actual values
Identifying roles and focus areas
sets up
Identifying measurement goals
Weighting importance and inherent risk
Developing security metrics
Normalization process
Definition of target values
Measuring actual values
Comparison and Evalutaion

Figure 5: Needs assessment process model

With the step-by-step documentation of the measurement process, a detailed view of the identified needs is gained, thus providing a basis for developing a company specific SETA program. The research study contributes to information security research as it focuses on reducing the identified lack of generic process models in the area of needs assessment of SETA programs and the measurement of actual behavior. Further the mentioned approach enables dynamic depiction of the current state of end-users' security awareness and behavioral compliance and its changes over time. The continuous intervention between researchers and practitioners results in a procedure model that assists organizations in implementing a needs assessment for SETA programs. The model supports IS managers in identifying and evaluating gaps in end-users' security awareness and behavioral compliance. Based on these findings, it provides a basis for designing an adequate SETA program.

III. Table of contents

IV. List of figures

V. List of tables

VI. List of abbreviations

A	Appendix
AB	Actual Behavior
ACM	Association for Computing Machinery
ADR	Action Design Research
AGREE	Agreeableness
AHP	Analytic Hierarchy Process
AIS	Association for Information Systems
AMCIS	Americas Conference on Information Systems
AR	Action Research
ATT	Attitude
BFI	Big Five Inventory
BI	Behavioral Intentions
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Coping Appraisal
cf.	Compare
CIA	Confidentiality, integrity and availability
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COBIT	Control Objectives for Information and Related Technology
COMP	Compliance
CON	Conscientiousness
CULT	Culture
DSR	Design Science Research
e.g.	exempli gratia / for example
ECIS	European Conference on Information Systems
ECO	Economic
Eds.	Editors

EJIS	European Journal on Information Systems
EMO_STAB	Emotional Stability
EPI	Eysenck Personality Inventory
EXTRA	Extraversion
FFI	Five Factor Inventory
FFM	Five Factor Model
GDT	General Deterrence Theory
GQM	Goal Question Metric
H	Hypothesis
HICSS	Hawaii International Conference on System Science
HUM	Human
I	Importance
ICIS	International Conference on Information Systems
IEC	International Electrotechnical Commissions
IEEE	Institute of Electrical and Electronics Engineers
IJSODIT	International Journal of Social and Organizational Dynamics in IT
IPIP	International Personality Item Pool
IS	Information Systems
ISACA	Information Systems Audit and Control Association
ISM	Information Security Management
ISO	International Organization for Standardization
ISP	Information Security Policy
ISR	Information Systems Research
IT	Information Technology
IV	Impact Value
IWI	Institute für Wirtschaftsinformatik
KOR	Korea
LISREL	Linear Structural Relations
MISQ	Management Information Systems Quarterly

MKWI	Multikonferenz der Wirtschaftsinformatik
N.A.	Not available
NIST	National Institute of Standards and Technology
OPEN	Openness
ORG	Organization
p.	Page
PBC	Perceived Behavioral Control
PCA	Principal Component Analysis
PCOS	Perceived Certainty of Sanctions
PEOU	Perceived Ease of Use
PIR	Personality Inventory Revised
PLS	Partial Least Squares
PMT	Protection Motivation Theory
pp.	Pages
PSOS	Perceived Severity of Sanctions
PSOT	Perceived Security of Threats
PU	Perceived Usefulness
PV	Perceived Vulnerability
Q	Question
RC	Response Costs
RE	Response Efficacy
RP	Risk Potential
RQ	Research Question
S	Sanctions
SCT	Social Cognitive Theory
SEM	Structural Equation Model
SETA	Security Education, Training and Awareness
SLT	Social Learning Theory
SN	Subjective Norm

SP	Special Publication
STRAT	Strategic
TA	Threat Appraisal
TAM	Technology Acceptance Model
TECH	Technical
TPB	Theory of Planned Behavior
TRA	Theory of Reasoned Action
USA	United States of America
VHB	Verband der Hochschullehrer für Betriebswirtschaft
WI	Wirtschaftsinformatik
WKWI	Wissenschaftliche Kommission Wirtschaftsinformatik

0. Overview of publications

The author found his affinity to the research field of behavioral science in the context of information security during the preparation of a seminar paper in 2007 at the Information Systems Institute, Leibniz Universität Hannover. In this work, the author presented a security awareness concept that was based on the concept of the nature of human beings and different motivational aspects. The work was refined and published as the "IWI Discussion Paper # 23" (cf. Appendix A11). Two years later, the author enhanced this work with different theoretical constructs from education and additional empirical data and finished it as the author's diploma thesis. The thesis was shortened, refined and published as the "IWI Discussion Paper #36" during his doctoral time. An essay, which was based on a homework in the doctoral research seminar "Wissenschaftstheorie" at the Wirtschaftswissenschaftliche Fakultät, Leibniz Universität Hannover, appeared in the "IWI Discussion Paper # 40" (cf. Appendix A12). This essay which was entitled "Aspekte der Wirtschaftsinformatikforschung 2009" discusses the differences between reference models and procedure models in the German IS discipline. The fourth IWI discussion paper (# 49) dealt with the discussion of an IT-Governance Implementation Project Model which was based on the IS standards COBIT and ValIT (cf. Appendix A13). The fifth IWI discussion paper presents a state of the art overview of all publications within the German IS conference "Wirtschaftsinformatik Tagung" (cf. Appendix A14).

The author's first publication was entitled "Critical Success Factors for Adoption of Integrated Information Systems in Higher Education Institutions – A Meta Analysis". It was presented at the "Americas Conference on Information Systems (AMCIS)" and published in the conference proceedings. The aim of this paper was to provide a systematic meta-analysis and a state of the art overview of critical success factors for selection and implementation of integrated IS in the higher education sector. Even if this research paper is off-topic, the research methodology and the gained experiences contributed to other research papers of this thesis (cf. Appendix A2).

The first publication in the research field of information security from an executives' perspective was entitled "Towards a sustainable and efficient component-based information security framework". This publication was presented at the German IS conference "Multikonferenz der Wirtschaftsinformatik (MKWI)" and published in the proceedings. In this research paper, a holistic, multidimensional ISM framework was discussed and empirically examined (cf. Appendix A3). The results build the theoretical basis for the second publication in this research field, entitled "Personality Traits and Information Security Management: An Empirical Study of Information Security Executives" which was presented at the "International Conference on Information Systems (ICIS)" and published in the proceedings. Based on the attitudes of holistic ISM, the influence of personality traits was investigated (cf. Appendix A4). Build upon the limitations of this paper, the third (and the fourth) publication discussed the influence of external constructs such as compliance on the relationship between personality traits and attitude. The third publication was entitled “Management of Technical Security Measures: An Empirical Examination of Personality Traits and Behavioral Intentions” which was presented at the “Hawaii International Conference on System Science (HICSS)” and published in the proceedings (cf. Appendix A5). The authors extended the paper theoretically and enhanced the research model by the integration of control variables and published it in the international IS journal “International Journal of Social and Organizational Dynamics in IT (IJSODIT)” (cf. Appendix A6).

The first publication in the research field of end-users’ security awareness and behavioral compliance was entitled “Employees’ information security awareness and behavior: A literature review”. It was presented at the international IS conference “HICSS” and published in the proceedings (cf. Appendix A7). In addition, the paper was extended and published in the international journal “Management Research Review” (cf. Appendix A8). In this paper, a state of the art overview of applied behavioral theories is given and research gaps are discussed. Based on these findings, the third publication “Towards a Needs Assessment Process Model for Security, Education, Training and Awareness Programs - An Action Design Research Study” aims to close the gap of limited research in the field of concrete process models and the measurement of actual behavior. The paper is presented and publicated in the conference proceedings at the “European Conference on Information Systems (ECIS)” (cf. Appendix A9). Another publication, publicated in the Journal of Information Security, deals with behavioral determinants that explain the use of security measures in smartphones (cf. Appendix A10).

A summary of all publications can be found in Table 1. The research papers that are discussed within this thesis are marked by naming its chapters. To receive an indication on the quality of publications, each paper was classified according to journal and conference rankings. Rankings implicate an overall assessment of the research quality in a specific research area within the publication type (Hennig-Thurau et al., 2004). Therefore, one ranking for business research (VHB Jourqual 2.1, 2009) and one ranking for IS research (WKWI: Wissenschaftliche Kommission Wirtschaftsinformatik, 2008) was applied, both encompassing international publications.

Table 1: Overview of publications

	No.	Titel	Authors	Outlet	Author ranking	Ranking VHB JQ2.1	Ranking WKWI	Chapter	Appendix
	1.	Aspekte der Wirtschaftsinformatik 2009	Markus Neumann, Achim Plückebaum, Jörg Uffen, Michael H. Breitner	IWI Discussion Paper #40, 2010	3.	-	-	3.	A1
	2.	Critical Success Factors for Adoption of Integrated Information Systems in Higher Education Institutions – A Meta Analysis	Lubov Lechtchinskaia, Jörg Uffen, Michael H. Breitner	Proceedings of Americas Conference on Information Systems (AMCIS), 2011	2.	D	B	3.1.1	A2
Part A	3.	Towards a Sustainable and Efficient Component-Based Information Security Framework	Jörg Uffen, Robert Pomes, Michael H. Breitner	Proceedings of the Multikonferenz der Wirtschaftsinformatik (MKWI), 2012	1.	D	C	4.1	A3
	4.	Personality Traits and Information Security Management: An Empirical Study of Information Security Executives	Jörg Uffen, Nadine Guhr, Michael H. Breitner	Proceedings of the International Conference on Information Systems (ICIS), 2012	1.	A	A	4.2	A4
	5.	Management of Technical Security Measures: An Empirical Examination of Personality Traits and Behavioral Intentions	Jörg Uffen, Michael H. Breitner	Proceedigs of the 46th Hawaii International Conference on System Science (HICSS), 2013	1.	C	B	4.3	A5
	6.	Management of Technical Security Measures: An Empirical Examination of Personality Traits and Behavioral Intentions	Jörg Uffen, Michael H. Breitner	International Journal of International Journal of Social and Organizational Dynamics in IT (IJSODIT), 2013	1.	-	-	4.3	A6
Part B	7.	Employees' Information Security Awareness and Behavior: A Literature Review	Benedikt Lebek, Jörg Uffen, Markus Neumann, Bernd Hohler, Michael H. Breitner	Proceedigs of the 46th Hawaii International Conference on System Science (HICSS), 2013	2.	C	B	5.1	A7
	8.	Information Security Awareness and Behavior: A Theory-based Literature Review	Benedikt Lebek, Jörg Uffen, Markus Neumann, Bernd Hohler, Michael H. Breitner	Management Research Review, 2013	2.	C	-	5.1	A8
	9.	Towards a Needs Assessment Process Model for Security, Education, Training, and Awareness Programs - An Action Design Research Study	Benedikt Lebek, Jörg Uffen, Markus Neumann, Michael H. Breitner	Proceedings of the European Conference on Information Systems (ECIS), 2013	2.	B	A	5.2	A9
	10.	Personality Traits and Cognitive Determinants - An Empirical Investigation of the Use of Smartphone Security Measures	Jörg Uffen, Nico Kaemmerer, Michael H. Breitner	International Journal of Information Security	1.	-	-		A10
	11.	Entwicklung von Security Awareness Konzepten unter Berücksichtigung ausgewählter Menschenbilder	Jörg Uffen, Robert Pomes, Claudia M. König, Michael H. Breitner	IWI Discussion Paper #23, 2008	1.	-	-		A11
	12.	Stärkung des IT-Sicherheitsbewusstseins unter Berücksichtigung psychologischer und pädagogischer Merkmale	Jörg Uffen, Michael H. Breitner	IWI Discussion Paper #36, 2009	1.	-	-		A12
	13.	Discussion of a IT-Governance Implementation Project Model Using COBIT and ValIT	Christoph Meyer, Jörg Uffen, Michael H. Breitner	IWI Discussion Paper #49, 2011	2.	-	-		A13
	14.	20 Jahre Internationale Tagung Wirtschaftsinformatik: Profil einer Konferenz	Jörg Uffen, Stefan Hoyer, Michael H. Breitner	IWI Discussion Paper #54, 2013	2.	-	-		A14

1. Introduction

1.1 Motivation of this thesis

Organizations and companies are heavily dependent on information systems (IS) to carry out their business processes and strategies. Information systems are defined as integrated sets of resources, procedures and people that aim for capturing, storing, processing and communicating information (Gupta, 2011). The extent of the organizational IS environment is for example driven by globalization, increasing customer and supplier expectations, rapidly changing technology and the pressure to increase the efficiency. As a consequence, IS are becoming more and more complex, making it increasingly difficult to protect the organizational information assets. Security attacks or security incidents can lead to dire consequences for every organization, including loss of prestige and credibility, corporate liability, and monetary damage (Bulgurcu et al., 2010). For example, in the latest survey of the Computer Security Institute an overall average annual loss of $300,000 caused by security incidents is reported (Richardson, 2008). In addition, 77% of respondents of Ernst & Young's 2012 Global Information Security Survey reported a considerably rise of security incidents in the last two years. Because only a fraction of security incidents are currently discovered (Hoffer and Straub, 1989; Whitman, 2003), these surveys underestimate the problem (D'Arcy et al., 2008). Therefore, organizations are more and more concerned about the protection of organizational information assets (Straub and Welke, 1998; Taylor, 2006).

As a result, information security has developed to one of the main managerial priorities in many organizations. To ensure information security, researchers are in consent that ISM needs to emphasize three semantic dimensions: confidentiality, integrity and availability (CIA) (see e.g. Eloff and Eloff, 2005; Saleh et al., 2006; Torres et al., 2006). In detail, confidentiality represents the prevention of unauthorized disclosure; integrity ensures that information cannot be modified by unauthorized individuals; and availability makes sure that information are available to authorized individuals when needed (Siponen and Oinas-Kukkonen, 2007). In a more human-oriented and extended view, additional objectives are responsibility, reliability, authenticity (ISO/IEC 13335) and non-repudiation (Siponen and Oinas-Kukkonen, 2007). These fundamental elements need to be considered in the organizational information security and risk strategies. To meet these objectives, researchers and practitioners have discussed various information security approaches with different numbers and labels of dimensions. The authors highlight the importance of an optimized, multidimensional, holistic ISM approach to efficiently protect technology, processes, people, and other organizational factors (Da Veiga and Eloff, 2007; Hu et al., 2006; May and Dhillon, 2010). Various information security architectures, frameworks and best-practices such as COBIT or ISO/IEC 27000-series have been developed in order to assist organizations in implementing holistic information security. These either indicate that efficient information security is a holistic and multidisciplinary topic that is cutting horizontally across organizational business units within and over organizational boarders along the entire value-added chain. Therefore, the incorporation of several dimensions, such as social and technical issues, into ISM models, frameworks, or architectures has become an area of focus in information security research (May and Dhillon 2010). For example, in their literature review, Zafar and Clark (2009) classified information security research paper according to its relevance by the IBM Information Security Capability Reference Model (IBM, 2006). This reference model encompasses eight information security dimensions – governance, privacy, threat mitigation, transaction and data integrity, identity and access management, application security, physical security and personal security (IBM, 2006; Zafar and Clark, 2009). Eloff and Eloff (2005) introduced an integrated information security architecture approach that includes network security, user access control, personnel security and regulatory aspects.

ISM approaches can be generally separated into two essential components – technical and non-technical information security components. The former incorporates technical security mechanisms, including anti-virus protection, virtual private networks and encryption tools. However, technical security mechanisms are insufficient as long as other factors are not taken into account. These are part of the second, non-technical security component that includes for example human-related issues, organizational issues and regulatory requirements. One important topic is the consideration of behavioral aspects. Since researchers and practitioners highlight that the weakest link in information security is the human factor, represented by employees or end-users (D’Arcy et al., 2008; Spears and Barki, 2010; Siponen, 2000), an emerging research stream considers end-users’ security awareness and security related behavior with the aim of identifying and evaluating specific behavioral factors that explain actual behavior (Bulgurucu et al., 2010).

Other human-related topics in information security research deal with the management perspective. According to ISO/IEC 27001, ISM is determined as an essential element of an organizational management system, in order “to establish, implement, operate, monitor, review, maintain and improve information security”. The aim of ISM is to maximize the prevention and deterrence of security threats (D’Arcy et al., 2008) by adopting efficient security mechanisms that address both information security components. But due to an increasing number of complex information security risks, the management of a holistic information security concept is often challenging for organizations (Eloff and Eloff, 2005). For example, when implementing technical security measures, numerous organizational issues such as the impact on employee productivity have to be taken into account. From the behavioral and cognitive perspective, management and the way they cope with potential information security risks directly affects both, technical and non-technical, components of information security.

Based on these premises, this cumulative doctoral thesis focuses on the investigation of behavioral factors, cognitive processes and the roots of both within the information security context. The human factor is regarded from two perspectives – the employee or end-user (hereafter referred to end-user) side and the management level represented by information security executives (Figure 6). Hevner et al. (2004) stated that IS research "is the scientific analysis of the interplay of people, organizations, and technology (Silver et al., 1995) and therefore contributes to and relies on various disciplines such as organizational theory, management sciences, cognitive sciences, and computer sciences". This thesis makes either use of several research areas – information security, psychology, behavioral and cognitive theories, and multivariate statistics. In the following, a deeper motivation will be presented with the purpose to introduce the outlined research questions. The research questions are adapted from the in chapter 0 (Overview of publications) mentioned publications that are in the scope of this thesis. The order of the publications has been selected based on their contribution to the research objective.

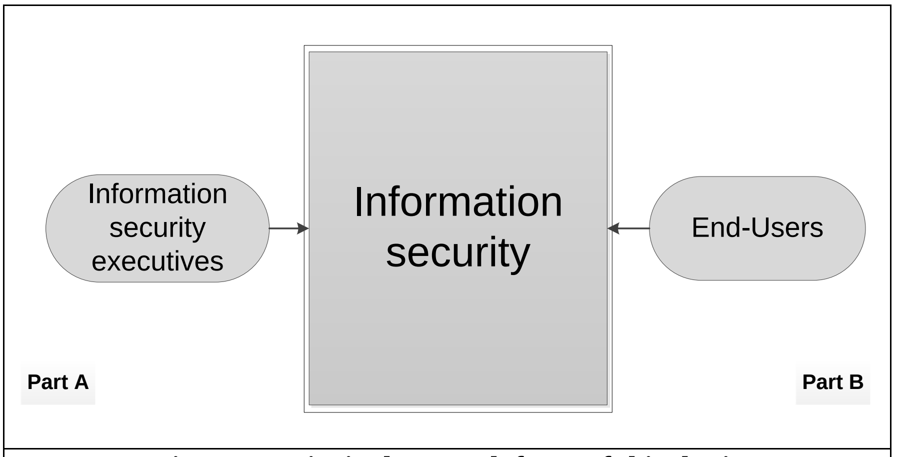


Figure 6: Principal research focus of this thesis

1.2 Derivation of research questions

1.2.1 Target group: Executive level

In recent years, behavioral factors and the underlying cognitive processes have become an important area of focus in information security research. Empirical studies that focus on the human factor in the information security context tend to emphasize the end-user or employee rather than the executive level. Little effort has yet been made to examine the influence of personal attitudes or individual behavioral patterns of information security executives and their impact on the technical and non-technical information security dimensions. As a consequence, the first step was to identify a generally accepted ISM framework that incorporates holistic information security dimensions. But given the stated importance of the implementation of a holistic, multidimensional ISM approach (see chapter 1.1), there is still a lack of generally accepted models or frameworks with coherent information security dimensions or labels (Kritzinger and Smith, 2008; May and Dhillon, 2010). Standards and guidelines are useful tools to compensate this gap, but these are focused on the practical application rather than the theoretical use within research studies.

The aim of the research contribution of Uffen et al. (2012a) was to present a holistic and multi-dimensional information security framework that is based on academic and practical knowledge. An information security framework within the context of this paper is represented by the interaction of interdisciplinary sub-areas, relevant for efficient and sustainable implementation of information security. The adequacy of information security component-based frameworks is evaluated by their practical application. The resulting framework shall formerly guide organizations to ensure a holistic and consistent focus and help researchers to gain a global ISM view. In order to address both objectives the research questions are:

RQ1: Which information security dimensions are discussed within information security framework literature?

RQ2: How can these dimensions be consolidated considering their practical relevance?

These results, especially the results of the comprehensive literature review and the consolidated information security dimension, build the theoretical foundation of a holistic ISM approach. To ensure that each identified information security dimension is aligned with the organizational objectives, some dimensions need to receive more attention and in turn should receive more resources. But the consideration and valuation of each dimension depends on the decisions of responsible information security executives. Therefore, the role and responsibility of information security executives in this research field have been shown to be a critical success factor (McFadzean et al., 2007; Straub and Welke, 1998). Their individual differences in personality, attitudes and behavior cause potential information security risks and directly influence the level of each information security dimension.

In IS research, personality traits have been shown to be a valuable instrument to summarize individual differences in personality into fundamental facets of each individual. These traits determine cognitive processes and behavioral patterns that remain more or less stable across time (Costa et al., 1991). The combination of both approaches is investigated in the second research paper (see Uffen et al., 2012b). The purpose of that paper was to investigate how personality traits between information security executives affect the specific dimensions of a holistic ISM approach within organizations and companies. Personality traits were measured with the use of a standardized measurement model – namely Five Factor Model (FFM) by Costa and McCrae (1991). Holistic information security was measured by the way information security executives perceive each dimension. This research paper is driven by the assumption that information security executives' actions, decisions and behavioral intentions in each dimension of information security are essentially influenced by their personalities. The following research question is explored by testing an integrated research model:

RQ3: Which personality traits of an information security executive have a major influence on technical and non-technical components of information security management?

The results and critical analysis of the empirically tested research model possessed new research questions. Some relationships between personality traits and the attitudinal holistic ISM constructs were shown to be insignificant. It is expected that the relationship between both personality traits and the attitudinal constructs is more complex than a simple linear one. These relationships must be focused more in detail. One option is the incorporation of external factors that might have an influence on the personality-attitude relationships. In empirical research studies, it has been shown to be fruitful to incorporate moderators into research models with the aim to improve their predictive power (Cooke and Sheeran, 2004).

The third research paper in this research area deals with the personality-attitude relationship of information security executives (see Uffen et al., 2013a). The research model is modified in order to obtain a better understanding of potential external factors and to analyze the relationship more precisely. Because the management of technical security measures is one of the daily tasks of an information security executive, the attitudinal constructs of the technical dimension of information security is taken into account. Organizations and companies face compliance requirements that must be taken into account in the decision-making processes of information security executives. Compliance factors include legal requirements, international standards and guidelines, and internal security policies. Therefore, the influence of compliance factors is integrated as a potential moderator into the personality-attitude relationship. In order to underline the complexity of the personality-attitude relationship, control variables are further integrated in the research model and discussed in a second, modified research paper (see Uffen et al., 2013b). The following research questions were posed:

RQ4: Which and how do personality traits of an information security executive affect his or her attitude towards managing technical security measures?

RQ5: To what extent are compliance factors potential moderators between personality traits and attitude towards managing technical security measures?

1.2.2 Target group: End-User level

As stated in Chapter 1.1, target subjects of behavioral research studies in the information security domain were mostly limited to end-users (e.g. Shropshire et al., 2006). The misuse of IS resources represent a significant threat to organizations and companies (D’Arcy et al., 2009). Since researchers and practitioners realized that end-users are the weakest link in information security (Bulgurucu et al., 2010), security, education, training, and awareness (SETA) programs have gained increasing attention in theory and practice. This leads to an emerging discussion on how to increase security awareness and assure security-compliant behavior. As a result, interdisciplinary behavioral theories, including theories from psychology, pedagogy and criminology, were incorporated into integrated behavioral information security models (Karjaleinen and Siponen, 2011) with the aim to explain and predict employees' security awareness and related behavior.

The aim of the first (and second) research study that deals with the target group of end-users is to provide a state-of-the art overview of applied behavioral theories within the mentioned research field (see Lebek et al., 2013a; Lebek et al., 2014). Prior literature analyses were published twelve years ago (Siponen, 2000), or focused on other security awareness topics (Abraham, 2011). The literature review contributes to the understanding and extension of the body of knowledge aggregated in this area. In addition, the literature review bears the potential to uncover research gaps and paves the way for further rigorous research. This leads to the following research question:

RQ6: Which theories have been recently used in IS literature to explain employees' security related awareness and behavior?

One result of the literature review is that there is no generally agreed SETA approach which focuses on the basic organizational requirements. Another shortcoming in this research field is the reliability of behavioral intention as a predictor of actual security behavior. End-users' real behavioral outcomes are mainly measured with the use of self-reports. Practitioners face difficulties in addressing and implementing the theoretical assessed behavioral constructs that determine end-users' security awareness and behavior into an organization specific efficient and sustainable SETA approach. There is a gap between the needed knowledge of practitioners of which interventions to apply and the theoretically founded explanations of end-users' security related behavior (Workman et al., 2008). According to Roseman and Vessey (2008), research should provide relevance for practitioners in order to prevent research from becoming an end unto it-self.

Before implementing a SETA program in an organization, the planning and design process needs to receive attention in order to ensure that the SETA program is aligned with the organizational objectives (Kruger and Kearney, 2006). The purpose of the third publication is to provide a systematic and organization-specific research approach that aims to identify, evaluate and depict the state of end-users security awareness and security-related behavior. To assess applicability within multiple organizations, the derived needs assessment for SETA programs is generalized. Realizing the gap between organizational relevance and methodological rigor, a relatively new research approach, namely action design research (ADR) by Sein et al. (2011) is adapted. ADR allows the continuous interaction between practitioners and researchers with the objective to design and evaluate a concrete IS artifact. Within that publication, the following research question was explored:

RQ 7: What are the design principles for developing and implementing a needs assessment process for SETA programs that considers an organization's individual context?

Table 2 summarizes the identified research gaps, the underlying research questions, and the research contribution of this thesis.

Table 2: Research gap, research questions, and contributions

	Research gap	Research question	Research contribution
Part A	No generally accepted holistic information security management approach	RQ1: Which information security dimensions are discussed within information security framework literature?	Definition of a holistic ISM approach containing of seven dimensions
		RQ2: How can these dimensions be consolidated considering their practical relevance?	
	Current behavioral research mainly focuses on employees' perspective	RQ3: Which personality traits of an information security executive have a major influence on technical and non-technical components of information security management?	Empirical findings that personality traits are influential in determining holistic ISM
		RQ4: Which and how do personality traits of an information security executive affect his or her attitude towards managing technical security measures?	Empirical testing that the relationship between personality traits and attitude is moderated by external variables
		RQ5: To what extent are compliance factors potential moderators between personality traits and attitude towards managing technical security measures?	
Part B	No state of the art research in employees' security awareness and behavioral compliance	RQ6: Which theories have been recently used in IS literature to explain employees’ security related awareness and behavior?	An overview of applied behavioral models that predict and explain end-users' behavior
	Practitioners face difficulties in implementing theoretical behavioral models that address SETA programs	RQ7: What are the design principles for developing and implementing a needs assessment process for SETA programs that considers an organization’s individual context?	Definition of a needs assessment process model for SETA programs

1.3 Thesis structure and problem contribution

The purpose of this cumulative doctoral thesis was to identify and explain certain behavioral aspects from different human perspectives within organizational information security context. Overall, the thesis consists of two independent parts. First, behavioral aspects out of the perspective of information security executives are examined. Second, from the perspective of end-users, the current state of security awareness and behavioral compliance is investigated. The theoretical frame, behavioral research in organizational information security, connects both parts with one another but the underlying research focus diverge (Figure 7).

Figure 7: Structure of the thesis

Introduction

- Motivation of this Thesis (1.1)
- Derivation of Research Questions (1.2)
- Thesis Structure and Problem Contribution (1.3)

Theoretical Foundation – Behavioral Models

- Theory of Planned Behavior (2.1)
- Five Factor Model (2.2)

Research Methodology

- Qualitative Research Methods (3.1)
- Quantitative Research Methods (3.2)

Part A
Personality Traits and Information Security Management

- Holistic Information Security Management Approach (4.1)
- Information Security Executives‘ Personality Traits and Attitude towards holistic ISM (4.2)
- Information Security Executives‘ Attitudes Towards Technical Security Measures (4.3)

Part B
End-users‘ Information Security Awareness and Compliant Behavior

- Security Awareness and Compliant Behavior: A Literature Review (5.1)
- Towards a Needs Assessment Process Model for SETA Programs (5.2)

Thesis Conclusion and Limitations

- Overall Conclusions (6.1)
- Overall Limitations (6.2)

The first three chapters and chapter 6 build the frame of both parts. Starting with a motivation in the context of information security, Chapter 1 outlines the research questions and gives an overview of both parts. In order to explain the theoretical foundation of part A and B, chapter 2 explains two important behavioral models, namely the TPB and the Five Factor Model (FFM) more in detail. Since both behavioral models are essential in this thesis, a common understanding and a precise terminology of both approaches is needed (Bortz and Döring, 2006). Chapter 0 provides an overview of the different research methods that were required to conduct the research presented in this thesis. These include a broad methodological classification of behavioral science and design science, followed by a discussion of applied qualitative (sub-chapter 3.1) and quantitative (sub-chapter 3.2) research methods. The following two chapters (chapters 4 and 5) are the main parts of this thesis, each discussing a summary of results of the respective publications. Both chapters are structured according to their content and not listed in order of importance. This was necessary, because the sub-chapters are building upon one another. Chapter 4 and 5 start with a preamble, which briefly discuss the background of the publications, followed by a short introduction in order to specify the research topic. Then, beside the explanations in chapter 2, the theoretical foundation of the underlying publication is introduced. This is followed by a discussion of the main results. The conclusion of each sub-chapter builds an interaction of conclusion, contribution and limitations. Lastly, the final chapter (chapter 6) summarizes the results of both research areas, outlines the overall limitations and provides directions for future research.

2. Behavioral models

In both examined research areas in this thesis, behavioral models from interdisciplinary areas are applied for explaining and predicting target individuals behavior. For this reason this section will explain the theoretical underpinnings of the two most important applied behavioral models – Theory of Planned Behavior and Personality Traits.

2.1 Theory of planned behavior

One in research frequently applied behavioral model is the Theory of Reasoned Action (TRA)/Theory of Planned Behavior (TPB). Fishbein and Ajzen (1975) illustrated a basic approach to explain an individual's actual behavior by investigating their behavioral intentions (BI). BI are shown to be proximal cognitive antecedents of actual behavior or actions (Ajzen, 1991) and index the motivation to perform a certain behavior. In TRA, BI is determined by two cognitive constructs – attitude (ATT) and subjective norm (SN). The ATT construct stems on the salient beliefs and feelings of an individual that indexes his/her overall evaluation of a specific behavior. It represents the degree to which a specific behavior is positively or negatively valued (Ajzen, 1991). The second TRA construct is determined by the social pressure to perform a specific behavior. The term SN reflects an individual's beliefs about whether important others think he/she should engage in a specific behavior (Fishbein and Ajzen, 1975; Ajzen, 1991). Even if these two constructs are shown to form the underlying foundation of BI, the influence of ATT and SN on BI can differ and is not of the same weight (Miller, 2005). Shortcomings of the TRA are represented by additional external factors that might influence BI. For example Sheppard et al. (1988) emphasized that the model neglects practical restrictions such as environmental factors, the own ability or limitations in time. Therefore Ajzen (1991) modified the TRA and added a construct, perceived behavioral control (PBC) which was shaped by Bandura's (1982) concept of self-efficacy. This construct accounts for requisite resources necessary for performing a specific behavior (Ajzen, 1991). The PBC construct has been shown to influence both BI and AB. It reflects actual control and with greater increase of PBC, BI is likely to increase (Conner and Abraham, 2001).

As well as TRA, TPB does not account for the influence of external variables that might have a direct influence on BI and actual behavior and are outside the purview of the TPB proper. Ajzen and Fishbein (1975) have recognized the importance of external variables but theorize that these influence actual behavior indirectly through the cognitive constructs contained within TPB (Ajzen, 1991; Ajzen and Fishbein, 1975). The authors explicitly stated that personality traits are such external variables.

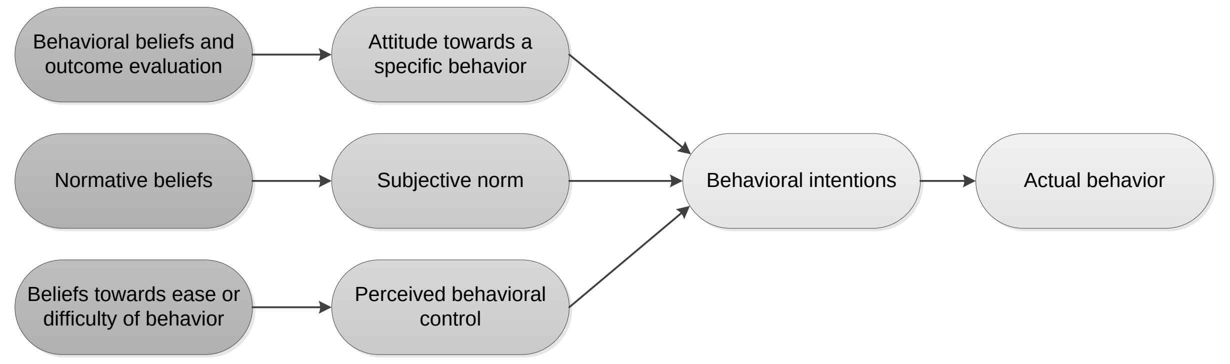

Behavioral beliefs and outcome evaluation
Attitude towards a specific behavior
Normative beliefs
Subjective norm
Behavioral intentions
Actual behavior
Beliefs towards ease or difficulty of behavior
Perceived behavioral control

Figure 8: Theory of planned behavior (cf. Ajzen, 1991)

2.2 Five factor model of personality

Personality researchers developed different classification systems with the purpose to link individual differences into fundamental facets of each human being. These resulting personality traits determine cognitive and behavioral patterns that are more or less stable across different situations (Costa et al., 1991). Personality traits are defined as the agile organization within the individual "of those psycho physiological systems that determine his characteristics behavior and thought" (Allport 1961, p. 28). In psychological research there is consent that the domain of personality can be summarized to five broad constructs (Costa et al., 1991; Digman, 1990). The most frequently applied taxonomy in personality research is referred to as the "Big Five" or "Five Factor Model (FFM)" (Barrick et al., 2001). These five constructs are often labeled as agreeableness, extraversion, neuroticism, openness and conscientiousness (e.g. Barrick et al., 2001; Digman, 1990; Costa et al., 1991; McCrae and John, 1992). Agreeableness primarily represents a trait of interpersonal tendencies (Barrick et al., 2001) in the sense of trusting others and caring for them (Judge et al., 2002). Extraversion describes individuals that have strong preferences in social interaction and are lively active (Costa and McCrae, 1992). Neuroticism refers to the proneness to experience disturbing and unpleasant emotions (Rhodes et al., 2002). Openness is a dimension that represents an individual's receptivity to experience and try new ideas and different things (Costa and McCrae, 1992). Conscientiousness refers to an individual's intrinsic motivation to achieve success in different job situations and to operate at a high level (Costa et al., 1991). Table 3 lists the five broad personality constructs and gives examples of the underlying facets.

Table 3: Personality traits characteristic facets

Personality Trait	Factor Characteristic Facets
Conscientiousness	Being competent, dutiful, willing for achievement, persistent, self-disciplined, organized, responsible, and systematic
Openness	Being curious, imaginative, creative, open to new and innovative ideas, critical, intelligent, and experienced

Extraversion	Being positive emotional, assertive, active, ambitious, outgoing, amicable, assertive, talkative, and sociable
Agreeableness	Being good-natured, straightforward, trustful, willing for cooperation, helpful, affable, tolerant, sensitive, and kind
Neuroticism	Being anxious, pessimistic, temperamental, worried, paranoid, insecure, negative emotional, and impulsive

Personality traits are collected with the use of standardized personality inventories. These are for example the Big Five Inventory (BFI) by John (1990), Eysenck Personality Profiler (EPP) by Eysenck and Wilson (1991) or the International Personality Item Pool (IPIP) by Goldberg (1999). In addition, psychologists used the 240 item personality inventory (NEO-PI-R) to get detailed evidence to an individuals' personality. Others use the, better applicable for mass surveys, 60 item NEO Five Factor Inventory (FFI) by Costa and McCrae (1992). These inventories present a pre-defined number of statements that describe feelings, beliefs or behaviors. Each participant is questioned to indicate the degree of whether the statement represents their individual behaviors. In general, the personality inventories have been tested to a variety of respondents from different nations. Therefore, the success of this approach is represented by its heuristic and parsimony value in classifying individual differences in personality and the robustness across different languages and settings (Jang et al., 1996). Additional beneficial properties for researchers are that these inventories are relatively inexpensive, easy to administer and objective to score (Morgan and Harmon, 2001).

Across a wide spectrum of human-computer interactions, researchers have shown that personality traits are substantial predictors of behavior and beliefs (e.g. McElroy et al. 2007; Nov and Ye 2008). Table 4 presents some examples of personality traits adoption in IS research.

Table 4: Research examples of personality traits in IS research

#	Authors	Research Topic	FFM Traits
1	Bansal et al., 2010	Information Sensitivity, privacy, and trust	All
2	Bansal, 2011	Security and Privacy Concerns	All
3	Bedingfield and Thal, 2008	Project Managers	All
4	Benlian and Hess, 2010	Evaluation of ERP Systems	All
5	Chittaranjan et al., 2011	Smartphone Usage	All
6	Correa et al., 2010	Social Media Use	All
7	Devaraj et al., 2008	Technology Acceptance	All
8	Goswami et al., 2009	Mindfulness in IT Adoption	CON, OPEN
9	Jahng et al., 2002	E-Business	All
10	Junglas et al., 2008	Threat Appraisal	All
11	Krishman et al., 2010	Cyberloafing	All
12	Landers and Lounsbury, 2006	Internet Usage	CON, AGREE, EXTRA

13	Lin and Ong, 2010	IS Continuance Intention	All
14	Maier et al., 2012	Intention - Behavior Gap	-
15	McElroy et al., 2007	Internet Use	All
16	Nov and Ye, 2008	Technology Acceptance	OPEN
17	Pierce and Hansen, 2008	Virtual Teams	All
18	Shropshire et al., 2006	Security-Compliant Behavior	CON, AGREE
19	Svendsen et al., 2011	Technology Acceptance	All
20	Vance et al., 2009	Protection Motivation Theory	CON, NEURO

3. Research methodology

The IS domain is characterized by a plurality of applied research methods. In addition, IS researchers successfully transferred various areas from other disciplines into the IS domain (Österle et al., 2010), especially instruments from natural and formal sciences and engineering (Wilde and Hess, 2007). This leads to a heated "rigor versus relevance" debate within the community. On the macro level, two fundamental IS research paradigms can be differentiated (i.e. Hevner et al., 2004; Österle et al., 2010; Wilde and Hess, 2007). On the one hand the design-science oriented paradigm is mainly applied in the European IS domain, especially in the German speaking countries and Scandinavia (Österle et al., 2010). The European IS domain, as a relatively young IS domain, is characterized by the application of principles, methods and tools to design, implementation, operation and evaluation of IS artifacts with the aim to establish as an independent discipline compared to the neighboring disciplines business economics and informatics (Greiffenberg, 2003; Neumann et al., 2010). McKay and Marshall (2007) emphasize that design science is domain-independent and interdisciplinary in which domain specific knowledge of design practices are aggregated (McKay and Marshall, 2007). The main focus of the design science research paradigm lies in the development and evaluation of artificial IS outcome objects (Gregory, 2010). These so called IS artifacts can be constructs, models, methods, or instantiations, or a combination thereof (March and Smith, 1995; Gregory, 2010) as well as concepts (Järvinen, 2007). Hevner et al. (2004) emphasize that the design science paradigm seeks to develop artifacts that "define the ideas, practices, technical capabilities, and products through which the analysis, design, implementation, management, and the use of information systems can be effectively and efficiently accomplished" (Hevner et al., 2004, p. 76). IS artifacts intended to solve a class of general organizational problems rather than solving a problem in a specific organizational environment (Hevner et al., 2004; Hrastinski et al., 2008).

The Anglo-Saxon IS domain is mainly based on the behavioral science research paradigm (Österle et al., 2010), which has its roots in natural science (Bhadauria 2006; Hevner et al., 2004). Behavioral science involves the organizational and especially human phenomena by focusing on the explanation and prediction of management, analysis, design, implementation, and use of information systems (Hevner et al., 2004). Rather than the design of an IS artifact, the behavioral science paradigm focuses on the observation of IS characteristics and user behavior (Österle et al., 2010) with the use of the empirical examination of hypotheses (Becker and Pfeiffer, 2006).

Due to the predominance of the behavioral science paradigm in the Anglo-Saxon IS domain, most relevant IS journals e.g. Management Information Systems Quarterly (MISQ) or Information Systems Research (ISR) follow behaviorism as the preferred research paradigm (Österle et al., 2010). Combined with the call for more cumulative research by Mertens in 2005 (Mertens, 2005 cited in Neumann et al., 2010), a shift to more descriptive topics in the European IS research community is identifiable. The leading German-speaking IS researchers seek to position design science research in the international IS research community (Österle et al., 2010). The authors underline the lacking practical relevance of scientific results and demand for concrete accepted criteria for transparent and well-documented results (Österle et al., 2010). Hevner et al. (2004) calls for a combination of both research paradigms in which designed IS artifacts are based on behavioral science theories and behavioral science predicts and explains the created IS artifacts (Hevner et al., 2004). Therefore, behavior science and the development of IS artifacts are not dichotomous (Lee, 2000) resulting in a "multi-facettedness" of IS research (Niehaves, 2007).

Table 5: Behavioral vs. Design Science Research (based on Bhadauria, 2006; Hevner et al., 2004; March and Smith, 1995; Niehaves, 2007)

Factor	Behavioral Science Paradigm	Design Science Paradigm
Focus	People	Technology
Nature	Descriptive	Prescriptive
Object of Study	Natural and artificial phenomena are studied	Artificial phenomena are studied
	Human-Computer Interaction	IS artifact design
Results/ IS outputs	explaining and predicting organizational human phenomena	creating effective artifacts
Objective	seeks to answer 'what is true'	seeks to answer 'what is effective'
Method	observational studies and experiments but mostly empirical in nature	primarily experimentation, observation can be made
Relation to knowledge	primarily knowledge-producing	primarily knowledge-using
	theorize and justify	build and evaluate
Normative dimension	problem understanding paradigm	problem solving paradigm
	reactive with respect to technology which is viewed as given	proactive with respect to technology

In this thesis, both research paradigms are applied, while the primarily applied methodological research approach is the behavioral science research paradigm. Part A of this thesis addresses the development and justification of behavioral theories and models that focus on individual differences and cognitive processes within the information security context from information security executives' perspective. Based on identified research gaps, these theories and models explain and predict human-related phenomena with the aim to increase efficiency of organizational information security. The design science research paradigm is applied in part B of this thesis. In particular, chapter 5.2 applies

ADR as the underlying research method, resulting in the design and evaluation of a process model which represents the IS artifact.

It becomes obvious that in this thesis multiple research methods are applied to analyze and evaluate the proposed research questions and to collect and test the empirical data. More specific, beside literature reviews which are the basis for every single publication, five research methods are employed in the scope of this thesis. Some research methods are used to build the necessary basis for the application of other research methods. In IS discipline, one way to distinguish between research methods is the classification of qualitative and quantitative methods (e.g. Myers, 1997; Lee and Hubona, 2009). In the following sub-chapters two types of qualitative and three types of quantitative research approaches are distinguished. Note that these five types are not exhaustive; a broader overview can be found in Palvia et al. (2004) or Wilde and Hess (2007).

3.1 Qualitative research methods

3.1.1 Content analysis

Content analysis “is a research technique for making replicable and valid inferences from texts to the contexts of their use” (Krippendorf, 2004; p. 18). Research studies which apply qualitative content analysis as the underlying research method aim to interpret the content of text data with the use of systematic classification processes of coding and identification of themes or patterns (Hsiu-Fang and Shannon, 2005). In this sense, analysis objects can include for example written texts (e.g. research paper, manuals) or transcripts of spoken texts (interviews, speech) (Mayring, 2000). With the use of content analysis techniques the complexity of data or information is reduced by consolidating fragments into different predefined or identified categories (Neuendorf, 2002). In literature reviews, a purely quantitative evaluation of for example identified literature clusters is not sufficient for a synthesis of findings (Seuring and Gold, 2011). Therefore, content analysis is an effective way for analyzing research paper in a systematic, rule-bound, and theory driven way (Mayring, 2008).

One option for a detailed content analysis process can be found in Lechtchinskaia et al. (2011) (Figure 9) and in parts in Uffen et al. (2012a), which are based on the guidelines of Mayring (2000; 2008). With the use of a comprehensive literature review, a qualitative content analysis was conducted for synthesizing and consolidating the material. First, after delimitating the context of investigation, formal categories are defined, providing the coding background for the subsequent content analysis (Mayring, 2008, Seuring and Gold, 2011). The classification of the material is derived using two approaches: first inductive code generation followed by deductive code generation. Applying an inductive approach, noticeable attributes are derived from the identified material, leading into a continuous category building and application process (Mayring, 2000). During literature analysis, these categories are continuously validated and extended in a deductive way (Hsiu-Fang and Shannon, 2005). This open-ended approach has been proven as useful for synthesizing and consolidating the material. Especially the separation into transparent steps allows the researcher to check for traceability and inter-subjective verifiability (Mayring, 2008; Seuring and Gold, 2011). For example further statistical analysis can be applied to assess for inter- and intra-coder reliability, and validity (Lechtchinskaia et al., 2011). However, the qualitative content analysis is one of various other and comparable research methods to analyze material (Hsiu-Fang and Shannon, 2005).

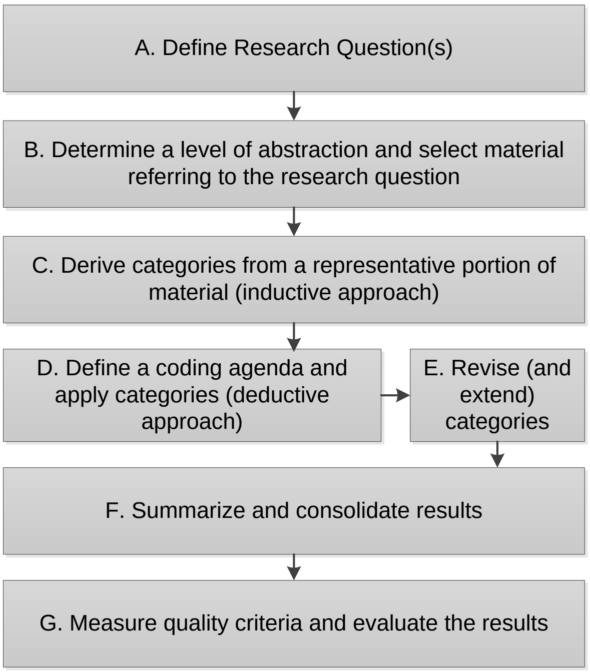

A. Define Research Question(s)
B. Determine a level of abstraction and select material referring to the research question
C. Derive categories from a representative portion of material (inductive approach)
D. Define a coding agenda and apply categories (deductive approach)
E. Revise (and extend) categories
F. Summarize and consolidate results
G. Measure quality criteria and evaluate the results

Figure 9: Qualitative research approach (cf. Lechtchinskaia et al., 2011)

3.1.2 Action design research

The ADR approach is a qualitative research method that cumulates two research approaches: design science research and action research (AR) (Iivari, 2007; Sein et al., 2011).

AR’s aim is to solve a current practical problem by expanding scientific knowledge (Baskerville and Myers, 2004). Thus, it links theory with practice by combining thinking with doing (Susman, 1983; Sein et al., 2011). Due to the increasing debate about methodological rigor and practical relevance, an isolated application of AR as the underlying research methodology has been criticized (Sein et al., 2011). For example, Anaman (2008) stated that AR is „mostly glorified consulting”. In a similar vein, Goldkuhl (2008) emphasized that AR does not lead to enhanced scientific knowledge of high credibility. Design science research (explanation see above) is often criticized due to its dominant thinking of a technological view of the IS artifact and less attention to the organizational context (Sein et al., 2011).

To avoid this criticism and close the gap between organizational relevance and methodological rigor, IS researchers emphasized an integrated approach of DSR and AR (Iivari 2007; Lee, 2007; Sein et al. 2011). Iivari (2007) first mentioned the term "action design research". Sein et al. (2011) introduced the ADR approach with the objective of increasing the organizational relevance by integrating a continuous interaction of practitioners and researchers, and increase methodological rigor by design and evaluation of generalized IS artifacts that solve a class of problems through formalized learning from organizational intervention.

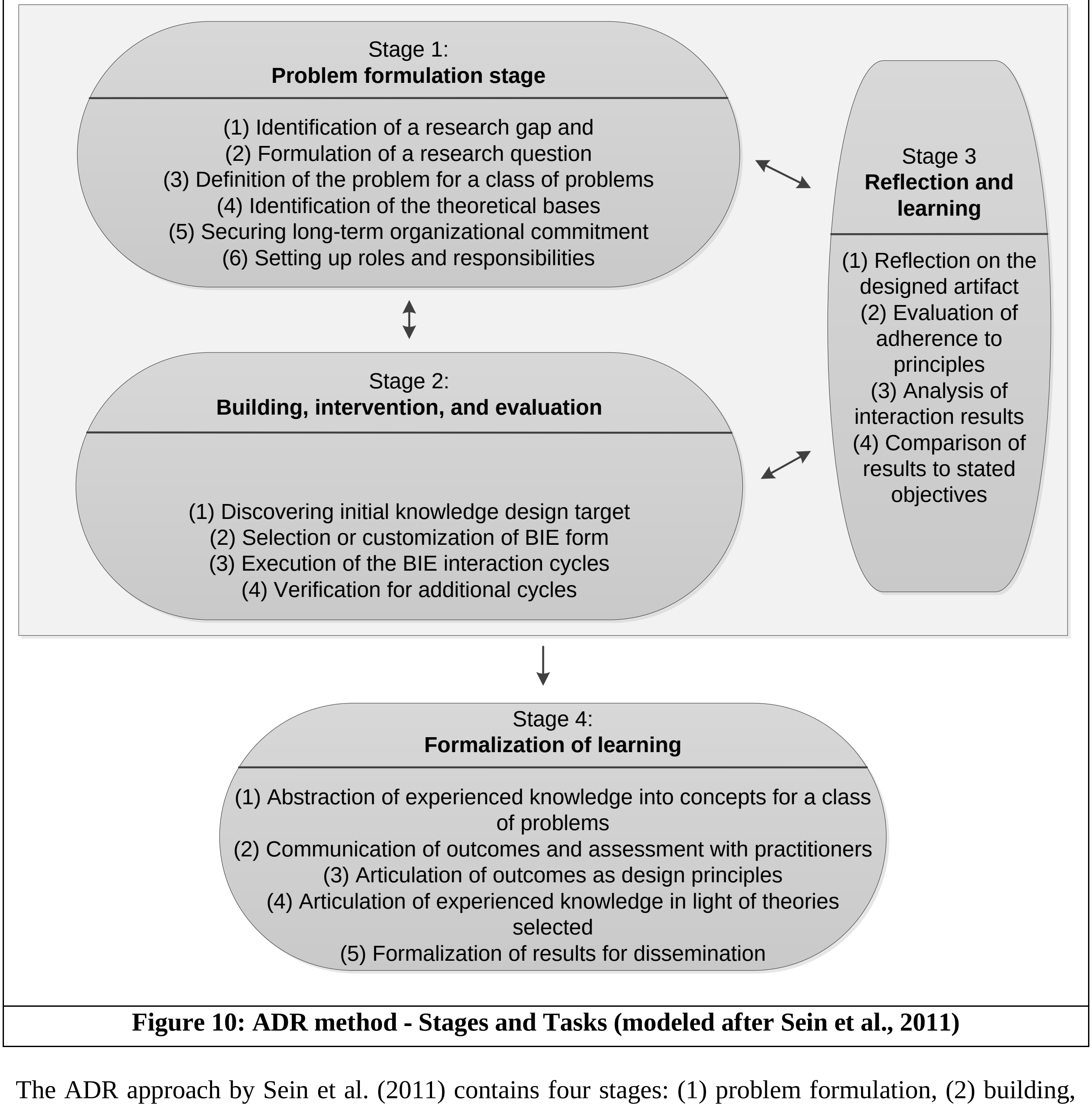

Stage 1:
Problem formulation stage
(1) Identification of a research gap and
(2) Formulation of a research question
(3) Definition of the problem for a class of problems
(4) Identification of the theoretical bases
(5) Securing long-term organizational commitment
(6) Setting up roles and responsibilities
Stage 2:
Building, intervention, and evaluation
(1) Discovering initial knowledge design target
(2) Selection or customization of BIE form
(3) Execution of the BIE interaction cycles
(4) Verification for additional cycles
Stage 3
Reflection and learning
(1) Reflection on the designed artifact
(2) Evaluation of adherence to principles
(3) Analysis of interaction results
(4) Comparison of results to stated objectives
Stage 4:
Formalization of learning
(1) Abstraction of experienced knowledge into concepts for a class of problems
(2) Communication of outcomes and assessment with practitioners
(3) Articulation of outcomes as design principles
(4) Articulation of experienced knowledge in light of theories selected
(5) Formalization of results for dissemination

Figure 10: ADR method - Stages and Tasks (modeled after Sein et al., 2011)

The ADR approach by Sein et al. (2011) contains four stages: (1) problem formulation, (2) building, intervention and evaluation, (3) reflection and learning, and (3) formalization of learning. This approach underlies the principle of an organizational problem to be solved by action research, and then use design science principles to build an artifact to solve this concrete problem. Afterwards, the lessons learned are reflected and generalized. More in detail, the problem formulation stage is based on design-science principles by Hevner et al. (2004). It identifies a specific organizational problem and conceptualizes a research opportunity in consideration of existing technologies and theories (for this and the following see Sein et al., 2011). Based on the research opportunities, the artifact is build with a continuous interaction of researchers and practitioners. The second stage results in the design of the IS artifact. A continuous reflection and learning process to apply the solution to a broader class of problems is recommended during the first two stages. In the last stage, this learning process is formalized. Figure 10 illustrates the four stages and depicts the tasks in the respective stages, which need to be undertaken by the researcher.

In their research paper, Sein et al. (2011) applied their proposed ADR model in a research project at Volvo IT. The authors explicitly stated that “ADR is useful for open-ended IS research problems that require repeated intervention in organizations to establish the in-depth understanding of the artifact-context relationship needed to develop a socio-technical design agenda for a specific class of problems” (Sein et al., 2011; p. 52, 53). This was especially the objective in the publication presented in chapter 5.2.

3.2 Quantitative research methods

3.2.1 Survey

Surveys are defined as a cross-sectional, longitudinal, quantitative research method, which aims to generalize from a specific sample to a population (Babbie, 1990; Creswell, 2008). The rationale of surveys is to reduce the gap between theory and practice, and increase the value for practitioners. Survey research is appropriate for answering “how and why is a phenomenon happening”, when the research object must be studied in its natural setting, and the control of the dependent and independent constructs is not possible (Pinsonneault and Kraemer, 1993). More specific, one of the most widely applied types of quantitative research is the confirmatory, theory testing research method (Forza, 2002). This research method’s aim is testing the adequacy of theoretically grounded concepts, models and propositions about how and why predefined constructs and variables are in a causal relationship to each other (Creswell, 2008; Forza, 2002; Glasow, 2005; Pinsonneault and Kraemer, 1993). Forza (2002) proposes a six-step approach which presupposes a predefined theoretical model or conceptual framework. This approach focuses on (a) the translation process from a theoretical model into the empirical domain, (b) the research design including the consideration of constraints and the definition of target groups, (c) the pilot test, (d) data collection and analysis and (e) the reporting of results with discussion, interpretation and writing a report (Forza, 2002).

Structured and unstructured quantitative data are typically gained with the use of questionnaires. A questionnaire contains a specific number of items with different scales. Within the context of this thesis, quantitative questionnaires are used completely structured and closed-ended. The participants are questioned to evaluate their attitude and opinions to a pre-specified statement on a bipolar and equidistant 5-point Likert Scale (see Likert, 1932). Most research studies within this thesis are based upon primary data (e.g. Uffen et al., 2013c; Lebek et al., 2013a,b,c), but also secondary data play an important role (e.g. Uffen et al., 2013a,b). Research studies containing primary analysis techniques are based on original data, in which a researcher plans the survey design as a method to evaluate the research question, collects the data, summarizes and makes inferences from the data and evaluates the results (Church, 2001). Secondary analysis techniques are applied of researchers that were not involved in the planning of the research study or the collection of the data (Church, 2001). Such analysis is defined as the re-analysis of existing data for the purpose of answering existing or new research questions with better statistical analysis techniques (Glass, 1976). For example, in Uffen et al., 2013a, existing empirical data were used for answering the proposed research question. The empirical data were collected in a prior work at the Institute of Information Systems, Gottfried Wilhelm Leibniz Universität, by, and published in a monograph, Dr. Robert Pomes (Pomes, 2011). In this work, the author connected personality traits of information security decision makers with four information security dimensions. With the use of correlation analysis, a technique of bivariate statistics, the collected empirical data of information security decision makers were analyzed (Pomes, 2011). Correlations are used to measure the relation between two constructs, neither of those are independent constructs (Backhaus et al., 2011). Thus, with the use of statistical methods from multivariate statistics and enhanced theoretical knowledge (personality traits, TPB, holistic information security), this data source was re-analyzed. At all, two data analyzing techniques of multivariate statistics are applied: principal component analysis and structural equation modeling.

3.2.2 Principal component analysis

Principal component analysis (PCA) is a multivariate data analysis technique with the purpose to identify latent constructs within a number of items (Backhaus et al., 2011). It is a dimension reduction method that seeks the linear combinations of a number of items that maximizes their variance (Zou et al., 2006). The number of components can be determined by two optional procedures. On the one hand a scree or elbow test is possible to plot calculated eigenvalues according to their size. Eigenvalues represent the value of variance explained by each principal component resulting that the first identified component indicates the highest amount of variance in the data (Suhr, 2005). In a graph, the eigenvalue’s slope goes from steep to flat that all components which are after the “elbow” are not considered (Backhaus et al., 2011; Abdi and Williams, 2010). The second option is to keep those components whose eigenvalues are larger than 1 (so called Kaiser criterion, cited in Backhaus et al., 2011). After defining the number of components, and in order to allow an interpretation of the results, PCA involves a rotation of the identified components (Abdi and Williams, 2010). The most widely applied, and also important in this thesis, rotation method is orthogonal. With the use of orthogonal rotation, factor loadings are equivalent to correlations between observed items and the underlying component (Suhr, 2005).

Researchers apply PCA with the objective to extract important information from a data observation and express this information as a set of new orthogonal constructs which are also referred to as principal components (Abdi and Williams, 2010). Further, PCA is often applied as a dimension reduction method and in line as a quality criterion in combination with SEM (see Uffen et al., 2012a).

3.2.3 Structural equation modeling

Structural Equation Modeling (SEM) is either a data analysis technique of multivariate statistics. Recently, SEM has become more and more important in any research discipline, including social science, psychology, marketing, organization, and business science (e.g. Bagozzi, 2011; Gefen et al., 2011; Podsackoff et al., 2003). In IS research, SEM has become a quasi-standard for empirical studies with the aim to evaluate theoretical models empirically (Chin, 1998; Gefen et al., 2011). SEM is based on two traditions – an econometric emphasis that allows prediction and a psychometric focus that models concepts or frameworks by measuring latent (unobserved) constructs which are based on diverse indicators (Chin, 1998). Compared to other data analysis techniques such as principal component analysis, or multiple regression analysis, SEM is an example of a second generation technique that allows researchers to perform path analytic modeling with latent variables (Chin, 1998; Fornell and Larcker, 1987).

Two SEM-approaches can be distinguished – covariance-based SEM and variance-based SEM (PLS) (Jöreskog and Sörbom, 1982). The first approach evaluates the sample covariance or correlation matrix consistence of a specified research model (Jöreskog and Sörbom, 1982). Software tools such as LISREL assess the maximum fit between parameter estimates and correlation matrix, meaning that the estimates are improved so long, until no fitting improvement is possible (Reinartz et al., 2009). This is contrary to PLS or variance-based SEM approach. PLS is defined as a causal modeling technique that maximizes the explained variance of the in a theoretical model defined dependent latent construct (Hair et al., 2011). Variance-based SEM is preferable compared to covariance-based SEM, when the emphasis is on theory development, prediction of latent constructs and identification of relationships between them and the sample size is relatively small (100 observations can be sufficient) (Reinartz et al., 2009). These divergences in both SEM approaches lead to a wide discussion of the suitability in research studies (e.g. Hair et al., 2011; Reinartz et al., 2009). In this thesis, the focus lies on the application of the PLS approach. The motivations that led to this choice are given in each publication.

Measurement model links latent constructs to formative and/or reflective indicators and the structural model provides the relationships between the latent constructs (Chin, 1998). Constructs are the basic elements of a theory or measurement model. Items or indicators measure the latent construct of a specific measurement model. In the course of operationalization of the latent constructs, it is important to distinguish between formative and reflective measurement models (Figure 11). In the PLS approach, latent constructs can be modeled with both, formative and reflective indicators (MacKenzie et al., 2011). Formative indicators are measures that are not correlated to each other and cause or form the creation or change in a latent construct (Chin, 1998). These so called causal indicators reflect the idea that the indicators are causing instead of being caused by the latent construct (MacCallum and Browne, 1993). Reflective measurement models or constructs are indicated by observed measures that are affected by an unobservable, latent construct (MacCallum and Browne, 1993). A latent construct is measured reflectively due to the interchangeability of the items, the direction of causality, the covariation among the items, and the nomological net of the constructs that should not differ (Petter et al., 2007). In other words, while in reflective measurement models changes in the latent construct cause changes in the indicators, in formative measurement models changes in the indicators cause changes in the value of the latent construct (Diamantopoulos and Winklhofer, 2001; Diamantopoulos et al., 2008; Hair et al., 2011).

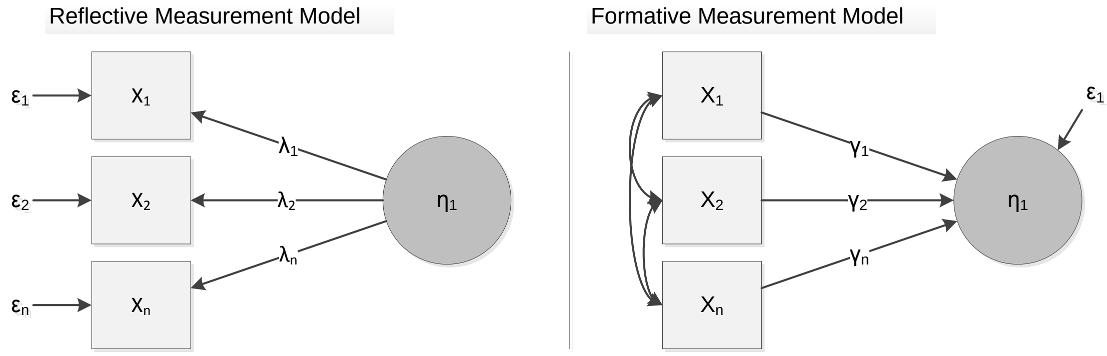


Figure 11: Reflective vs. formative measurement models

In literature, an omnipresent discussion is about the misspecification of indicators (e.g. Diamantopoulos et al., 2008). Most researchers apply reflective measurement models without even questioning their appropriateness (Diamantopoulos et al., 2008). For example, in their critical literature review of measurement model specification in three strategic management journals, Podsakoff et al. (2006) found out that 62 percent of constructs contained misspecifications. Misspecifications can lead to theoretical and empirical misinterpretation. To avoid these misspecifications, researchers must design the measurement models with care to ensure that the specified model is connected to the theory.

The application of PLS requires an analysis of different quality criteria. Typically, a two-step process is necessary, separated by the assessment of quality criteria of the structural and the measurement model (Hair et al., 2011). With regard to reflective and/or formative measurement models, different quality criteria need to be observed. The first step is to examine measurement model by calculating indicators' reliability and validity (for this and the following see: Hair et al., 2011). With regard to reflective and/or formative measurement models, the concrete quality criteria are different. If these quality criteria are shown to be adequate, the second step involves an assessment of the structural model including the examination of the parameter estimates' stability. Individual path coefficients' significance is assessed with the use of bootstrapping. However, in literature, diverse quality criteria are discussed (for details see e.g. Chin, 1998; Hair et al., 2011) whose description goes beyond the scope of this thesis. The applied quality criteria are stated separately in each publication.

4. Personality traits and information security management

4.1 Information security dimensions – A holistic approach

4.1.1 Preamble

This chapter is based on the research paper with the title “Towards a Sustainable and Efficient Component-based Information Security Framework” (Uffen et al., 2012a). The paper was published and presented at the German IS conference “Multikonferenz der Wirtschaftsinformatik” in Braunschweig, Germany (February 29 – March 2, 2012). The MKWI is the second biggest conference in the German IS field, providing a platform for especially German-speaking researchers to present and discuss their research findings. The paper was submitted to the Mini-Track “Integriertes Ertrags-, Compliance- und Risikomanagement” which belongs to the Track “Informationsmanagement”. The conference proceedings are rated by the WKWI and GI-FB WI with a “C” (WKWI, 2008). The VHB-Jourqual2.1 (2011) rated the MKWI with a “D”.

Note: For the purpose of this thesis, the following formulations and statements show a summarized version of the initial paper with an extended view to the limitations. For a detailed view of the paper see Uffen et al. (2012a).

4.1.2 Introduction

ISM needs to address any security related issues to obtain sustainable and efficient information security in their organization. The ISM domain is no longer exclusively a technical one, moreover strategic, human, economic, and other aspects have to be considered (Eloff and Eloff, 2005). It is important that ISM takes a holistic, multidimensional approach that fits the organizational requirements and needs and incorporates the organizational units and stakeholders. This leads to an increasing discussion of researchers and practitioners about the number and content of information security dimensions that need to be taken into account (D’Arcy et al., 2009). National and international standards organizations provide fundamental best-practices, guidelines, and standards, for example the “National Institute for Standards and Technology (NIST)” special publications such as SP 800-39 or the German “Bundesamt für Sicherheit in der Informationstechnik” (BSI) such as IT-Grundschutz-Standards. But organizations often face difficulties in managing an approach that considers holistic information security dimensions (Eloff and Eloff, 2005) because there is no generally accepted framework or model with a coherent number of dimensions (Kritzinger and Smith, 2008; May and Dhillon, 2010).

Given the variety of academic publications on the topic of information security frameworks, there is still a lack of approaches that combine theoretically and practically substantiated principles. The aim of this paper is to give a state of the art of information security dimensions that are part of an information security framework and summarize these findings to an all encompassing holistic framework. To evaluate the practical relevance empirical data from information security executives are used. The resulting framework shall assist organizations and researchers to ensure a consistent and holistic view that address the organizational information security requirements (Da Veiga and Eloff, 2007).

In the context of this thesis, an information security framework is based on the interaction of interdisciplinary dimensions and sub-components, relevant for efficient and sustainable implementation of information security. Sub-components in the following concretize dimensions and are integrated parts of information security frameworks. Sub-components are determined by numerous detailed items.

The research design consists of four steps. During previous step, critical information security success factors are identified using a comprehensive literature review combined with a qualitative content analysis. In the second step, general components are systematically summarized and consolidated, resulting in a comprehensive list of information security components. This forms the basis for the evaluation of the practical relevance. Based on the practical assessment of information security components and using principle component analysis (PCA) (Backhaus et al., 2011), the results are summarized and interpreted.

4.1.3 Theoretical background on information security components

Reviewing literature is an adequate method for analyzing and synthesizing prior research in order to indicate a “firm foundation for advancing knowledge” (Webster and Watson, 2002). Several researchers have discussed different component-based information security frameworks (see e.g. Chiang et al., 2009; Park et al., 2010; Saleh et al., 2006; Torres et al., 2006; Trčeck 2003).

From the identified information security frameworks, the first step was to identify the underlying components. For that purpose, a qualitative content analysis as described in chapter 3.1.1 is applied. This results in a comprehensive list of items, which needed to be summarized and consolidated for better interpretation. From literature, the examination of items lead to several sub-components that reveal that ISM can be summarized to seven dimensions – technical, human, organizational, compliance/monitoring, economical, cultural and strategic. The dimensions and the underlying sub-components are presented in the following:

- Technical dimension: ISM faces complex technical security challenges (see e.g.Eloff and Eloff, 2005). In consideration of growing operational sophistication of current security risks, technical security is one of the major parts to assure information security (Park et al., 2010). Management faces risky decisions considering the effective implementation of several countermeasures such as intrusion detection systems (IDS) or firewalls in its information security architecture (Cavusoglu et al., 2009). According to Park et al. (2010), practitioners need to reflect how to secure a seamless flow of data under in consideration of technical constraints and the emergence of new and continuously changing security threats. Nevertheless, the implementation of massive technological security components is in vain without complementary other security components, especially the human component (Bulgurucu et al., 2010; Park et al., 2010).

- The organizational dimension is represented by managerial activities. The implementation of information security requires top-management support, sponsorship and commitment (Broderick, 2006). ISM has to define concrete requirements, for example how to react systematically and methodologically in terms of security breaches. These points are critical since these decisions are accompanied by operational and technical components (Torres et al., 2006). The harmonization of organizational objectives with business and information security strategies is challenging (Park et al., 2010). Further, increasing operation and interaction with external partners require coordination on management level (Chiang et al., 2006).
- The weakest link in information security is still the human factor (Yildrim et al., 2011). Mistakes, end-user ignorance, and deliberate acts can lever every technical countermeasure (Bulgurucu et al., 2010). Therefore, behavioral aspects have to be considered, directed and monitored to guarantee compliance with organizational security policy and legal requirements (Da Veiga and Eloff, 2007). Appropriate methods to improve security awareness and enhance security-related behavior are SETA programs (Werlinger et al., 2009). Further, selective allocation of authorization in terms of identity and access management has an additional preventive effect (Tashi and Ghernouti-Hélie, 2009).
- ISM has to balance costs and benefits in their security-related decisions (Park et al., 2010). But organizations rarely undertake return on investment calculations on for example security investments (Torres et al., 2009). IT departments often face challenges in budgetary restrictions (Werlinger et al., 2009) but investments in information security are not straightforward (Torres et al., 2006). Information security threats are changing rapidly, so security decisions are often time-critical (Park et al., 2010). In such situations, fast decision-processes with adequate financial resources are indispensable. Consequently ISM faces the challenge to coordinate every security component in an economic way considering the requirements of the organization (Tashi and Ghernouti-Hélie, 2009).
- The compliance dimension is represented by organization internal factors such as information security policies and guidelines as well as external factors such as information security expectations of stakeholders and other third parties, legal requirements, best-practices, and important standards such as ISO/IEC 27002 or COBIT. Further, continuous monitoring as

well as auditing procedures are important to guarantee that policies, processes, and people are in line with the organizational objectives, strategies and visions (Da Veiga and Eloff, 2007).

- The integration of information security into corporate culture is essential (Trček, 2003), meaning that employees across an organization must live and shape the security culture. For example ethical conduct, such as not using organizational internet connections for private purpose, has to be regarded as an accepted way of conduct (Da Veiga and Eloff, 2007). Further, trust is an established issue in information security culture (Tudor, 2000). Da Veiga and Eloff (2007) stated that mutual trust between management and its employees is important when implementing new information security procedures and instruct end-users through behavioral changes in daily information security operations (Da Veiga and Eloff, 2007). Security compliant behavior must be embedded in employees' minds.
- Information security strategies are specified plans of organizational future objectives, which in consideration of their resources, give an input of the future development of an IS (Torres et al., 2006). The information security strategy is as an integrated part of corporate strategy. The strategic components build the basis for ISM (see e.g. Tashi and Ghernouti-Hélie, 2009; Da Veiga and Eloff, 2007) especially for business continuity management (Trček, 2003). After putting into operation, the organizations have to evaluate outcomes and critically examine their information security strategies (Park et al., 2010).

4.1.4 Evaluation of practical relevance

The identified security dimensions need to be evaluated due to their practical relevance. To gain practical implications, the authors used empirical data from information security executives in this research field (see chapter 3.2.1). The information security parts of the empirical data contained the seven main components and their related sub-components, but were unstructured. Participants were information security executives such as Chief (Information) Security Officers (C(I)SO) from German-speaking countries, which were identified through information security online social networks (Xing, CIO.com, ITheads.com). After data cleansing, principle component analysis (PCA) with varimax rotation was applied to validate the practical application of the identified components (see section 3.2.2).

Two PCAs were applied, one on the sub-component level and one on the dimension level. In step one, PCA is used for identifying sub-components within each dimension. This means that the pool of items was analyzed with a PCA in order to reduce the number of items to a specific number of sub-components. The results were compared to the pool of items identified in the above mentioned literature review. Based on these findings, the sub-components were analyzed based on their content and further categorized to one of the seven information security dimensions (Table 6). In step two the commonalities within the dimensions were verified. The results of the second PCA are not important for the following chapters and are therefore discussed shortly in this thesis. For more information to the second PCA see the original paper (Uffen et al., 2012a). To identify a valid number of factors, latent root criterion was used; only factors with eigenvalues greater than 1 were selected. For each analysis KMO-criterion is above 0.728 which is acceptable to perform factor analysis (Kaiser, 1974).

Table 6: Results of PCA

	Factor	Eigen-value	Variance (%)	Cum. Variance (%)	Item	Interpretation	Factor loading
Technical	**TECH1**	3.142	28.566	28.566	T1 T2 T3 T4	Network administration	0.730 0.696 0.689 0.521
	TECH2	1.351	12.279	40.845	T5 T6 T7	Critical system administration	0.758 0.680 0.501
	TECH3	1.085	9.862	50.707	T8 T9 T10	Cryptography	0.756 0.606 0.601
Human	**HUM1**	1.358	27.164	27.164	H1 H2	User management and user awareness	0.743 0.741
	HUM2	1.146	22.917	50.081	H3 H4	Competency	0.839 0.687
	HUM3	1.018	20.359	70.440	H5	Access	0.899
Organizational	**ORG1**	1.497	29.933	29.933	O1 O2	Top-Management support	0.843 0.820
	ORG2	1.216	24.322	54.255	O3 O4	Leadership and coordination (Middle Management)	0.784 0.766
	ORG3	1.033	20,663	74.918	O5	Effective risk management	0.955
Compliance and Monitoring	**COMP1**	2.541	25.408	25.408	C1 C2	Regulatory and legislative standards	0.831 0.771
	COMP2	1.458	14.585	39.993	C3 C4 C5	Control approaches and objectives	0.821 0.607 0.510
	COMP3	1.248	12.484	52.477	C6 C7 C8 C9	Monitoring	0.793 0.627 0.617 0.527
Economic	**ECO1**	1.310	32.746	32.746	E1 E2	Monetary factors	0.797 0.653
	ECO2	1.009	25.220	57.966	E3 E4	Non-monetary factors	0.800 0.579
tur	**CULT1**	1.244	31.093	31.093	Cu1	Ethical and identification values	0.814

					Cu2		0.637
	CULT2	1.036	25.860	56.953	Cu3	Trust	0.707
					Cu4		0.644
Strategic	**STRAT1**	2.243	44.863	44.863	S1	Information security strategy management	0.872
					S2		0.771
					S3		0.716
	STAT2	1.043	20.855	65.718	S4	Business continuity	0.841
					S5		0.763

The main results of the first PCA are discussed in the following. Each sub-component is shown in italics:

- Technical sub-components: The implementation of technical security measures requires: *network administration* which contains IT application security such as installation, administration, and monitoring of for example firewalls, antivirus, backup and data recovery; *critical system administration* which intrusion detection systems or risk system access control administration, and *cryptography* which specifies built-in encryption, security certificate creation and management or electronic signature and electronic data interchange (EDI) administration.
- Human sub-components: This component contains: *user management and user awareness*, *competency* and *access*. The main factor includes SETA programs as proposed in chapters 1.2.2 and 4.1.3; the second factor deals with the promotion of competence on employee level as well as support of management competence in information security related topics. The latter addresses an effective organizational user access management containing authorization or identity management concepts.
- Organizational sub-components: These components contain the *top-management support* such as top management awareness of and involvement in security-related topics, *the leadership and coordination* on a middle management level e.g. delegation or other classical management tasks, and an *effective risk management* as part of holistic identification and handling of security risks.
- Compliance and Monitoring sub-components: The *regulatory and legislative standards* address ISM and other compliance standards represented by for example ISO/IEC 27002 or COBIT. *Control approaches and objectives* contain general concepts, guidelines and checklists such as internal information security concepts or the implementation of internal controls procedures as proposed by COBIT. *Monitoring* includes the monitoring of internal misuse of IS resources, controlling of security systems or interface monitoring.
- Economic sub-components: This component can be separated to *financial* and *non-financial factors*. Information security decisions have direct financial impacts such as project budgets, running costs or unwanted/ unexpected cost for example in a case of a security incident. Non-

financial factors are represented by time-related considerations, potential penalties or lost customer orders because of bad reputation.

- Cultural sub-components: This component is represented by *ethical conduct and identification values*, and *trust*. Living organization's values and the relating acceptance of corporate principles are important factors for sustainable information security which have to be targeted on a long-term basis. In addition, trust among employees and management has to be generated using, for example confidence-building measures.
- Strategic sub-components: Strategies require an appropriate *management* which contains visions, objectives and goals, documented in regard of current and future orientation and b*usiness continuity* which includes emergency plans or security manuals that ensure short recovery times in the case of unavailable IS infrastructure.

These 18 mentioned factors have to be considered with a special focus aligned with the organizational objectives in an ISM approach. The above mentioned components are not exhaustive and need to be tailored to the specific organizational requirements. However, the analysis of the identified information security components leads to the assumption that the dimensions can further be divided into long- and short-term dimensions. To proof this assumption, a second PCA on the dimension level was conducted. The second PCA results into two main factors. The first factor contains the technical, human, organizational and compliance dimension and the second factor include the cultural, economic and strategic dimensions. These results underline the assumptions. Practitioners should realize the interaction of short-term and long-term security elements to ensure sustainable and efficient implementation of information security.

4.1.5 Conclusion, limitations and outlook

The paper of Uffen et al. (2012a) identifies and discusses a holistic ISM approach containing of seven dimensions – technical, human, organizational, compliance/monitoring, economic, strategic and cultural. Given the body of knowledge towards ISM approaches, this study combines theoretically and empirically grounded principles. The study starts with a comprehensive literature review to identify as many security-related items as possible. Followed by a structured consolidation, the practical relevance was tested with empirical data of 174 information security executives. The results show a spectrum of 18 information security sub-components which assist information security executives to implement and manage a sustainable and efficient ISM approach. Information security practitioners can use the approach in order to design new - or review existing - information security programs in organizations.

One limitation of the study relates to the empirical database. Each answer of participants depends on the individual risk tolerance during implementation of information security (see e.g. Anderson and Choobineh, 20080). The questions in this study were not examined with participants who are for example completely risk-averse. Further, every organization that participated in the study was from a German-speaking country. Considering differences in the cultural and legal environment, it is likely that information security executives in other countries have different attitudes or reactions towards the implementation factors of information security within organizations. Further, the initial scope of data collection was not the investigation of information security dimensions. But these dimensions were also contained in the database and compared to personality traits. Therefore the authors found the PCA appropriate. Thus, the ISM approach needs to be tested in real-world environments. The empirical investigation of information security executives only measures their attitude and does not show the applicability in a real-world phenomenon. One option may be an applicability check of the ISM approach. Based on these findings, the number or labels of components may differ to the above mentioned.

A further limitation addresses the comparability to international standards or guidelines. For example the proposed ISM approach needs to be compared to ISO/IEC 27002. In the present study, only academic relevant information security sub-components were extracted. International standards were not taken into account. Nevertheless, some of the research studies, identified in the literature review, were based on ISO/IEC 17799 or ISO/IEC 27002. For future research, the results can be extended to a more international context and compared in consideration of cultural differences. Furthermore this study can be extended taking the information security executives´ personality into consideration with personality models.

4.2 Personality traits and holistic information security management

4.2.1 Preamble

This chapter is based on the research paper with the title “Personality Traits and Information Security Management: An Empirical Study of Information Security Executives” (Uffen et al., 2012b). The paper was published and presented at the international IS conference “International Conference on Information Systems” in Orlando, Florida (December 16 – December 19, 2012). The ICIS is the most prestigious and biggest IS conference worldwide, providing a platform for researchers to present and discuss their research findings. The conference guarantees high quality and professional focus of published research papers. This is reflected by the 4,000 members from more than 95 universities worldwide.

The paper was submitted to the Mini-Track “Enterprise Information Security” which belongs to the Track “IS Security and Privacy”. The conference proceedings are rated by the WKWI (WKWI, 2008) and VHB-Jourqual2.1 (2011) with an “A”.

4.2.2 Introduction

The way management – or information security executives – deal with information security risks, behave in different situations and valuate the importance of the in chapter 4.1 information security dimensions varies from individual to individual and depends on personality and other cognitive factors (Straub and Welke 1998; Vroom and von Solms 2004). Therefore, increasing attention in information security research has been paid to individual differences of the management level. For example, Li and Tan (2009) found out that psychological and behavioral processes are more important than demographic factors in explaining the behavior of a Chief Information Officer (CIO). Sharma and Yetton (2003) emphasized the positive influence of CIOs on employee's cognitive beliefs, attitudes, and behavioral factors when dealing with information security. Ashenden (2008) highlighted the need for management soft skills to effectively change organizational culture and to improve communication between end-users, information security executives, and senior managers. In the context of ISM, only few studies have investigated how individual differences between information security executives affect holistic information security management. This was the purpose of the publication of Uffen et al. (2012b). Individual differences are measured using the Five Factor Model (FFM) (Costa and McCrae 1991). The way an information security executive perceives holistic ISM is measured by his or her attitude towards the above mentioned technical and six non-technical dimensions of information security – strategy, organization, human, culture, compliance, and economy.

The relationship between information security executives' individual differences in personality and information security is investigated for several reasons. First, personality traits have become more and more an important issue in IS research, because they determine an individual's cognitive processes, attitudes, and behaviors (Junglas et al. 2008). Yet a number of research studies have shed some light in the investigation of individual differences in the IS domain (e.g. Lee and Larsen 2009; Benlian and Hess 2010; McElroy et al. 2007). In information security research, target subjects of previous studies were limited to end-users or employees (e.g. Shropshire et al. 2006) and did not focus on executive level. Incorporating personality traits of information security executives has largely been ignored. Second, researchers have called for more rigorous research in the information security domain (e.g. Kotulic and Clark 2004; Zhao et al. 2009). The role and responsibility of information security executives have been shown to be main predictors of success (e.g. McFadzean et al. 2007; Straub and Welke 1998). Third, focusing on the problem from a holistic, multidimensional rather than a simple, one-dimensional ISM approach allows us to examine and evaluate the illustrated phenomena on a global view. Personality traits show how information security executives' individual differences determine the strength of a person's attitude towards the technical and non-technical dimensions of information security. In this emerging research topic, a global focus is beneficial for practitioners and researchers alike. Therefore the research study of Uffen et al. (2012b) makes a theoretical contribution by conceptualizing that information security executives’ beliefs and decisions are essentially driven by their personalities.

4.2.3 Theoretical background and research model

To get a valid theoretical foundation of holistic information security, the above mentioned ISM approach is applied (see chapter 4.1). In detail, prior work of Da Veiga and Eloff (2007), Kritzinger and Smith (2008), Ma and Pearson (2005), Saleh et al. (2007) and Werlinger et al. (2010) in combination with information security standards build the theoretical background. Personality traits are measured with the five broad constructs of agreeableness (AGREE), extraversion (EXTRA), openness (OPEN), conscientiousness (CON), and emotional stability (EMO_STAB) (e.g. Costa et al., 1991; Digman, 1990; see a further theoretical background in chapter 2.2). Research studies that focus on information security executive’s personality when assessing the impact on information security are still lacking. Therefore, hypotheses about the influence of an information security executive’s personality traits and their attitude towards the technical and non-technical dimensions of ISM are developed. The integrated research model proposes an explanation of the relationship between information security executives’ individual differences and the attitude and behavioral intention towards holistic ISM (Figure 12 and Table 7)

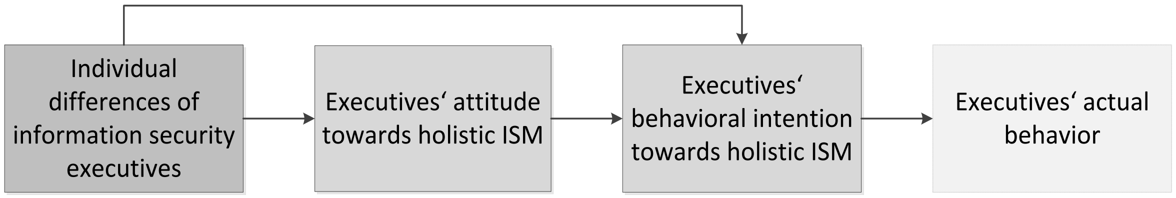

Individual differences of information security executives
Executives‘ attitude towards holistic ISM
Executives‘ behavioral intention towards holistic ISM
Executives‘ actual behavior

Figure 12: General research model

Table 7: Description of research model constructs

Construct	Description	General sources
Personality traits	reflect cognitive and behavioral patterns that show stability across situations and an universal range of use	Catell, 1965
Attitude towards holistic ISM	describes an information security executive’s belief that taking holistic security measures is a desirable behavior that helps to enhance information security in an organization	Fishbein & Ajzen, 1975; Ajzen, 1991
Behavioral intentions towards holistic ISM	represents an executive’s intention to protect the information and technology resources of an organization from potential security breaches by applying a holistic management approach	Fishbein & Ajzen, 1975; Ajzen, 1991; Bulgurcu et al., 2010

Prior research has shown that personality traits are resistant to transformation but vary in their respective relevance to their related object (Junglas et al. 2008). Barrick et al. (2001) demonstrated that some but not every personality traits are more relevant in explaining different factors of behavior. For example, individuals with a higher degree of agreeableness emphasize considerable interpersonal interaction (Mount et al. 1998), while extraversion is related with greater training proficiency (Hough 1992; Barrick et al. 2001). Both traits are characterized by social interaction factors in human beings. Consequently, agreeableness and extraversion are put in relationship to those information security dimensions that contain considerable interpersonal interaction. In contrast, openness has been shown to be an important personality trait in research studies that focus less on interpersonal interaction (Mount et al. 1998). Moreover, individuals who have less emotional stability tend to be more risk-averse (Lauriola and Levin 2001) and less goal-oriented (Judge and Ilies 2002). Both are expected to be indicators of information security executives' attitude toward the strategic and the economic dimension of ISM. Conscientiousness is a personality trait of intrinsic motivation and a high level of job performance (Barrick et al. 2001; Devaraj et al. 2008). Because of the facets of need for achievement and dutifulness, conscientiousness is more relevant in research studies that attempt to investigate multiple factors of performance. These findings show that due to the variety of information security dimensions, specific personality traits are hypothesized to be related to some, but not every one of the technical and non-technical ISM components. A hypothesized relationship is relevant when it is appropriate, and is grounded in and supported by theoretical and empirical research studies.

Based on these results, an integrated research model with 16 relationships between personality traits and the seven attitudinal holistic ISM dimensions are developed. In addition, seven hypotheses between the attitudinal constructs and behavioral intention were included. Figure 13 shows the integrated research model in detail. The relationships are shortly summarized in the following. Conscientiousness has been shown to be the most important personality trait within the research of information security behavior (Hu et al., 2008; Shropshire et al., 2006). In addition, Barrick et al. (2001) have shown a significant relationship between conscientiousness and general job performance. Due to the facets of conscientiousness, e.g. dutifulness, persistence, self-discipline or working hard, it is postulated that information security executives with a higher degree of conscientiousness react more carefully in different situations (Li et al., 2006). This leads to the hypothesized relationship of conscientiousness and every of the technical and non-technical ISM dimensions. The second personality trait, openness, is associated with creativity, receptiveness to innovative ideas, intelligence and imaginativeness. Owing on a broader life experience, these facets are quintessential aspects for technical, strategic, and compliance dimension of information security. Further, openness is not an useful predictor for dimensions with interpersonal interactions or an economic focus. Extraversion and agreeableness are positively related to jobs that include considerable interpersonal interaction (Barrick et al., 2001). Extraversion is associated with being positive emotional, ambitious, and energetic in social situations. Agreeableness shows its facets in situations when interpersonal interaction involves helping and cooperating with others (Barrick et al., 2001). Both traits are therefore hypothesized to have a positive relationship to attitude towards those dimensions with considerable social and interpersonal interaction, represented by the human and organizational ISM dimension. The fifth personality trait, emotional stability, has been shown to be a valid predictor of job performance (Barrick et al., 2001) that has a positive effect on project outcome (Bedingfield and Thal, 2008). Owing on its facets like a lack of pessimism and a tendency not to worry (McCrae and Costa, 1999), emotional stability is hypothesized to be related to the technical, strategic, and economic dimension of ISM.

4.2.4 Measurement model validation and analysis

The revised research model was tested statistically using empirical data of 174 information security executives (see chapter 3.2.1). In that data pool, personality was measured using the 60 item NEO-FFI format by Costa and McCrae (1992). The ISM constructs were developed by prior literature as proposed in chapter 4.1 with a total of 33 indicators. The attitudinal constructs are shaped by the TPB: an individual's attitude towards holistic ISM determines their behavioral intention to apply information security holistically in daily job tasks. The empirical data were analyzed using PCA as dimension reduction technique and SEM for model testing and validation (see chapter 3.2.3). Measurement validation and model testing were conducted using the SEM freeware tool SmartPLS (V 2.0.M.3). The application of SEM is advantageous due to the large number of items, the flexibility to model a relationship among criterion variables and multiple predictors, to design unobservable latent variables, and statistically model testing (Chin, 1998). The decision whether a construct is determined as reflectively or formatively was examined by the relationship between each indicator and the underlying constructs. Prior literature has shown that personality traits are conceptualized as reflective constructs, where the unobservable can be as giving "rise to something observed" (Haenlein and Kaplan, 2004). The seven ISM constructs are conceptualized as formative. Formative indicators define the characteristics of and changes in the underlying ISM construct (Bagozzi, 2011; Diamantopoulus, 2011). The content of these constructs indicate that the ISM indicators cause the underlying construct and therefore only a formative operationalization is possible (MacCallum and Browne, 1993).

For measurement model validation, the SEM guidelines as proposed by Chin (1998) were applied. For reflective model measurement, composite reliability, item reliability, convergent, and discriminant validity were examined. After purification of some items that had low factor loadings, the evidence of reliability, convergent validity, and discriminant validity have shown that the measurement model is appropriate for testing the structural model. The quality criteria for the formative measurement model are assessed using multicollinearity and communality (Diamantopoulos, 2011). Both quality criteria were met on all levels.

4.2.5 Summary of results

The structural model results (Figure 13) show that information security executives' personality traits are influential in determining attitudes towards the technical and non-technical dimensions of ISM.

The findings suggest that the technical, compliance, strategic ($p < 0.01$), and organizational dimension are positively related to behavioral intention to apply information security in a holistic focus. Interestingly, attitude towards the human and cultural dimension of ISM does not show a significant influence to the behavioral intention construct. In this regard, it is possible that information security executives differently valuated the importance of these dimensions.

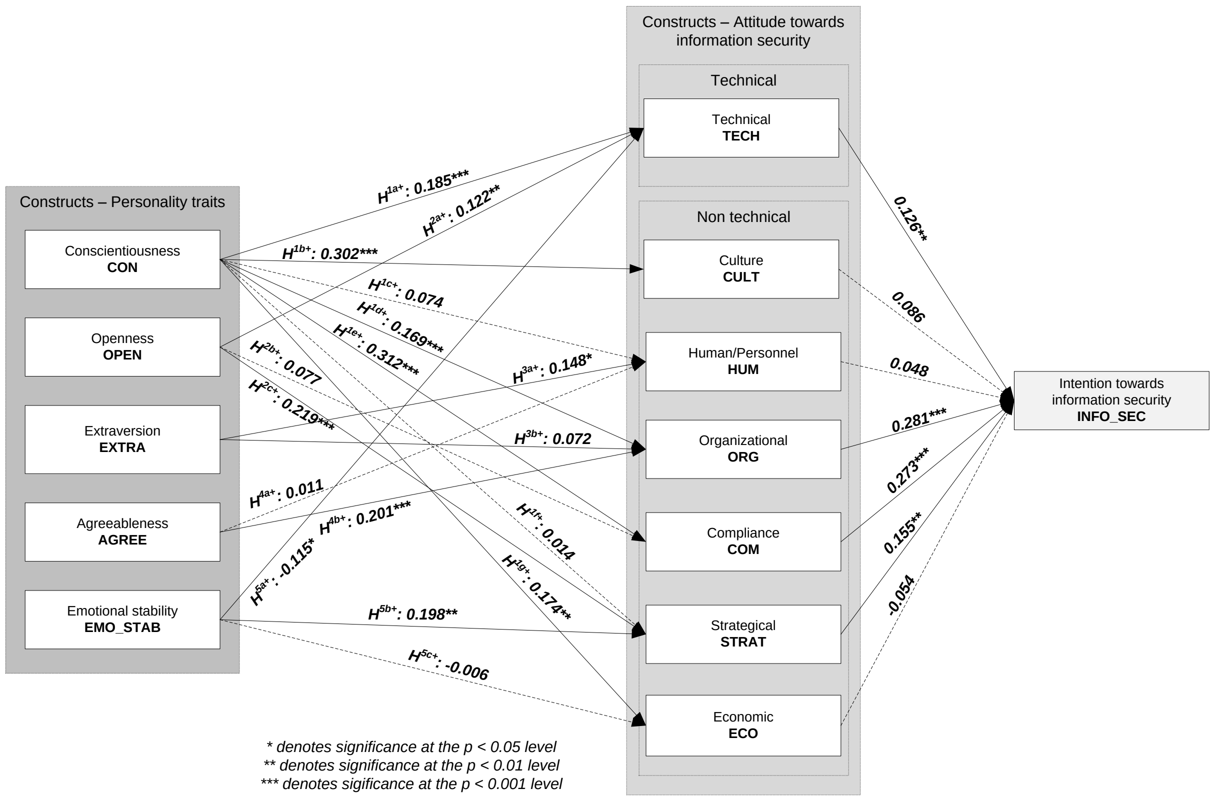


Figure 13: Results of structural equation modeling

The attitudes towards holistic ISM vary depending on different personality traits. To start with conscientiousness, five out of seven significant positive relationships were identified. Due to the facets of conscientiousness, the results are not surprising. Conscientiousness indicates persistence and intrinsic motivation towards specific job tasks, which can imply a more structured focus on the five significant dimensions of ISM. However, the human and the strategic dimension were not found to be influenced by conscientiousness. Reasons can be the specific topic of information security, whose dimensions can be affected by other external constructs. For example, strict preventative technical security measures can influence the attitude towards the human dimension in a negative way. In addition, unforeseen issues or failures in information security were not elements of the conscientiousness facets. The second personality trait, openness, is positively related to the technical and the strategic dimension, but is not significantly related to the compliance dimension of ISM. Openness is associated with being creative and unconventional. Strict regulatory requirements may leave little room to act out these specific facets. Extraversion is positively related to the human dimension but the influence to the organizational dimension of ISM was not found to be influential. Interpersonal interaction is mostly associated with the human dimension and therefore relevant to extravert information security executives. This fact can result into deeper positive attitudes towards the human dimension than towards the organizational dimension, because there is more interpersonal interaction than in the organizational dimension of ISM. Agreeableness shows its positive relationship in the opposite direction. Agreeable information security executives trust their environment and strive for harmony. Therefore one reason for non-significance of the relationship between agreeableness and the human dimension of ISM can be that information security executives' attitudes are diversified due to no common way of handling the human challenge in information security (see also the chapters of part B in this thesis). Finally, emotional stability is positively related to the strategic and technical, and not significantly related to the economic dimension of ISM. Contrary to the hypothesized relationship between emotional stability and the technical dimension of ISM, the path coefficient is negative. Emotionally stable individuals tend to view innovative technical advances in their daily job tasks as important and helpful (Devaraj et al., 2008). Therefore one reason for that result can be that the experience in information security incidents might be overestimated by information security executives in a way that might result in worse attitudes towards preventative technical security measures. On the other side, Junglas et al. (2008) pointed out that emotional stability shows its facets only in affective situations. Therefore, emotional stability may only be significant in a trait-relevant situational cue (Junglas et al., 2008).

4.2.6 Conclusion, limitations and outlook

The paper provides an insight into the influence of personality traits on the attitude towards holistic ISM. Recent studies have acknowledged the influence of personality traits on IS success outcome objects. Research studies that investigated the influence of personality traits in the information security context were limited to the end-user or employee level. Prior research that focuses information security executives as target object have focused on tasks and skills, and less on the behavioral patterns and how these factors impact the information security in a holistic way. Incorporating personality traits from executives' perspective into attitudinal constructs of holistic ISM has largely been ignored. This relatively unstudied domain is novel and certainly worthy for investigation. Using techniques of multivariate statistics, the integrated model shows that attitudes towards different ISM dimensions vary depending on different personality traits. For example, openness and conscientiousness were found to significantly influence information security executives' attitude towards the technical dimension of ISM.

The results lead to the following theoretical and practical implications and future research directions. Together with other behavioral models, this research paper can open an area for the development of a comprehensive model for assessing holistic information security management in organizations or companies. Knowing that personality traits are stable in a long-term view, short-term effects that have been shown to be influential to cognitive processes can be integrated into this model. For instance, the influence of the opinions of significant others on an individual's attitudes can be integrated into the proposed research model. Further, it would be interesting to investigate whether there is empirical support for the hypothesized relationships in other organizational units and if cultural and regulatory differences might affect the attitudinal constructs of information security executives. From a practical perspective, the results show that there is no "one size fits all" approach. The attitudinal constructs of information security executives are influenced by personality traits, and it can be assumed that his or her focus would be different. Consequently, if a company or organization understands the traits of its information security executives, it can enhance the information protection level. For example, these results might help companies and organizations in searching new team members in order to secure a specific part of there IS environment or to select existing team members in an information security project. Furthermore, established management approaches can be extended, taking the information security executives' personality traits into account. With the focus on a holistic ISM approach, this paper might also help develop or assess an executive's capabilities.

The study is subject to the following general limitations. First of all, the proposed research model is relatively complex with a huge number of hypothesized relationships and number of items. This can lead to misinterpretation and diverging results as it was potentially the case in the relationship between emotional stability and the technical dimension of ISM. Due to the characteristics of the research model, SEM is the only possible data analyzing technique. But researchers have begun criticizing the analyzing techniques. Other SEM analyzing techniques such as LISREL might lead to different results. Caution must be taken, when generalizing the results to an international population or to other industries. The empirical database contained only information security executives from German-speaking countries. For example, Hofstede and McCrae (2004) identified cross-national differences in personality traits that might also affect the presented results. In order to increase generalizability, follow-up studies are needed to examine the effects of cultural differences or the type of organization. In other words the FFM model measures individual differences in personality in five broad factors. It cannot be precluded that unacknowledged factors were not considered as being influential. In addition, the empirical data were collected via self-reported survey. There is a potential for common method variance (CMV) as proposed by Chang et al. (2010), McElroy et al. (2007) or Podsakoff and Organ (1986). These effects are tried to minimize ex ante and ex post. First, a number of procedural remedies in designing and administering the questionnaire were used. For example during the survey, no backtracking was possible. Ex post, to access the CMV, the Harman's single-factor test was applied (see Podsakoff et al., 2003). While the results do not preclude the existence of CMV, they do suggest that CMV is not of great concern.

To conclude, further research is needed to explore whether external factors that are not integrated in this study influence the relationship between personality traits and attitudes towards holistic ISM. For instance, it is possible that the industry and organization size, and as a result, stricter compliance requirements could affect attitudes towards specific dimensions of ISM. Further, there is no explicit focus on a specific personality dimension. This could be investigated in future with a specific focus on each personality dimension. Other opportunities for future research include the investigation of personality traits such as extraversion or agreeableness as potential moderators of the relationship between attitudes and intentions. These points were addressed with the research study presented in the next section.

4.3 Information security executives' attitudes towards technical security measures: An empirical examination of personality traits and behavioral intentions

4.3.1 Preamble

This chapter is based on the research paper with the title "Management of Technical Security Measures: An Empirical Examination of Personality Traits and Behavioral Intentions" (Uffen and Breitner, 2013a). The paper was published and presented at the IS conference "Hawaii International Conference on System Science" in Maui, Hawaii (January 07 – January 10, 2013). The HICSS is one of the oldest and continuous running IS conference worldwide and is ranked second in citation ranking among 18 IS conferences (Hock et al., 2006). The paper was submitted to the Mini-Track "Organizational and Social Dynamics in Information Technology" which belongs to the Track "Organizational Systems and Technology". The conference proceedings are rated by the WKWI and GI-FB WI with a "B" (WKWI, 2008). The VHB-Jourqual2.1 rated the HICSS with a "C".

In addition, this paper was published in the international IS journal "International Journal of Social and Organizational Dynamics in Information Technology" (Uffen and Breitner, 2013b). For this purpose, the HICSS paper was modified by further visual objects and an extension of the theoretical basis for example by presenting additional definitions of the used behavioral determinants. In comparison with the HICSS paper, in this paper the data were analyzed again, by using a different data analysis technique that includes control variables. The journal provides an international forum for educators, researchers, and practitioners to bridge the gap between social sciences and information technology. First published in 2011, the journal is not rated by any ranking yet.

4.3.2 Introduction

The results and critical examination of the statistically tested research model in chapter 4.2.5 possessed new research questions. Some relationships between personality traits and the attitudinal constructs towards holistic ISM were shown to be not significantly influential. This leads to the assumption that the relationships between personality traits and attitude towards holistic ISM are more complex than a simple linear relationship. These relationships are focused on more in detail by incorporating external factors that might have an influence on the personality-attitude relationships.

For this purpose, a more detailed view was necessary to obtain a deeper insight into the subject. Besides the human aspect in information security, various researchers have discussed about preventative technical security measures in early years (Straub and Welke, 1998; Farahmand et al., 2003). The management of technical security measures is defined as a part of daily tasks of an information security executive, whose activities, such as administration or running Virtual Private Networks (VPN), or being suspicious of and reacting to current security incidents aim at hindering network attacks. Therefore the paper focuses on the attitudinal construct of technical security measures in relationship to the three FFM traits of conscientiousness, openness and neuroticism, the counterpart of emotional stability. Drawing on the TPB (see chapter 2.1) the influence of personality traits on information security executive's attitude towards managing technical security measures is demonstrated. In contrast to the research model in section 4.2.3 and the statistical analyzing technique in chapter 4.2.4, moderators and control variables were included. In order to obtain a better understanding of the influence of external factors in the initial research model, compliance, as a potential moderator between personality traits and attitudes was included. Standards and guidelines that support information security executives in their daily tasks are becoming more and more important (Siponen & Willison, 2009) and are expected to potentially influence an information security executives decision in managing technical security measures.

4.3.3 Theoretical background and research model

Organizations are faced with contradictory requirements to deal with open IS on the one hand and assure high protection standards on the other. The adoption of security measures is complex and has to be balanced with a variety of organizational issues which include the impact on employee productivity, ethical and legal stipulations, and business and financial concerns. Technical security measures, for example the deployment of firewalls, anti-virus protection, VPN and encryption tools, make it increasingly difficult to attack an IS and gain access to sensitive organizational information. The activities of information security executives include for example administration, running, and monitoring of effective security devices that impede unauthorized access (Krankanhalli et al., 2003). In addition, legal requirements, international standards and internal security policies, must be taken into account while managing information security (Siponen & Willison, 2009). By adopting ISM standards and guidelines, organizations can commit to securing their organizational networks against external threats (Siponen & Willison, 2009). These guiding objects are referred as compliance factors within the context of this thesis. Since ISM standards guide information security executives in their decisions, it is expected that such compliance factors will influence their attitude and behavioral intention. Therefore, compliance factors can be potential external factors that cause changes in attitudes and behavior. This results in a sort of relationship between compliance factors and an executive's individual differences, cognitive processes, and behavioral factors towards the management of technical security measures.

The integrated model proposes an explanation of the relationship between personality traits and an information security executive's attitude and behavioral intention towards the management of technical security measures.

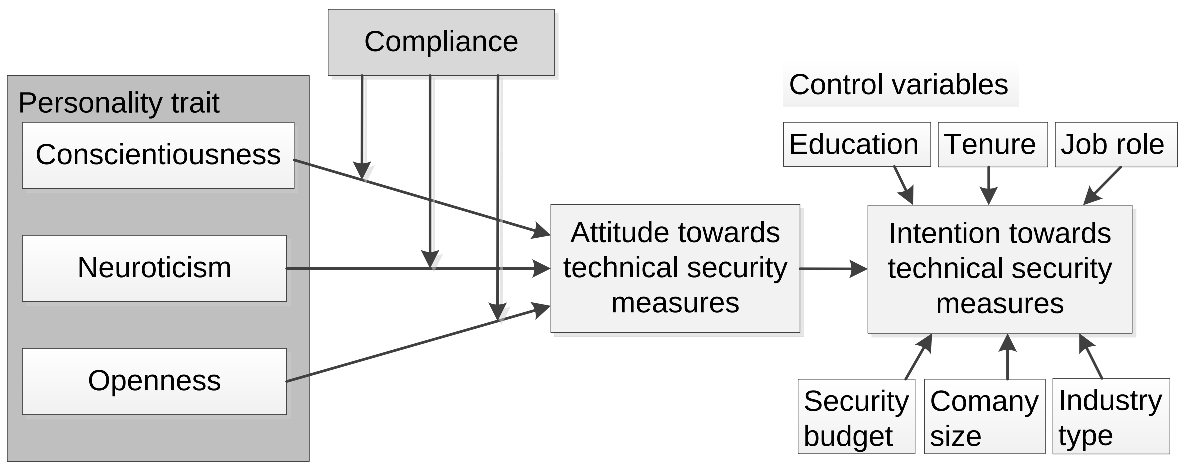


Figure 14: Integrated research model

The integrated research model indicates three direct relationships between personality traits and the attitude towards technical security measures. In addition, three moderating relationships and six control variables were included. Figure 14 shows the integrated research model in detail. The hypotheses to the moderating effects are shortly summarized in the following. Due to similarities to the argumentation as proposed in chapter 4.2.3, the hypotheses to the direct relationships between personality traits and attitude are not discussed in detail. Note that because of the different context of this paper, the theoretical background and argumentation is different compared to the paper presented in chapter 4.2.

The relationships between personality traits and attitudes do not occur in a vacuum. It is expected that information security executives' beliefs or attitudes are influenced by external factors such as information security standards or guidelines if these beliefs match their attitude and behavioral intention. For example, ISM guidelines and standards support an information security executive in their decisions while managing technical security measures (Ma & Pearson, 2005). But ISM guidelines and standards are generic in scope and do not precisely describe any specific security measure. Therefore, the usage of these ISM standards and guidelines cannot be seen as a direct behavior indicator. Moreover, dependent on the individual personality, these compliance factors might shape the attitude towards managing technical security measures. First, it must be determined whether compliance factors provide positive value in enhancing the attitude towards managing technical security measures. Since personality traits are shown to influence attitude (Devaraj et al., 2008; Fishbein & Ajzen, 1975), it is hypothesized that compliance is an external variable that moderates the relationship between the personality traits and an information security executive's attitude towards the management of security measures. The importance of these external variables or moderating effects between personality traits and cognitive processes has been highlighted by several researchers (Junglas et al., 2008; Tett and Burnett, 2003). Personality traits are stable in a long-term view (Costa and McCrae, 1992), thus other external factors are more likely to moderate the affect of these traits on attitudes towards management of security measures. This leads to the assumption that compliance factors are useful moderators in enhancing the integrated research model.

While conscientiousness, openness, and neuroticism are regarded as proximal determinants of an information security executive's attitudes towards the management of technical security measures, other individual variables (e.g. demographic variables) might also influence this component. Researchers suggest that individual variables need to be included as control variables in order to account for the impact on an individual's behavioral intentions. For example the upper-echelon theory as proposed by Hambrick and Mason (1984) explains the influence of demographic variables on behavioral output factors. According to this theory several researchers occupied an influence of individual demographic variables on (top) manager's behavior (see Li et al., 2006; Barker and Mueller, 2002; Hambrick and Mason, 1984). Findings suggest that longer-tenured IS executives are more likely to be psychologically committed in following their own opinion of how an IS environment should be run (Barker & Mueller, 2002). Thus, educational level and tenure are integrated in our research model as control variables.

A large, well-structured organization with strict compliance requirements due to the industry type is likely to have well-specified policies and resulting security measures. For example in the financial or health sector, the compliance requirements are stricter than in any other industry (Bulgurcu et al. 2010). Technical security measures may have a more important role in those industries. Hence, it is hypothesized that company size, and industry type, may lead to different behavioral intentions towards the management of security measures. Additionally, following Herath and Rao's (2009) argumentation, information security executives' job role and annual security budget are also included as control variables to account for differences in behavioral intentions among information security executives.

4.3.4 Data analysis procedures

As proposed in chapter 3.2.3, empirical data were analyzed via SEM in order to reflect latent independent and dependent variables. Since moderation effects are included in the research model, the guidelines from Chin et al. (1998; 2003) were used to test and validate the measurement model. To ensure measurement model quality, convergent validity, discriminant validity, individual item reliability and composite reliability are examined. Beside the convergent validity, whose factor loading of at least 0.635 are near the recommended 0.707 value, the quality criteria are met at all levels.

The measurement model including the moderating effects explains 20.0% (F=105.63, p<0.001) of the variance in attitude and 19.9% (F=42.73, p<0.001) of the variance in behavioral intention towards management of technical security measures; both values are significantly different from zero (Figure 15). By including compliance as a moderator of the relationship between personality traits and attitude towards the management of technical security measures, the research model explains an additional 6% ($\Delta R^2=0.058$, F=16.90, p<0.001) of the variance in attitude. Therefore the discussion of results focuses on the measurement model that includes the moderating effects.

4.3.5 Summary of results

Out of the hypothesized relationships, four were significantly supported. As predicted by TPB and the results from prior studies in information security research (e.g. Anderson & Agarwal, 2010; Johnston & Warkentin, 2010; Bulgurucu et al., 2010) an information security executive’s behavioral intention is strongly influenced by their attitude (β=0.450; p<0.001). Conscientiousness positively influences an information security executive’s attitude towards the management of technical security measures (β=0.204; p<0.01). On the other side, the relationships between openness/ neuroticism and attitude are not significant (H2: β=-0.108, n.s.; H3: β=0.040, n.s.). Compliance has a moderating effect on the relationship between the personality traits of conscientiousness/ openness and attitude towards the management of technical security measures (H4: β=0.154, p<0.05; H6: β=0.241, p<0.01). No moderating effect on the relationship between neuroticism and attitude could be identified (β=0.066, n.s.).

Turning to the four control variables, beside industry type and education no significant impact on explaining an executive’s intention towards technical security measures could be identified. This suggests that an information security executive’s behavioral intention towards technical the management of security measures varies based on the underlying educational status and the industry type of an organization.

The relationships of personality traits to attitude towards the management of technical security measures have varying results. Of the personality traits, only conscientiousness has a significant relationship to attitude. Again, this result is not surprising, because conscientiousness has been shown to be a valid predictor in various job tasks (Barrick et al., 2001). Conscientious information security executives believe that managing technical security measures provides a positive value in their job tasks. In addition, compliance has a moderating effect on the relationship between conscientiousness and attitudes towards the management of technical security measures. This indicates that when information security executives are confronted with ISM standards or guidelines, conscientiousness has a stronger effect on attitude.

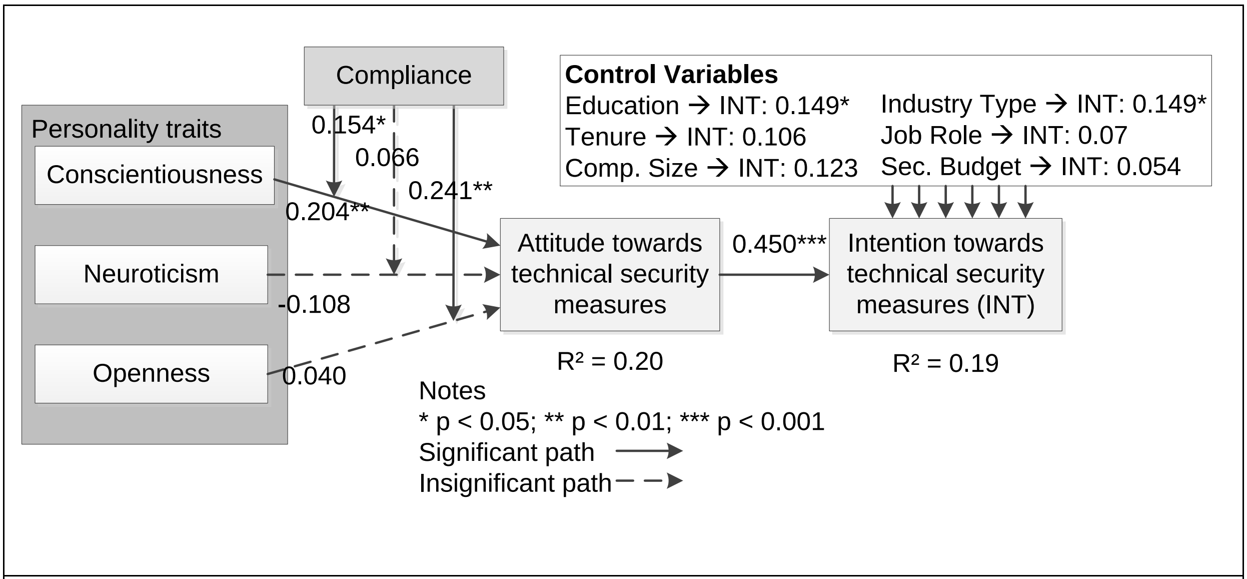


Figure 15: Results of structural equation model testing

Openness is associated with flexibility and the critically examination of changes in existing requirements, norms, and rules. This justifies the strong moderating effect of the compliance factors, since ISM standards and guidelines support an information security executive in, for example, critically examining the current status of technical security measures. Even if ISM standards and guidelines are generic in scope, the relationship between openness and attitudes towards technical security measures becomes stronger under the influence of these factors. The relationships between neuroticism as well as openness and attitude towards the management of security measures do not have statistical support. Despite Ajzen's (1991) expectations and according to Devaraj et al. (2008) who emphasized that personality traits are external variable within TPB, one reason for non-significance can be that for example openness can have a direct relationship to behavioral intentions towards the management of technical security measures. The significance of the moderating effect of compliance has shown that the relationship between both openness and attitude might be more complex.

4.3.6 Conclusion, limitations and outlook

The initial attempt of the presented research paper is to demonstrate that the relationship between an information security executive's personality traits and their attitude towards the management of technical security measures is more complex than a single, direct relationship. In the information security context, compliance factors play an important role in supporting information security executives' decisions. Therefore, compliance factors were integrated as potential moderators of the relationship between the personality traits and attitude. In addition, control variables such as tenure or the industry type were integrated and tested. Results indicate that in two cases compliance factors play a moderating role between personality traits and attitude. Of the six control variables, education and the industry type were shown to have a significant effect on behavioral intention towards the management of technical security measures. These findings prove the initial assumptions about the complexity of influence factors in the information security decision-making process. The results indicate that ISM guidelines and standards can support information security executives in their daily tasks.

In addition to the limitations presented in chapter 4.2.6, this research paper is subject to following shortcomings. First, the explanatory power of the proposed integrated research model ($R^2 = 0.20$) seems low. However, in social science, research studies that incorporate personality traits into behavioral research models often face problems with low R^2. Therefore, researchers emphasize that a R^2 value in the range of 10-20% is quite acceptable (Junglas et al., 2008). In measuring personality traits, it is not always possible to get a higher R^2. Further, the direct relationships between neuroticism as well as openness to attitude are not significant. These relationships must be focused on more in detail for additional external factors in future research. Future research can include additional external variables such as moderators in order to better explain the relationship between personality traits and cognitive behavioral factors. Institutional size, the number, status, and complexity of concurrent security measures or cultural differences as group-level moderating factors, can enhance the relationship between personality traits and attitude. Another limitation deals with the measurement of behavioral intentions rather than actual behavior. Due to the sensitive context, obtaining empirical data about actual behavior in, for example, real life situations that are relevant to information security have been shown to be difficult (Kotulic et al., 2004). To close this gap, and to link that with personality traits, one option to alleviate this limitation is the use of scenario techniques (Bulgurucu et al., 2010). Providing richer information about hypothetical information security situations and indirectly asking about attitudes towards technical security measures lead to a better impression of an information security executive’s true behavioral intention. Another limitation of this paper is that the compliance construct was measured with abstraction and was initially not created with the purpose of a moderator. The pre- and post integration into the above-mentioned scenario might provide a more detailed explanation about the relationship between personality traits and attitudes towards the management of technical security measures.

5. End-users' information security awareness and compliant behavior

5.1 Security awareness and compliant behavior: A literature review

5.1.1 Preamble

The following chapter is based on the research paper with the title "Employees' Information Security Awareness and Behavior: A Literature Review" (Lebek et al., 2013a). The paper was published and presented at the international IS conference "Hawaii International Conference on System Science" in Maui, Hawaii (January 07 – January 10, 2013). The HICSS is one of the oldest and continuous running IS conference worldwide and is ranked second in citation ranking among 18 IS conferences (Hock et al., 2006). The paper was submitted to the Mini-Track "Emerging Risks and Systemic Concerns in Information Security Research and Applications" which belongs to the Track "Internet and the Digital Economy". The conference proceedings are rated by the WKWI and GI-FB WI with a "B" (WKWI, 2008). The VHB-Jourqual2.1 by Schrader and Hennig-Thurau (2011) rated the MKWI with a "C".

In addition, this paper was submitted and accepted for publication in the international IS journal "Management Research Review" (Lebek et al., 2014). For this purpose, the initial HICSS paper was modified by including concrete definitions of the behavioral determinants and the references were enlarged by updating to the year 2013 and including the complete reviewed literature database. The journal publishes a wide range of research paper about the latest management research. It is not rated by the WKWI and GI-FB WI because it is not explicitly specified to the IS context (WKWI, 2008). The VHB-Jourqual2.1 by Schrader and Hennig-Thurau (2011) rated the journal with a "C".

5.1.2 Introduction

The implementation of technical security measures is insufficient as long as end-users or employees are not aware of potential security risks and do not behave security compliant (Bulgurucu et al., 2010; Spears and Barki, 2010; see also chapter 4.1). Employees are regarded as the weakest link in information security (Siponen, 2000; Spears and Barki, 2010). To achieve information security, researchers emphasize the importance of security education, training, and awareness (SETA) programs (Abraham, 2011; D'Arcy et al., 2009) as non-technical security measures for preventing security breaches by employees. Therefore, the investigation of security awareness and compliant-behavior has become more and more important over the past decade. The information security discipline has developed to an interdisciplinary research domain that applies theories from social psychology and criminology in order to explain and predict employees' security-related behavior and awareness (Mishra and Dhillon, 2005).

The objective of this publication was to identify which behavioral theories have been recently applied in the human information security dimension. A literature review was conducted, to comprehensively assess applied behavioral theories in the research field of end-users' information security awareness and compliant-behavior within the past decade. Prior literature reviews in this research field were conducted with different research objectives. For example, Siponen (2000) analyzed various approaches for minimizing user-related faults in information security. The author identified the underlying behavioral theories, but the focus of the research study was approach-related. Since this study was published twelve years ago, a state of the art overview of applied behavioral theories was necessary. In addition, several researchers conducted literature reviews in this field to provide the theoretical basis for further research. These literature reviews were not the essential part of the studies. For example, Mishra and Dhillon (2005) gave an overview of behavioral theories in information security research in order to introduce the theory of anomie to their research field. Aurigemma and Panko (2012) presented behavioral theories to discuss an information security policy (ISP) compliance framework. With a comprehensive literature review in the research field of end-users' information security awareness and compliant behavior the aim of this paper is to synthesize existing knowledge and identify research gaps for further research.

5.1.3 Research design

The research design consists of two phases. The quality of a literature review depends strongly on the search process (vom Brocke et al., 2009). Therefore, first relevant literature is identified by conducting a rigorous literature search in IS databases. Second, the identified literature is analyzed by clustering, and summarizing applied behavioral theories in information security awareness and compliant behavior. The underlying research methodology is adopted by Webster and Watson (2002). As discussed by vom Brocke et al. (2009), the recommendation for validity and reliability were taken into account. The literature search was conducted through ten IS literature databases: AISeL, ScienceDirect, IEEEXplore, JSTOR, SpringerLink, ACM, Wiley, Emerald, InformsOnline, Palgrave Macmillan. The search terms were pre-defined to conduct the literature search including "security awareness", "awareness training", "awareness program", "awareness campaign", "security education", "security motivation", "security behavior" and "personnel security". Papers were selected if it contained at least one of the search terms in the title, abstract or keywords. In total, 3,423 potentially relevant papers were identified.

Webster and Watson (2002) and vom Brocke et al. (2009) recommended focusing on high-quality conferences and journals. The authors decided to include also literature of minor relevance. This was necessary because there are journals which are specialized in the field of information security (e. g.

"Computers & Security", or "Information Management & Computer Security") and therefore contribute to the research objective even if these papers are not highly rated in international conference or journal rankings (e. g. AIS, Walstrom and Hardgrave (2001), Willcocks et al., (2008)). Non-academic papers that underlie no peer-review process (e. g. whitepapers) were excluded. The literature review was focused to English written papers. The paper selection process was as follows: Papers that do not address behavioral theories of end-users' information security awareness and behavior were excluded. Every paper was manually screened based on title, abstract and if necessary through the full text. This process resulted in a number of 95 articles, relevant for further analysis. In addition, a backward and a forward search were carried out (Webster and Watson, 2002). The final literature database contains 113 papers, identified to be relevant for the purpose of this paper. A complete list of the identified papers can be found in the appendix and are marked with an "A" (Appendix 8).

The researchers independently analyzed the papers by identifying the applied behavioral theory, their underlying constructs, the research methodology and the underlying statistical results. Then the results were categorized to behavioral theory, constructs, and research methodology. The complete list of behavioral theories was developed inductively during the review process of each identified paper. A total of 54 behavioral theories that were applied in the contemplated research field were identified. The majority of the identified theories were used in two or fewer papers. Table 8 shows the seven primary applied behavioral theories. The main focus in the reviewed research domain lies on behavioral theories such as TRA/TPB, GDT, PMT, and TAM.

Table 8: Frequency of applied theories

Applied research theory	Frequency
Theory of reasoned action (TRA)/ Theory of planned behavior (TPB)	27
General deterrence theory (GDT)	17
Protection motivation theory (PMT)	10
Technology acceptance model (TAM)	7
Social cognitive theory (SCT)	3
Constructivism	3
Social learning theory (SLT)	3

A list of research methodologies was defined prior to reading the papers in detail. Eight different research methodologies were identified: deductive analysis, modeling, experiment, action research, case study, grounded theory, literature review, empirical research (qualitative/quantitative).

Table 9: Percentage of applied research methods

Applied research method	%
Empirical research - qualitative - quantitative	50 (5) (45)
Modeling	14
Action research/ Case study	13

Experiment	12
Deductive analysis	9
Literature review	2
Grounded theory	1

Quantitative empirical research is pre-dominant in the examined research field (Table 9). Little qualitative empirical research is done yet. Further, there is little research in literature reviews and grounded theory. The remaining four methodologies (i. e. deductive analysis, modeling, experiment, and action research/case study) have been applied relatively evenly, but considerably infrequently in contrast to empirical research.

5.1.4 Theoretical background of the four identified behavioral theories

The most frequently used theories in the research field are the TRA/TPB, GDT, PMT and TAM (Table 8). The following discussion is based only on these behavioral models that were applied with a specific focus to end-users' security awareness and behavioral compliance. A short summary of those is presented in Table 10.

Table 10: Overview of applied behavioral theory

Behavioral theory	General determinants	Description
Theory of planned behavior (TPB)	ATT, SN, PBC	Reflects the degree of intentional behavior to engage in that behavior
General deterrence theory (GDT)	PSOS, PCOS	Relies on the idea that individuals weigh the cost and the benefit of committing a crime
Protection motivation theory (PMT)	TA (PSOT, PV), CA (RC, PBC RE)	Determines an individual's processes while coping with a threat
Technology acceptance model (TAM)	PU, PEOU	Reflects the degree of individual acceptance and actual use of information systems objects

ATT: Attitude towards Behavior; **AB**: Actual Behavior; **BI**: Behavioral Intention; **CA**: Coping Appraisal; **SN**: Subjective Norm; **PBC**: Perceived Behavioral Control; **PCOS**: Perceived Certainty of Sanctions; **PEOU**: Perceived Ease of Use; **PSOS**: Perceived Severity of Sanctions; **PSOT**: Perceived Severity of Threat; **PU**: Perceived Usefulness; **PV**: Perceived Vulnerability; **RC**: Response Costs; **RE**: Response Efficacy; **TA**: Threat Appraisal

To start with TPB (for a detailed overview, see chapter 2.1), in the context of end-users' security awareness and behavioral compliance, the behavioral intention to comply with the information security policy (ISP) is dependent on his/her overall evaluation of and normative beliefs towards compliance-related behavior and the greater the feeling of reflected actual control over those actions, the greater the behavioral intention (Aurigemma and Panko, 2012; Bulgurcu et al., 2010).

The General Deterrence Theory (GDT) is adapted from criminal justice research, and based on rational decision making. The theory emphasizes that perceived severity (PSOS) and certainty (PCOS) of sanctions or punishments determine the decision to engage in a security related crime by balancing the cost and benefits (Straub, 1990). Research studies that deal with end-users' security awareness and behavioral compliance have mainly focused on security countermeasures and other preventative strategies that impact the employees' intention to misuse IS (Bulgurucu et al., 2010; D'Arcy et al., 2009).

Adapted from health psychology, the Protection Motivation Theory (PMT) explains the coping process with potential security threats by predicting a variety of protective behaviors (Rogers, 1983). An end-users's attitude towards information security is determined by the evaluation of two cognitive mediated appraisals: threat appraisal (TA) and coping appraisal (CA) (Bulgurcu et al., 2010). The first consists of two factors, perceived severity of threats (PSOT) and perceived vulnerability (PV) and comprises the threat perception. The latter is determined by response costs (RC), PBC and response efficacy (RE), which represent an individual's ability to cope with potential threat. An end-user who is aware of security risks forms beliefs about perceptions of these threats and the coping response (Anderson and Agarwal, 2010; Herath and Rao, 2009).

The Technology Acceptance Model (TAM) is a parsimonious model that represents antecedents of technology acceptance via two constructs: perceived usefulness (PU) and perceived ease-of-use (PEOU). PU is defined as an individual's subjective probability that the use of a specific technology or innovation will increase his/her individual performance. The second TAM construct, PEOU, denotes the degree to which an individual expects the target system to be free of effort (Venkatesh et al., 2003). In the security awareness context, TAM determines the employees' intention to comply with information security policy (ISP), which is influenced by both, PEOU and PU, afforded through the use of e.g. ISPs (Al-Omari et al., 2012).

Each theory specifies behavioral factors that have been tested and evaluated in multiple studies. The identified behavioral theories and their underlying constructs are summarized into the following meta-model (Figure 16).

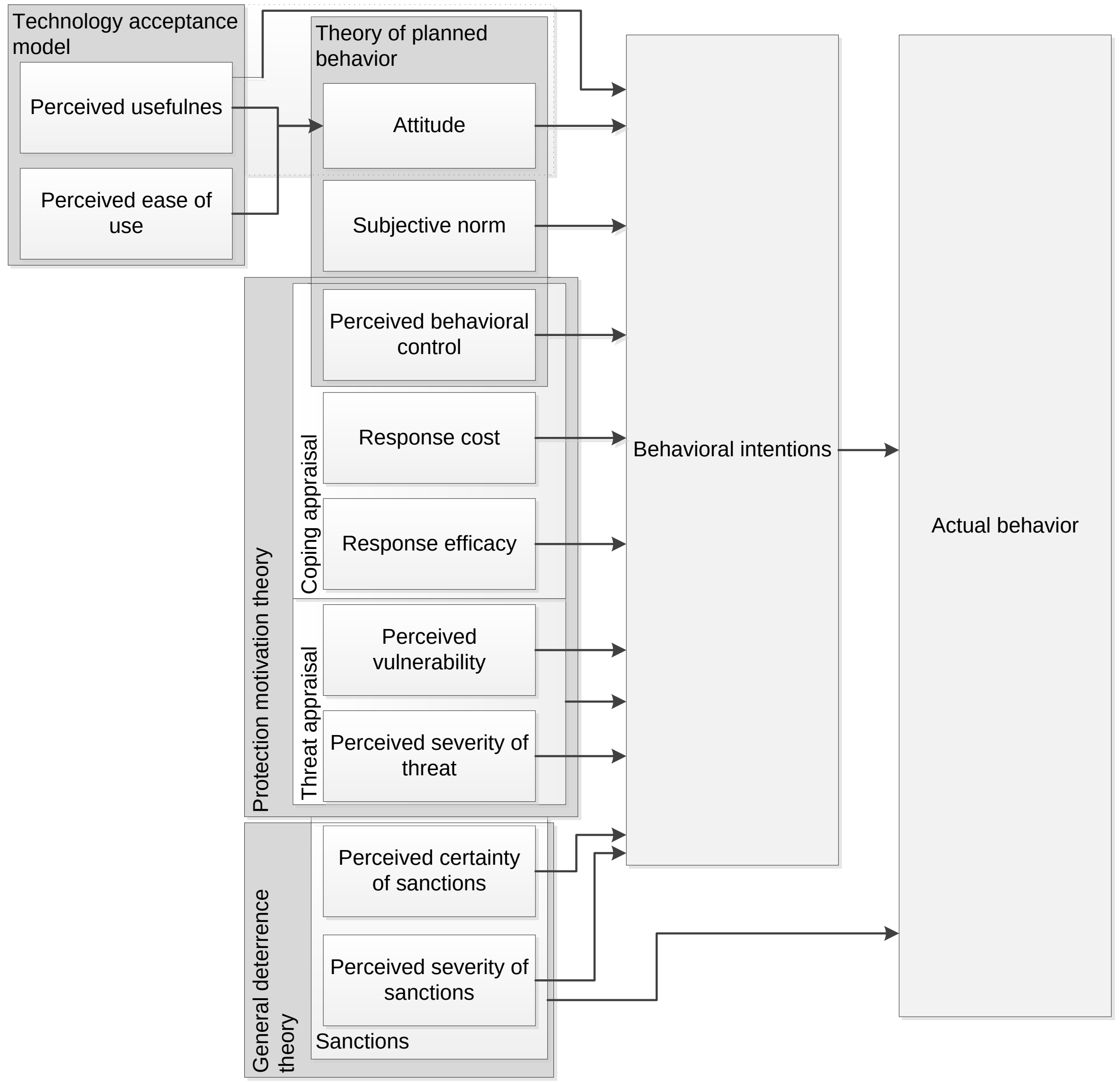

Technology acceptance model
Perceived usefulnes
Perceived ease of use
Theory of planned behavior
Attitude
Subjective norm
Perceived behavioral control
Protection motivation theory
Coping appraisal
Response cost
Response efficacy
Threat appraisal
Perceived vulnerability
Perceived severity of threat
General deterrence theory
Perceived certainty of sanctions
Perceived severity of sanctions
Sanctions
Behavioral intentions
Actual behavior

Figure 16: Meta-Model of primary applied behavioral theories

Since various research studies focused on the original behavioral theories, there is also evidence that external factors such as organizational or work-related factors are also influential (Kukafka et al., 2003). Disregarding these factors and relationships can lead to inefficiencies. As a result, some researchers added theoretical extensions of additional factors hypothesized to influence the individual behavior (e. g. ISP fairness (Bulgurucu et al., 2010), situational support (Johnston et al., 2010), visibility (Pahnila et al., 2007).

5.1.5 *Summary of results*

The analysis of the identified papers showed partly divergent results. Therefore, a qualitative content analysis is applied to get a detailed impression of the behavioral theories and their relationships. These relations will be shortly synthesized in the following. Table 11 presents a detailed compilation of the underlying constructs, their relationships and the statistical significance.

Table 11: Summary of construct relationships

Construct				Author °	Significance	β value	Sample size	Data source
Independent construct	# Items	Dependent construct	# Items					
Theory of planned behavior/ Theory of reasoned action (TPB/TRA)								
ATT	4	BI	3	A14	**	0.25	464	Employees (several Companies)
	4		3	A15	***	0.27	464	Employees (several Companies)
	-		-	A13	**	0.48	464	Employees (several Companies)
	3		3	A26	*	0.316	332	US Students and IS Professionals
	3		3	A26	-	0.298	227	KOR Students and IS Professionals
	3		3	A41	-	0.073	312	Employees (several Companies)
	3		3	A43	**	0.29	332	Students and IS Professionals
	4		5	A46	***	0.48	124	IS Professionals
	4		2	A66	-	0.079	60	Students
	3		4	A76	***	0.537	240	Employees (1 Company)
	5		4	A113	*	0.18	176	Employees (several Companies)
BI	2	AB	2	A66	**	0.386	60	Students
	3		3	A75	*	0.04	917	Employees (4 Companies)
	4		3	A76	***	0.869	240	Employees (1 Company)
	3		3	A93	***	0.98	917	Employees (4 Companies)
	3		3	A94	*	0.04	917	Employees (4 Companies)
PBC	3	BI	3	A14	**	0.22	464	Employees (several Companies)
	2		3	A26	**	0.193	332	US Students and IS Professionals
	2		3	A26	*	0.197	227	KOR Students and IS Professionals
	3		3	A41	*	0.172	464	Employees (several Companies)
	2		3	A43	**	0.16	332	Students and IS Professionals
	7		5	A46	**	0.17	124	IS Professionals
	3		3	A52	**	0.187	215	N.A.
	6		2	A66	**	0.300	60	Students
	3		3	A75	*	-	464	Employees (several Companies)
	3		3	A93	***	0.31	917	Employees (4 Companies)
	3		3	A94	*	0.17	917	Employees (4 Companies)
	8		5	A51	*	0.376	202	Healthcare Professionals
	4		4	A113	***	0.43	176	Employees (several Companies)
SN	3	BI	3	A14	**	0.29	464	Employees (several Companies)
	2		3	A26	-	-	332	US Students and IS Professionals
	2		3	A26	**	0.324	227	KOR Students and IS Professionals

	5		3	A40	***	0.395	312	Employees (several Companies)
	5		3	A41	***	0.313	464	Employees (several Companies)
	2		2	A42	**	-.48	726	Employees (several Companies)
	3		3	A43	-	-	332	Students and IS Professionals
	4		5	A46	**	0.19	124	IS Professionals
	2		3	A52	***	0.298	215	N.A.
	5		2	A66	**	0.210	60	Students
	4		3	A75	*	-	917	Employees (4 Companies)
	3		-	A89	-	0.07	1449	Employees (4 Companies)
	4		4	A76	***	0.235	240	Employees (1 Company)
	4		3	A94	*	0.45	917	Employees (4 Companies)
	4		4	A113	-	0.02	176	Employees (several Companies)
Technology acceptance model (TAM)								
ATT	3	BI	3	A43	**	0.29	332	Students and IS Professionals
	3		3	A26	**	0.316	332	US Students and IS Professionals
	3		3	A26	**	0.298	227	KOR Students and IS Professionals
	4		3	A112	*	0.20	118	Employees (1 Company)
PEOU	3	ATT	3	A43	-	-	332	Students and IS Professionals
	4		4	A112	**	0.26	118	Employees (1 Company)
	3		3	A26	-	-	332	N.A.
	3		3	A26	***		227	Employees (1 Company)
PU	2	ATT	3	A26	**	0.5	332	US Students and IS Professionals
	2		3	A26	**	0.298	227	KOR Students and IS Professionals
	3		3	A43	**	0.52	332	Students and IS Professionals
	4		4	A112	**	0.50	118	Employees (1 Company)
	3	BI	3	A43	-	-	332	Students and IS Professionals
	4		3	A112	-	0.11	118	Employees (1 Company)
General deterrence theory (GDT)								
PCOS	2	BI	2	A23	-	-.065	269	Employees (several Companies)
	2		3	A40	***	0.260	312	Employees (several Companies)
	2		3	A41	**	0.155	312	Employees (several Companies)
	2		2	A42	**	-.20	726	Employees (several Companies)
	4		3	A112	-	0.03	118	Employees (1 Company)
PSOS	2	BI	2	A23	**	-.176	269	Employees (several Companies)
	3		3	A40	**	-.209	312	Employees (several Companies)
	3		3	A41	**	-.139	312	Employees (several Companies)
	2		2	A42	**	-.14	726	Employees (several Companies)
S	4	AB	3	A93	***	0.09	917	Employees (4 Companies)

	4		3	A75	*	-	917	Employees (4 Companies)
	6		3	A94	***	0.09	917	Employees (4 Companies)
	2	BI	-	A89	-	0.04	1449	Employees (4 Companies)
	4		4	A76	-	-	240	Employees (1 Company)
Protection motivation theory (PMT)								
PBC	7	BI	5	A46	**	0.17	124	IS Professionals
	3		3	A41	*	0.172	312	Employees (several Companies)
	6		3	A75	*	-	917	Employees (4 Companies)
	6		3	A93	***	0.31	917	Employees (4 Companies)
	3		3	A94	*	0.17	917	Employees (4 Companies)
CA	3	AB	3	A76	-	-	240	Employees (1 Company)
RC	5	BI	5	A46	-	-.12	124	IS Professionals
RE	6	BI	5	A46	**	0.27	124	IS Professionals
	3		3	A52	*	0.213	215	N.A.
	6		3	A75	-	-	917	Employees (4 Companies)
	6		3	A93	*	0.06	917	Employees (4 Companies)
	3		3	A94	-	-.02	917	Employees (4 Companies)
PSOT	7	BI	5	A46	*	-.20	124	IS Professionals
PV	7	BI	5	A46	**	0.20	124	IS Professionals
TA	6	BI	3	A75	*	-	917	Employees (4 Companies)
	6		3	A93	***	0.24	917	Employees (4 Companies)
	6		3	A94	*	0.12	917	Employees (4 Companies)
	5	AB	3	A76	***	0.278	240	Employees (1 Company)

° = The references can be found in the Appendix (A8)

Seven research papers could be identified that applied the TPB as a whole with every core construct. Interestingly, these research studies have focused on BI as a predictor of actual behavior (AB) towards compliance with ISP rather than its real actual outcome. Numerous authors emphasize the difficulties in observing AB and use BI instead as the dependent variable that indicates AB (e. g. Ifinedo, 2012; Pahnila et al., 2007; Zhang et al., 2009). The assessment of BI rather than AB is grounded theoretically and technically. On the one hand, several researchers have shown a strong and consistent relationship between both constructs (Venkatesh et al., 2003; Webb and Sheeran, 2006) in a non-information security context. On the other hand, technically measurement is argued to be difficult due to the sensitive context (e.g. Andserson and Agarwal, 2010; Vroom and von Solms, 2004), the large and diverse sample sizes (Bulgurcu et al., 2010; Bulgurcu et al., 2009), and the theoretical background of the applied theory (Siponen and Vance, 2010). For example Anderson and Agarwal (2010) and Siponen and Vance (2010) argue that the relationship between BI and AB is grounded in the TPB and TRA and has been shown to be proven empirically.

The results prove that the three core constructs of TPB are strong predictors of BI. More specifically, the evaluated relationships between PBC and BI are significant, with at least $p < 0.05$. The PBC construct is rooted in Bandura’s work on self-efficacy (Bandura 1982). Self-efficacy is applied in ten research studies. It reflects the beliefs about the ability to comply with the information security policy (for example Bulgurcu et al., 2010; Dinev et al., 2009; Herath and Rao, 2009; Ifinedo, 2012; Johnston et al., 2010; Johnston and Warkentin, 2010; Pahnila et al., 2007; Siponen et al., 2007; Siponen et al., 2010; Warkentin et al., 2011). Controllability is represented by an individual’s perception about availability of resources and opportunities to actually comply with information security policy (Al-Omari et al., 2012; Hu and Dinev, 2007). However, some authors used a combination of both constructs to conceptualize PBC (Hu and Dinev, 2007; Zhang et al., 2009). Turning to SN, a statistical significance of the relationship between SN and BI could be identified in 11 out of 15 research studies. To explore the influence of significant others in the decision making process, researchers used different labeled constructs for example normative beliefs (Bulgurcu et al., 2010; Pahnila et al., 2007; Pahnila et al. 2007 (2); Siponen et al., 2010) or general social determinants (Limayem and Hirt, 2003). These represent the SN construct (Albrechtsen and Hovden, 2010). Further, 11 out of 14 relationships between ATT and BI are significantly related. Attitude is a broad term that leaves room for interpretation. In three cases ATT has no significant relationship to BI. Herath and Rao (2009) stated that the insignificant effect may be due to context, sample, or other extraneous reasons.

Turning to TAM, some authors adapted the TAM constructs PEOU and PU as predictors of ATT and emphasized the relationship between ATT and BI (Dinev et al., 2009; Hu and Dinev, 2007; Xue et al., 2011). In other research studies, the ATT construct was eliminated by emphasizing a direct relationship between PEOU and PU to BI (Hu and Dinev, 2007; Xue et al., 2011). These studies imply that both TAM constructs are less related to ATT. Dinev et al. (2009) argued that even if an employee may not prefer a specific object, he or she might still use it as long as it increases job performance (Dinev et al., 2009). Interestingly, two studies tested the relationship between PU and BI and no study suggested a statistical significance (Hu and Dinev, 2007; Xue et al., 2011) but together with Dinev et al. (2009), the authors showed a positive significant relationship between PU and ATT.

The GDT and the core constructs of PSOS and PCOS as a whole were related to BI in four studies (D’Arcy et al., 2009; Herath and Rao, 2009 (2); Hovav and D’Arcy, 2012; Xue et al., 2011). In the context of this paper and due to the theoretical base of GDT, the focus on the BI construct is different than for example in TPB or TAM. BI reflects an end-users’s perception as to whether a violation of specific portions of the organizational information security policy may increase his or her general utility. However, of the six research paper that investigated PCOS as a predictor of the BI construct, three were significant at a minimum $p < 0.01$. PSOS has been shown to be significant in four research paper (D’Arcy et al., 2009; Herath and Rao, 2009 (1); Herath and Rao, 2009 (2); Hovav and D’Arcy, 2012).

The core constructs of PMT are significantly related to BI. For example, Ifinedo (2012) investigated a significant relationship by separation the TA construct to perceived severity (PSOT) and perceived vulnerability (PV), while three research studies considered the single TA construct (Pahnila et al. (2007); Siponen et al. (2007) and Siponen et al. (2010)). As proposed by Pahnila et al. (2007) response efficacy (RE) and self-efficacy refer to coping appraisal (CA). In addition, the relationship between RE and BI was shown to be significant in three cases (Ifinedo, 2012; Johnston and Warkentin, 2010; Siponen et al., 2007).

5.1.6 Discussion

BI, ATT, motivations or satisfaction are not verifiable by means other than self reporting (Podsakoff and Organ, 1986). This is the explanation, why the majority of researchers apply TRA/TPB, TAM, GDT or PMT with the use of quantitative methods to test their hypotheses. Self-reports to measure security-related behavior might lack validity, because these are prone to the problems of common method variance, consistency motif and social desirability (Podsakoff and Organ, 1986). Workmann et al. (2008) criticized that self reports are not sufficient predictors of end-users' AB, because end-users' self-reported perceptions of security behavior are not bound to be in line with their AB. To get a better insight in end-users' AB, observation seems to be a valid instrument. But information security is a sensitive topic and organizations are unwilling to reveal information that provides insights into their current information security status (Kotulic and Clark, 2004). In addition, security awareness and compliant-behavior is widespread (e. g. password strength, encrypting sensitive e-mails, etc.), meaning that it is impossible to observe all aspects of security behavior for a large amount of end-users. Therefore, observations alone are insufficient. Evidence must be gathered from real work situations over a longer period of time. Long-time data in actual working environment can be observed for example with the use of log-files as done by Venkatesh et al. (2003) and Workmann et al. (2008). Regarding the relationship between BI and AB, only five research papers examined the relationship between end-users' BI and AB. Although these studies found a significant relationship between both constructs, all five studies used self reports to assess end-users' AB. Of particular note is that many research papers postulate a strong and consistent relationship between BI and AB by referring to Venkatesh et al. (2003). Venkatesh et al. (2003) also used self reported data in a non information security environment. Therefore the assignability of the results needs to be questioned as end-users' BI is a truly reliable predictor for AB or are there any external or environmental factors that mitigate the influence of BI on AB. For example, as referred in TRA/TPB, an end-user might intend to behave in compliance with the organization's ISP because of his/her strong self-efficacy and normative beliefs but is not able to transform his/ her intentions into real work situations. Reasons can be due to a heavy workload in combination with complex security measures. This BI – AB gap implicates that employees have positive intentions but subsequently fail to enact those BI. To alleviate this BI – AB gap, the application of scenario techniques is possible (Bulgurucu et al., 2010). Providing detailed information about potential information security situations and indirectly questioning the attitude towards information security might lead to a better impression of an end-users's true BI.

As can be seen in Table 11, researchers face low response rates. Within the reviewed literature, only five studies included more than 500 respondents (Hovav and D'Arcy, 2012; Pahnlia et al., 2007 (1); Siponen and Vance, 2010; Siponen et al., 2007; Siponen et al., 2010). Empirical samples are useful as long as these are representative and generalizable. Other researchers surveyed students or IS professionals. These samples do not reflect the population of interest. With reference to internal, external and construct validity, surveying students is seen more critically than having a smaller sample size as long as it represents reality (Sivo et al., 2004).

Another aspect is that practitioners face the problem of how the proposed theoretical constructs that were found to be determining end-users' behavior can be adopted in real life situations. A gap between theoretically explanations of influence factors of end-users' security awareness and compliant behavior and the need to know which interventions to apply by practitioners has grown (Workman et al., 2008). For example Roseman and Vessey (2008) emphasized that academic literature should provide more relevance for practitioners in order to prevent research from becoming an end unto it-self. Therefore it is necessary to design and validate concrete measures and process models based on already existing theoretical knowledge of individual factors. This can add value to the research field and can mitigate the gap between theory and practice.

5.1.7 Conclusion, limitations and outlook

The presented work gives a state-of-the-art overview of behavioral theories that were applied in the context of end-users' security awareness and compliant-behavior. In total, 113 publications were identified and analyzed. The four primarily applied behavioral theories are the TPB, GDT, PMT and TAM. A meta-model that explains end-users' security awareness and compliant behavior was introduced by assembling the core constructs of those theories. Based on empirically tested research models, a discussion of factors with a proven significant influence on end-users' security behavior was presented.

Results indicated that several research studies used the core constructs of the original behavioral theory without adding additional external factors that explained BI or AB. In the research field, a dominance of quantitative work has been identified. Qualitative studies like action research and interview studies could add value to the research field. Furthermore, it could be shown that the reliability of BI as a predictor of actual security behavior needs further attention in this research field. End-users' AB is mainly measured with the use of self-reports. A stronger consideration of other research methodologies such as experiments or case studies is required. In addition, few research studies addressed concrete practical relevant process models in order to adapt the theoretically examined behavioral factors in real life situations. In order to close this gap between theory and practice, the development of measures and process models that influence end-users' security awareness and behavior based on already existing theoretical knowledge is necessary. These shortcomings are the motivation for the research study presented in the next chapter.

Turning to the limitations of this publication, although a rigorous approach was used to search relevant literature, there are possible shortcomings concerning the identified literature. On the one hand, only search terms in English language were used. Relevant literature in other language, for example from the German-speaking IS research, were not taken into account. Therefore it is possible that the results as proposed in Table 11 are not complete and can vary based on the results of research studies that are provided not in English language. Another limitation is presented by the list of search terms that were predefined and not developed inductively. One arising problem in IS research is the proliferation of terms that describe similar topics and concepts. A second search process with extended search terms which were identified during the literature analysis process should be conducted to find further literature that is relevant in the context of this literature review. By excluding non-peer-reviewed research papers (e.g. books, whitepapers) only publications of controlled quality were included in the analysis process. Even though it is expected that books might also include valuable contributions that enhance research in the examined field. It can therefore not be excluded that some contributions might be missing in this literature review.

As mentioned above, a manual approach for identifying applied theories and research methodologies was chosen. To avoid mistakes, the authors integrated countermeasures to assess reliability and validity (vom Brocke et al., 2009). Nevertheless, the application of latent semantic analysis to our dataset could be a useful addition by discovering more coherent concepts. Further, due to the complexity of the subject matter and the diversity of identified theories, an in-depth analysis of the four primarily applied theories was presented. Other behavioral theories beside the TPB, GDT, PMT, and TAM might enhance the results by explaining other important factors that explain and predict end-users' security awareness and compliant-behavior.

5.2 Towards a needs assessment process model for SETA programs – Implications from an action design research study

5.2.1 Preamble

This chapter presents the summary of the research paper with the title "Towards a Needs Assessment Process Model for Security, Education, Training and Awareness Programs - An Action Design Research Study" (Lebek et al., 2013c). The paper was presented at the 21st European Conference on Information Systems (ECIS) in Utrecht, Netherlands (June 5 – June 8, 2013) and published in its proceedings. The ECIS is Europe's biggest and most prestigious IS conference and the second biggest IS conference worldwide. The conference provides a platform for both researchers and practitioners to discuss research findings, problems and opportunities, and exchange new and exciting ideas (ECIS

2013). The conference guarantees high quality and a professional focus of published research papers as the acceptance rates have been roughly in the range of 30 percent (ECIS 2012).

The paper was submitted to the Track "IS Security and Privacy". The conference proceedings are rated by the WKWI and GI-FB WI with an "A" (WKWI, 2008). The VHB-Jourqual2.1 by Schrader and Hennig-Thurau (2011) rated the ECIS with a "B".

5.2.2 Introduction

The results of the literature review presented in chapter 5.1 showed that in the context of security awareness and compliant-behavior, generally accepted models and approaches for practice are still lacking. Practical relevant information security research is still in its beginnings and practitioners face the problem of how to adopt empirically validated constructs into real life situations. Therefore organizations often face difficulties in managing an efficient and sustainable SETA approach in order to enhance the employees' security awareness and compliant behavior (Eloff and Eloff, 2005). On the other side, researchers face the problem that information security is a sensitive topic and organizations are unwilling to reveal information that provides insights into their current information security status (Kotulic and Clark, 2004). Although both, researchers and practitioners, have proclaimed the benefits of SETA programs (Straub and Welke, 1998; D'Arcy et al., 2009) there is still a need for research that closes the gap between organizational relevance and methodological rigor.

In the planning phase of a SETA program, the organizational objectives need to be taken into account first. To ensure that SETA programs are efficiently aligned with organizational objectives, important areas need to receive more attention and in turn should receive more resources than others (Kruger & Kearney, 2006). As Abdulrazeg (2012) emphasized, security behavior cannot be improved if it cannot be measured. Therefore the purpose of this publication was to determine a risk and priority measurement method that assists organizations in capturing, evaluating, and depicting the current state of end-users security awareness and behavior. The organizational needs in enhancing security awareness and behavior are concretized by presenting a process model. This process model was developed and tested in an international engineering company and addresses the importance of a needs assessment. To build a bridge between organizational relevance and methodological rigor, a research approach that is relatively new in IS research, namely ADR as proposed in chapter 3.1.2 was adapted. With the use of different cycles, ADR allows continuous interaction between researchers and practitioners in early stages.

5.2.3 Research design

The underlying research methodology was adopted by Sein et al.`s ADR approach (Sein et al., 2011). As can be found in Figure 17, four stages and five cycles were relevant to design the process model for a needs assessment in the security awareness and compliant-behavior context. The first stage was motivated by a problem perceived in the practical setting of an international acting engineering company for which the co-authors of the author of this thesis work. This company initially faced the problem of how to identify measureable values of end-users' security awareness and compliant behavior. An ADR team was formed that consisted of researchers and one alumnus from the Information Systems Institute at the Leibniz Universität Hannover and members of the SETA project team within the target company, including the CIO and the information security project manager. The shared competencies facilitated the problem definition and formulation.

The results of the problem formulation in stage one provides the groundwork for the following three stages. In the second stage, building, intervention and evaluation, the process model to conduct a SETA needs assessment is designed and evaluated. It consists of five iterative cycles that is carried out in a real-world environment. These five cycles are represented by an interaction process at three levels: researchers, practitioners (IS management) and employees. In the first cycle, the alpha version of the process model was developed. In cycle two, the process model was introduced to practitioners for the purpose of evaluation. The first practical iteration did not shape the employee level because of the needed expertise of designing the IS artifact. Based on feedback from the practitioners, beta version of the initial process model was developed. The applicability of the proposed needs assessment process model was presented and pre-tested within IT department of the target company. In cycle five, based on the feedback of the participating employees, the process model was refined until the final version was reached and adopted by the participating organization. The following stage, reflection and learning, evaluates the developed process model and was carried out simultaneously to the previous stage. The feedback loops from the cycles one to four allow transferring experiences from the problem solution within the target organization into knowledge that addresses the broad class of problems and is applicable for other organizations. Additionally, the continuous reflection and learning stage helped to gain a better understanding of the problem. The fourth and last stage aims to provide a general solution for a broad class of problems as it outlines the results of this study as design principles.

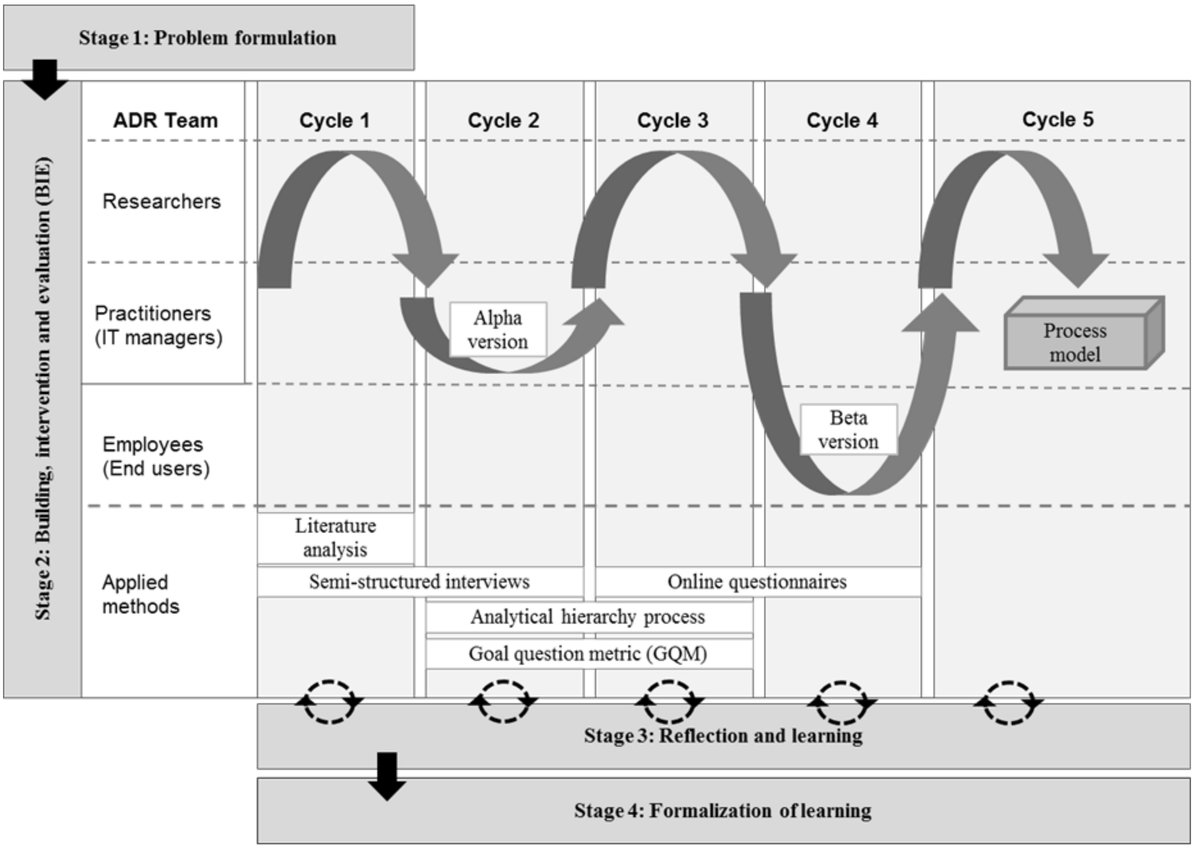

Stage 1: Problem formulation
Stage 2: Building, intervention and evaluation (BIE)
ADR Team
Cycle 1
Cycle 2
Cycle 3
Cycle 4
Cycle 5
Researchers
Practitioners (IT managers)
Employees (End users)
Applied methods
Alpha version
Beta version
Process model
Literature analysis
Semi-structured interviews
Online questionnaires
Analytical hierarchy process
Goal question metric (GQM)
Stage 3: Reflection and learning
Stage 4: Formalization of learning

Figure 17: Applied ADR method

5.2.4 Development of the process model for a SETA needs assessment

First, the problem formulation for research and practice needs to be taken into account. Part of the first phase of a SETA program is the execution of a needs assessment (NIST SP-800-50). A needs assessment determines the current level of security awareness and shows the potential need for action by defining the capabilities of SETA programs. The theoretical foundation was based on both, theoretical and practical models and guidelines. On the theoretical side, prior work of Kruger and Kearney (2006) were used. Both authors developed a prototype to measure security awareness levels of employees. However, the needs assessment was underrepresented in their work. On the practical side, the NIST SP-800-50 provides guidelines for SETA needs assessments in organizations.

The initial process model was primarily based on two data sources: First the results of a comprehensive literature review and second the results of semi-structured interviews. These were conducted with six IS managers of the target company with the aim of collecting the company specific requirements and objectives regarding the needs assessment process in the context of a SETA program. Based on these results, the initial rudimentary process model (alpha version) for identifying the needs in security awareness and behavioral compliance is designed. This process model is presented in Figure 18.

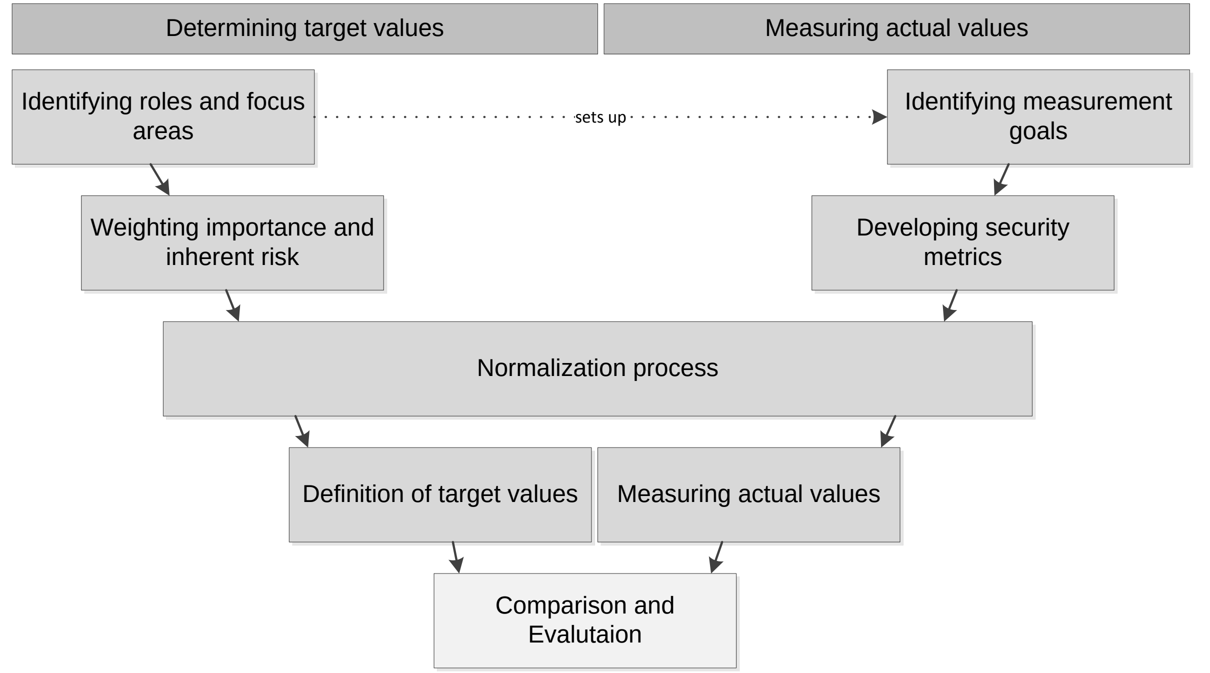

Determining target values
Measuring actual values
Identifying roles and focus areas
sets up
Identifying measurement goals
Weighting importance and inherent risk
Developing security metrics
Normalization process
Definition of target values
Measuring actual values
Comparison and Evalutaion

Figure 18: Needs assessment process model

The ADR team pointed out that evaluating of security awareness and security behavior for every end-user in the target company is inapplicable. For this reason, it was decided to focus on several perspectives on end-users' security behavior. First, end-users in different roles and positions demonstrate different security-related behavior, resulting in a role-based view. Second, the concept of focus areas from Kruger and Kearney (2006) was adopted and finally associated with the end-users' role and position. Focus areas represent critical risk areas in which the behavior of the end-user is evaluated (e.g. the use of mobile devices). Because each focus area does not contain the same risk potential in the target company, the focus areas need to be weighted amongst each other. Further, the ADR team concluded that the assessed focus areas vary in their importance for the different roles. For example, the focus area "use of mobile devices" is less important for end-users that do not use mobile devices in their work environment, such as the role of application developers. After the definition process of end-users' roles and focus areas, the measurement goals were defined. For this purpose applicable security metrics were identified. Since prior research studies evaluated the models with the use of self-reported data (see the results of chapter 5.1), the integration of real life data that determines AB (e.g. system monitoring data, incident records) into the measurement process were preferable. The definition of desired behavior is assessed by transforming the role and focus area specific importance and risk weightings into specific target values. In order to evaluate a gap between AB and desired behavior, a normalization process was needed to ensure that target and actual values were comparable.

5.2.5 Definition and weighting of roles and focus areas

The roles of end-users were determined by the target company's business processes and organization chart. The focus areas are defined based on semi-structured interviews with IS experts within the company and the perspectives of prior academic research. For example, Drevin et al. (2007) developed a value-focused security awareness approach whose fundamental objects included a network of focus areas that need to be taken into account in information security decisions. The authors identified thirteen mean objectives, e.g. maximize logical access control, minimize virus infection, and responsible use of e-mail and internet. In order to gain a practical view on relevant focus areas, several information security reports that report actual focus areas were analyzed (e.g. Verizon – 2011 Data Breach Investigation Report; KPMG - The e-Crime Report 2011). Based on the literature analysis, a list of focus areas was developed. These were generic in scope resulting in each focus area had to be validated within the context of the target company.

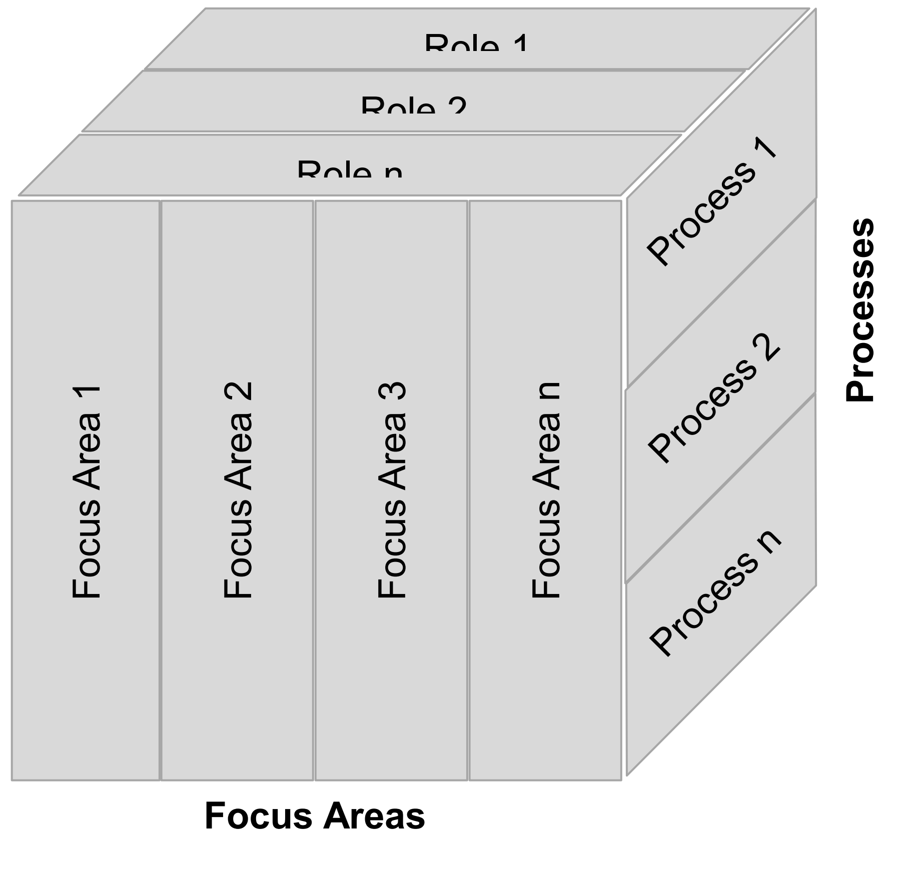


Figure 19: General relationship between focus areas, roles and processes

With the use of semi-structured interviews of six IS experts of the target company, the interviewees were asked about the number and relevance of the focus areas for the target company. This process leads into a list of nine critical areas of information security awareness: access control, client workplace, storage media, mobile devices, software, internet, e-mail, handling of critical information, and physical safeguarding of the workplace. In the next step, the experts were questioned to determine relevant factors that accounted for each focus area in the target company from his or her point of view. For example, for the focus area “use of mobile devices”, the experts named “damage to devices”, "network access", "apps", and "securing of mobile devices". Figure 19 illustrates the general relationship between focus areas, roles and processes.

The inherent risk potential (RP) for each focus area and the importance (I) of each focus area per role were determined with the use of the analytic hierarchy process (AHP) as proposed by Saaty (1980). This method was developed to solve complex, multi-criteria decision problems. AHP provides explicit specifications in analysis, intuitiveness, validated measurement scales, and has robust built-in consistency assessments. Following the AHP approach, a specified number of questions were developed for pairwise comparison of the focus area's RP and I. The weights were obtained from an expert team and the company's CIO with the use of an online questionnaire.

The results of the pairwise comparison were aggregated in a (n x n) comparison matrix. Normalized eigenvectors with a sum to one indicated the relative I/RP for the different focus area measures. For each respondent a judgment matrix was developed. This procedure was needed to calculate the average risk and priority matrix for each focus area. Overall weights were derived by calculating the average value of each expert's individual weightings of I and RP, resulting in two matrix, one for I and the other for RP for each focus area. The impact value (IV) of each focus area per role IV = I * RP was calculated. Table 12 provides an example for IVs on behalf of two focus areas.

Table 12: Example of impact values

Focus areas	Roles			
	Management	Onsite staff	Server administration	Application development
Focus area 1	0.11	0.18	0.11	0.14
Focus area 2	0.30	0.28	0.27	0.22

The IV was used to determine target values on a scale ranging from 0 to 100 with the use of a spreadsheet application. The current awareness level was obtained by comparing to the target corridors. These were derived in accordance with the expert team in the following range: 100 - 75 = good; 74.9 - 50 = average; 49.9 - 25 poor; 24.9 and less = unacceptable. The lower limit of the section 'good' (=75) was multiplied by (1+IV) for each focus area and role. In order to avoid having target corridors that were too small, the minimum size of the corridor 'good' was set up 10 points to 85. All other lower limits were raised by the same amount. The resulting target corridors for two example focus areas from Table 12 are shown in Table 13.

Table 13: Example of target corridors

Focus areas	Roles											
	Management			Onsite staff			Server administration			Application development		
	G	A	P	G	A	P	G	A	P	G	A	P
Focus area 1	83	58	33	88	63	38	83	58	33	85	60	35
Focus area 2	90	65	40	90	65	40	90	65	40	90	65	40

G = Good; A = Average; P = Poor

5.2.6 Actual behavior measurement

AB was measured with the use of security metrics. The selection of security metrics was done by applying the goal-question-metric (GQM) approach introduced by Basili and Weis (1984). The GQM is a validated approach that facilitates the selection and implementation of security metrics and aligns them to the specified focus areas. Originally used to develop software metrics, the GQM has been applied in the information security context (e.g. Abdulrazeg et al., 2012; Hayden, 2010). In general, the GQM approach is applied in three steps (Ebert et al., 2005). First of all, concrete targets for improving security behavior were defined. All nine goals were derived from the focus areas defined above. In the second step, based on these targets, concrete questions were developed. For this purpose, the results of literature analysis (chapter 5.2.4) and the factors which were named during the expert team interviews to define the focus areas were used. These questions related to the essential aspects of target achievement. In the third step, the corresponding security metrics were defined by the ADR team. Figure 20 shows an excerpt from the GQM approach used within the example focus area "mobile devices".

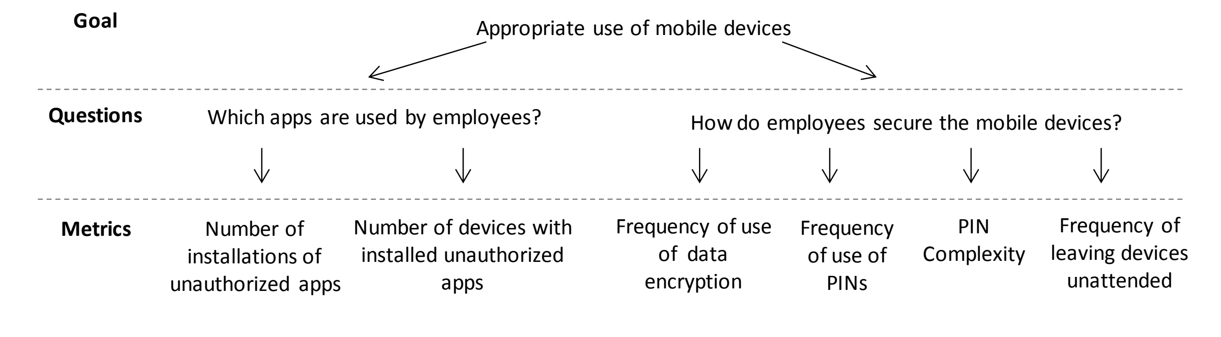

Goal
Appropriate use of mobile devices
Questions
Which apps are used by employees?
How do employees secure the mobile devices?
Metrics
Number of installations of unauthorized apps
Number of devices with installed unauthorized apps
Frequency of use of data encryption
Frequency of use of PINs
PIN Complexity
Frequency of leaving devices unattended

Figure 20: Example of the GQM approach for the focus area "mobile devices"

While discussing the results with the target company's information security manager and IT security expert, it became apparent that some of the defined security metrics are unnecessary to obtain. For example, since the use and complexity of PINs for mobile devices is technically restricted, the corresponding metrics were dropped. Other metrics were withdrawn since no explicit regulations had been defined within the company's information security policies.

Within the target company, reliable data sources were determined to collect these metrics. Some metrics, for example the frequency of writing down a password, could not be obtained from either system monitoring data or incident management records. Therefore, additional methods for collecting these security metrics became necessary. In a discussion round with the ADR team, it became obvious to use self-reporting data from end-users. A survey was sent to 50 end-users, 29 of which returned a completed questionnaire. The survey was structured as follows: At the beginning, each participant had to select his or her role within the organization. Based upon role specification, the survey tool provided a role-specific set of questions. To give an example, the survey of the roles "application development" and "server administration" did not contain the mobile device block, since mobile devices were not used during their work. The survey was divided into two sections. First, the participants were questioned about security behavior in the focus areas that are relevant for their role. In the second section, the end-users were asked about their beliefs or attitudes towards information security in the respective focus areas.

A potential gap in security awareness was evaluated by comparing the collected, normalized data with the target corridors as proposed in chapter 5.2.5. A score ranging from 0 to 100 for both the behavior and the attitude measurements were determined per role and focus area. In order to achieve comparability between self-reported data and system data, the experiences of the expert team members were resorted. The system based security metrics were evaluated with a five-point Likert scale. After that a score that averaged each evaluated metric was determined. The overall score was determined by averaging the three single scores (Table 14).

Table 14: Scores for an example role

	Points
Score behavior:	89.1 (●●)
Score attitude:	82.7 (●)
Score monitoring:	60.0 (●)
Overall score (Ø):	77.3 (●)
Target value (good)	85.0 (●●)
Difference to corridor 'good':	-7.7

●● = Good; ● = Average

Lastly, the overall scores were compared to the determined target corridors for each role. The degrees of goal achievement were transferred to the awareness map (Table 15). The difference between each role’s overall score and the lower limit of the company specific target corridor ‘good’ was calculated.

Table 15: Example of the overall awareness map

Focus areas	**Roles**			
	Management	Onsite staff	Server administration	Application development
Focus area 1	●● (+1.9)	● (-16.43)	● (-4.92)	● (-7.73)
Focus area 2	●(-14.97)	● (-23.75)	n/a	n/a

●● = Good; ● = Average; (+/- X) difference from overall score to the lower limit of the corridor ‘good’

5.2.7 Formalization of learning

According to the ADR approach, each stage and cycle during the BIE stage was reflected to learn from the practical intervention. Through formalization, the experienced knowledge was transformed into general design principles that contribute to academic knowledge to the respective research field. A summary of results is presented in the following:

- Integration of key-members of the organization: It is necessary to consider key-members of the organization (i.e. management, experts, key-users) to reduce potential barriers understand the purpose. Experts and key-users provide valuable experiences that complement measured data.

- Employee perspectives: Different observation levels should be integrated to enable a selective analysis of the state of the art of employees' security awareness and behavior. The selection and combination of observation levels depends on the organizational context.
- Weighting of target values: Focus areas are critical risk areas of employees' security awareness and behavior. In determining adequate target values, the risk potential and importance of each focus area has to be evaluated.
- Definition of adequate security metrics: A standardized process for developing metrics that correspond to organization-specific focus areas is a basic condition to ensure the validity and reliability of measuring employees' security awareness and behavior.
- Use of reliable data sources: Instead of relying on self-reported data of employees, the use of reliable data sources such as system monitoring data are needed. The integration of system monitoring data requires the establishment of a mature and detailed monitoring process.
- Normalization process: To make metrics comparable, normalization of data is needed.
- Presentation of results: By depicting results from the evaluation process in an awareness map, needs for training and awareness measures can easily be illustrated. Proper documentation of the measurement process is necessary to develop concrete measures.

5.2.8 Summary of results and implications

First, the management support place an important role to conduct a needs assessment process in a company. The concept of management support has been shown to be a necessary condition in the information security context (e.g. Kotulic and Clark, 2004). Second, the expert team forms the connector to the research and practice, since the expert team fits the needs assessment process to the company specific requirements. In addition, the experts were able to compensate for insufficient data from system monitoring. With an inclusion of key users, employees better understand and accepted the purpose of the project. Further, the results indicated that security awareness and behavioral compliance is a complex role and focus-area specific problem with multiple different security metrics. Therefore it is necessary to integrate different perspectives into the needs assessment process. The focus areas need to be defined organization specific to meet the objectives. The I and RP of each focus area diverge dependent on the roles which results in a weighting process. The adoption of the AHP approach has been shown to be applicable in developing specific weights. Problems arose with the use of surveys to conduct pairwise comparisons. The participants faced problems in understanding the focus areas. Due to the low number of respondents the problem was solved by individually explaining the focus areas. The survey consisted of 180 pairwise comparisons, which meant a high workload for each expert team member. In other organizations with stricter information security requirements, this might lead to inefficiencies. To avoid this problem, an a priori method that allows the interactions between researchers and participants (e.g. focus group discussions) to perform the AHP process is recommended.

The GQM approach to measure end-users' AB provides an adequate way for developing security metrics from the targets set up by the defined focus areas. System data are considered to be more reliable than results from self-reported data to evaluate AB. However, the experience of this study showed that the use of self-reported data were necessary in order to gain full coverage of end-users' security awareness and behavioral compliance. A further problem emerged in regard to the comparison of system and self-reported data. Adjustments were needed to make the data comparable. But the available system data were not sufficiently detailed, e.g. metrics for unauthorized software installations were available for the whole company and not for a specific organizational unit or a role. Therefore, other companies that apply these procedures need a mature system monitoring process for successfully integrating system monitoring data into the SETA needs assessment process. By normalizing collected metrics to a range from 0 to 100, the measurements were made comparable.

The presentation of the degree of target achievement in an awareness map enables a quick initial overview of the current state of end-users' security awareness and behavioral compliance. In addition, with a step-by-step documentation of the measurement process, a more detailed view of the identified needs was gained, thus providing a basis for developing a company specific SETA program.

5.2.9 Conclusion, limitations and outlook

The purpose of this research study was to close the identified gap between theory and practice (see chapter 5.1.7) by providing a needs assessment process model for SETA programs. For this purpose ADR has been applied. ADR is a research methodology that allows a continuous interaction between researchers and practitioners and guarantees that the measures are aligned with the company's objectives. An ADR team was built that consisted of researchers and IS managers from an international engineering company. The target value definition as well as the development of a reliable and valid measurement process was emphasized as major challenges to conduct a SETA needs assessment. The initial process model was developed and refined during several cycles of feedback loops between researchers and practitioners, after general design principles were set up. The study aims to focus on theoretically founded explanation of end-users' security awareness and compliant-behavior in combination with the need of practitioners to know which interventions to apply. The continuous intervention between researchers and practitioners results in a procedure model that assists organizations in implementing a needs assessment for SETA programs. The model supports IS managers in identifying and evaluating a gap in end-users' security awareness and behavioral compliance. Based on these findings, it provides a basis for designing an adequate SETA program. Turning to the academic side, this study contributes to information security research as it focuses on reducing the identified lack of generic process models. This study facilitates the development of concrete training and awareness measures to enhance end-users’ security awareness and behavioral compliance. Further the mentioned approach enables dynamic depiction of the current state of employees’ security awareness and behavioral compliance and its changes over time.

Some general limitations exist: First, this research study applies an ADR approach in order to solve a specific company-specific problem and derive solutions for a class of problems. It could be proven that ADR is suitable for drawing design principles for SETA needs assessment processes from a company specific context. But the needs assessment procedure only was tested within one single company that participated in the research process. Therefore, generalizability of the results can be questioned. On the other side, Lee and Baskerville (2003) emphasized that a greater sample size within qualitative research studies is not an indicator of better generalizability. However, the results of this research study will benefit from further evaluation and refinement by including several companies into for example a field study. It would be valuable to include cross-organizational differences that might affect the needs assessment for SETA programs. For example, in financial or health care sector, information security requirements are stricter than in the engineering company of this research study. Future research can focus on organizational differences in branch or company size and compare those results to the results of this study. Further, the suggested needs assessment procedure model was applied to one business process within the target company and measures end-users’ security awareness and behavioral compliance in two out of nine focus areas. Even if the authors do not expect substantial changes to the general design principles, further experience is needed. For example, the presented design principles can be refined with the experience from practitioners or end-user feedback during an organization wide roll-out of the needs assessment process. Another limitation is that the focus of this paper was to develop and validate a needs assessment approach. This represents the first step in the overall process of implementing a SETA program. Future research should investigate this needs assessment approach in a long-term view. Based on the needs assessment approach, the development of concrete information security awareness and training measures has to be evaluated and has to prove its applicability. Further, it would be valuable for the information security community that future research provides a generic list of security metrics in order to complement the proposed process model.

6. Thesis conclusion, limitations, and future research

6.1 Conclusion

This chapter outlines the overall conclusion, contribution and limitations of this thesis. This thesis was motivated by identified research gaps within the context of behavioral science in the information security context. The global focus lies on the question of how organizations can implement information security efficiently. Two human perspectives were considered in the seven discussed research studies. In part A the management level represented by information security executives was taken into account. In part B the focus lies on the end-user or employee level. For this purpose, multiple research methods from both IS research paradigms were applied to investigate the specific artifacts. In IS research, this approach has been shown to be appropriate and valuable (Hevner et al., 2004; Mingers, 2003). The combinations of different research methods within each paper can be broadly summarized by the examined objectives and topics. Starting with the investigation of information security executives, by developing and justifying behavioral theories and models that focus on individual differences and cognitive processes, the use of empirical data were essential to test the hypothesized relationships. The research models and the hypotheses development were based on thorough IS literature which has been identified with a comprehensive literature analysis and a qualitative content analysis. The empirical data were analyzed with the use of techniques of multivariate statistics. The examination of the second human perspective, end-user level, was evaluated with the use of qualitative research methods but also quantitative research methods played an important role. The needs assessment process model was developed on behalf of the ADR approach as proposed by Sein et al. (2011). The experience of this research approach showed that for data collection qualitative as well as quantitative methods were necessary. The groundwork for this research study is based on a comprehensive literature review followed by a qualitative content analysis. In the following, a short summary of results of each study is presented.

The purpose of the first presented publication in chapter 4.1 was to present a holistic information security framework. This framework is based on the interaction of interdisciplinary dimensions and sub-components, relevant for efficient and sustainable implementation of information security. Little research combined empirically and theoretically substantiated principles to a general holistic ISM approach. Starting with the use of a comprehensive literature review with the purpose of identification of ISM components, the practical relevance was tested using empirical data from information security executives. Results suggested that holistic ISM contains of seven holistic information security dimensions, namely technical, organizational, human, strategic, cultural, economical, and compliance/monitoring. These dimensions consist of 18 sub-components. The seven information security dimensions build the groundwork for the research study presented in chapter 4.2. The second research study focuses on information security executives' behavior, cognitive processes and individual differences. Since information security executives cause potential ISM risks, directly influence an organization's information security level with their decisions and differently valuate the importance of each information security dimension, the behavioral and cognitive factors were investigated more in detail. Behavior depends on personality traits and other cognitive factors such as attitudinal constructs. For this purpose, the personality traits were considered as influence factors for attitudes towards the seven dimensions of holistic ISM. The hypothesized relationships were validated with the use of empirical data of German-speaking information security executives. Results showed that there is no "one size fits all" solution. Information security executives' personality traits have a significant relationship on the attitudinal constructs towards holistic ISM. For example, agreeableness was found to be influential to attitude towards the organizational dimension of ISM, while openness and emotional stability were found to have a positive relationship to the technical dimension of ISM. The results further indicated that in some cases the relationships between personality traits and attitude are more complex than a single linear one. Chapter 4.3 with the presentation of two research studies shed more light in the complexity of those relationships by integrating the moderator "compliance" and six control variables. For that purpose the personality traits of conscientiousness, neuroticism, and openness were put into relation to ATT and BI towards managing technical security measures. Findings suggested that when information security executives use information security standards or guidelines in their daily work tasks, the personality traits of conscientiousness and openness will have a stronger effect on ATT towards managing security measures. In addition, the organization industry type and the educational level of the information security executives were shown to have a significant influence on BI.

From the end-users perspective, a variety of researchers discuss explanations for end-users' security awareness and compliant behavior. Chapter 5.1 presents a theory-based literature review of the extant approaches that explain and predict employees' security awareness and behavior over the past decade. In total, 113 research papers were identified and analyzed, focusing on the four main behavioral theories, TPB, GDT, PMT, and TAM. By synthesizing results of empirically tested research models, a discussion of factors that were proven to have a significant influence on end-users' security awareness and behavior or behavioral intentions, is presented. The results of this literature review demonstrated that in the context of end-users' security awareness and behavioral compliance, generally accepted models and approaches that are applicable for practitioners are still lacking. Further, little research was done to investigate the relationship between BI and AB. Both shortcomings implicate that practitioners face difficulties in putting these theoretical constructs into real life situations. With the use of SETA programs, companies and organizations provide their employees awareness of information security risks and the necessary skills to protect their information security assets. Chapter 5.2 puts the identified research gap and the organization specific requirements of a SETA program together and presents a needs assessment procedure. Using ADR as a research methodology that contributes to practical and academic knowledge, the research study aims to present a systematic approach to capture, evaluate, and depict the current state of employees' security awareness and behavior. AB is evaluated by determining the target values and measuring actual values with respect to security metrics. The initial process model was developed and refined during several cycles of feedback loops between researchers and practitioners, after general design principles were set up. End-users' actual behavior is evaluated by determining the target values and measuring actual values with respect to security metrics, however, the experience of this study showed that the use of self-reported data were also necessary in order to gain full coverage of employees' security awareness and behavior compliance. The resulting presentation of the degree of target achievement was proposed in an awareness map that enables a quick initial overview of the gap between organizational objectives and the current state of end-users' security awareness and behavioral compliance.

6.2 Limitations and outlook

In this last section, the major limitations that need to be considered when interpreting the results of this thesis are outlined and directions for future research are presented. Since the limitations of the seven research studies were already picked out in the according chapter, the limitations presented in this section focus on the outcomes of the whole thesis and will be more in detail.

To start with the generalizability, it has to be noted that the empirical studies and interviews were conducted with specific subjects from German-speaking countries. In chapter 4 especially in the chapters 4.2 and 4.3 the model testing was based on an empirical database of 174 information security executives from different industry types, ages, and educational level. In part B, the ADR team, or the expert team (Chapter 5.2) consisted of employees with an information security background, working at a German engineering company. This has to be considered when transferring the results to any other industry or to any other than the information security discipline. Therefore it is possible that single selection bias could exist, although information security executives provide a high level of confidence in the quality of their answers (Hsu et al., 2012). Both of the research areas still demand an empirical confirmation by a larger and/or more diverse sample of participants for enhancing the body of information security knowledge. Future research studies are recommended to the following points:

- In both research studies, future research should concentrate on a larger and more diverse sample size that represents information security executives (or experts in the research area as proposed in chapter 5.2) as a whole.
- In addition, the needs assessment process model needs to be validated in additional companies and organizations and compared to the presented results.

Focusing on information security executives from different industry types may lead to completely different results. For example, in the financial or health care sector, the regulative requirements are much stricter than in an engineering company. In the research studies of part A, this can lead to different beliefs or attitudes towards holistic ISM because compliance factors need to be taken into account. Regarding the needs assessments approach, the individual risk assessment during the interview and survey cycle can lead to completely different results, if other target groups were questioned. To give an example, educational level, risk tolerance or even risk aversion can have an influence on their decisions. On the other side, a lack of competencies in the field of risk assessment, AHP, or GQM might also lead to divergent results in the process model development. In addition, it should be considered that generalizing the results to any other national or international context need to take cultural or political differences into account. These were not part in the presented research papers of this thesis. For example, Dinev et al. (2009) demonstrated that cultural factors are influential moderators in end-users' attitudes and behavior. By adopting the TPB, the authors suggested that cultural differences need to be taken into account when designing effective information security policies and practices. These limitations lead to the following suggestions for future research:

- In the field of holistic ISM, future studies should expand the proposed research model in chapter 4.2 to include an international context by integrating cultural differences.
- Further, to increase generalizability, future research should examine the influence of organizational objects such as size or type or other individual objects such as educational level, gender, or age into the personality – attitude relationship and investigate their influence.
- In the field of end-users' security awareness and behavioral compliance, future research should focus differences in culture by extending the study as proposed in chapter 5.2 to an international context.
- During the risk assessment of I and inherent RP, the influence of individual factors should be considered, whether these lead to different results.
- Both research fields can be extended in future research by examine the decision making process and the resulting AB. The question will be whether the indicated individual differences and their relation to ATT or an identified gap in security awareness will lead to concrete decisions to enhance organizational information security.

In addition to the above mentioned factors that need to be considered, other external factors might influence the output of the presented research studies. For example, organizational support for IT (Chen et al., 2010), actual adoption of security measures, organizational computerization (Yeh and Chang, 2007), and information security culture (Schlienger and Teufel, 2003) were shown to be influential factors in the IS context. For example in the context of the needs assessment process model for SETA programs, the current level of security measures was considered in the process model by the assessment of I and inherent RP and the selection of security metrics. An a priori evaluation of the information security policies and information security culture was no part of these research studies. The basic requirements of efficient information security are the existence of detailed information security policies that determine the current state of security. Turning to part A within this thesis, external factors in addition to the above mentioned individual factors may enhance the presented research studies but makes the evaluation even more and more complex. The research model as proposed in section 4.2 contains of 13 constructs, 23 hypothesized relationships and including demographic statistics over 100 items. Additional external factors will enhance the complexity of the research model and participants will be confronted with again more than 100 questions. Therefore it is expected that additional factors might lead to inefficiencies within this research model. Follow-up studies are recommended to focus on one specific attitudinal dimension of ISM and/or only on specific personality traits. For example, the relationships between extraversion and agreeableness and the attitudinal information security constructs that contain interpersonal interaction can be examined more in detail by including the effects of the opinion of significant others. This leads to the following recommendation of future research studies:

- The field of personality traits and attitude towards holistic ISM can be enhanced with a focus to external factors. By going more in detail to the hypothesized relationships, additional influence factors can improve the statistical power of the research model
  Note: additional external factors will enhance the complexity of the research model that can lead to inefficiencies.
- Prior to adapting the proposed process model of needs assessment for SETA programs, the influence of for example the current state of information security policy communication and information culture needs to be examined.

A further limitation that concerns both research areas is the phenomenon of single session sampling. Both research areas present a time extract without focusing the long term view. To study changes in behavior or decisions, the next step towards a long-term view will be the examination of both research areas over time. Interesting in both research fields would be the investigation of the benefits that were provided with the adoption of the proposed research models in a real world example. For example, in the research area presented in chapter 4, information security executives' personality traits are shown to be more or less stable over time (Costa et al., 1991). On the other side, attitude towards ISM can change, depending on for example information security incidents and individual experience. Additional research is recommended that takes a long term view into account and examines the influence of behavioral changes over time and can be rooted in individual differences. A first impression of this research field can be found in Maier et al. (2012). Based on different scenarios, for example after a security incident situation or with the adoption of innovative technical security measures, the influence of personality traits on attitudes towards holistic ISM can be measured again and compared to the results as suggested in chapter 4.2. In the second research area, the needs assessment process model needs to be evaluated in a post view after an executed SETA program in order to investigate the usefulness of investments. For that purpose, the applicability after a period of time needs to be evaluated whether the introduced approaches (AHP, GQR) meet their goals. Thus, additional research studies that deal with the following topics are suggested:

- Further research studies need to take the long term view into account. It could be interesting whether behavior and decisions vary over a period of time and can be determined by individual differences.
- Additionally, the benefits of the proposed research models need to be applied in real world examples and the benefits (compared to the costs) need to be investigated over time.

To become more general, both research areas represent excerpts of real-life situations. The personality traits in chapters 4.2 and 4.3and the attitudinal constructs are based on self-reported data. The measurement of behavior in real-life situations for example during a security incident or in the context of SETA programs (chapter 5.1 and 5.2) the receiving of suspicious emails is difficult to measure. In addition, the collection and evaluation of actual behavior data are time consuming and cost intensive. Employee monitoring is an intrusion into individual rights and regulated by labor law. Therefore, the proposed research results in both areas may be incomplete in regard to the measurement of AB. Due to the sensitive context of information security, self-reported data were necessary to gain an insight into the behavioral aspects of the respondents. As stated in section 5.1, the use of self-reported data to measures security-related attitudes and respective behavior might lack validity. Self-reports are prone to the problems of common method variance, consistency motif and social desirability (Podsakoff and Organ, 1986). Even if it was tried to minimize these effects with the use of specific measures (see chapter 4.2.6), those problems cannot be precluded at all. Including the above mentioned limitations to the generalizability of the results, external validity as proposed by Bortz and Döring (2006) cannot be guaranteed. One possible option to prove the presented results in real life situations can be the application of different other research methodologies such as scenario analysis or laboratory experiments. For example, Johnston and Warkentin (2010) selected a laboratory experiment to study individual’s security actions towards the mitigation of threats. This would also be applicable in both presented research areas and shows that research studies in both areas are still in its beginnings. These shortcomings lead to the following needs for future research:

- Both research areas need to be enhanced by evaluation of external validity. Due to limited AB measurement in the proposed research studies, practical relevance needs to be proven and checked whether the results lead to the same, in the research studies presented, results.

The last limitation addresses the basic groundwork used in this thesis, especially in the chapters 4.2 and 4.3. Both research areas are shaped by behavioral models which have been applied in different context. However, these behavioral models show an excerpt of the real cognitive processes within an individual. For example, the TPB (chapter 2.1 and 5.1) implies that BI is a proximal cognitive antecedent of actions and behavior (Fishbein and Ajzen, 1975). BI is determined by the interplay of three constructs, ATT, SN and PBC. On the other side, the applied FFM measures individual differences in five dimensions. Critics have challenged both models. The literature analysis presented in section 5.1 showed that the labels of the constructs were not used consistent. To give an example, Bulgurucu et al. (2010) applied the TPB construct SN and called it normative beliefs, but contained the same content. Further in personality research, there is a disagreement about the labels, the number of constructs and the content of the five personality traits (Barrick et al., 2001). Oreg (2003) has demonstrated that other personality traits such as risk aversion, self-esteem or resistance to change highly correlate with the dimensions of the FFM. This is an additional indicator why social science research studies face low explanatory power of their models (see also section 4.3.6). In both research studies (section 4.2 and 4.3), ATT, as an indicator of BI, was applied; the other two TPB constructs were not considered and can lead to misinterpretations. The labels and contents of the FFM were applied by using the 60 item NEO-FFI format by Costa et al. (1991). Thus, the following recommendations are given for future research:

- Future research can apply other personality measures such as the BFI (John, 1990) or the IPIP (Goldberg, 1999) and evaluate the results in comparison with those as indicated in the chapters 4.2 and 4.3. In addition, a comparable behavioral model with other cognitive determinants than the proposed TPB can be applied and taken into relation to personality traits.

References

Abdi, H., and Williams, L.J., “Principal Component Analysis,” *Wiley Interdisciplinary Reviews: Computational Statistics* 2(4), pp. 433 – 459, 2010.

Abdulrazeg, A.A., Norwawi, N., and Basir, N., “Security Measurement Based On GQM to Improve Application Security During Requirements Stage,” *International Journal of Cyber-Security and Digital Forensics* 1(3), pp. 211-220, 2012.

Abraham, S., “Information Security Behavior: Factors and Research Directions,” in: *Proceedings of the American Conference on Information Systems (AMCIS)*, Paper 462, 2011.

Ajzen, I., “Theory of Planned Behavior,” *Organizational Behavior and Human Decision Processes* 50(2), pp. 179-211. 1991.

Albrechtsen, E., and Hovden, J., “Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study,” *Computers and Security* Vol. 29, pp. 432 – 445, 2010.

Allport, G. W., Pattern and growth in personality, Holt, Rinehart and Winston, New York, 1961.

Al-Omari, A., El Gayar, O., and Deokar, A., “Security Policy Compliance: User Acceptance Perspective,” in: *Proceedings of the 45th Hawaii International Conference on System Sciences (HICSS)*, pp. 3317-3316, 2012.

Anaman, M., Lycett, M., and Love, S., “Enhancing Customer Experience within the Mobile Telecommunications Industry,” in: *Proceedings of the European Conference on Information Systems*, Galway (Ireland), Paper 188, 2008.

Anderson, C.L., and Agarwal, R., “Practicing Safe Computing: A multimethod empirical examination of home computer user behavioral intentions,” *MIS Quarterly* 34(3), pp. 613-643. 2010.

Anderson, E.E., and Choobineh, J. “Enterprise Information Security Strategies,” *Computers and Security* 27(1), pp. 22-29, 2008.

Ashenden, D., “Information security management: A human challenge?” *Information Security Technical Report* 13(4), pp. 195-201, 2008.

Aurigemma, A., and Panko, R., “A Composite Framework for Behavioral Compliance with Information Security Policies,” in: *Proceedings of the 45th Hawaii International Conference on System Sciences (HICSS)*, pp. 3248-3257, 2012.

Babbie, E.R., Survey Research Methods, 2nd Edition, Wadsworh Publishing Company, Belmont (USA), 1990.

Backhaus, K., Erichson, B., Plinke, W., and Weiber, R., Multivariate Analysemethoden: eine anwendungsorientierte Einführung, 13. Auflage, Springer Verlag, Berlin, 2011.

Bagozzi, R.P., "Measurement and Meaning in Information Systems and Organizational Research: Methodological and Philosophical Foundations," *MIS Quarterly* 35(2), pp. 261–292, 2011.

Bandura, A., "Self-Efficacy Mechanism in Human Agency," *American Psychologist* 37(2), pp. 122-147, 1982.

Bansal, G., Zahedi, F.M., and Gefen, D., "The Impact of Personal Dispositions on Information Sensitivity, Privacy Concern and Trust in Disclosing Health Information Online," *Decision Support Systems* 49(2), pp. 138–150, 2010.

Bansal, G., "Security concerns in the nomological network of trust and Big5: First Order Vs. Second Order," in: *Proceedings of the 32nd International Conference on Information Systems*, Shanghai (China), Paper 9, 2011.

Barker, V.L., and Mueller, G.C., "CEO characteristics and firm R&D spending," *Management Science* 48(6), pp. 782-802. 2002.

Barrick, M.R., Mount, M.K., and Judge, T.A., "Personality and performance at the beginning of the new millennium: What do we know and where do we go next?" *International Journal of Selection and Assessment* 9(1), pp. 9-29, 2001.

Basili, V., and Weiss, D., "A Methodology for Collecting Valid Software Engineering Data," *Software Engineering* 10(6), pp.728-738, 1984.

Baskerville, R., and Myers, M.D., "Special Issue on Action Research in Information Systems: Making IS Research Relevant to Practice Foreword," *MIS Quarterly* 28(3), pp. 329–335, 2004.

Becker, J., and Pfeiffer, D., „Beziehungen zwischen behavioristischer und konstruktionsorientierter Forschung in der Wirtschaftsinformatik," in: Zelewski, S., and Akca, N., Fortschritt in den Wirtschaftswissenschaften – Wissenschaftstheoretische Grundlagen und exemplarische Anwendungen, Deutscher Universitäts-Verlag, Wiesbaden, pp. 1-17, 2006.

Bedingfield, J.D., and Thal, A.E., "Project manager personality as a factor for success," in: *Proceedings of Portland International Center for Management of Engineering and Technology*, Cape Town (South Africa), pp. 1303-1314, 2008.

Benlian, A., and Hess, T., "Does personality matter in the evaluation of ERP Systems? Findings from a conjoint study," in: *Proceedings of the 18th European Conference on Information Systems*, Pretoria (South Africa), Paper 109, 2010.

Bhadauria, V., "Can Critical Realism „inform" Information Systems?" In: *Proceedings of the 12th Americas Conference on Information Systems,* Acapulco (Mexico), pp. 3622–3628, 2006.

Bortz, J., and Döring, N., Forschungsmethoden und Evaluation für Human- und Sozialwissenschaftler (4th revised ed.). Heidelberg: Springer. 2006.

Broderick, J.S., "ISMS, security standards and security regulations," *Information Security Technical Report II,* pp. 26-31, 2006.

Bulgurcu, B., Cavusoglu, Ha., and Benbasat, I., "Roles of Information Security Awareness and Perceived Fairness in Information Security Policy Compliance," in: *Proceedings of the 15th American Conference on Information Systems (AMCIS),* San Francisco (USA), Paper 419, 2009.

Bulgurcu, B., Cavusoglu, Ha., and Benbasat, I., "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness," *MIS Quarterly* 34(3), pp. 523-548, 2010.

Cattell, R.B., "The Scientific Analysis of Personality," Aldine Publishing Company, Chicago, 1965.

Cavusoglu, Ha., Raghunathan, S., and Cavusoglu, Hu., "Configuration of and Interaction Between Information Security Technologies: The Case of Firewalls and Intrusion Detection Systems," *Information Systems Research* 20(2), pp. 198-217, 2009.

Chang, S.-J., van Witteloostuijn, A., and Eden L., "From the Editors: Common method variance in international business research," *Journal of International Business Studies* Vol. 41, pp. 178-184, 2010.

Chiang, T.J., Kouh, J.S., and Chang, R.-I., "An Ontology-based Approach to the Information Security Management," *International Journal of Computer Science and Network Security* 9(11), pp. 181-189, 2009.

Chin, W.W., "Commentary: Issues and opinion on structural equation modeling," *MIS Quarterly 22(1),* pp. vii-xvi, 1998.

Chin, W.W., Marcolin, B.L., and Newsted, P.R., "A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study," *Information Systems Research* 14(2), pp. 189-217, 2003.

Chittaranjan, G., Blom, J., and Gatica-Perez, D., “Who’s Who with Big Five: Analyzing and Classifying Personality Traits with Smartphones,” In: *Proceedings of the 15th Annual International Symposium on Wearable Computers (ISWC),* Martigny (Switzerland), pp. 29–36, 2011.

Church, R.M., “The effective use of secondary data,” *Learning and Motivation* Vol. 33, pp. 32-45, 2001.

COBIT, Information Systems Audit and Control Association (ISACA), “COBIT 5: A Business Framework for the Governance and Management of Enterprise IT,” 2005.

Conner, M., and Abraham, C., “Conscientiousness and the Theory of Planned Behavior: Toward a more Complete Model of the Antecedents of Intentions and Behavior,” *Personality and Social Psychology Bulletin* 27(11), pp. 1547–1561, 2001.

Cooke, R., and Sheeran, P., “Moderating of Cognition-Intention and Cognition-Behavior Relations: A Meta-Analysis of Properties of Variables from the Theory of Planned Behavior,” *British Journal of Social Psychology* 43(2), pp. 159-186, 2004.

Correa, T., Hinsley, A.W., and Zuniga, H.G., “Who Interacts on the Web?: The Intersection of Users’ Personality and Social Media Use,” *Computers in Human Behavior* 26(2), pp. 247–253, 2010.

Costa, P.T.Jr., and McCrae, R.R., Revised NEO Personality Inventory (NEO-PI-R) and NEO Five Factor Inventory (NEO-FFI) professional manual, Odessa, Fl: Psychological Assessment Resources, 1992.

Costa, P.T.Jr., McCrae, R.R., and Dye, D., “Facet scales for agreeableness and conscientiousness: A revision of the NEO Personality Inventory,” *Personality Individual Differences* (9:12), pp. 887-898, 1991.

Creswell, J.W., Qualitative, quantitative, and mixed methods approaches, 2nd Edition, Sage, Thousand Oaks, 2008.

D’Arcy, J., Hovav, A., and Galletta, D., “User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach,” *Information Systems Research* 20(1), pp. 79-98, 2009.

Da Veiga, A., and Eloff, J. H. P., “An information security governance framework,” *Information Systems Management* 24(4), pp. 361-372, 2007.

Devaraj, S., Easley, R. F., and Crant, J. M., “How does personalty matter? Relating the Five-Factor Model to Technology Acceptance and Use,” *Information Systems Research* 19(1), pp. 93-115. 2008.

Diamantopoulos, A., “Incorporating formative measures into covariance-based structural equation models,” *MIS Quarterly* 35(2), pp. 335-358, 2011.

Diamantopoulos, A., and Winklhofer, H.M., “Index Construction with formative Indicators: An Alternative to Scale Development,” *Journal of Marketing Research* 38(2), pp. 269 – 277, 2001.

Diamantopoulos, A., Riefler, P., and Roth, K.P., “Advancing Formative Measurement Models,” *Journal of Business Research* 61(12), pp. 1203–1218, 2008.

Digman, J.M., “Personality Structure: Emergence of the Five-Factor Model,” *Annual Review of Psychology* Vol. 41, pp. 417–440, 1990.

Dinev, T., Goo, J., Hu, Q., and Nam, K., “User Behavior Toward Protective Technologies - Cultural Differences Between the United States and South Korea,” *Information Systems Journal* 19(4), pp. 391-412, 2009.

Drevin, L., Kruger. H.A., and Steyn, T., “Value-focussed assessment of ICT security awareness in an academic environment,” *Computer and Security* 26(1), pp. 36-43, 2007.

Ebert, C., Dumke, R., Bundschuh, M., and Schmietendorf, A., Best Practices in Software Measurement - How to use metrics to improve project and process performance, Springer, Berlin, 2005.

Eloff, J.H.P., and Eloff, M.M., “Information Security Architecture,” *Computer Fraud and Security* 11(1), pp. 10-16, 2005

Ernst and Young, “Fighting to Close the Gap – Ernst and Young’s 2012 Global Information Security Survey,” Retrieved 03-25-2013 from http://www.ey.com/Publication/vwLUAssets/Fighting_to_close_the_gap:_2012_Global_Information_Security_Survey/$FILE/2012_Global_Information_Security_Survey___Fighting_to_close_the_gap.pdf

Eysenck, H.J. and Wilson, G.D., The Eysenck Personality Profiler. London: Corporate Assessment Network Ltd. 1991.

Farahmand, F., Navathe, S.B., Enslow, P.H., and Sharp, G.P., “Managing Vulnerabilities of Information Systems to Security Incidents,” in: *Proceedings of the 5th International Conference on Electronic Commerce*, Montreal (Canada), pp. 348 – 354, 2003.

Fishbein, M., and Ajzen, I., Belief, attitude, intention and behavior. John Wiley, New York, 1975.

Fornell, C., and Larcker, D., A., “Second Generation of Multivariate Analysis: Classification of Methods and Implications for Marketing Research,” *Review of Marketing* Vol. 51, pp. 407–450, 1987.

Forza, C., “Surveys – Survey research in operations management: A process-based perspective,” *International Journal of Operations and Production Management* 22(2), pp. 152–194, 2002.

Gefen,D., Rigdon, E.E., and Straub, D., “An Update and Extension to SEM Guidelines for Administrative and Social Science Research,” *MIS Quarterly* 35(2), pp. iii–xiv, 2011.

Glasow, P.A., “Fundamentals of Survey Research Methodology,” Retrieved February 02-28-2013 from http://www.mitre.org/work/tech_papers/tech_papers_05/05_0638/05_0638.pdf

Glass, G.V., “Primary, secondary, and meta-analysis of research,” *Educational Researcher* 5(10), pp. 3 – 8, 1976.

Goldberg, L.R., “A broad-bandwith, public-domain, personality inventory measuring the lower-level facets of several Five-Factor models,” in: Mervielde, I., Deary, I.J., de Fruyt, F., and Ostendorf F. (Eds.), Personality psychology in Europe Vol. 7, pp. 7–28, 1999.

Goswami, S., Teo, H.H., and Chan, H.C., “Decision-maker mindfulness in IT adoption: The role of informed culture and individual personality,” in: *Proceedings of the 30th International Conference on Information Systems*, Phoenix (USA), Paper 203, 2009.

Gregory, R.W., “Design Science Research and the Grounded Theory Method: Characteristics, Differences, and Complementary Uses,” in: *Proceedings of the 18th European Conference on Information Systems*, Pretoria (South Africa), Paper 45, 2010.

Greiffenberg, S., “Methoden als Theorien der Wirtschaftsinformatik,” In: Uhr, W., Esswein, W., and Schoop, E. (Editor), Wirtschaftsinformatik 2003 / Band II – Märkte, Medien, Mobilität, Physica Verlag, Heidelberg, pp. 947-968, 2003.

Gupta, E., “Information Systems”, in: Thakur, R.R., Thukral, S., Sahu, N., and Gupta, V. (Editor), Entrepreneurship and SMEs: Building Competencies, Macmillan, New Dehli (India), pp. 97–103, 2011.

Haenlein, M., and Kaplan, A. M., “A Beginner`s Guide to Partial Least Squares Analysis,” *Understanding Statistics* 3(4), pp. 283-297, 2004.

Hair, J.F., Ringle, C.M., and Sarstedt, M., “PLS-SEM: Indeed a Silver Bullet,” *Journal of Marketing Theory and Practice* 19(2), pp. 139–151, 2011.

Hambrick, D.C., and Mason, P.A., “Upper echelons: The organization as a reflection of its top managers,” *Academy of Management Review* 9(2), 193-206. 1984.

Hayden, L., IT Security Metrics - A Practical Framework for Measuring Security and Protecting Data, McGraw-Hill Publ. Comp., 2012.

Hennig-Thurau, T., Gianfranco, W., and Schrader, U., “VHB-Jourqual: Ein Ranking von betriebswirtschaftlich-relevanten Zeitschriften auf der Grundlage von Expertenurteilen,” *Zeitschrift für betriebswirtschaftliche Forschung* Vol. 56, pp. 520–545, 2004.

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

Herath, T., and Rao, H.R., “Protection motivation and deterrence: a framework for security policy compliance in organizations,” *European Journal on Information Systems* 18(2), pp. 106-125, 2009.

Hevner, A., March, S., Park, J., and Ram, S., “Design science in information systems research,” *MIS Quarterly, 28*(1), pp. 75-105, 2004.

Hock C., Hee-Woong K., and Weai C.T., “Information System Citation Patterns from ICIS Articles,” *Journal of the American Society for Information Science and Technology* 57(9), pp. 1263-1274, 2006.

Hoffer, J.A., Straub, D.W., “The 9 to 5 underground: Are you policing computer crimes?” *Sloan Management Review* 30(4), pp. 35–43, 1989.

Hofstede, G., and McCrae, R.R., “Personality and culture revisited: Linking traits and dimensions of culture,” *Cross-Cultural Research* 38(1), pp. 52-88, 2004.

Hough, L. M., “The Big Five personality variables – construct confusion: Description versus prediction,” *Human Performance* 5(1), pp. 139-155, 1992.

Hovav, A., D’Arcy, J., “Applying an Extended Model of Deterrence across Cultures: An Investigation of Information Systems Misuse in the U.S. and South Korea,” *Information and Management* 49(2), pp. 99 – 110, 2012.

Hrastinski, S., Carlsson, S., Henningsson, S., and Keller, C., “On How to Develop Design Theories for IS Use and Management,” in: *Proceedings of the 16th European Conference on Information Systems*, Galway (Ireland), Paper 138.

Hsiu-Fang, H., and Shannon, S.E., “Three Approaches to Qualitative Content Analysis,” *Qualitative Health Research* 15(9), pp. 1277 – 1288, 2005.

Hu, Q., and Dinev, T. “The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies,” *Journal of the Association for Information Systems* 8(7), pp. 386-408, 2007.

Hu, Q., Dinev, T., Hart, P., and Cooke, D., “Top Management Championship and Individual Behavior Towards Information Security: An Integrative Model,” in: *Proceedings of the 16th European Conference on Information Systems*, Galway (Ireland), pp. 1310-1321, 2008.

IBM, “IBM Information Security Framework,” Retrieved 03-08-2013 from http://www-935.ibm.com/services/us/igs/pdf/g510-6454-information-security-framework.pdf

Ifinedo, P., “Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory,” *Computers and Security* 31(1), pp. 83-95, 2012.

Iivari, J., “A paradigmatic analysis of information systems as a design science,” *Scandinavian Journal of Information Systems* 19(2), pp. 39-63, 2007.

ISO/IEC 13335, International Organization for Standardization and International Electrotechnical Commissions, “Information Technology – Security Techniques – Management of Information and Communications Technology Security – Part 1: Concepts and Models for Information and Communications Technology Security Management (ISO/IEC 13335-1:2004),” 2004.

ISO/IEC 27001, International Organization for Standardization and International Electrotechnical Commissions, “ISO/IEC 27001:2005: Information Technology – Security Techniques – Information Security Management Systems – Requirements,” 2005.

Jahng, J.J., Jain, H., and Ramamurthy, K., “Personality Traits and Effectiveness of Presentation of Product Information in E-Business Systems,” *European Journal of Information Systems* 11(3), pp. 181–195, 2002.

Jang, K.L., and Livesley, W.J., “Heritability of the Big Five Personality Dimensions and Their Facets: A Twin Study,” *Journal of Personality* 64(3), pp. 577–592, 1996.

Järvinen, P., “Action Research is Similar to Design Science,” *Quality and Quantity* 41(1), pp. 37-54, 2007.

John, O.P., Donahue, E.M., and Kentle, R.L., The Big Five Inventory—Versions 4a and 54. Berkeley: University of California, Berkeley, Institute of Personality and Social Research. 1991

Johnston, A.C., and Warkentin, M., “Fear appeals and information security behaviors: An empirical study,” *MIS Quarterly* 34(3), pp. 549-566, 2010.

Johnston, A.C., Wech, B., Jack, E., and Beavers, M., “Reigning in the Remote Employee: Applying Social Learning Theory to Explain Information Security Policy Compliance Attitudes,” in: *Proceedings of the 16th American Conference on Information Systems (AMCIS),* Lima (Peru), Paper 493, 2010.

Jöreskog, K.G., and Sörbom, D., “Recent developments in structural equation modeling,” *Journal of Marketing research* 19(4), pp. 404–416, 1982.

Judge, T.A., and Ilies, R., “Relationship of personality to performance motivation: A meta-analytic review,” *Journal of Applied Psychology* 87(4), pp. 797-807, 2002.

Junglas, I.A., Johnson, N.A., and Spitzmüller, C., “Personality Traits and Concern of Privacy: An empirical Study in the Context of Location-Based Services,” *European Journal of Information Systems* 17(4), pp. 387-402, 2008.

Kaiser, H.F., “An Index of Factorial Simplicity,” *Psychometrica* 39(1), pp. 31-36, 1974.

Karahanna, E., and Watson, R. T., “Information systems leadership,” *IEEE Transactions on Engineering Management* 53(2), pp. 171-176, 2006.

Karjalainen, M., and Siponen, M., “Toward a New Meta-Theory for Designing Information Systems (IS) Security Training Approaches,” *Journal of the Association for Information Systems* 12(8), Paper 3, 2011.

Kotulic, A. G., and Clark, J. G., “Why there aren’t more information security research studies,” *Information and Management* 41(5), pp. 597-607, 2004.

KPMG, “The e-Crime Report 2011 – Managing Risk in a Changing Business and Technology Environment,” Retrieved 03-22-2013 from http://www.kpmg.com/CZ/cs/IssuesAndInsights/ArticlesPublications/Press-releases/Documents/KPMG_E-Crime-report-2011.pdf

Krankanhalli, A., Hock-Hai, A., Bernard, C.Y.T., and Kwok-Kee, W., “An integrative study of information systems security effectiveness,” *International Journal of Information Management* 23(2), pp. 139-154. 2003

Krippendorf, K., Content Analysis: An Introduction to its Methodology, Sage Publications, Thousand Oak, California (USA), 2004.

Krishnan, S., Lim, V.K.G., and Teo, T.S.H., “How does personality matter? Investigating the impact of Big-Five personality traits on cyberloafing,” in: *Proceedings of the 31st International Conference on Information Systems*, Saint Louis (USA), Paper 6, 2010.

Kritzinger, E., and Smith, E., “Information security management: An information security retrieval and awareness model for industry,” *Computer and Security, 27*(5-6), pp. 224-231, 2008.

Kruger, H.A., and Kearney, W.D., “A prototype for assessing information security awareness,” *Computers and Security* 25(4), Pages 289-296, 2006.

Kukafka, R., Johnson, S.B., Linfante, A., and Allegrantec, J.P., “Grounding a new information technology implementation framework in behavioral science: a systematic analysis of the literature on IT use,” *Journal of Biomedical Informatics* Vol. 36, pp. 218–227, 2003.

Landers, R.N., and Lounsbury, J.W., “An Investigation of Big Five and Narrow Personality Traits in Relation to Internet Usage,” *Computers in Human Behavior* 22(2), pp. 283–293, 2006.

Lauriola, M., and Levin, I. P., “Personality traits and risky decision-making in a controlled experimental task: An exploratory study,” *Personality and Individual Differences* 31(2), pp. 215-226, 2001.

Lechtchinskaia, L., Uffen, J., and Breitner, M.H., “Critical Success Factors for Adoption of Integrated Information Systems in Heigher Education Institutions – A Meta-Analysis,” in: *Proceedings of the 17th Americas Conference on Information Systems*, Detroit (USA), Paper 53, 2011.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., and Breitner, M.H., “Employees' Information Security Awareness and Behavior: A Literature Review,” in: *Proceedings of the 46th Hawaii International Conference on System Science*, Maui (USA), pp. 2978 – 2987, 2013a.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., and Breitner, M.H., “Information Security Awareness and Behavior: A Theory-based Literature Review,” Will appear in: *Management Research Review* 37(11), 2014.

Lebek, B., Uffen, J., Neumann, M., and Hohler, B., “Towards a Needs Assessment Process Model for Security, Education, Training and Awareness Programs - An Action Design Research Study,” in: *Proceedings of the 21st European Conference on Information Systems*, Utrecht (Netherlands), Paper 110, 2013c.

Lee, A.S., “Action is an Artifact: What Action Research and Design Science Offer to Each Other,” in: Kock, N. (ed.), Information Systems Action Research: An Applied View of Emerging Concepts and Methods, Springer, New York (USA), pp. 43–60, 2007.

Lee, A.S. and Hubona, G.S., “A Scientific Basis for Rigor in Information Systems Research,” *MIS Quarterly* 33(2), pp. 221–243, 2009.

Lee, A.S., “Systems Thinking, Design Science, and Paradigms. Heeding three Lessons from the Past to Resolve Three Dilemmas in the Present to Direct a Trajectory for Future Research in the Information Systems Field,” in: *Proceedings of the 11th International Conference on Information Management*, Kaohsiung (Taiwan), Keynote speech, 2000.

Lee, A.S., and Baskerville, R.L., “Generalizing Generalizability in Information Systems Research,” *Information Systems Research* 14(3), pp. 221–243. 2003.

Lee, Y., and Larsen, K. R., “Threat or coping appraisal: determinants of SMB executives’ decision to adopt anti-malware software,” *European Journal of Information Systems* 18(2), pp. 177-187, 2009.

Li, Y., Tan, C.-H., Teo, H.-H., and Tan, C.Y., “Innovative Usage of Information Technology in Singapore Organizations: Do CIO characteristics make a difference?” *IEEE Transactions on Engineering Management* 53(2), pp. 177-190. 2006.

Likert, R., “A technique for the measurement of attitudes,” *Archives of Psychology* 22(140), pp. 1 – 55, 1932.

Limayem, M., and Hirt, S.G., “Force of Habit and Information Systems Usage: Theory and Initial Validation,” *Journal of Association for Information Systems* Vol. 4, pp. 65-97, 2003.

Lin, M.Y.-C., and Ong, C.-S., “Understanding Information Systems Continuance Intention: A Five-Factor Model of Personality Perspective,” in: *Proceedings of the 14th Pacific Asia Conference on Information Systems*, Taipei (Taiwan), pp. 367–376, 2010.

Ma, Q., and Pearson. J.M., “ISO 17799: Best practices in information security management?” *Communications of the Association for Information Systems* 15(1), pp. 577-591, 2005.

MacCallum, C., and Browne, M.W., “The Use of Causal Indicators in Covariance Structure Models: Some Practical Issues,” *Psychological Bulletin* 114(3), pp. 533–541, 1993.

MacKenzie, S.B., Podsakoff, P.M., and Podsackoff, N.P., “Construct Measurement and Validation Procedures in MIS and Behavioral Research: Integrating new and Existing Techniques,” *MIS Quarterly* 35(2), pp. 293–334, 2011.

Maier, C., Laumer, S., Eckhardt, A., and Weitzel, T., “Using User Personality to Explain the Intention-Behavior Gap and Changes in Beliefs: A Longitudinal Analysis,” in: *Proceedings of the International Conference on Information Systems*, Orlando (USA), Paper 14, 2012.

March, S.T., and Smith, G., “Design and Natural Science Research on Information Technology,” *Desicion Support Systems* 15(4), 251-266, 1995.

May, J., and Dhillon, G., “A holistic approach for enriching information security analysis and security policy formation,” in: *Proceedings of the 18th European Conference on Information Systems,* Pretoria (South Africa), Paper 146, 2010

Mayring, P., “Qualitative Content Analysis,” *Qualitative Social Research* 1(2), pp. 1–10, 2000.

Mayring, P., Qualitative Inhaltsanalyse – Grundlagen und Techniken, Beltz Verlag, Weinheim (Germany), 2008.

McCrae, R. R., and Costa, P., “A five factor theory of personality,” in: L. A. Lawrence and O. P. John (eds.), Handbook of personality – Theory and research, New York: Guilford Press, pp. 139-153, 1999.

McCrae, R. R., and John, O. P., “An introduction to the Five-Factor Model and its applications,” *Journal of Personality* 60(2), pp. 175-215, 1992.

McElroy, J. C., Hendrickson, A. R., Townsend, A. M., and DeMarie, S. M., “Dispositional factors in internet use: Personality versus cognitive styles,” *MIS Quarterly* 31(4), pp. 809-820, 2007.

McFadzean, E., Ezingeard, J.-N., and Birchall, D. W., “Perception of risk and the strategic impact of existing IT on information security strategy at board level,” *Online Information Review* 31(5), pp. 622-660, 2007.

McKay, J., and Marshall, P., “Science, Design, and Design Science: Seeking Clarity to Move Design Science Research Forward in Information Systems,” in: *Proceedings of the 18th Australasian Conference on Information Systems*, Toowoomba (Australia), pp. 604-614, 2007.

Mertens, P., “Gefahren für die Wirtschaftsinformatik – Risikoanalyse eines Faches, Erweiterte Fassung des gleichnamigen Vortrags auf der Tagung Wirtschaftsinformatik 2005 in Bamberg,“ *Arbeitspapier Nr. 1/2005, Bereich Wirtschaftsinformatik I,* Universität Erlangen-Nürnberg, Nürnberg, 2005.

Miller, K., Communications Theories: Perspectives, Processes, and Contexts, McGraw Hill, Boston et al., 2005.

Mishra, S., and Dhillon, G., “Information systems security governance research: A behavioral perspective,” *Proceedings of the 1st Annual Symposium on Information Assurance, Academic Track of 9th Annual NYS Cyber Security Conference,* pp. 18-26, 2005.

Morgan, G., and Harmon, R., “Data Collection Techniques,” *Journal of the American Academy of Child and Adolescent Psychiatry* 40(8), pp. 973–977, 2001.

Mount, M. K., Barrick, M. R., and Stewart, G. L., “Five-Factor model of personality and performance in jobs involving interpersonal interactions,” *Human Performance* 11(2-3), pp. 145-165, 1998.

Myers, M.D., “Qualitative Research in Information Systems,” *MIS Quarterly* 21(2), pp. 241–242, 1997.

Neuendorf, K.A., “The content analysis guidebook,” Sage Publications, Thousand Oak, London (GB), 2002.

Neumann, M., Plückebaum, A., Uffen, J., and Breitner, M.H., Aspekte der Wirtschaftsinformatikforschung 2009, *IWI Discussion Paper* Vol. 40, Institut für Wirtschaftsinformatik, Leibniz Universität Hannover, 2010.

Niehaves, B., “On Epistemological Diversity in Design Science – New Vistas for a Design-Oriented IS Research?” in: *Proceedings of the 28th International Conference on Information Systems*, Montreal, pp. 1-13, 2007.

NIST SP-800-39, National Institute of Standards and Technology, “Managing Information Security Risks – Organization, Mission, and Information System View,” 2011.

NIST SP-800-50, National Institute of Standards and Technology, “Building an Information Technology Security Awareness and Training Program,” 2003.

Nov, O., and Ye, C., “Personality and Technology Acceptance: Personal innovativeness in IT, openness and resistance to change,” in: *Proceedings of the 41st Hawaii International Conference on System Science*, Big Island (USA), Paper 448, 2008.

Österle, H., Becker, J., Frank, U., Hess, T., Karagiannis, D., Krcmar, H., Loos, P., Mertens, P., Oberweis, A., and Sinz, E.J., “Memorandum on design-oriented information systems research,” *European Journal on Information Systems* Vol. 20, pp. 1-4, 2010.

Pahnila, S., Siponen, M.T., and Mahmood, A., “Employees' Behavior towards IS Security Policy Compliance,” *Proceedings of the 40th Hawaii International Conference on System Sciences (HICSS),* pp. 156–165, 2007.

Pahnila, S., Siponen, M.T., and Mahmood, A., “Which Factors Explain Employees’ Adherence to Information Security Policies? An Empirical Study,” in: *Proceedings of the Pacific Asia Conference on Information Systems (PACIS)*, Paper 73, 2007.

Palvia, P., Mao, E., Midha, V., Pinkani, P., and Salam, A.F., “Research Methodologies in MIS: An Update,” *Communications of the Association for Information Systems* Vol. 14, pp. 526–542, 2004.

Park, S., Ahmad, A, and Ruighaver, A.B., “Factors Influencing the Implementation of Information Systems Security Strategies in Organizations,” in: *Proceedings of the International Conference on Information Science and Applications (ICISA)*. Seoul (Korea), pp. 1–6, 2010.

Petter, S., Straub, D., and Rai, A., “Specifying formative constructs in information systems research,” *MIS Quarterly* 31(4), pp. 623–656, 2007.

Pierce, E. A., and Hansen, S. W., “Leadership, Trust, and Effectiveness in Virtual Teams,” in: *Proceedings of the 29th International Conference on Information Systems*, Paris (France), Paper 43, 2008.

Pinsonneault, A., and Kraemer, K.L., “Survey research methodology in management information systems: An assessment,” *Journal of Management Information Systems* 10(2), pp. 75–106, 1993.

Podsackoff, P.M., MacKenzie, S.B., Podsackoff, N.P., and Lee, J.Y., “The Mismeasure of Management and its Implications for Leadership Research,” *Leadership Quarterly* 14(2), pp. 614–656, 2003.

Podsakoff, N.P., Shen, W., and Podsakoff, P.M., “The Role of Formative Measurement Models in Strategic Management Research: Review, Critique, and Implications for Future Research,” *Research Methodology in Strategy and Management* Vol. 3, pp. 197–252, 2006.

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

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

Pomes, R., Informationssicherheit und Persönlichkeit: Konzept, Empirie und Handlungsempfehlungen, Grin-Verlag, München (Germany), 2011.

Reinartz, W.J., Haenlein, M., and Henseler, J., “An Empirical Comparison of the Efficacy of Covariance-based and Variance-based SEM,” *Faculty and Research – Working Paper* 44, pp. 1 – 49, 2009.

Rhodes, R.E., Courneya, K.S., and Jones, L.W., "Personality, the Theory of Planned Behavior, and Exercise: A Unique Role for Extroversion's Activity Facet," *Journal of Applied Social Psychology* 32(8), pp. 1721–1736, 2002.

Richardson, R., "CSI Computer Crime and Security Survey," Retrieved 03-25-2013 from https://www.hlncc.com/docs/CSIsurvey2008.pdf

Rogers, R.W., "Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation Theory," in: Cacioppo, J., and Petty, R. (Eds.): Social Psychophysiology, Guilford, New York, 1983.

Rosemann, M., and Vessey, I., "Toward Improving the Relevance of Information Systems Research to Practice: The Role of Applicability Checks," *MIS Quarterly* 32(1), pp. 1–22, 2008.

Saaty, T.L., Multicriteria Decision Making: The Analytic Hierarchy Process, McGraw-Hill. 1980.

Saleh, M.S., Alrabiah, A., and Bakry, S.H., "Using ISO 17799:2005 information security management: a STOPE view with six sigma approach," *International Journal of Network Management* Vol. 17, pp. 85-97, 2006.

Sein, M.K., Henfridsson, O., Purao, S., Rossi, M., and Lindgren, R., "Action Design Research," *MIS Quarterly* 35(1), pp. 37–56, 2011.

Seuring, S., and Gold, S., "Conducting content-analysis based literature reviews in supply chain management," *Supply Chain Management: An International Journal* 17(5), pp. 544–555, 2011.

Sharma, R., and Yetton, P., "The contingent effects of management support and task interdependence on successful information systems implementation," *MIS Quarterly* 27(4), pp. 553-556, 2003.

Sheppard, B.H., Hartwick, J., and Warshaw, P.R., "The Theory of Reasoned Action: A Meta-Analysis of Past Research with Recommendations for Modifications and Future Research," *Journal of Consumer Research* 15(3), pp. 325-343, 1988.

Shropshire, J., Warkentin, M., Johnston, A. C., and Schmidt, M. B., "Personality and IT security: An application of the five-factor model," in: *Proceedings of the 12th Americas Conference on Information Systems*, Acapulco (Mexico), pp. 3443-3449, 2006.

Silver, M.S., Markus, M.L., and Beath, C.M., "The Information Technology Interaction Model: A Foundation for the MBA Core Course," MIS Quarterly 19(3), pp. 361–390, 1995.

Siponen, M., and Willison, R., "Information security management standards: Problems and solutions," *Information and Management* 46(5), pp. 267-270, 2009.

Siponen, M., and Oinas-Kukkonen, H., "A Review of Information Security Issues and Respective Research Contributions," *The Database for Advances in Information Systems* 38(1), pp. 60–81, 2007.

Siponen, M., Pahnila, S., and Mahmood, M. A. "Compliance with Information Security Policies: An Empirical Investigation," *Computer* 43(2), pp. 64-71, 2010.

Siponen, M.T., "Critical analysis of different approaches to minimizing user-related faults in information systems security: implications for research and practice," *Information Management and Computer Security* Vol. 8, pp. 197-209, 2000.

Siponen, M.T., and Osborn Vance, A. "Neutralization: New Insights into the Problem of Employee Systems Security Policy Violations," *MIS Quarterly* 34(3), pp. 487-502, 2010.

Siponen, M.T., Pahnila, S., and Mahmood, A., "Employees' Adherence to Information Security Policies: An Empirical Study," *IFIP Advances in Information and Communication Technology* Vol. 232, pp. 133–144, 2007.

Sivo, S., Saunders, S., Chang, Q., and Jiang, J.J., "How low should you go? Low response rates and the validity of inference in IS questionnaire research," *Journal of the Association for Information Systems* 7(6), pp. 351-414, 2004.

Spears, J.L., and Barki, H., "User Participation in Information Systems Security Risk Management", *MIS Quarterly* 34(3), pp. 503-522, 2010.

Straub, D. W., and Welke, R. J., "Coping with systems risk: security planning models for management decision making," *MIS Quarterly* 22(4), pp. 441-469, 1998.

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

Suhr, D., "Principal Component Analysis vs. Exploratory Factor Analysis," in: *Proceedings of the 30th Annual SAS Users Group International Conference,* Philadelphia (USA), Paper 203-30, 2005.

Susman, G., "Action Research: A sociotechnical perspective," in: Morgan, G. (ed.), Beyond Method: Strategies for Social Research, Sage Publications, Newbury Park (CA), pp. 95–113, 1983.

Svendsen, G., Johnsen, J.-A. K., Almas-Sorensen, L., and Vitterso, J., "Personality and Technology Acceptance: The Influence of Personality Factors on the Core Constructs of the Technology Acceptance Model," *Behaviour & Information Technology* 32(4), pp. 323–334, 2013.

Tashi, I., and Ghernouti-Hélie, S., "Information Security Management is not only Risk Management," in: *Proceedings of the 4th International Conference on Internet Monitoring and Protection (ICIMP),* Venice (Italy), pp. 116 – 123, 2009.

Taylor, R., "Management perception of unintentional information security risks," in: *Proceedings of the 27th International Conference on Information Systems*, Milwaukee (USA), pp. 1581-1597, 2006.

Tett, R.P. and Burnett, D.D., "A personality trait-based interactionist model of job performance," *Journal of Applied Psychology* 88(3), pp. 500-517. 2003.

Torres, J.M., Sarriegi, J.M., and Santos, N.S., "Managing Information Systems Security: Critical Success Factors and Indicators to Measure Effectiveness," in: *Proceedings of the 9th International Conference on Information Security*, Samos Island (Greece), pp. 530–545, 2006.

Trček, D., "An Integral Framework for Information Systems Security Management," *Computers and Security* 22(4), pp. 337-360, 2003.

Tudor, J.K., Information Security Architecture – An integrated approach to security in an organization, Auerbach Publications, Boca-Raton (FL), 2000.

Uffen, J., Pomes, R., and Breitner, M.H., "Towards a Sustainable and Efficient Component-Based Information Security Framework," in: *Proceedings of the Multikonferenz Wirtschaftsinformatik 2012*, Braunschweig (Germany), pp. 959 – 970, 2012a.

Uffen, J., Guhr, N., and Breitner, M.H., "Personality Traits and Information Security Management: An Empirical Study of Information Security Executives," in: *Proceedings of the International Conference on Information Systems*, Orlando (USA), 2012b.

Uffen, J., and Breitner, M.H., "Management of Technical Security Measures: An Empirical Examination of Personality Traits and Behavioral Intentions," in: *Proceedings of the 46th Hawaii International Conference on Systems Science*, Maui (USA), pp. 4551 – 4560, 2013a.

Uffen, J., and Breitner, M.H., "Management of Technical Security Measures: An Empirical Examination of Personality Traits and Behavioral Intentions," *International Journal of International Journal of Social and Organizational Dynamics in IT* (IJSODIT), pp. 14-31, 2013b.

Uffen, J., Kaemmerer, N., and Breitner, M.H., "Personality Traits and Cognitive Determinants - An Empirical Investigation of the Use of Smartphone Security Measures," *Journal of Information Security* 4(4), pp. 203-212, 2013c.

Vance, A., Siponen, M., and Pahnila, S., “How Personality and Habit Affect Protection Motivation,” in: *Pre-ICIS Workshop on Information Security and Privacy* (WISP), pp. 14–21, 2009.

Verizon, “2011 Data Breach Investigations Report,” Retrieved 01-16-2013 from http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

Venkatesh, V., Morris, M.G., Davis, G.B., and Davis, F.D., “User Acceptance of Information Technology: Toward a Unified View,” *MIS Quarterly* 27(3), pp. 425-478, 2003.

VHB-JOURQUAL2.1, *VHB-JOURQUAL 2.1 Ranking von betriebswirtschaftlich relevanten Zeitschriften auf der Grundlage von Urteilen der VHB-Mitglieder*, Retrieved 02-04-2013, from http://vhbonline.org/service/jourqual/vhb-jourqual-21-2011/

vom Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R., and Cleven, A., “Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process,“ *Proceedings of the European Conference on Information Systems (ECIS)*, pp. 2206–2217, 2009.

Vroom, C., and von Volms, R., “Towards information security behavioural compliance,” *Computers and Security* 23(3), pp. 191-198, 2004.

Wacker, J. G., “A definition of theory: research guidlines for different theory building research methods in operations management,” *Journal of Operations Management* 16(4), pp. 361-385, 1998.

Walstrom, K.A., and Hardgrave, B.V., “Forums for Information Systems Scholars: III,” *Information and Management* Vol.39, pp. 117-124, 2001.

Warkentin, M., Johnston, A.C., and Shropshire, J., “The influence of the informal social learning environment on information privacy policy compliance efficacy and intention,” *European Journal on Information Systems (EJIS)* 20(3), pp. 267-284, 2011.

Webb, T.L., and Sheeran, P., “Does Changing Behavioral Intentions Engender Behavior Change? A Meta-Analysis of the Experimental Evidence,” *Psychological Bulletin* 132(2), pp. 249–268, 2006.

Webster, J. Watson, R.T., “Analyzing the Past to Prepare for the Future: Writing a Literature Review,” *MIS Quarterly* Vol. 26, pp. xiii-xxiii, 2002.

Weiber, R., and Mühlhaus, D., Strukturgleichungsmodellierung – Eine anwendungsorientierte Einführung in die Kausalanalyse mit Hilfe von AMOS, SmartPLS und SPSS. Heidelberg et al., Springer, 2010.

Werlinger, R., Hawkey, K., and Beznosov, K., "An integrated view of human, organizational, and technological challenges of IT security management," *Information Management and Computer Security* 17(1), pp. 4-19, 2008.

Werlinger, R., Hawkey, K., and Beznosov, K., "An integrated view of human, organizational, and technological challenge of IT security management," *Information Management and Computer Security* 17(1), pp. 4-19, 2009.

Whitman, M. E., "Enemy at the gate: Threats to information security," *Communications of the ACM* 46(8), pp. 91–95, 2003.

Wilde, T., and Hess, T., "Forschungsmethoden der Wirtschaftsinformatik – Eine empirische Untersuchung," *Wirtschaftsinformatik* Vol. 49, pp. 280-287, 2007.

Willcocks, L., Whitley, E.A., and Avgerou, C., "The Ranking of Top IS Journals: A Perspective from the London School of Economics", *European Journal of Information Systems (EJIS)*, Vol. 17, pp. 163-168, 2008.

WKWI - Wissenschaftliche Kommission Wirtschaftsinformatik im Verband der Hochschullehrer für Betriebswirtschaft e.V., G.-F.-W. -F., WI-Mitteilung der WKWI und des GI-FB-WI. WI Orientierungslisten. *Wirtschaftsinformatik* 50(2), pp. 155-163, 2008.

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

Xue, Y., Liang, H., and Wu, L., "Punishment, Justice, and Compliance in Mandatory IT Settings," *Information Systems Research* 22(2), pp. 400-414, 2011.

Yildrim, E.Y., Akalp, G., Aytac, S., and Bayram, N., "Factors Influencing Information Security Management in small- and medium-sized enterprises: A case study from Turkey," *International Journal of Information Management* 31(4), pp. 360-365, 2011.

Zafar, H., and Clark, J.G., "Current State of Information Security Research in IS," *Communications of the Association for Information Systems* 24(1), pp. 572–596, 2009.

Zhang, J., Reithel, B., Brian, J., and Li, H., "Impact of perceived technical protection on security behaviors," *Information Management and Computer Security* 17(4), pp. 330-340, 2009.

Zhao, X., Xue, L., and Whinston, A. B., "Managing interdependent information security risks: A study of cyberinsurance, managed security service and risk pooling," in: *Proceedings of the 30th International Conference on Information Systems*, Phoenix (USA), Paper 49, 2009.

Zou, H., Hastie, T., and Tibshirani, R., “Sparse Principal Component Analysis,” *Journal of Computational and Graphical Statistics* 15(2), pp. 265 – 286, 2006.

Appendices

APPENDIX 14 (A14): 20 JAHRE INTERNATIONALE TAGUNG WIRTSCHAFTSINFORMATIK: PROFIL EINER KONFERENZ **159**

Appendix 1 (A1)

Authors: Markus Neumann, Achim Plückebaum, Jörg Uffen, Michael H. Breitner

Title: Aspekte der Wirtschaftsinformatik 2009

In: IWI-Discussion Paper #40, Institut für Wirtschaftsinformatik, Leibniz Universität Hannover.

Abstract

Die folgende Arbeit ist von Doktoranden der Wirtschaftsinformatik im Rahmen des Promotionskurses„Wissenschaftstheorie“ im Sommersemester 2009 erstellt worden. In einemPromotionsstudium an einer Universität (lat. universitas = Gesamtheit (der Lehrenden undLernenden), älteste und traditionell ranghöchste Form einer Hochschule (Brockhaus, 2001))wird von Doktoranden erwartet, dass sie lernen, selbständig wissenschaftlich zu arbeiten.

Der Begriff Wissenschaft kommt von „Wissen schaffen“: es geht also um den Begriff „Wissen“und den Prozess des „Wissenschaffens“ (Erwerb, Kategorisierung, Speicherung usw.).Das Berufsbild des Wissenschaftlers von den Anfängen bis heute und die historische Entwicklungder einzelnen Wissenschaftsdisziplinen werden im Rahmen der Wissenschaftsgeschichtebehandelt. In der hier primär adressierten Wissenschaftstheorie (= Methodologie), die oft alswichtiges Teilgebiet der modernen, theoretischen Philosophie gesehen wird, stehen dann dieMethoden der Bildung, Bewährung und Anwendung wissenschaftlicher Theorien und Begriff sowie die Voraussetzungen, Strukturen, Ziele und Auswirkungen von Wissenschaft im Mittelpunkt.Einerseits steht die Ökonomie (= Wirtschaftswissenschaften, griech. oikos = „Haus“plus nomos = „Gesetz bzw. Herrschaft“) im Mittelpunkt, d. h. u. a. deren Abgrenzung zuanderen Wissenschaftsdisziplinen und deren typische Methoden, Prinzipien, Theorien undBegriffen. Die Wirtschaftsinformatik wiederum basiert auf der Betriebswirtschaftslehre alsTeilgebiet der Ökonomie sowie der praktischen und angewandten Informatik (= Informationplus Automatik oder Mathematik), zum kleineren Teil aber auch auf anderen Wissenschaftsdisziplinenwie z.B. der Mathematik. Die nachfolgende Hausarbeit „Referenzmodelle vs. Vorgehensmodelle: Wissenschaftstheoretische Grundlagen und Ableitung eines Kriterienkataloges“ von Diplom-Wirtschaftsinformatiker Markus Neumann, Diplom-Kaufmann Achim Plückebaum und Diplom-Ökonom Jörg Uffen verfolgt deshalb interdisziplinäre Forschungsansätze: eine typische Stärke – manchmal leider auch Schwäche – der modernen Wirtschaftsinformatik.

Appendix 2 (A2)

Title: Critical Success Factors for Adoption of Integrated Information Systems in Higher Education Institutions – A Meta Analysis

Authors: Lubov Lechtchinskaia, Jörg Uffen, Michael H. Breitner

In: Proceedings of the 17th Americas Conference on Information Systems, Detroit, USA, Paper 53, 2011.

Link: http://aisel.aisnet.org/amcis2011_submissions/53/

Abstract

Integrated information systems continuously develop into a strategic instrument for higher education institutions. In contrast to private companies, specific characteristics of higher education institutions in regards to their organizational structure as well as their management and operations require a tailored project management approach. There is need for thorough research and practical recommendations for implementation of integrated information systems in higher education institutions. This paper provides a systematic meta-analysis and a state of the art overview of critical success factors for selection and implementation of integrated information systems based on the characteristic of the higher education sector. A qualitative content analysis is applied to receive a comprehensive list of critical success factors for higher education institutions. The mostly named critical success factors are stakeholder participation, business process reengineering and communication which align well with the peculiarities of the higher education sector.

Appendix 3 (A3)

Title: Towards a Sustainable and Efficient Component-Based Information Security Framework

Authors: Jörg Uffen, Robert Pomes, Michael H. Breitner

In: Proceedings of the Multikonferenz Wirtschaftsinformatik 2012, Braunschweig (Germany), pp. 959 – 970, 2012.

Abstract

Information security and information systems (IS) security both have top management priority in many companies and organizations. In various information security models researchers recommend several important components to sustainably and efficiently enforce information security. There is little research aiming at approaches that combine theoretically and empirically substantiated principles. To fill this research gap, the aim of this paper is to discuss the adequacy of "academic" information security components, to analyze practical relevance using an empirical study and to consolidate identified factors using a principle component analysis to enhance applicability. Findings suggest two main factors which are identified as short-term and long-term as well as 18 sub-components. The results can assist companies and organizations in sustainably and efficiently implementing information security.

Appendix 4 (A4)

Title: Personality Traits and Information Security Management: An Empirical Study of Information Security Executives

Authors: Jörg Uffen, Nadine Guhr, Michael H. Breitner

In: Proceedings of the International Conference on Information Systems, Orlando (USA), 2012.

Link: http://aisel.aisnet.org/icis2012/proceedings/ISSecurity/5/

Abstract

Executives' behavior causes potential information security management risks and has a direct influence on the security level of information systems and management. This behavior depends on personality traits and other cognitive factors. First, a comprehensive literature review and a status quo analysis are presented. We consider the constructs of the Five Factor Model (FFM) as influence factors for attitudes towards technical and non-technical dimensions of information security management. Then, the hypothesized relationships are validated using empirical data from 174 information security executives. The results suggest that multiple facets of an information security executive's personality have a significant effect on his or her attitude towards selected information security management activities. For example, conscientiousness is positively related to a person's attitude towards the technical and organizational activities of information security. From these findings, theoretical and practical implications and recommendations are discussed.

Appendix 5 (A5)

Title: Management of Technical Security Measures: An Empirical Examination of Personality Traits and Behavioral Intentions

Authors: Jörg Uffen, Michael H. Breitner

In: Proceedings of the 46th Hawaii International Conference on Systems Science, Maui (USA), pp. 4551 – 4560, 2013.

Abstract

Organizations are investing substantial resources in technical security measures that aim at preventively protecting their information assets. The way management – or information security executives – deals with potential security measures varies individually and depends on personality traits and cognitive factors. Based on the Theory of Planned Behavior, we examine the relationship between the personality traits of conscientiousness, neuroticism and openness with attitudes and intentions towards managing technical security measures. The highly relevant moderating role of compliance factors is also investigated. The hypothesized relationships are analyzed and validated using empirical data from a survey of 174 information security executives. Findings suggest that conscientiousness is important in determining the attitude towards the management of technical security measures. In addition, the findings indicate that when executives are confronted with information security standards or guidelines, the personality traits of conscientiousness and openness will have a stronger effect on attitude towards managing security measures than without moderators.

Appendix 6 (A6)

Title: Management of Technical Security Measures: An Empirical Examination of Personality Traits and Behavioral Intentions

Authors: Jörg Uffen, Michael H. Breitner

In: International Journal of Social and Organizational Dynamics in IT, 3(1), pp. 14-31, 2013.

Abstract

Organizations are investing substantial resources in technical security measures that aim at preventively protecting their information assets. The way management – or information security executives – deals with potential security measures varies individually and depends on personality traits and cognitive factors. Based on the Theory of Planned Behavior, we examine the relationship between the personality traits of conscientiousness, neuroticism and openness with attitudes and intentions towards managing technical security measures. The highly relevant moderating role of compliance factors is also investigated. The hypothesized relationships are analyzed and validated using empirical data from a survey of 174 information security executives. Findings suggest that conscientiousness is important in determining the attitude towards the management of technical security measures. In addition, the findings indicate that when executives are confronted with information security standards or guidelines, the personality traits of conscientiousness and openness will have a stronger effect on attitude towards managing security measures than without moderators.

Appendix 7 (A7)

Title: Employees' Information Security Awareness and Behavior: A Literature Review

Authors: Benedikt Lebek, Jörg Uffen, Markus Neumann, Bernd Hohler, Michael H. Breitner

In: Proceedings of the 46th Hawaii International Conference on System Science, Maui (USA), pp. 2978 – 2987, 2013.

Abstract

Today’s organizations are highly dependent on information management and processes. Information security is one of the top issues for researchers and practitioners. In literature, there is consent that employees are the weakest link in IS security. A variety of researchers discuss explanations for employees’ security related awareness and behavior. This paper presents a theory-based literature review of the extant approaches used within employees’ information security awareness and behavior research over the past decade. In total, 113 publications were identified and analyzed. The information security research community covers 54 different theories. Focusing on the four main behavioral theories, a state-of-the-art overview of employees’ security awareness and behavior research over the past decade is given. From there, gaps in existing research are uncovered and implications and recommendations for future research are discussed. The literature review might also be useful for practitioners that need information about behavioral factors that are critical to the success of an organization’s security awareness.

Appendix 8 (A8)

Title: Information Security Awareness and Behavior: A Theory-based Literature Review

Authors: Benedikt Lebek, Jörg Uffen, Markus Neumann, Bernd Hohler, Michael H. Breitner

Will appear in: Management Research Review 37(11), 2014.

Abstract

Today’s organizations are highly dependent on information management and processes. Information security is one of the top issues for researchers and practitioners. In literature, there is consent that employees are the weakest link in IS security. A variety of researchers discuss explanations for employees’ security related awareness and behavior. This paper presents a theory-based literature review of the extant approaches used within employees’ information security awareness and behavior research over the past decade. In total, 144 publications were identified and analyzed. The information security research community covers 54 different theories. Focusing on the four main behavioral theories, a state-of-the-art overview of employees’ security awareness and behavior research over the past decade is given. From there, gaps in existing research are uncovered and implications and recommendations for future research are discussed. The literature review might also be useful for practitioners that need information about behavioral factors that are critical to the success of an organization’s security awareness.

Information Security Awareness and Behavior: A Theory-based Literature Review

1. Introduction

Today's organizations are highly dependent on information systems (IS). Consequently, they implement technical measures to mitigate threats to information security (Aurigemma and Panko, 2012). To achieve IS security, the literature proposes information security policies (Bulgurcu et al., 2010; Pahnila, 2007) and Security Education, Training and Awareness (SETA) programs (Abraham, 2011; D'Arcy and Hovav, 2009) as non-technical measures for preventing security breaches by employees. Since literature refers to employees as the weakest link in IS security (Spears and Barki, 2010; Siponen, 2006), employees' information security awareness and behavior has garnered increasing academic attention over the past decade. In this interdisciplinary research domain, theories from social psychology and criminology were adopted to IS literature (Mishra and Dhillon, 2005) in order to explain and predict employees' security-related behavior and awareness. Despite the huge amount of studies conducted within this context, there is still no up-to-date overview of used theories and main results.

Therefore, in this paper we present the results of a comprehensive literature review that was designed to identify applied theories and understand the cognitive determinants in the research field of employees' information security awareness and behavior within the past decade. A prior literature analysis was conducted by Siponen (2000). The authors analyzed different approaches to minimizing user-related faults in information security. Although the underlying theories were identified, the focus of the study was approach-related. An up-to-date overview of applied theories is necessary to guide further research, since the previous study was published twelve years ago. Another literature analysis by Abraham (2011) focused on factors that influence security behavior (i.e., policies, communication practices, peer influences, etc.) and not on theories. In addition, several target-oriented literature reviews were conducted. 'Target oriented' means that the literature review was conducted to provide the theoretical basis for further research within the same article (e.g., model construction) and is not the essential part of the article. For instance, Mishra and Dhillon (2005) gave a short overview of behavioral theories in IS security literature in order to introduce the theory of anomie to the research field. Another paper by Aurigemma and Panko (2012) surveyed behavioral theories to present an information security policy (ISP) behavioral compliance framework.

The aim of this paper is to provide an up-to-date overview of applied theories by discussing the following research question:

Q: Which theories have recently been used in IS literature to explain employees' security related awareness and behavior?

To answer this question, in the following sections, we present findings from a systematic literature review of a total of 144 publications that deal with employees' security awareness and behavior theories. Relevant literature from 2000 until today was sought in academic databases and analyzed with a focus on both applied theory and research methodology. We introduce a meta-model that explains employees' information security behavior by assembling the core constructs of four primary applied theories. By synthesizing results of prior empirically tested research models based on adopted theories, a discussion of factors that were proven to have a significant influence on employees' security behavior or intentions is presented. Additional factors used in the research domain are also identified. Gaps in existing research are presented in the discussion of the results of the literature analysis. Recommendations for future studies that refer to research studies and the subject of investigation are also given. The results provided by our work can be used by practitioners in order to increase employees' security related behavior, and also by researchers in order to extend and improve information security awareness and behavior models.

2. Research Methodology

To synthesize and extend the current body of knowledge, the underlying research design consists of two phases: First, relevant literature is identified by conducting a structured literature search, since the quality of a literature review strongly depends on the search process (vom Brocke et al., 2009). Second, the identified literature is analyzed with the purpose of identifying applied theories and methodologies in the contemplated research field.

2.1 Literature Search Process

In order to present a wide-spread overview of applied theories, we chose the structured approach presented by Webster and Watson (2002) as the underlying methodology. Guidelines from vom Brocke et al. (2009) indicate that a rigorous literature search must be valid and reliable. In our case, validity is based on the selected databases, publications, covered period, keywords used, and the application of a forward and backward search. The term reliability refers to the replicability of the literature search process (vom Brocke et al., 2009). To fulfill this requirement, the search process was documented comprehensively.

To fulfill the requirement for validity, we searched through ten databases: AISeL, ScienceDirect, IEEEXplore, JSTOR, SpringerLink, ACM, Wiley, Emerald, InformsOnline, and Palgrave Macmillan. The search terms were defined in a common preparatory session with four experts in this research field. These include *security awareness*, *awareness training*, *awareness program*, *awareness campaign*, *security education*, *security motivation*, *security behavior,* and *personnel security*. The databases were searched to determine whether a publication contained at least one of the search terms in the title, abstract, or keywords. If the field of search (i.e., title, abstract, or keywords) could not be specified in the search query, a full text search was conducted. In total, 4,168 potentially relevant publications were identified.

To select relevant publications in the considered research field, inclusion and exclusion criteria were defined. We chose to focus not only on high-quality literature, as recommended by Webster and Watson (2002) and vom Brocke et al. (2009) but also to include conferences or journals that are not highly rated in international conference or journal rankings. This is necessary because some of these conferences or journals specialize in the field of IS security (e.g. ‘computers & security’, ‘Information Management & Computer Security’) contain numerous publications dealing with topics that are relevant for this literature review. However, non-academic publications (such as whitepapers) were excluded. Furthermore, only publications from after the year 2000 and only publications written in English were taken into account.

Publications that do not primarily deal with the topic of employees’ information security awareness and behavior were also filtered out. This was done by manually screening articles based on title, abstract and if necessary, by skimming through the full text. Following this process, 95 articles were determined to be relevant. Subsequently a backward as well as a forward search was carried out (Webster and Watson, 2002). The backward search was performed manually, whereas the forward search was conducted by using Web of Science (www.webofscience.com). As a result, eighteen additional relevant articles were identified. In total, 144 articles were identified to be relevant for this literature review (they are marked with a “*” in the references). Table 1 shows the number of publications for each journal or conference that were identified as relevant.

Table 16: Number of publications for each journal or conference

Journal	Count
Computers & Security	12
Information Management & Computer Security	10
European Journal of Information Systems	5
MIS Quarterly	5

Journal of the Association for Information Systems	4
Decision Support Systems	2
Information & Management	2
Information Security South Africa	2
Information Security Technical Report	2
Information Systems Journal	2
Journal of Information Privacy and Security	2
Others*	14
Conference	**Count**
Americas Conference on Information Systems	19
Hawaii International Conference on System Sciences	6
International Conference on Information Systems	3
Pacific Asia Conference on Information Systems	3
European Conference on Information Systems	2
International Conference on Information Security and Assurance	2
Others*	16

* only one relevant publication per journal/conference

2.2 Literature Analysis

In order to limit mistakes and subjective biases, a two-step analysis process was chosen and performed by two researchers. First, each researcher independently determined the applied theory and research methodology for each paper. Second, results were categorized with regard to theory and methodology and the results were compared to those of the other researcher. Divergences were discussed until conformity was reached. The list of theories was developed inductively while reviewing the articles.

Following the broad definition of the term 'theory' used in recent IS literature (e.g. Karjalainen and Siponen, 2011), we identified a total of 54 theories that are applied in the considered research field. The majority of the identified theories were used in two or fewer publications. Considering the frequency of use, seven primary theories were identified as stated in Table 2.

Table 17: Most frequently used theories

Theory	Frequency of Use
Theory of Reasoned Action (TRA) / Theory of Planned Behavior (TPB)	27
General Deterrence Theory (GDT)	17
Protection Motvation Theory (PMT)	10
Technology Acceptance Model (TAM)	7
Social Cognitive Theory (SCT)	3
Constructivism	3
Social Learning Theory (SLT)	3

These theories can be divided into behavioral theories (TRA/TPB, GDT, PMT, TAM) and learning theories (Constructivism, SCT, SLT). Our main focus in the reviewed research domain is on behavioral theories. Due to the complexity of the subject matter and the limited length of this paper, we chose to present an in-depth analysis of the four dominantly applied behavioral theories.

In addition to the approach to analyzing the applied theories, a list of research methodologies was defined prior to reading the publications in detail. We distinguish between eight different research methodologies: deductive analysis, modeling, experiment, action research, case study, grounded theory, literature review, empirical research (qualitative/quantitative).

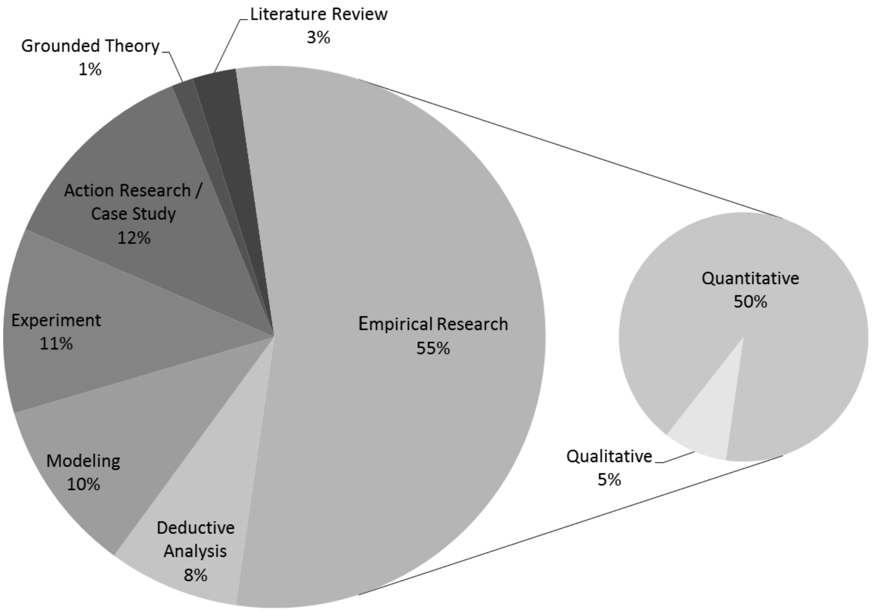


Figure 21: Frequency of applied research methodologies

Figure 1 illustrates that quantitative empirical research is dominant in the examined research field. In contrast, little qualitative empirical research is done. Even less work has been done in literature reviews and grounded theory. The remaining four methodologies (i.e., deductive analysis, modeling, experiment, and action research/case study) have been applied relatively evenly, but considerably infrequently in contrast to empirical research.

3. Behavioral Science in Information Security Research

Researchers have incorporated multidisciplinary theories, including theories from psychology, sociology, and criminology into behavioral information security success outcome models. The most frequently applied theories in the examined research field are the Theory of Reasoned Action/Theory of Planned Behavior (TRA/TPB), General Deterrence Theory (GDT), Protection Motivation Theory (PMT) and Technology Acceptance Model (TAM).

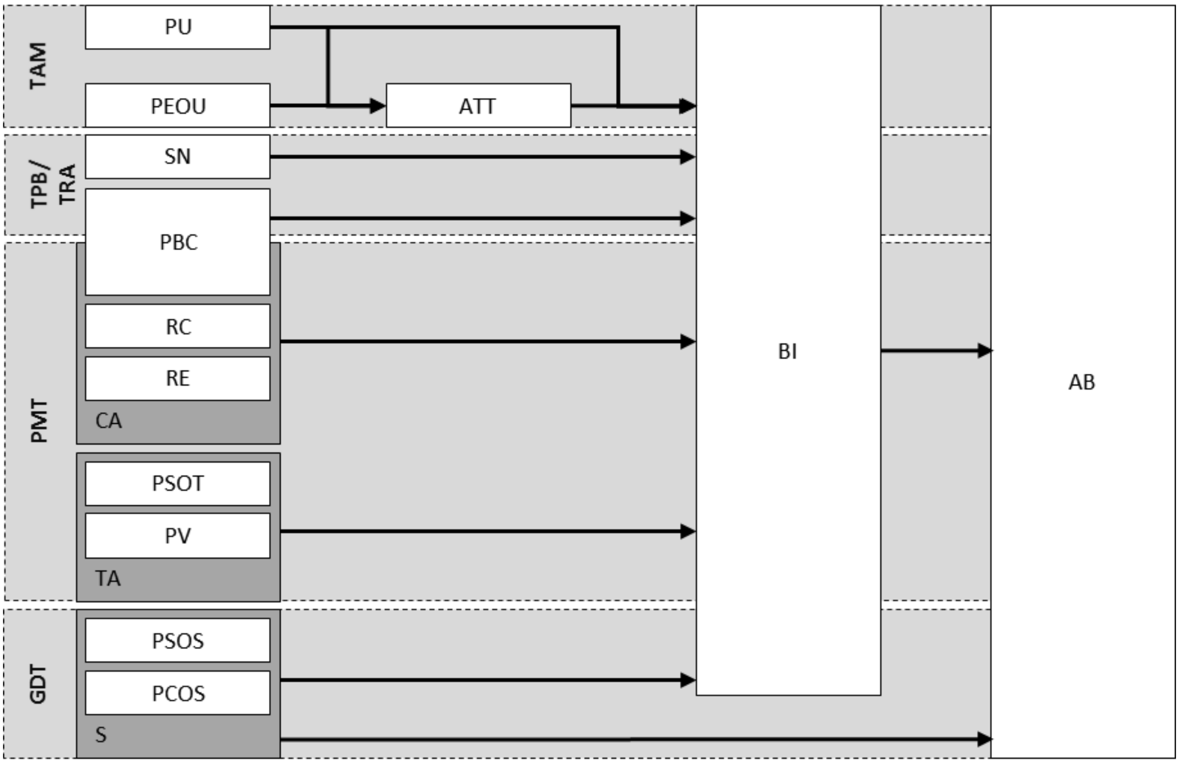
Theory of Reasoned Action/Theory of Planned Behavior: In the context of information security behavioral compliance, the employee's intention to comply with information security policies (ISP) depends on his/her overall evaluation of and normative beliefs towards compliance-related behavior. The greater the feeling of reflected actual control over those actions, the greater the intention to comply with ISP (Aurigemma and Panko, 2012; Bulgurcu et al., 2010).

General Deterrence Theory: Adapted from criminal justice research, GDT is based on rational decision making. GDT states that perceived severity (PSOS) and certainty (PCOS) of sanctions or punishment influence employees' decision regarding ISP compliance by balancing the cost and benefits (Bulgurcu et al., 2010; D'Arcy et al., 2009).

Protection Motivation Theory: Researchers argue that an employee's attitude towards information security is shaped by the evaluation of two cognitive mediated appraisals: threat appraisal (TA) and coping appraisal (CA) (Bulgurcu et al., 2010). An employee who is aware of potential security risks forms attitudes towards perceptions of these threats and the coping response (Anderson and Agarwal, 2010; Herath and Rao, 2009).

Technology Acceptance Model: In the security awareness context, the TAM determines the employees' intention to comply with information security policy, which is influenced by perceived usefulness (PU) and perceived ease-of-use (PEOU) of information security measures (Al-Omari et al., 2012).

All four theories explain employees' behavioral intention or actual behavior by adapting different factors. The above mentioned behavioral theories were combined, resulting in a meta-model as presented in figure 2. It provides an overview of factors used to explain employees' information security awareness and behavior. Each behavioral factor has been tested and evaluated in multiple studies.



ATT: Attitude towards Behavior; **AB**: Actual Behavior; **BI**: Behavioral Intention; **CA**: Coping Appraisal; **N**: Subjective Norm; **PBC**: Perceived Behavioral Control; **PCOS**: Perceived Certainty of Sanctions; **PEOU**: Perceived Ease of Use; **PSOS**: Perceived Severity of Sanctions; **PSOT**: Perceived Severity of Threat; **PU**: Perceived Usefulness; **PV**: Perceived Vulnerability; **RC**: Response Costs; **RE**: Response Efficacy; **S**: Sanctions; **SN:** Subjective Norm; **TA**: Threat Appraisal

Figure 22: Meta-model of primary used theories

4. Results

In general, the contextual analysis showed that several researchers discussed numerous factors that could affect employees' information security awareness and behavior. The descriptive analysis of consolidated publications showed partly divergent results. Therefore, a qualitative content analysis is worthwhile to determine the relations between the specific constructs within the behavioral theories. These relations will be briefly synthesized in the following section. A detailed compilation of constructs, their relationships, and the statistical significance can be found in Table 3. A list of items that were used in the various studies can be found in the appendix which can be requested via e-mail from the authors.

Table 18: Construct relationships

Constructs	Author(s)	ca	β	N	Source

Independent Variable	Items	Dependent Variable	Items					
TPB/ TRA								
ATT	4	BI	3	Bulgurcu et al. (2010)	**	.25	464	Employees
	-		-	Bulgurcu et al. (2009a)	***	.27	464	Employees
	4		3	Bulgurcu et al. (2009b)	**	.48	464	Employees
	3		3	Dinev et al. (2009)	*	.316	332	Students/IS Professionals
	3		3	Dinev et al. (2009)	-	.298	227	Students/IS Professionals
	3		3	Herath and Rao (2009b)	-	.073	312	Employees
	3		3	Hu and Dinev (2007)	**	.29	332	Students/IS Professionals
	4		5	Ifinedo (2012)	***	.48	124	IS Professionals
	4		2	Limayem and Hirt (2003)	-	.079	60	Students
	3		4	Phanila et al. (2007a)	***	.537	240	Employees
	3		3	Hu et al. (2012)	***	.360	148	Employees
	6		7	Al Omari et al. (2012b)	*	.119	878	Employees
	5		4	Zhang et al. (2009)	*	.18	176	Employees
BI	2	AB	2	Limayem and Hirt (2003)	**	.386	60	Students
	3		3	Phanila et al. (2007a)	*	.04	917	Employees
	4		3	Phanila et al. (2007b)	***	.869	240	Employees
	3		3	Siponen et al. (2007)	***	.98	917	Employees
	3		3	Siponen et al. (2010)	*	.04	917	Employees
PBC	3	BI	3	Bulgurcu et al. (2010)	**	.22	464	Employees
	2		3	Dinev et al. (2009)	**	.193	332	Students/IS Professionals
	2		3	Dinev et al. (2009)	*	.197	227	Students/IS Professionals
	3		3	Herath and Rao (2009b)	*	.172	464	Employees
	2		3	Hu and Dinev (2007)	**	.16	332	Students/IS Professionals
	7		5	Ifinedo (2012)	**	.17	124	IS Professionals
	3		3	Johnston et al. (2010)	**	.187	215	N.A.
	6		2	Limayem and Hirt (2003)	**	.300	60	Students
	3		3	Phanila et al. (2007a)	*	-	464	Employees
	3		3	Siponen et al. (2007)	***	.31	917	Employees
	3		3	Siponen et al. (2010)	*	.17	917	Employees
	8		5	Johnston et al. (2010)	*	.376	202	Healthcare Professionals
	3		3	Hu et al. (2012)	***	0.360	148	Employees
	6		7	Al Omari et al. (2012b)	*	.199	878	Employees
	4		4	Zhang et al. (2009)	***	.43	176	Employees
SN	3	BI	3	Bulgurcu et al. (2010)	**	.29	464	Employees
	2		3	Dinev et al. (2009)	-	-	332	Students/IS Professionals
	2		3	Dinev et al. (2009)	**	.324	227	Students/IS Professionals
	5		3	Herath and Rao (2009a)	***	.395	312	Employees
	5		3	Herath and Rao (2009b)	***	.313	464	Employees
	2		2	Hovav and D'Arcy (2012)	**	-.48	726	Employees
	3		3	Hu and Dinev (2007)	-	-	332	Students/IS Professionals
	4		5	Ifinedo (2012)	**	.19	124	IS Professionals

	2		3	Johnston et al. (2010)	***	.298	215	N.A.
	5		2	Limayem and Hirt (2003)	**	.210	60	Students
	4		3	Phanila et al. (2007a)	*	-	917	Employees
	3		-	Siponen et al. (2010)	-	.07	1449	Employees
	4		4	Phanila et al. (2007b)	***	.235	240	Employees
	4		3	Siponen et al. (2010b)	*	.45	917	Employees
	3		3	Hu et al. (2012)	***	.366	148	Employees
	5		7	Al Omari et al. (2012)	*	.233	878	Employees
	4		4	Zhang et al. (2009)	-	.02	176	Employees
TAM								
ATT	3	BI	3	Hu and Dinev (2007)	**	.29	332	Students/IS Professionals
	3		3	Dinev et al. (2009)	**	.316	332	Students/IS Professionals
	3		3	Dinev et al. (2009)	**	.298	227	Students/IS Professionals
	4		4	Herath et al. (2012)	***	.49	174	Students
	4		3	Xue et al. (2011)	*	.20	118	Employees
PEOU	4	ATT	4	Herath et al. (2012)	*	.20	174	Students
	3		3	Hu and Dinev (2007)	-	-	332	Students/IS Professionals
	4		4	Xue et al. (2011)	**	.26	118	Employees
	3		3	Dinev et al. (2009)	-	-	332	Students/IS Professionals
	3		3	Dinev et al. (2009)	***		227	Students/IS Professionals
PU	4		4	Herath et al. (2012)	*	.27	174	Students
	2		3	Dinev et al. (2009)	**	.5	332	Students/IS Professionals
	2		3	Dinev et al. (2009)	**	.298	227	Students/IS Professionals
	3		3	Dinev et al. (2009)	**	.52	332	Students/IS Professionals
	4		4	Xue et al. (2011)	**	.50	118	Employees
	3	BI	3	Dinev et al. (2009)	-	-	332	Students/IS Professionals
	4		3	Xue et al. (2011)	-	.11	118	Employees
GDT								
PCOS	2	BI	2	D'Arcy et al. (2009)	-	-.065	269	Employees
	2		3	Herath and Rao (2009a)	***	.260	312	Employees
	2		3	Herath and Rao (2009b)	**	.155	312	Employees
	2		2	Hovav and D'Arcy (2012)	-	-.06	360	Employees
	2		2	Hovav and D'Arcy (2012)	**	-.20	366	Employees
	4		3	Xue et al. (2011)	-	.03	118	Employees
PSOS	2	BI	2	D'Arcy et al. (2009)	**	-.176	269	Employees
	3		3	Herath and Rao (2009a)	**	-.209	312	Employees
	3		3	Herath and Rao (2009b)	**	-.139	312	Employees
	2		2	Hovav and D'Arcy (2012)	**	-.14	360	Employees
	2		2	Hovav and D'Arcy (2012)	-	-.04	366	Employees
S	4	AB	3	Siponen et al. (2007)	***	.09	917	Employees
	4		3	Phanila et al. (2007a)	*	-	917	Employees
	6		3	Siponen et al. (2010b)	***	.09	917	Employees
	2	BI	-	Siponen et al. (2010a)	-	.04	1449	Employees
	4		4	Phanila et al. (2007b)	-	-	240	Employees
PMT								
PBC	7	BI	5	Ifinedo (2012)	**	0.17	124	IS Professionals
	3		3	Herath and Rao (2009b)	*	0.172	312	Employees

	6		3	Phanila et al. (2007a)	*	-	917	Employees
	6		3	Siponen et al. (2007)	***	0.31	917	Employees
	8		4	Herath et al. (2012)	*	0.17	174	Students
	3		3	Siponen et al. (2010b)	*	0.17	917	Employees
CA	3	AB	3	Phanila et al. (2007a)	-	-	240	Employees
RC	5	BI	5	Ifinedo (2012)	-	-0.12	124	IS Professionals
RE	6	BI	5	Ifinedo (2012)	**	0.27	124	IS Professionals
	3		3	Johnston et al. (2010)	*	0.213	215	N.A.
	6		3	Phanila et al. (2007a)	-	-	917	Employees
	6		3	Siponen et al. (2007)	*	0.06	917	Employees
	3		3	Siponen et al. (2010a)	-	-0.02	917	Employees
PSOT	7	BI	5	Ifinedo (2012)	*	-0.20	124	IS Professionals
PV	7	BI	5	Ifinedo (2012)	**	0.20	124	IS Professionals
TA	4	BI	4	Herath et al. (2012)	***	0.30	174	Students
	6		3	Phanila et al. (2007a)	*	-	917	Employees
	6		3	Siponen et al. (2007)	***	0.24	917	Employees
	6		3	Siponen et al. (2010b)	*	0.12	917	Employees
	5	AB	3	Phanila et al. (2007a)	***	0.278	240	Employees

Due to certain difficulties with observing actual security compliant behavior (Vroom and von Solms, 2004), numerous authors emphasize the use of employees' behavioral intention (BI) as the dependent variable that predicts employees' actual behavior (AB) (e.g., Ifinedo, 2012; Pahnila et al., 2007; Zhang et al., 2009). Assessing BI rather than AB is grounded theoretically and technically. Several researchers demonstrated a strong and consistent relationship between the two constructs (Venkatesh et al., 2003; Webb and Sheeran, 2006) in non-information security context. From a technical point of view, measurement of actual behavior is argued to be difficult due to the sensitive context of information security (e.g., Anderson and Agarwal, 2010; Vroom and von Solms, 2004), the large and diverse sample sizes (Bulgurcu et al., 2010; Bulgurcu et al., 2009), and the theoretical background of the applied theory (Siponen and Vance, 2010). In a theoretical context, some authors (e.g., Anderson and Agarwal, 2010; Siponen and Vance, 2010) argue that the relationship between behavioral intention and actual behavior is grounded in the Theory of Planned Behavior (TPB) and Theory of Reasoned Action (TRA) by Abraham (2011) and has been shown to be proven empirically by (Anderson and Agarwal, 2010). A number of studies emphasized the relationship between employees' actual behavior and behavioral intention (e.g., Limayem and Hirt, 2003; Siponen et al., 2010; Siponen et al., 2007).

Further results demonstrate that the main constructs of the Theory of Planned Behavior are strong predictors of behavioral intention. More specifically, 92% of the evaluated relationships between perceived behavioral control (PBC) and behavioral intention are significant, with at least $p < 0.05$. In general, the determination of the PBC construct is twofold, which allows a detailed examination of internal and external factors. The main influence on the PBC construct comes from Bandura's work on self-efficacy (Bandura 1982). Self-efficacy is applied in ten research studies. It reflects the individual's personal beliefs about his or her ability to comply with the information security policy (for example Bulgurcu et al., 2010; Dinev et al., 2009; Herath and Rao, 2009; Ifinedo, 2012; Johnston et al., 2010; Johnston and Warkentin, 2010; Pahnila et al., 2007; Siponen et al., 2007; Siponen et al., 2010; Warkentin et al., 2011). In contrast, controllability represents an individual's perception about available resources and opportunities to actually comply with information security policy (Al-Omari et al., 2012; Hu and Dinev, 2007). Some authors used a combination of the two constructs to conceptualize PBC (Hu and Dinev, 2007; Zhanf et al., 2009). A statistical significant influence of subjective norm (SN) on behavioral intention was shown in six of eight studies. To explore the social influence in the context of security awareness, researchers used different labeled constructs, including normative beliefs (Bulgurcu et al., 2010; Pahnila et al., 2007; Pahnila et al. 2007 (2); Siponen et al., 2010) or general social determinants (Limayem and Hirt, 2003), which represent the subjective norm construct (Albrechtsen and Hovden, 2010). Further, eight out of ten relationships between employees' attitude towards information security (ATT) and their behavioral intention are significant, with six strong relationships at p < 0.01 level. The attitude construct is a broad term that has been investigated from different perspectives (Dinev et al., 2009). In the context of TPB, employees' attitude (ATT) reflects the users' positive or negative feelings with regard to complying with the information security policy (Ifinedo, 2012; Pahnila et al. 2007; Zhang et al., 2009; Hu and Dinev, 2007). In two cases, employee attitudes were not significant with BI. Herath and Rao (2009) stated that the insignificant effect may be due to context, sample, or other extraneous reasons. The authors combined the Protection Motivation Theory (PMT) and General Deterrence Theory (GDT) based on the core constructs of Theory of Planned Behavior (TPB) and used a sample of 312 employees from 78 organizations.

Seven studies aggregated the core constructs of TPB as a whole (Bulgurcu et al., 2010; Dinev et al., 2009; Hu and Dinev, 2007; Herath and Rao, 2009; Ifinedo, 2012; Siponen et al., 2010; Zhang et al., 2009). Numerous studies combined other theories with the core constructs of TPB (Bulgurcu et al., 2010; Herath and Rao, 2009; Hu and Dinev, 2007). Based on Theory of Reasoned Action (TRA), the Technology Acceptance Model (TAM) predicts the attitude towards the acceptance of objects as factors of adoption and use. Therefore, some authors empirically studied employees' perceived ease of use (PEOU) and perceived usefulness (PU) of information security mechanisms as predictors of their attitudes and emphasized the relationship between attitude and behavioral intention (Dinev et al., 2009; Hu and Dinev, 2007; Xue et al., 2011). Other authors eliminated the attitude construct and emphasized a direct relationship between perceived ease of use and perceived usefulness (Hu and Dinev, 2007; Xue et al., 2011). These studies imply that both constructs form the Technology Acceptance Model are less related to employees' attitude towards information security. It is argued that even if a user does not prefer a specific object, he or she might still use it if it increases job performance (Dinev et al., 2009). Interestingly, no study suggested a significant relationship between perceived usefulness and behavioral intention (Hu and Dinev, 2007; Xue et al., 2011) but together with Dinev et al. (2009), the authors showed a positive significant relationship between the two constructs.

Turning to General Deterrence Theory (GDT), the constructs of perceived severity of sanctions (PSOS) and perceived certainty of sanctions (PCOS) were related to behavioral intention (D'Arcy et al., 2009; Herath and Rao, 2009 (2); Hovav and D'Arcy, 2012; Xue et al., 2011). In the security awareness context and due to the theoretical base of GDT, the theory focuses on a different perspective of the intention construct. Employees' behavioral intentions are measured as users' perception as to whether a violation of specific portions of information security policy may increase his or her general utility. Some studies incorporated additional constructs to the core constructs of GDT (Pahnila et al., 2007; Pahnila et al., 2007 (2); Siponen and Vance, 2010; Siponen et al.; 2007). For example, the general construct of sanctions (S) is divided into formal sanctions, informal sanctions, and shame (Siponen and Vance, 2010). Of the six studies that investigated PCOS as a predictor of the behavioral intention, three were significant, at a minimum p < 0.01. PSOS has been shown to be significant in four cases (D'Arcy et al., 2009; Herath and Rao, 2009 (1); Herath and Rao, 2009 (2); Hovav and D'Arcy, 2012).

Studies using the Protection Motivation Theory are characterized by the application of a plethora of different constructs (Herath and Rao, 2009 (2)). The core constructs were shown to be related to BI. The Threat Appraisal (TA) construct was shown to be a predictor of behavioral intention by four research studies (Ifinedo, 2012; Pahnila et al., 2007; Siponen et al.; 2007; Siponen et al.; 2010). While Ifinedo (2012) investigated a significant relationship by separation of perceived severity (PSOT) and perceived vulnerability (PV) as TA constructs Pahnila et al. (2007); Siponen et al. (2007) and Siponen et al. (2010) considered the whole construct. Response efficacy (RE) and self-efficacy refer to coping appraisal (CA) (Pahnila et al.; 2007). In contrast to the Theory of Planned Behavior, the two constructs are viewed from a different perspectivefrom constructs of CA mechanisms (Aurigemma and Panko, 2012). The relationship between RE and behavioral intention was shown to be significant in three cases (Ifinedo, 2012; Johnston and Warkentin, 2010; Siponen et al., 2007).

In order to extend and improve the standard behavioral theories, several other constructs were introduced by academic literature in order to explain employees' IS-security-related behavior. With the purpose of explaining employees' behavioral intention, fifteen factors beyond the standard theories (i.e., TRA/TPB, TAM, GDT, PMT) were examined. Twelve of them were found to have a significant effect on BI. For example, the strength of an employee's identification with and involvement in an organization (organizational commitment) shows a highly significant effect on BI (Herath and Rao, 2009 (2)). Herath et al. (2009 (1)) discovered that an employee's perceived effectiveness of behaving securely influences BI. Moreover, the employee's awareness of the ISP (Johnston et al., 2010), as well as his or her technology awareness (Hu and Dinev, 2007) determine the security-related BI. Johnston et al. (2010) show that employees' awareness of ISP depends on the degree an employee perceives his environment to be favorable toward fulfilling a given task (situational support), the degree to which a company provides instructions to fulfill a task (verbal persuasion), and an employee's indirect experience with a task through observation (vicarious experience). With the introduction of the neutralization theory, Siponen and Vance (2010) showed that the use of neutralization techniques reduces the perceived harm of violating the ISP and therefore influences an employee's BI.

Eight further constructs were used in literature to explain employees' attitude towards information security (ATT). General information security awareness (ISA) was found in Bulgurcu et al. (2009 (1)); Bulgurcu et al. (2009 (2)); Bulgurcu et al. (2010) to have a significant influence on ATT at the minimum $p < 0.01$ level. The perceived fairness of a company's ISP is significant at the $p < 0.001$ level (Bulgurcu et al., 2009 (2)). Whereas the perceived costs of non-compliance with an organization's information security policy affect employees' attitudes (Bulgurcu et al., 2009 (1); Bulgurcu et al., 2010), the impact of perceived benefits of compliance and perceived costs of compliance are ambiguous. Both factors are significant according to (Bulgurcu et al., 2010), but not significant according to (Bulgurcu et al., 2009 (1)). Phanila et al. (2007 (2)) show that perceived behavioral control has a strong significant effect not only on employees' behavioral intentions, but also on attitudes towards information security.

5. Discussion and Implications

The four identified dominant behavioral theories explain employees' BI by using a variety of factors. Therefore, the development of a meta-model as proposed in Figure 2 was applicable. The core construct relationships from each theory were adopted by most publications that apply the respective theory. A solid confirmation of existing construct relationships in the context employees' security behavior is provided by existing literature, so future studies can focus more on additional constructs than on examining already confirmed core construct relationships.

Since factors like employees' intentions, attitudes, motivations or satisfaction are not verifiable by means other than self-reporting (Podsakoff and Organ, 1986), it is not unexpected that the majority of reviewed literature applying TRA/TPB, TAM, GDT or PMT uses quantitative methods to test the hypotheses. However, the use of self-reports to measure security-related behavior might lack validity, because self-reports are prone to the problems of common method variance, consistency motif, and social desirability (Podsakoff and Organ, 1986), and results may be biased. According to Workmann et al. (2008), self-reports are not sufficient predictors of employees' AB, because employees' self-reported perceptions of security behavior are not necessarily in line with their AB. At first glance, observation seems to be an instrument for gathering more objective data. Due to the sensitive nature of security-related data, organizations are unwilling to reveal information that provides insights into a company's current information security status (Kotulic and Clark, 2004). In addition, it is impossible to observe all aspects of security behavior (e.g., password strength, encrypting sensitive e-mails, etc.) for a large amount of employees, which means that observations alone are also insufficient. If researchers are able to develop a trustful environment (Kotulic and Clark, 2004), a combination of self-reporting and observational sampling in triangulation, as proposed by Workman et al. (2008), is an appropriate means of reducing the lack of qualitative and interpretive studies in this research field. As already stated in (Bulgrucu et al., 2009 (2)), case studies including employees from one or more companies would be useful for further research. As an alternative to case studies, experimental studies, as used by Johnston and Warkentin (2010), for example, are also a method of observing employees' actual behavior. However, observations under laboratory conditions change the nature of the subject matter (Podsakoff and Organ, 1986), as employees' behavior is not observed in their actual working environment. Evidence must be gathered from real work situations, including a variety of real tasks over a longer period of time. One method of observing long-time data in actual working environments is proposed by Venkatesh et al. (2003) and Workmann et al. (2008) with the analysis of log-files.

Due to the difficulties in observing useful empirical data (Kotulic and Clark, 2004), low response rates and the survey of students and IS professionals can be seen in nearly every empirical study. For instance, within the reviewed literature, only five studies included more than 500 respondents (Hovav and D'Arcy, 2012; Pahnlia et al., 2007 (1); Siponen and Vance, 2010; Siponen et al., 2007; Siponen et al., 2010). An empirical sample is relevant as long as it is representative and generalizable. Samples consisting of students and/or IS professionals do not reflect the population of interest. With reference to internal, external, and construct validity, surveying students and IS professionals is seen more critically than having a smaller sample size, as long as it represents reality (Sivo et al., 2004). With regard to globally acting organizations, more studies are required that focus on the differences in awareness in an international context, such as that of Dinev et al. (2009).

Regarding the relationships between constructs, only five studies examined the relationship between employees' BI and AB (c.f. Table 2). Although a significant relationship was found between the two constructs, all five studies used self-reporting to assess employees' actual behavior. The problems with self-reported data are already mentioned above. Many other studies postulate a strong and consistent relationship between BI and AB by referring to Venkatesh et al. (2003). Since the authors also used self-reported data and did not deal with security-related behavior, the assignability of the results has to be challenged. The question arises as to whether an employee's BI is a truly reliable predictor for AB, or if there are any external or environmental factors mitigating the influence of BI on AB. For example, an employee might intend to behave in compliance with the organization's ISP because of his strong self-efficacy and normative beliefs (c.f. TRA/TPB), but is not able to transform his or her intentions into actual behavior. One reason for this could be heavy workload in combination with complex security measures. The BI – AB gap implicates that individuals hold positive BI, but subsequently fail to enact those BI. In addition, changes in BI do not consequently lead to changes in AB (Fishbein and Ajzen, 1975; Webb and Sheeran, 2006). Meta-analytic evidence demonstrates that changes in BI lead to AB in a lower degree (Webb and Sheeran, 2006). One option to alleviate the BI – AB gap is the application of scenario techniques (Bulgurucu et al., 2010; Uffen and Breitner, 2013). If detailed information is provided about potential information security situations and indirectly attitudes towards information security are questioned indirectly, it might lead to a better impression of an individual's true intention.

According to Roseman and Vessey (2008), academic literature should provide relevance for practitioners in order to prevent research from becoming an end unto itself. The research topic covered by our work is highly relevant for practice, because dependency on IT systems has increased rapidly over the last years and there is a high demand in security measures that go beyond technical solutions. The key question for practitioners is how to influence employees' behavior to reduce information security risks. Previous research shows a gap between theoretically grounded explanations of employees' security behavior and the need of practitioners to know which interventions to apply (Workman et al., 2008). Our results contribute toward closing this gap by providing an overview of factors that were shown to have a significant influence on employees' behavioral intentions and their actual behaviors. Practitioners are therefore able to focus on these factors to define effective security measures and information security awareness programs. Security practitioners should keep in mind the variety of influence factors, resulting in a behavior-specified information security awareness program. Our findings suggest that effective security awareness programs are dependent on several behavioral influence factors. Based on our results, additional research can support practitioners by developing and validating measures that are able to significantly influence key factors.

6. Limitations

Although a rigorous approach was used to search relevant literature, there are limitations concerning the search terms used and the identified literature. We only used search terms in English. Moreover, the list of search terms was predefined and not developed inductively. A second search process with terms gathered during the literature analysis process should be conducted to find further literature that is relevant in the context of this literature review. By excluding non-peer-reviewed publications (e.g., books and whitepapers), only publications of controlled quality were included in the analysis process. Even though we expect that books might also include valuable contributions that were introduced at conferences or published in journals, some contributions might be missing in this literature review.

One major challenge of IT research is the proliferation of terms to describe similar concepts. As mentioned in section 2.2, we chose a manual approach to identifying applied theories and research methodologies. Nevertheless, the application of latent semantic analysis to our dataset could be a useful addition by discovering more coherent concepts.

Further, due to the complexity of the subject matter and the diversity of identified theories, we chose to present an in-depth analysis of the four primarily applied theories.

7. Conclusion and Outlook

This paper presents a theory-based literature review of the extant security awareness in behavioral research. In total, 113 publications were identified and analyzed. The four primarily applied theories are TPB, GDT, PMT, and TAM. A meta-model that explains employees' IS security behavior is introduced by assembling the core constructs of those theories. By synthesizing results of empirically tested research models, a discussion of factors with a proven significant influence on employees' security behavior is presented.

Since solid evidence of relationships between the main constructs of TPB, GDT, PMT, and TAM is provided by academic literature, future empirical studies have to focus on additional factors that influence employees' information security awareness and behavior instead of on measuring core construct relationships. Due to the dominance of quantitative work, qualitative studies like action research and interview studies could add value to the research field. Furthermore, the reliability of behavioral intention as a predictor of actual security behavior needs further attention. Regarding the weaknesses of self-reporting as a measure of employees' actual behavior, a stronger consideration of additional research methodologies such as experiments or case studies is required. In order to prevent an emerging gap between theory and practice, the development of measures and process models to influence employees' security awareness and behavior based on already existing theoretical knowledge is necessary.

References

[1] J.H. Abawajy, K. Thatcher, T-H. Kim, “Investigation of Stakeholders Commitment to Information Security Awareness Programs”, Proceedings of the International Conference on Information Security and Assurance, pp. 472-476, 2008.*

[2] S. Abraham, “Information Security Behavior: Factors and Research Directions”, Proceedings of the American Conference on Information Systems, Paper 462, 2011.*

[3] Ajzen, "The Theory of Planned Behavior", Organizational Behavior and Human Decision Processes, Vol. 50, No. 2, pp.179-211, 1991.

[4] Al Arifi, H. Tootell, P. Hyland, “Information Security Awareness in Saudi Arabia“, CONF-IRM Proceedings, Paper 57, 2012.*

[5] M. Alnatheer, T. Chan, K. Nelson, “Understanding and Measuring Information Security Culture”, Proceedings of the Pacific Asia Conference on Information Systems, Paper 144, 2012.*

[6] E. Albrechtsen, “A Qualitative Study of Users’ View on Information Security”, Computers & Security, Vol. 26, No. 4, pp. 276 – 289, 2007.*

[7] E. Albrechtsen, J. Hovden, “Improving Information Security Awareness and Behavior through Dialogue, Participation and Collective Reflection. An Intervention Study”, Computers & Security, Vol. 29, No. 4, pp. 432 – 445, 2010.*

[8] Al-Omari, O. El-Gayar, A. Deokar, “Information Security Policy Compliance: A User Acceptance Perspective”, Proceedings of the Midwest Association for Information Systems, Paper 12, 2011.*

[9] Al-Omari, O. El-Gayar, A. Deokar, “Security Policy Compliance: User Acceptance Perspective”, Proceedings of the 45th Hawaii International Conference on System Sciences, pp. 3317-3326, 2012a.*

[10] Al-Omari, O. El-Gayar, A. Deokar, “Information Security Policy Compliance: The Role of Information Security Awareness” Proceedings of the American Conference on Information Systems, Paper 16, 2012b.*

[11] K.A. Alshare, P.L. Lane, “A Conceptual Model for Explaining Violations of the Information Security Policy (ISP): A Cross Cultural Perspective”, Proceedings of the American Conference on Information Systems, Paper 366, 2008.*

[12] C.L. Anderson, and R. Agarwal, “Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Behavioral Intentions”, MIS Quarterly, Vol. 34, No. 3, 2010, pp. 613-643, 2010.

[13] S. Aurigemma, R. Panko, “A Composite Framework for Behavioral Compliance with Information Security Policies”, Proceedings of the Hawaii International Conference on System Sciences, pp. 3248-3257, 2007.*

[14] K. Aytes, T. Conolly, “A Research Model for Investigating Human Behavior Related to Computer Security”, Proceedings of the American Conference on Information Systems, pp. 2027-2031, 2003.*

[15] Banerjee, S.K. Pandey, “Research on Software Security Awareness: Problems and Prospects”, ACM SIGSOFT Software Engineering Notes, Vol. 35, No. 5, pp. 1-5, 2010.*

[16] N. Boon Yuen, A. Kankanhalli, “Processing Information Security Messages: An Elaboration Likelihood Perspective”, Proceedings of the European Conference on Information Systems, Paper 113, 2008.*

[17] S.R. Boss, L.J. Kirsch, I. Angermeier, R.A. Shingler, R.W. Boss, “If Someone Is Watching, I’ll Do What I’m Asked: Mandatoriness, Control, And Information Security”, European Journal of Information Systems, Vol. 18, No. 2, pp. 151-164, 2009.*

[18] M. Boujettif, Y. Wang, “Constructivist Approach to Information Security Awareness in the Middle East”, Proceedings of the International Conference on Broadband, Wireless Computing, Communication and Applications, pp. 192-199, 2010.*

[19] R. Brody, W. Brizzee, I. Cano, “Flying Under the Radar: Social Engineering”, International Journal of Accounting and Information Management, Vol. 20, No. 4, pp. 335-347, 2012.*

[20] Bulgurcu, H. Cavusoglu, I. Benbasat, “Effects of Individual and Organization Based Beliefs and the Moderating Role of Work Experience on Insiders' Good Security Behaviors”, Proceedings of the International Conference on Computational Science and Engineering, pp. 476-481, 2009a.*

[21] Bulgurcu, H. Cavusoglu, I. Benbasat, “Roles of Information Security Awareness and Perceived Fairness in Information Security Policy Compliance”, Proceedings of the American Conference on Information Systems, Paper 419, 2009b.*

[22] Bulgurcu, H. Cavusoglu, I. Benbasat, “Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness”, MIS Quarterly, Vol. 34, No. 3, pp. 523-548, 2010. *

[23] M. Burns, A. Durcikova, J. Jenkins, “What Kind of Interventions Can Help Users From Falling for Phishing Attempts: A Research Proposal for Examining Stage-Appropriate Interventions”. Proceedings of the 46th Hawaii International Conference on System Sciences, pp. 4023-4032, 2013.*

[24] M. Burns, A. Durcikova, J. Jenkins, “On Not Falling For Phish: Examining Multiple Stages of Protective Behavior of Information Systems End-Users”. Proceedings of the 33rd International Conference on Information Systems, Paper 87, 2012.*

[25] M. Chan, I. Woon, A. Kankanhalli, “Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior”, Journal of Information Privacy Security, Vol. 1, No. 3, pp. 18-41, 2005.*

[26] Charoen, M. Raman, L. Olfman, “Improving End User Behaviour in Password Utilization: An Action Research Initiative”, Systemic Practice and Action Research, Vol. 21, No. 1, pp. 55-72, 2008.*

[27] C.C. Chen, B.D. Medlin, R.S. Shaw, “A Cross-Cultural Investigation of Situational Information Security Awareness Programs”, Information Management & Computer Security, Vol. 16, No. 4, pp. 360-376, 2008.*

[28] P.A. Chia, S.B. Maynard, A.B. Ruighaver, “Exploring Organisational Security Culture: Developing a Comprehensive Research Model”, IS ONE World Conference, 2002.*

[29] M. Clarke, Y. Levy, “Initial Validation and Empirical Development of the Construct of Computer Security Self-Efficacy”, Proceedings of the Pre-ICIS Workshop on Information Security and Privacy, Paper 4, 2012.*

[30] B.D. Cone, C.E. Irvine, M.F. Thompson, T.D. Nguyen, “A Video Game for Cyber Security Training and Awareness”, Computers & Security, Vol. 26, No. 1, pp. 63-72, 2007.*

[31] Conklin, G. Dietrich, “Modeling End User Behavior to Secure a PC in an Unmanaged Environment”, Proceedings of the American Conference on Information Systems, Paper 449, 2005.*

[32] J. D’Arcy, A. Hovav, “Does One Size Fit All? Examining the Differential Effects of IS Security Countermeasures”, Journal of Business Ethics, Vol. 89, No. 1, pp. 59-71, 2009.*,

[33] J. D’Arcy, A. Hovav, “The Role of Individual Characteristics on the Effectiveness of IS Security”, Proceedings of the American Conference on Information Systems, pp. 1395-1402, 2004.*

[34] J. D’Arcy, A. Hovav, D. Galletta, “User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach”, Information Systems Research, Vol. 20, No. 1, pp. 79-98, 2009.*

[35] J. D'Arcy, T. Herath, “A Review and Analysis of Deterrence Theory in the IS Security Literature: Making Sense of the Disparate Findings”, European Journal of Information Systems (EJIS), Vol. 20, No. 6, pp. 643-658, 2011.*

[36] F.D. Davis, R.P. Bagozzi, and P.R. Warshaw, “User Acceptance of Computer Technology: A Comparison of Two Theoretical Models,” Management Science, Vol. 35, No. 8, pp. 982-1003, 1989.

[37] T. Dinev, J. Goo, Q. Hu, K. Nam, “User Behavior Toward Protective Technologies - Cultural Differences Between the United States and South Korea”, Information Systems Journal, Vol. 19, No. 4, pp. 391-412, 2009.*

[38] R.C. Dodge, C. Carver, A.J. Ferguson, “Phishing for User Security Awareness”, Computers & Security, Vol. 26, No. 1, pp. 73-80, 2007.*

[39] S. Dojkovski, S. Lichtenstein, M.J. Warren, “Fostering Information Security Culture in Small and Medium Size Enterprises: An Interpretive Study in Australia”, European Conference on Information Systems, pp. 1560-1571, 2007.*

[40] L. Drevin, H. A. Kruger, T. Steyn, “Value-Focused Assessment of ICT Security Awareness in an Academic Environment”, Computers & Security, Vol. 26, No. 1, pp. 36-43, 2007.*

[41] R. El-Haddadeh, A. Tsohou, M. Karyda, “Implementation Challenges For Information Security Awareness Initiatives in E-Government”, Proceedings of the European Conference on Information Systems, Paper 179, 2012.*

[42] M. Eminağaoğlu, E. Uçar, S. Eren, “The Positive Outcomes of Information Security Awareness Training in Companies – A Case Study”, Information Security Technical Report, Vol. 14, No. 4, pp. 223-229, 2009.*

[43] J. Fan, P. Zhang, “Study on E-Government Information Misuse Based on General Deterrence”, Proceedings of the International Conference on Service Systems and Service Management, pp. 1-6, 2011.*

[44] M. Fishbein, I. Ajzen, “Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research”, Reading, MA: Addison-Wesley, 1975.

[45] W. Flores, M. Ekstedt, “A Model for Investigating Organizational Impact on Information Security Behavior”, Proceedings of the Pre-ICIS Workshop on Information Security and Privacy, Paper 12, 2012.*

[46] W. Flores, M. Korman, “Conceptualization Of Constructs For Shaping Information Security Behavior: Towards A Measurement Instrument”. Proceedings of the Pre-ICIS Workshop on Information Security and Privacy, Paper 11, 2012.*

[47] S.M. Furnell, M. Gennatou, P.S. Dowland, “A Prototype Tool for Information Security Awareness and Training”, Logistics Information Management, Vol. 15, No. 5, pp. 352-357, 2002.*

[48] S.M. Galvez, I.R. Guzman, “Identifying Factors that Influence Corporate Information Security Behavior”, Proceedings of the American Conference on Information Systems (AMCIS), Paper 765, 2009.*

[49] J.J. Gonzalez, “Exploring Collaborative Modeling as Teaching Method”, Proceedings of the 45th Hawaii International Conference on System Sciences (HICSS), pp. 190-196, 2012.*

[50] M. Guimaraes, H. Said, R. Austin, “Experience with Videogames for Security”, The Journal Of Computing Sciences in Colleges, Vol. 27, No. 3, pp. 95-104, 2012.*

[51] T. Gundu, S.V. Flowerday, "The Enemy Within: A Behavioural Intention Model and an Information Security Awareness Process," Proceedings of the Annual Conference on Information Security South Africa, pp. 1-8, 2012.*

[52] K.H. Guo, Y. Yuan, N.P. Archer, C.E. Connelly, “Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model”, Journal of Management Information Systems, Vol. 28, No. 2, pp. 203-236, 2011.*

[53] Hadasch, B. Mueller, A. Maedche, “Exploring Antecedent Environmental and Organizational Factors to User Caused Information Leaks: A Qualitative Study”, Proceedings of the European Conference on Information Systems, Paper 127, 2012.*

[54] J.M. Hagen, E. Albrechtsen, “Effects on Employees' Information Security Abilities by E-Learning”, Information Management & Computer Security, Vol. 17, No. 5, pp. 338-407, 2009.*

[55] J.M. Hagen, E. Albrechtsen, J. Hovden, “Implementation and Effectiveness of Organizational Information Security Measures”, Information Management & Computer Security, Vol. 16, No. 4, pp. 377-397, 2008.*

[56] Harnesk, J. Lindström, “Shaping security behaviour through discipline and agility: Implications for information security management”, Information Management & Computer Security, Vol. 19, No. 4, pp. 262-276, 2011.*

[57] J. Heikka, “A Constructive Approach to Information Systems Security Training: An Action Research Experience”, Proceedings of the American Conference on Information Systems, Paper 319, 2008.*

[58] T. Herath, H. R. Rao, “Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness”, Decision Support Systems, Vol. 47, No. 2, pp. 154-165, 2009a.*

[59] T. Herath, H.R. Rao, “Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organizations”, European Journal on Information Systems, Vol. 18, No. 2, pp. 106-125, 2009b.*

[60] T. Herath, R. Chen, J. Wang, K. Banjara, J. Wilbur, H.R. Rao, “Security Services as Coping Mechanisms: An Investigation into User Intention to Adopt an Email Authentication Service”, Information Systems Journal, 2012.*

[61] Hovav, J. D’Arcy, “Applying an Extended Model of Deterrence across Cultures: An Investigation of Information Systems Misuse in the U.S. and South Korea”, Information & Management, Vol. 49, No. 2, pp. 99-110, 2012.*

[62] Hu, Y.Y. Wang, “Teaching Computer Security Using Xen in a Virtual Environment”, Proceedings of the International Conference on Information Security and Assurance, pp. 389-392, 2008. *

[63] Q. Hu, T. Dinev, “The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies”, Journal of the Association for Information Systems, Vol. 8, No. 7 pp. 386-408, 2007.*

[64] Q. Hu, T. Dinev, P. Hart, D. Cooke, “Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture”, Decision Sciences Journal, Volume 43, Number 4, 2012*

[65] P. Ifinedo, “IT Security and Privacy Issues in Global Financial Services Institutions: Do Socio-Economic and Cultural Factors Matter?”, Proceedings of the Conference on Privacy, Security and Trust, pp. 75–84, 2008.*

[66] P. Ifinedo, “Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory”, Computers & Security, Vol. 31, No. 1, pp. 83-95, 2012.*

[67] S. Jahner, H. Krcmar, “Beyond Technical Aspects of Information Security: Risk Culture as a Success Factor for IT Risk Management”, Proceedings of the American Conference on Information Systems, Paper 462, 2005.*

[68] J. Jenkins, A. Durcikova, M. Burns, “Get a Cue on IS Security Training: Explaining the Difference between how Security Cues and Security Arguments Improve Secure Behavior”, Proceedings of the International Conference on Information Systems, 2011.*

[69] J.L. Jenkins, A. Durcikova, G. Ross, J.F. Nunamaker, "Encouraging Users to Behave Securely: Examining the Influence of Technical, Managerial, and Educational Controls on Users’ Secure Behavior", Proceedings of the International Conference on Information Systems, Paper 150, 2001.*

[70] J.L. Jenkins, A. Durcikova, M.B. Burns, “Forget the Fluff: Examining How Media Richness Influences the Impact of Information Security Training on Secure Behavior”, Proceedings of the 45th Hawaii International Conference on System Sciences, pp. 3288-3296, 2012.*

[71] A.C. Johnston, B. Wech, E. Jack, M. Beavers, “Reigning in the Remote Employee: Applying Social Learning Theory to Explain Information Security Policy Compliance Attitudes”, Proceedings of the American Conference on Information Systems, Paper 493, 2010.*

[72] A.C. Johnston, M. Warkentin, “Fear Appeals and Information Security Behaviors: An Empirical Study”, MIS Quarterly, Vol. 34, No. 3, pp. 549-566, 2010.*

[73] M. Karjalainen, M.T. Siponen, „Toward a New Meta-Theory for Designing Information Systems (IS) Security”, Journal of the Association for Information Systems, Vol. 12, No. 8, pp. 518-555, 2011.

[74] M. Kawakami, H. Yasuda, R. Sasaki, “Development of an E-learning Content-Making System for Information Security (ELSEC) and its Application to Anti-phishing Education”, Proceedings of the International Conference on e-Education, pp. 7-11, 2010.*

[75] L. Kirsch, S. Boss, “The Last Line of Defense: Motivating Employees to Follow Corporate Security Guidelines”, Proceedings of the International Conference on Information Systems, Paper 103, 2007.*

[76] Komatsu, D. Takagi, T. Takemura, “Human Aspects of Information Security: An Empirical Study of Intentional Versus Actual Behavior”, Information Management & Computer Security, Vol. 21, No. 1, pp. 5-15, 2013.*

[77] A.G. Kotulic, and J.G. Clark, “Why There Aren’t More Information Security Research Studies”, Information & Management, Vol. 41, No. 5, pp. 597-607, 2004.

[78] Kritzinger, E. Smith, „Information Security Management: An Information Security Retrieval and Awareness Model For Industry”, Computers & Security, Vol. 27, No. 5-6, pp. 224-231, 2008.*

[79] Kruger, L. Drevin, T. Steyn, “A Vocabulary Test to Assess Information Security Awareness”, Information Management & Computer Security, Vol. 18, No. 5, pp. 316-327, 2010.*

[80] H.A. Kruger, S. Flowerday, L. Drevin, T. Steyn, “An Assessment of the Role of Cultural Factors in Information Security Awareness”, Proceedings of the Annual Conference on Information Security South Africa, pp. 1-7, 2011.*

[81] H.A. Kruger, W.D. Kearney, “A Prototype for Assessing Information Security Awareness”, Computers & Security, Vol. 25, No. 4, pp. 289-296, 2006.*

[82] H.A. Kruger, W.D. Kearney, “Consensus Ranking – An ICT Security Awareness Case Study”, Computers & Security, Vol. 27, No. 7-8, pp. 254-259, 2008.*

[83] J. Lee, Y. Lee, “A Holistic Model of Computer Abuse within Organizations”, Information Management & Computer Security, Vol. 10, No. 2, pp. 57-63, 2002.*

[84] S.M. Lee, S.G. Lee, S. Yoo, “An Integrative Model of Computer Abuse Based on Social Control and General Deterrence Theories”, Information & Management, Vol. 41, No. 6, pp. 707-718, 2004.*

[85] Y. Levy, T.J. Ellis, “Towards a Framework of Literature Review Process in Support of Information Systems Research”, Proceedings of the Informing Science and IT Education Joint Conference, pp. 171-181, 2006.

[86] Liang, Y. Xue, “Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective”, Journal of the Association for Information Systems, Vol. 11, No. 7, pp. 394-413 2010.*

[87] G-Y. Liao, C-M. Wang, "Exploring the Influences of Implementation Intention on Information Security Behaviors", Proceedings of the American Conference on Information Systems, Paper 473, 2011.*

[88] J.S. Lim, A. Ahmad, S. Chang, S. Maynard, “Embedding Information Security Culture Emerging Concerns and Challenges”, Proceedings of the Pacific Asia Conference on Information Systems, Paper 43, 2010.*

[89] M. Limayem, S.G. Hirt, “Force of Habit and Information Systems Usage: Theory and Initial Validation”, Journal of Association for Information Systems, Vol. 4, No. 1, pp. 65-97, 2003.*

[90] T.J. Madden, P.S. Scholder, I. Ajzen, “A Comparison of the Theory of Planned Behavior and the Theory of Reasoned Action”, Personality and Social Psychology Bulletin, Vol. 18, No. 1, pp. 3-9, 1992.

[91] M. Mahbubur Rahim, A. Cheo, K. Cheong, “IT Security Expert’s Presentation and Attitude Changes of End-Users towards IT Security Aware Behaviour: A Pilot Study”, Proceedings of the Australasian Conference on Information Systems, pp. 780-790, 2008.*

[92] K. Marett, N. Ratnamalala, “Examining the Coping Appraisal Process in End User Security”. Proceedings of the Pre-ICIS Workshop on Information Security and Privacy, Paper 2, 2012.*

[93] Marks, Y. Rezgui, “A Comparative Study of Information Security Awareness in Higher Education Based on the Concept of Design Theorizing”, Proceedings of the International Conference on Management and Service Science, pp.1-7, 2009.*

[94] W.A. Mehrens, I.J. Lehman, “Using Standardized Tests in Education”, Longman Group United Kingdom, 1987.

[95] Meister, E. Biermann, “Implementation of a Socially Engineered Worm to Increase Information Security Awareness”, Proceedings of the International Conference on Broadband Communications, Information Technology & Biomedical Applications, pp. 343–350, 2008.*

[96] R.J. Mejias, “An Integrative Model of Information Security Awareness for Assessing Information Systems”, Proceedings of the 45th Hawaii International Conference on System Sciences, pp. 3259-3267, 2012.*

[97] M. Merhi, V. Midha, “The Impact of Training and Social Norms on Information Security Compliance: A Pilot Study”. Proceedings of the 33rd International Conference on Information Systems, Paper 73, 2012.*

[98] S. Mishra, G. Dhillon, “Information Systems Security Governance Research: A Behavioral Perspective”, Proceedings of the Symposium on Information Assurance, Academic Track of 9th Annual NYS Cyber Security Conference, pp.18-26, 2005.*

[99] S. Mishra, G. Leone, D. Caputo, R. Galabrisi, P. Draus, “The Role of Demographic Characteristics in Health Care Strategic Security Planning”, Proceedings of the 18th Americas Conference on Information Systems, Paper 16, 2012.*

[100] L. Myyry, M.T. Siponen, S. Pahnila, T. Vartiainen, A. Vance, “What Levels of Moral Reasoning and Values Explain Adherence to Information Security Rules? An Empirical Study”, European Journal on Information Systems, Vol. 18, No. 2, pp. 126-139, 2011.*

[101] B.-Y. Ng, A. Kankanhalli, Y. Xu, “Studying Users' Computer Security Behavior: A Health Belief Perspective”, Decision Support Systems, Vol. 46, No. 4, pp. 815-825, 2009.*

[102] K. Padayachee, “Taxonomy of Compliant Information Security Behavior”. Computers & Security, Vol. 31, No. 5, pp. 673-680, 2012.*

[103] S. Pahnila, M.T. Siponen, A. Mahmood, “Employees’ Behavior Towards IS Security Policy Compliance”, Proceedings of the 40th Hawaii International Conference on System Sciences, pp. 1-10, 2007a.*

[104] S. Pahnila, M.T. Siponen, A. Mahmood, “Which Factors Explain Employees’ Adherence to Information Security Policies? An Empirical Study”, Proceedings of the Pacific Asia Conference on Information Systems, Paper 73, 2007b.*

[105] M.R. Pattinson, G. Anderson, “How Well Are Information Risks Being Communicated to your Computer End-Users?”, Information Management & Computer Security, Vol. 15, No. 5, pp. 362-371, 2007.*

[106] D. Phelps, J. Gathegi, “Information System Security: Self-Efficacy and Implementation Effectiveness”, Proceedings of the American Conference on Information Systems, pp. 3353-3361, 2006.*

[107] P.M. Podsakoff, D. Organ, “Self-Reports in Organizational Research: Problems and Prospects”, Journal of Management, Vol. 12, No. 4, pp. 531–544, 1986.

[108] P. Puhakainen, M.T. Siponen, „Improving Employees’Compliance through Information System Security Training“, MIS Quarterly, Vol. 24, No.4, pp. 757-778, 2010.*

[109] Qing, X. Zhengchuan, T. Dinev, L. Hong, “Does Deterrence Work in Reducing Information Security Policy Abuse by Employees?”, Communications of the ACM, Vol. 54, No. 6, 2011.*

[110] S. Ramachandran, “Influences on Espoused and Enacted Security Cultures in Organizations”, Proceedings of the American Conference on Information Systems, Paper 128, 2006.*

[111] S. Ramachandran, S. Rao, “Security Cultures in Organizations: A Theoretical Model”, Proceedings of the American Conference on Information Systems, Paper 417, 2006.*

[112] R. Reid, J. van Niekerk, R. von Solms, „Guidelines for the Creation of Brain-Compatible Cyber Security Educational Material in Moodle 2.0”, Proceedings of the Annual Conference on Information Security South Africa, 2011.*

[113] Y. Rezgui, A. Marks, “Information Security Awareness in Higher Education: An Exploratory Study”, Computers & Security, Vol. 27, No. 7-8, pp. 241-253, 2008.*

[114] Rhee, C. Kim, Y. Ryu, “Self-Efficacy in Information Security: It’s Influence on End Users’ Information Security Practice Behavior”, Computers & Security, Vol. 28, No. 8, pp. 816-826, 2009.*

[115] R.W. Rogers, “Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation Theory”, in Social Psychophysiology, J. Cacioppo and R. Petty (Eds.), Guilford, New York, 1983.

[116] M. Rosemann, I. Vessey, “Toward Improving the Relevance of Information Systems Research to Practice: The Role of Applicability Checks”, MIS Quarterly, Vol. 32, No. 1, 2008.

[117] Ryan, “Information Security Awareness: An Evaluation among Business Students with Regard to Computer Self-efficacy and Personal Innovation”, Proceedings of the American Conference on Information Systems (AMCIS), Paper 251, 2007.*

[118] R.S. Shaw, C.C. Chen, A.L. Harris, H.J. Huang, “The Impact of Information Richness on Information Security Awareness Training Effectiveness”, Computers & Security, Vol. 52, No. 1, pp. 92-100, 2009.*

[119] Shropshire, M. Warkentin, A. Johnston, M. Schmidt, “Personality and It Security: An Application of the Five-Factor Model”, Proceedings of the American Conference on Information Systems (AMCIS), pp. 3443-3449, 2006.*

[120] Silva, S. Menezes, A. Costa, “A Model for Evaluating Information Security with a Focus on the User”, Proceedings of the Mediterranean Conference on Information Systems, Paper 25, 2012.*

[121] G. Silvius, T. Dols, “Factors Influencing Non-Compliance Behavior Towards Information Security Policies”. CONF-IRM Proceedings, Paper 39, 2012.*

[122] M.T. Siponen, S. Pahnila, M. A. Mahmood, “Compliance with Information Security Policies: An Empirical Investigation”, Computer, Vol. 43, No. 2, pp. 64-71, 2010a.*

[123] M.T. Siponen, “A Conceptual Foundation for Organizational Information Security Awareness”, Information Management & Computer Security, Vol. 8, No. 1, pp. 31-41, 2000.*

[124] M.T. Siponen, “Critical Analysis of Different Approaches to Minimizing User-Related Faults In Information Systems Security: Implications for Research and Practice”, Information Management & Computer Security, Vol. 8, No. 5, pp. 197-209, 2000.*

[125] M.T. Siponen, “Five Dimensions of Information Security Awareness”, Computers and Society, Vol. 31, No. 2, pp. 24-29, 2001.*

[126] M.T. Siponen, A. Osborn Vance, “Neutralization: New Insights into the Problem of Employee Systems Security Policy Violations”, MIS Quarterly, Vol. 34 No. 3, pp. 487-502, 2010b.*

[127] M.T. Siponen, S. Phanila, A.M. Mahmood, “A New Model for Understanding Users’ IS Security Compliance”, Proceedings of the Pacific Asia Conference on Information systems, Paper 48, 2006.*

[128] M.T. Siponen, S. Pahnila, A. Mahmood, “Employees’ Adherence to Information Security Policies: An Empirical Study”, Proceedings of the IFIP SEC, pp. 133-144, 2007.*

[129] S. Sivo, S. Saunders, Q. Chang, and J.J. Jiang, “How Low Should You Go? Low Response Rates and the Validity of Inference in IS Questionnaire Research”, Journal of the Association for Information Systems, Vol. 7, No. 6, pp. 351-414, 2004.

[130] J.-Y. Son, “Out Of Fear or Desire? Toward A Better Understanding of Employees’ Motivation to Follow IS Security Policies”, Information & Management, Vol. 48, No. 7, pp. 296-302, 2011.*

[131] J.-Y. Son, H-S. Rhee, “Out of Fear or Desire: Why do Employees Follow Information Systems Security Policies?”, Proceedings of the American Conference on Information Systems, Paper 268, 2007.*

[132] J.L. Spears, H. Barki, “User Participation in Information Systems Security Risk Management”, MIS Quarterly, Vol. 34, No. 3, pp. 503-522, 2010.*

[133] Stanton, P. Mastrangelo, K. Stam, J. Jolton, “Behavioral Information Security: Two End User Survey Studies of Motivation and Security Practices”, Proceedings of the American Conference on Information Systems (AMCIS), pp. 1388-1394, 2004.*

[134] J.M. Stanton, K.R. Stam, P. Mastrangelo, J.Jolton, “An Analysis of End User Security Behaviors”, Computers & Security, Vol. 24, No. 2, pp.124-133, 2005.*

[135] J.M. Stanton, K.R. Stam, I. Guzman, C. Caledra, “Examining the Linkage Between Organizational Commitment and Information Security”, Proceedings of the IEEE International Conference on Systems, Man and Cybernetics, pp. 2501-2506, 2003.*

[136] D.W. Straub, “Effective IS Security: An Empirical Study“, Information Systems Research, Vol. 1, No. 3, pp. 255-276, 1990.

[137] S. Talib, N. Clarke, S.M. Furnell, “An Analysis of Information Security Awareness within Home and Work Environments”, Proceedings of the International Conference on Availability, Reliability, and Security, pp. 196-203, 2010.*

[138] Thomson, J. Niekerk, “Combating Information Security Apathy by Encouraging Prosocial Organizational Behavior”, Information Management & Computer Security, Vol. 20, No. 1, pp. 39-46. 2012.*

[139] Tsohou, S. Kokolakis, “Aligning Security Awareness with Information Systems Security Management”, Proceedings of the Mediterranean Conference on Information Systems, Paper 73, 2009.*

[140] Tsohou, S. Kokolakis, M. Karyda, E. Kiountouzis, “Investigating Information Security Awareness: Research and Practice Gaps”, Information Security Journal: A Global Perspective, Vol. 17, No. 5-6, pp. 207-227, 2008.*

[141] Tsohou, M. Karyda, S. kokolakis, E. Kiountouzis, “Analyzing Trajectories on Information Security Awareness”, Information Technology & People, Vol. 25, No. 3, pp. 327-352, 2012.*

[142] Uffen, M.H. Breitner, “Management of Technical Security Measures: An Empirical Examination of Personality Traits and Behavioral Intentions”, Proceedings of the 46th Hawaii International Conference on System Science, pp. 4551-4560, 2013.

[143] Vance, M.T. Siponen, S. Pahnila, “Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory”, Information & Management, Vol. 49, No. 3-4, pp. 190–198, 2012.*

[144] V. Venkatesh, M.G. Morris, G.B. Davis, F.D. Davis, “User Acceptance of Information Technology: Toward a Unified View”, MIS Quarterly, Vol. 27, No. 3, pp. 425-478, 2003.

[145] vom Brocke, A. Simons, B. Niehaves, K. Riemer, R. Plattfaut, A. Cleven, „Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process“, Proceedings of the European Conference on Information Systems, pp. 2206–2217, 2009.

[146] vom Brocke, C. Buddendick, “Security Awareness Management - Konzeption, Methoden und Anwendung“, Proceedings of the Wirtschaftsinformatik Tagung, pp.1227-1246, 2007.*

[147] Vroom, R. von Solms, “Towards Information Security Behavioral Compliance”, Computer & Security, Vol. 23, No. 3, pp. 191-198, 2004.

[148] Waly, R. Tassabehji, M. Kamala, “Measures for Improving Information Security Management in Organisations: The Impact of Training and Awareness Programs”, Proceedings of the UK Academy for Information Systems Conference, Paper 8, 2012a.*

[149] Waly, R. Tassabehji, M. Kamala, “Improving Organizational Information Security Management: The Impact of Training and Awareness”, Proceedings of the 14th International Conference on High Performance Computing and Communications, pp. 1270 – 1275, 2012b.*

[150] Warkentin, A.C. Johnston, J. Shropshire, “The Influence of the Informal Social Learning Environment on Information Privacy Policy Compliance Efficacy and Intention”, European Journal on Information Systems (EJIS), Vol. 20, No. 3, pp. 267-284, 2011.*

[151] Warkentin, N. Malimage, K. Malimage, “Impact of Protection Motivation and Deterrence on IS Security Policy Compliance: A Multi-Cultural View”, Proceedings of the Pre-ICIS Workshop on Information Security and Privacy, Paper 20, 2012.*

[152] Warkentin, M. Mc Bride, I. Carter, A. Johnston, “The Role of Individual Characteristics on Insider Abuse Intentions” Proceedings of the 18h Americas Conference on Information Systems, Paper 28, 2012.*

[153] J. Warner, “Towards Understanding User Behavioral Intentions to Use IT Security: Examining the Impact of IT Security Psychological Climate and Individual Beliefs”, Proceedings of the American Conference on Information Systems, pp. 4536-4540, 2006.*

[154] T.L. Webb, P Sheeran, “Does Changing Behavioral Intentions Engender Behavior Change? A Meta-Analysis of the Experimental Evidence”, Psychological Bulletin, Vol. 132, No. 2, pp. 249-268, 2006.

[155] J. Webster, R.T. Watson, “Analyzing the Past to Prepare for the Future: Writing a Literature Review”, MIS Quarterly, Vol. 26, No. 2, pp. xiii-xxiii, 2002.

[156] P.A.H. Williams, “In a ‘Trusting’ Environment, Everyone is Responsible for Information Security”, Information Security Technical Report, Vol. 13, No. 4, pp.207-215, 2008.*

[157] R. Willison, “Understanding the Perpetration of Employee Computer Crime in the Organizational Context”, Information and Organization, Vol. 16, No. 4, pp. 304-324, 2006.*

[158] S. Woodhouse, “Information Security: End User Behavior and Corporate Culture”, Proceedings of the IEEE International Conference on Computer and Information Technology, pp. 767-774, 2007.*

[159] M.T. Workman, J. Gathegi, “Punishment and Ethics Deterrents: A Study of Insider Security Contravention”, Journal of the American Society for Information Science and Technology, Vol. 58, No. 2, pp. 212-222, 2007.*

[160] M. Workman, W.H. Bommer, D. Straub, “Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test”, Computers in Human Behavior, Vol. 24, No. 6, pp. 2799-2816, 2008.

[161] B.R. Worthen, W.R. Borg, K.R. White, “Measurement and Evaluation in the School”, Longman Group United Kingdom, 1993.

[162] Y. Xue, H. Liang, L. Wu, “Punishment, Justice, and Compliance in Mandatory IT Settings”, Information Systems Research, Vol. 22, No. 2, pp. 400-414, 2011.*

[163] J. Zhang, B. Reithel, J. Brian, H. Li, “Impact of Perceived Technical Protection on Security Behaviors”, Information Management & Computer Security, Vol. 17, No. 4, pp. 330-340, 2009.*

Appendix 9 (A9)

Title: Towards a Needs Assessment Process Model for Security, Education, Training and Awareness Programs - An Action Design Research Study

Authors: Benedikt Lebek, Jörg Uffen, Markus Neumann, Bernd Hohler, Michael H. Breitner

In: Proceedings of the 21st European Conference on Information Systems, Utrecht (Netherlands), Paper 110, 2013c.

Link: http://aisel.aisnet.org/ecis2013_cr/110/

Abstract

Employees are considered to be the weakest link in information systems (IS) security. Many companies and organizations started to implement security education, training and awareness (SETA) programs. These provide their employees awareness of information security risks and the necessary skills to protect a companies' or organizations' information assets. To ensure that SETA programs are efficiently aligned to an organization's objectives, it is essential to identify the most important areas on which to concentrate. In research, there is a lack of generic process models for conducting SETA needs assessments. In this study, we aim to close this gap by suggesting a systematic approach to capturing, evaluating, and depicting the current state of employees' security awareness and behavior. Actual behavior is evaluated by determining the target values and measuring actual values with respect to security metrics. In order to contribute to both, practical and academic knowledge, we used an action design research (ADR) approach to draw general design principles from organizational intervention within an international engineering company.

Appendix 10 (A10)

Title: Personality Traits and Cognitive Determinants - An Empirical Investigation of the use of Smartphone Security Measures

Authors: Jörg Uffen, Nico Kaemmerer, Michael H. Breitner

In: Journal of Information Security 4(4), pp. 202-212, 2013

Abstract

In the last years, increasing smartphones' capabilities have caused a paradigm shift in the way users view and use mobile devices. Although researchers have started to focus on behavioral models to explain and predict human behavior, there is limited empirical research about the influence of smartphone users' individual differences on the usage of security measures. The aim of this study is to examine the influence of individual differences on cognitive determinants of behavioral intention to use security measures. Individual differences are measured by the Five-Factor Model; cognitive determinants of behavioral intention are adapted from the validated behavioral models theory of planned behavior and technology acceptance model. An explorative, quantitative survey of 435 smartphone users served as data basis. The results suggest that multiple facets of smartphone user's personalities significantly affect the cognitive determinants, which indicate the behavioral intention to use security measures. From these findings, practical and theoretical implications for companies, organizations, and researchers are derived and discussed.

Appendix 11 (A11)

Title: Entwicklung von Security Awareness Konzepten unter Berücksichtigung ausgewählter Menschenbilder

Authors: Jörg Uffen, Robert Pomes, Claudia M. König Michael H. Breitner

In: IWI-Discussionpaper #23, Institut für Wirtschaftsinformatik, Leibniz Universität Hannover

Abstract

Die zunehmende Integration von Kunden, Lieferanten und Partnern in die Geschäftsprozesse von Unternehmen und allgemein von Organisationen aller Art macht die Sicherung und den Schutz der Informationssysteme immer wichtiger und auch komplexer. Unwissenheit oder leichte/grobe Fahrlässigkeit, aber auch Sabotage und Missbrauch, eigener Mitarbeiter stellen heute das größte Gefahrenpotential für Informationssysteme dar, während die Gefahr externer Angriffe durch Investitionen in Hard- und Software in den letzten Jahren abnahm. Das Risikomanagement fokussiert sich zunehmend auf das „Gefahrenpotential Mensch“: Die Sensibilisierung und vor allem die Motivation zum alltäglichen und allgegenwärtigen Mitdenken und Mitmachen steht im Mittelpunkt (Security Awareness Kampagne). Menschenbilder, z. B. des „Complex Man“, helfen für verschiedene Menschentypen verschiedene Anreizsysteme zu entwickeln, die sensibilisieren und motivieren. Diese Systeme mit positiven, aber auch negativen Anreizen (Sanktionen), sind die Basis für umfassende Security Awareness Konzepte, deren Entwicklung nachfolgend diskutiert und analysiert wird. Konkrete Handlungsempfehlungen für Unternehmen und Organisationen werden ausgearbeitet.

Appendix 12 (A12)

Title: Stärkung des IT-Sicherheitsbewusstseins unter Berücksichtigung psychologischer und pädagogischer Merkmale

Authors: Jörg Uffen, Michael H. Breitner

In: IWI-Discussion Paper #36, Institut für Wirtschaftsinformatik, Leibniz Universität Hannover

Abstract

Wissen und Informationen sind die Basis der Geschäftsprozesse und können durch den intelligenten Einsatz der Informations- und Kommunikationstechnologie innerhalb einer Organisation zu einer Steigerung der Wettbewerbsfähigkeit führen. Dies macht die Sicherung und den Schutz der Informationssysteme immer wichtiger. Doch trotz der in den letzten Jahren sich abzeichnenden Intensivierung von IT-Sicherheitsmaßnahmen im Hard- und Softwarebereich, stellen Unwissenheit, Fahrlässigkeit und Irrtum des Faktors Mensch in den Organisationen das größte Gefahrenpotenzial dar. Das Risikomanagement fokussiert sich zunehmend auf die Reduktion des „Risikofaktors Mensch“, indem komplexe Security Awareness Konzepte konzipiert werden, in denen eine Sensibilisierung und Motivation für nachhaltiges IT-Sicherheitsverhalten bewirkt werden soll. Pädagogische Ansätze und Menschenbilder, z. B. des „complex man“, über die individuelle Anreizsysteme entwickelt werden, sind die Basis für umfassende Security Awareness Konzepte. Deren Konkretisierung soll nachfolgend diskutiert und analysiert, indem konkrete Handlungsempfehlungen für Unternehmen und Organisationen herausgearbeitet werden sollen.

Appendix 13 (A13)

Title: Discussion of an IT-Governance Implementation Project Model Using COBIT and ValIT

Authors: Christoph Meyer, Jörg Uffen, Michael H. Breitner

In: IWI-Discussion Paper #49, Institut für Wirtschaftsinformatik, Leibniz Universität Hannover

Abstract

Best-practice frameworks like COBIT or Val IT provide useful support for a sustainable and efficient IT-Governance implementation in many companies and organizations. But today, IT departments face the challenge to manage both – IT functionality and business functionality in one IT-Governance implementation approach. This study discusses the combination of the COBIT and of the Val IT framework to give implications to identify the business value of IT investments while implementing COBIT. The resulting reference model helps companies and organizations to implement their individual IT-Governance approach with a business value focus. Findings suggest a six-step approach which is influenced by a central value governance and an exterior circle containing the management, business and IT objectives and the governance program.

Appendix 14 (A14)

Title: 20 Jahre Internationale Tagung Wirtschaftsinformatik: Profil einer Konferenz

Authors: Jörg Uffen, Stefan Hoyer, Michael H. Breitner

In: IWI-Discussion Paper #54, Institut für Wirtschaftsinformatik, Leibniz Universität Hannover

Abstract

Die Internationale Tagung Wirtschaftsinformatik, die bedeutendste Wirtschaftsinformatik-Konferenz im deutschsprachigen Raum seit 20 Jahren, bietet Wirtschaftsinformatikern und Informatikern eine wichtige Plattform, um aktuelle Forschungsergebnisse zu präsentieren und zu diskutieren. Bislang ist jedoch wenig über die Entwicklung favorisierter Themen und Methoden der Tagung bekannt. Diese Studie nimmt sich dieser Forschungslücke an und unter-sucht alle angenommenen Beiträge seit der ersten Tagung in 1993 in Münster. Wesentliche Ergebnisse sind z. B. die steigende Zahl englischsprachiger Beiträge, der abnehmende Anteil von Autoren aus nicht-akademischen Institutionen und die Zunahme der Autorenanzahl. Knapp 40% aller Beiträge kommen von nur zehn führenden Institutionen. 84,9% der Beiträge stammen aus Deutschland vor der Schweiz, Österreich und den USA. Vorherrschende Themenfelder sind IS Organisation & Strategie sowie Wirtschaftlichkeit und Gesellschaft. Methodisch sind am häufigsten konzeptionelle Arbeiten, vor Design Science und Fallstudien, zu finden. Deutlich zu erkennen ist in den letzten Jahren eine Verlagerung von einer Konzepterstellung zu quantitativen bzw. qualitativen Analysen.