

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


Der Wirtschaftswissenschaftlichen Fakultät der
Gottfried Wilhelm Leibniz Universität Hannover
zur Erlangung des akademischen Grades

Doktor der Wirtschaftswissenschaften
- Doktor rerum politicarum –

vorgelegte Dissertation

von

Diplom-Ökonom Jörg Uffen



2013

Acknowledgements

In German language:

Die vorliegende Arbeit ist während meiner Tätigkeit als externer Doktorand und wissenschaftlicher Mitarbeiter am Institut für Wirtschaftsinformatik der Leibniz Universität Hannover entstanden. In diesen knapp vier Jahren konnte ich die Gelegenheit nutzen und mich persönlich weiterentwickeln, wichtige Erfahrungen sammeln, Kontakte knüpfen und viele neue Freunde gewinnen. Aus diesem Grund bin ich einigen Menschen zu Dank verpflichtet.

Zunächst möchte ich mich bei meinem langjährigen Doktorvater, Herrn Prof. Dr. Michael H. Breitner bedanken, der die Betreuung übernahm und mir stetig durch seine anregenden, wertvollen Ratschläge und Ideen wichtige Impulse bei der Ausgestaltung dieser Arbeit gab. Insbesondere möchte ich ihm sowie Frau Dr. Claudia König für die stetige Diskussionsbereitschaft danken, ohne ihr umfangreiches Fachwissen wäre ein erfolgreicher Abschluss dieser Arbeit nicht möglich gewesen.

Herrn Prof. Stefan Wielenberg – Leiter des Instituts für Rechnungslegung und Wirtschaftsprüfung - möchte ich für die Übernahme des Zweitgutachtens danken.

Bedanken möchte ich mich auch bei meinen Co-Autoren (in alphabetischer Reihenfolge), insbesondere bei Benedikt Lebek, Lubov Kosch und Nadine Guhr, für die sehr angenehme Arbeitsatmosphäre und den stetigen Austausch.

Ferner möchte ich mich bei allen Kolleginnen und Kollegen des Instituts für Wirtschaftsinformatik für die angenehme Arbeitsatmosphäre und Hilfsbereitschaft bedanken. Zudem möchte ich mich bei den Kolleginnen und Kollegen des Niedersächsischen Hochschulkompetenzzentrums für SAP bedanken, insbesondere bei Halnya Zakhariya und Dr. Christian Schubert. Letzterer hat mir stets in wichtigen Zeiten den Rücken freigehalten.

Abschließend möchte ich Worte des Dankes an meine Eltern, Herta und Rudolf Uffen richten. Sie haben mich stets mit all ihrer Kraft und Sorge in jeglichen Dingen unterstützt. Ohne ihre Unterstützung und ihr entgegengebrachtes Verständnis wäre für mich diese Promotion nicht denkbar gewesen. Ihnen widme ich die vorliegende Arbeit.

Hannover, Juni 2013
Jörg Uffen

Erstprüfer:

Prof. Dr. Michael H. Breitner

Zweitprüfer:

Prof. Dr. Stefan Wielenberg

Vorsitzender der Prüfungskommission:

Jun.-Prof. Dr. Hans-Jörg von Mettenheim

Mitarbeitervertreterin:

Dr. Ute Lohse

I. Abstract

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

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 published 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) and

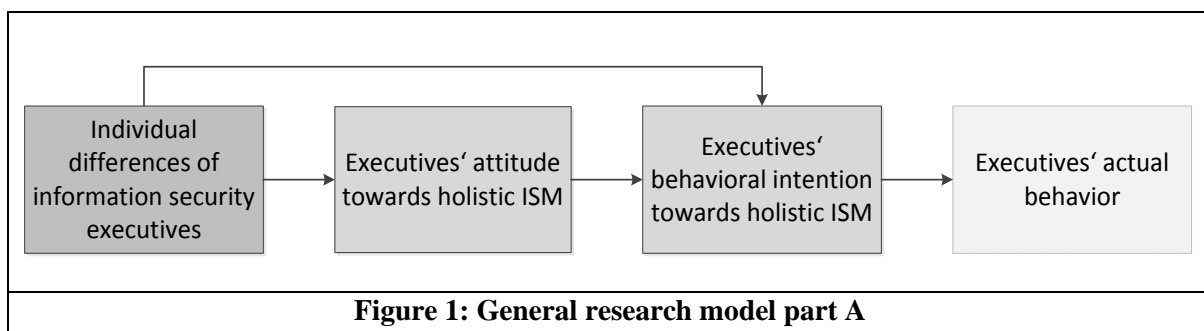
currently in review for publication in the international IS journal “Management Research Review” 2013,

- 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 (Figure 1). 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).



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 evaluates 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., 2013b). 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.

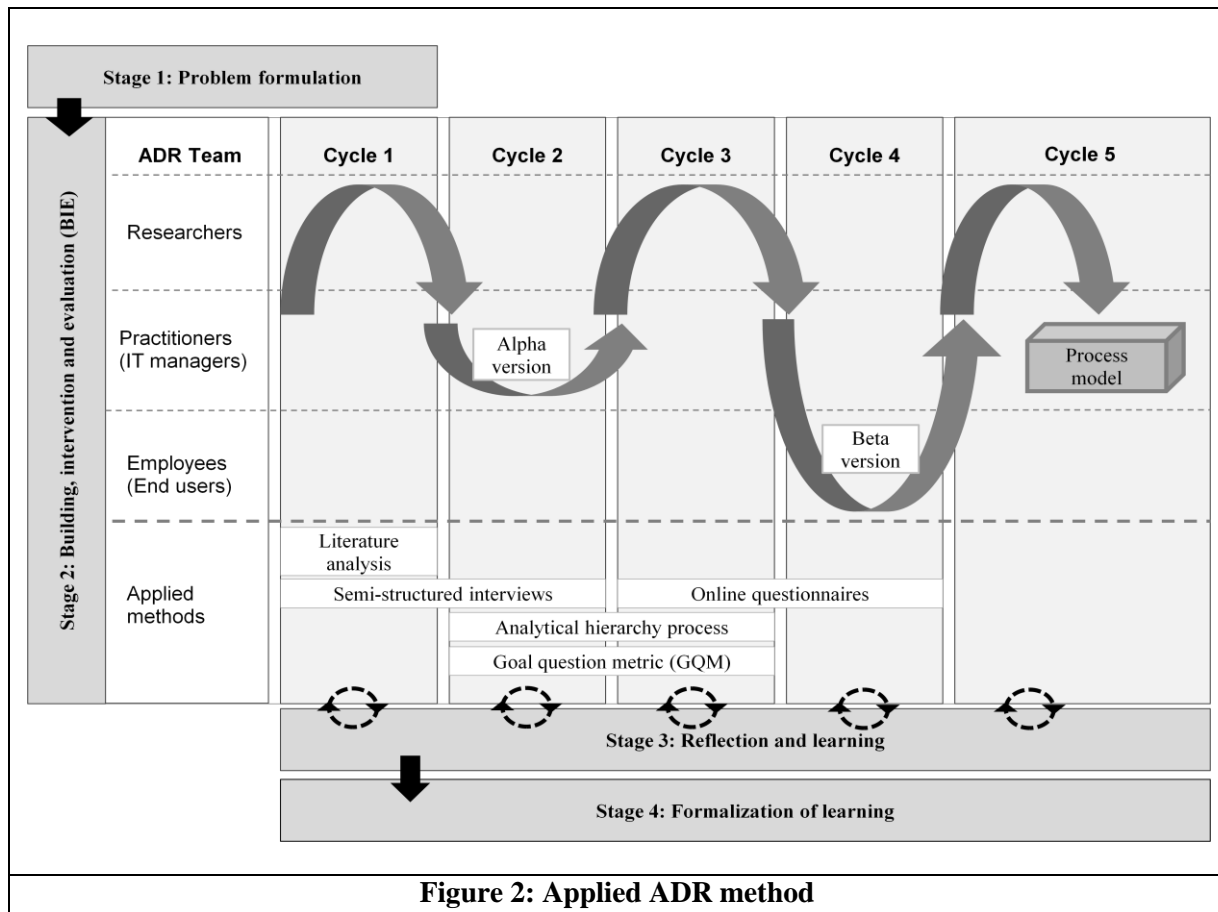


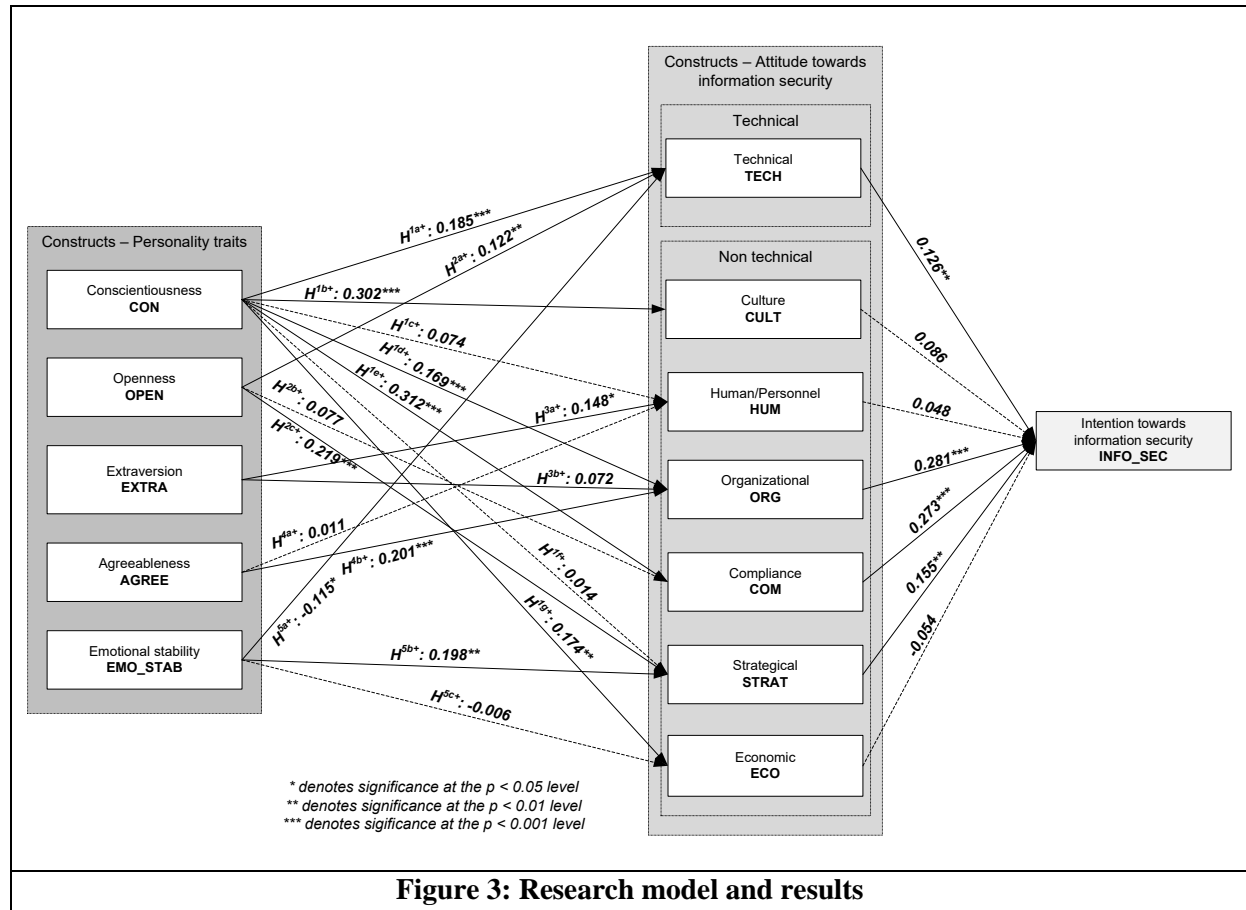
Figure 2: Applied ADR method

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

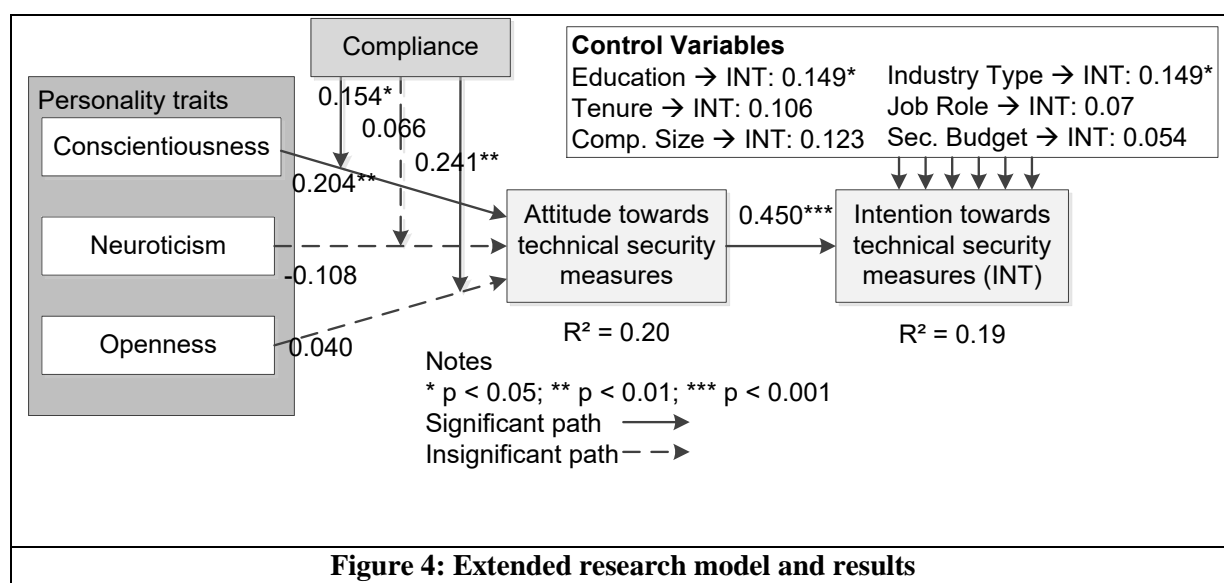
others (Barrick et al. 2001). Therefore, a hypothesized relationship between a specific personality trait and attitude is relevant when it is appropriate, and is grounded in and supported by theoretical and empirical research studies. Figure 3 provides the estimates and a summary of results of the hypothesized relationships.



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).



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

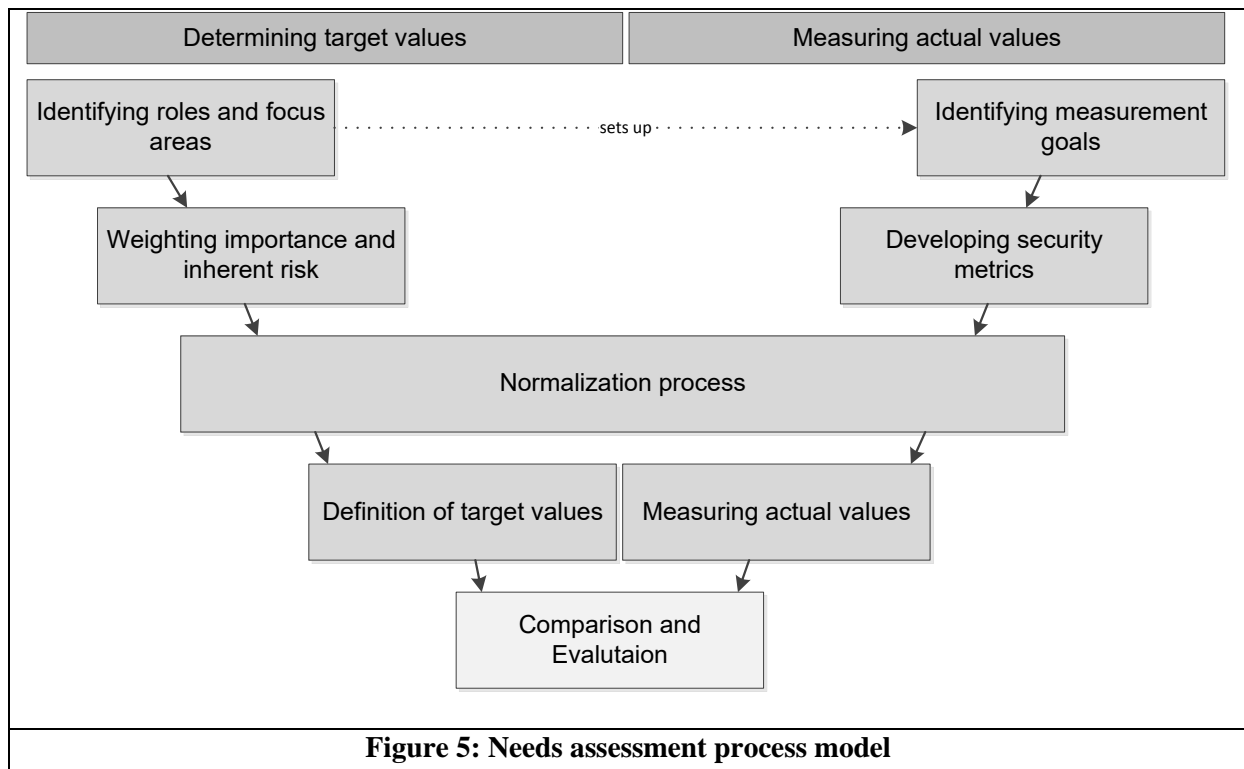
openness and attitude towards the management of technical security measures. In both cases, compliance is an external variable that moderates the relationships. Personality traits are stable in a long-term view (Costa & McCrae, 1992), thus other external factors such as compliance are more likely to 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 intentions 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.



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

I. ABSTRACT	I
II. MANAGEMENT SUMMARY	II
III. TABLE OF CONTENTS	XII
IV. LIST OF FIGURES	XVI
V. LIST OF TABLES	XVII
VI. LIST OF ABBREVIATIONS	XVIII
1. INTRODUCTION	25
1.1 MOTIVATION OF THIS THESIS	25
1.2 DERIVATION OF RESEARCH QUESTIONS	27
1.2.1 TARGET GROUP: EXECUTIVE LEVEL	27
1.2.2 TARGET GROUP: END-USER LEVEL	30
1.3 THESIS STRUCTURE AND PROBLEM CONTRIBUTION	32
2. BEHAVIORAL MODELS	34
2.1 THEORY OF PLANNED BEHAVIOR	34
2.2 FIVE FACTOR MODEL OF PERSONALITY	35
3. RESEARCH METHODOLOGY	38
3.1 QUALITATIVE RESEARCH METHODS	40
3.1.1 CONTENT ANALYSIS	40
3.1.2 ACTION DESIGN RESEARCH	41
3.2 QUANTITATIVE RESEARCH METHODS	43
3.2.1 SURVEY	43
3.2.2 PRINCIPAL COMPONENT ANALYSIS	45
3.2.3 STRUCTURAL EQUATION MODELING	45
4. PERSONALITY TRAITS AND INFORMATION SECURITY MANAGEMENT	48
4.1 INFORMATION SECURITY DIMENSIONS – A HOLISTIC APPROACH	48
4.1.1 PREAMBLE	48
4.1.2 INTRODUCTION	48
4.1.3 THEORETICAL BACKGROUND ON INFORMATION SECURITY COMPONENTS	49
4.1.4 EVALUATION OF PRACTICAL RELEVANCE	51

4.1.5	<i>CONCLUSION, LIMITATIONS AND OUTLOOK</i>	55
4.2	PERSONALITY TRAITS AND HOLISTIC INFORMATION SECURITY MANAGEMENT	56
4.2.1	<i>PREAMBLE</i>	56
4.2.2	<i>INTRODUCTION</i>	56
4.2.3	<i>THEORETICAL BACKGROUND AND RESEARCH MODEL</i>	57
4.2.4	<i>MEASUREMENT MODEL VALIDATION AND ANALYSIS</i>	59
4.2.5	<i>SUMMARY OF RESULTS</i>	60
4.2.6	<i>CONCLUSION, LIMITATIONS AND OUTLOOK</i>	62
4.3	INFORMATION SECURITY EXECUTIVES' ATTITUDES TOWARDS TECHNICAL SECURITY MEASURES: AN EMPIRICAL EXAMINATION OF PERSONALITY TRAITS AND BEHAVIORAL INTENTIONS	64
4.3.1	<i>PREAMBLE</i>	64
4.3.2	<i>INTRODUCTION</i>	64
4.3.3	<i>THEORETICAL BACKGROUND AND RESEARCH MODEL</i>	65
4.3.4	<i>DATA ANALYSIS PROCEDURES</i>	68
4.3.5	<i>SUMMARY OF RESULTS</i>	68
4.3.6	<i>CONCLUSION, LIMITATIONS AND OUTLOOK</i>	70
5.	<u>END-USERS' INFORMATION SECURITY AWARENESS AND COMPLIANT BEHAVIOR</u>	72
5.1	SECURITY AWARENESS AND COMPLIANT BEHAVIOR: A LITERATURE REVIEW	72
5.1.1	<i>PREAMBLE</i>	72
5.1.2	<i>INTRODUCTION</i>	72
5.1.3	<i>RESEARCH DESIGN</i>	73
5.1.4	<i>THEORETICAL BACKGROUND OF THE FOUR IDENTIFIED BEHAVIORAL THEORIES</i>	75
5.1.5	<i>SUMMARY OF RESULTS</i>	78
5.1.6	<i>DISCUSSION</i>	82
5.1.7	<i>CONCLUSION, LIMITATIONS AND OUTLOOK</i>	84
5.2	TOWARDS A NEEDS ASSESSMENT PROCESS MODEL FOR SETA PROGRAMS – IMPLICATIONS FROM AN ACTION DESIGN RESEARCH STUDY	85
5.2.1	<i>PREAMBLE</i>	85
5.2.2	<i>INTRODUCTION</i>	85
5.2.3	<i>RESEARCH DESIGN</i>	86
5.2.4	<i>DEVELOPMENT OF THE PROCESS MODEL FOR A SETA NEEDS ASSESSMENT</i>	88
5.2.5	<i>DEFINITION AND WEIGHTING OF ROLES AND FOCUS AREAS</i>	89
5.2.6	<i>ACTUAL BEHAVIOR MEASUREMENT</i>	91
5.2.7	<i>FORMALIZATION OF LEARNING</i>	93
5.2.8	<i>SUMMARY OF RESULTS AND IMPLICATIONS</i>	94
5.2.9	<i>CONCLUSION, LIMITATIONS AND OUTLOOK</i>	95
6.	<u>THESIS CONCLUSION, LIMITATIONS, AND FUTURE RESEARCH</u>	97
6.1	CONCLUSION	97
6.2	LIMITATIONS AND OUTLOOK	99
	<u>REFERENCES</u>	104

TASK SHARING	124
APPENDICES	127
APPENDIX 1 (A1): ASPEKTE DER WIRTSCHAFTSINFORMATIK 2009	129
APPENDIX 2 (A2): CRITICAL SUCCESS FACTORS FOR ADOPTION OF INTEGRATED INFORMATION SYSTEMS IN HIGHER EDUCATION INSTITUTIONS – A META ANALYSIS	198
APPENDIX 3 (A3): TOWARDS A SUSTAINABLE AND EFFICIENT COMPONENT-BASED INFORMATION SECURITY FRAMEWORK	210
APPENDIX 4 (A4): PERSONALITY TRAITS AND INFORMATION SECURITY MANAGEMENT: AN EMPIRICAL STUDY OF INFORMATION SECURITY EXECUTIVES	224
APPENDIX 5 (A5): MANAGEMENT OF TECHNICAL SECURITY MEASURES: AN EMPIRICAL EXAMINATION OF PERSONALITY TRAITS AND BEHAVIORAL INTENTIONS	247
APPENDIX 6 (A6): MANAGEMENT OF TECHNICAL SECURITY MEASURES: AN EMPIRICAL EXAMINATION OF PERSONALITY TRAITS AND BEHAVIORAL INTENTIONS	260
APPENDIX 7 (A7): PERSONALITY TRAITS AND MOBILE SECURITY: AN EMPIRICAL EXAMINATION OF SECURITY MEASURES IN SMARTPHONES	285
APPENDIX 8 (A8): EMPLOYEES' INFORMATION SECURITY AWARENESS AND BEHAVIOR: A LITERATURE REVIEW	298
APPENDIX 9 (A9): INFORMATION SECURITY AWARENESS AND BEHAVIOR: A THEORY-BASED LITERATURE REVIEW	315
APPENDIX 10 (A10): TOWARDS A ROLE ORIENTED NEEDS ASSESSMENT FOR SETA-PROGRAMS	343
APPENDIX 11 (A11): ENTWICKLUNG VON SECURITY AWARENESS KONZEPTEN UNTER BERÜCKSICHTIGUNG AUSGEWÄHLTER MENSCHENBILDER	356
APPENDIX 12 (A12): STÄRKUNG DES IT-SICHERHEITSBEWUSSTSEINS UNTER BERÜCKSICHTIGUNG PSYCHOLOGISCHER UND PÄDAGOGISCHER MERKMALE	368
APPENDIX 13 (A13): DISCUSSION OF A IT-GOVERNANCE IMPLEMENTATION PROJECT MODEL USING COBIT AND VALIT	408

**APPENDIX 14 (A14): 20 JAHRE INTERNATIONALE TAGUNG WIRTSCHAFTSINFORMATIK:
PROFIL EINER KONFERENZ** **423**