


Contributions to Organizational Information Security

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 Benedikt Lebek



2014

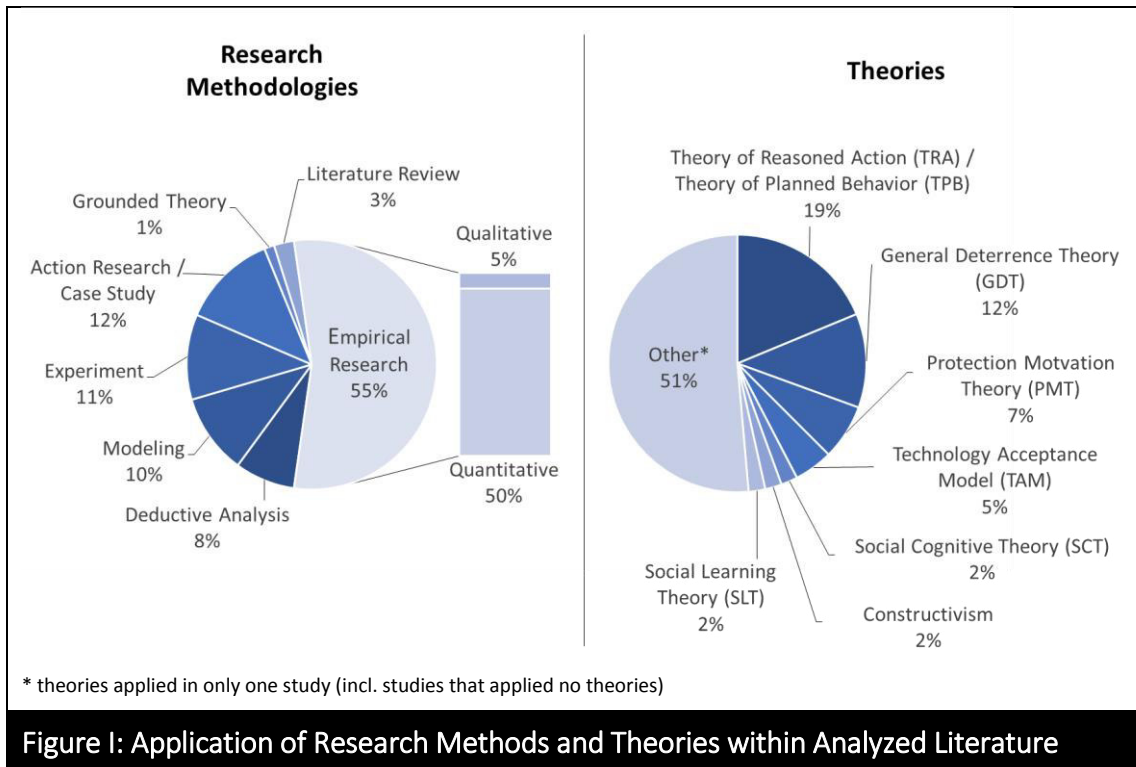
I. Abstract

Due to the proliferation of a wide variety of complex and multinational information security threats, organizations face the challenge of how to implement efficient and sustainable information security programs. This cumulative dissertation aims at contributing to the field of information security research while especially focusing on employees' information security awareness and behavior. Two research objectives are considered within this dissertation. The first addresses employees' information security awareness and behavior in general and is grounded on a comprehensive review and analysis of previous research in the contemplated research field within the last decade. By incorporating the concept of transformational leadership, the influence of supervisors and managers on employees' information security behavior was investigated. Furthermore, a systematic approach for capturing, evaluating, and depicting the current state of employees' security awareness and behavior in real working environments is proposed. The second objective focusses on the impact of consumerization of IT on organizational information security management. In this context, first the influence of security, privacy and legal concerns on employees' acceptance of the Bring-Your-Own-Device concept was investigated. Subsequently, the overarching concept of consumerization of IT was examined while investigating the impact of the emerging technologies mobile, social and cloud computing as well as big data on IS governance as the framework for organization information security. In order to pursue the research objectives, a multi method research approach was conducted, that incorporates methods from the quantitative and the qualitative research paradigm. By applying research methods that are established in the field of IS research academic rigor was ensured. By focussing on topics that are inspired from practical problems practical relevance of this dissertation is enhanced.

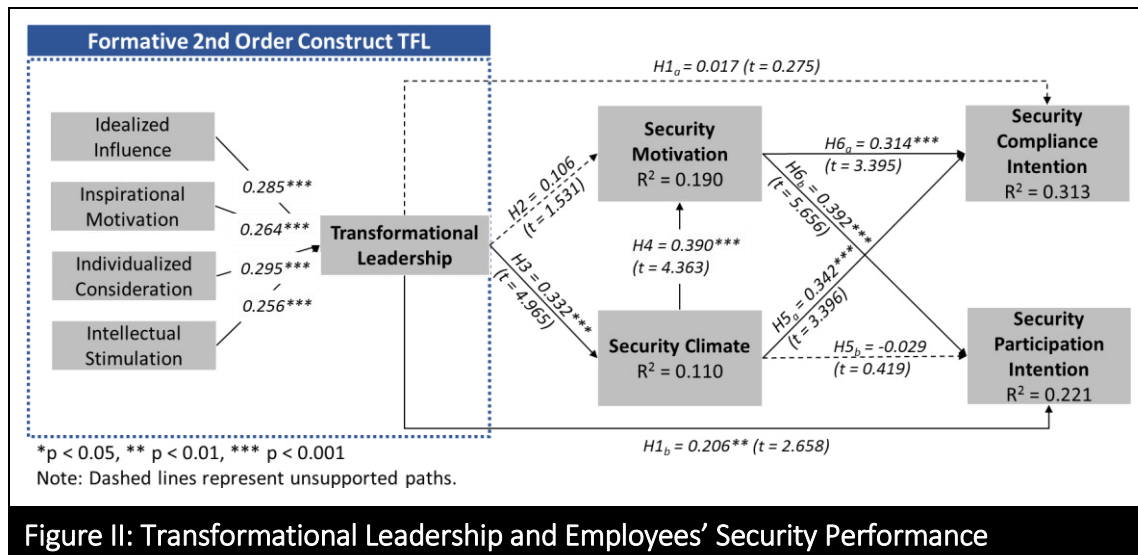
Keywords: *Employees' Information Security Awareness and Behavior | Security Education, Training and Awareness | Consumerization of IT | Bring Your Own Device | IT Governance | Nexus of Forces*

II. Management Summary

The global proliferation of threats to information security and the associated risks forces IS security managers not only to implement technical information security measures, but also to focus on employees' awareness and behavior. For this reason, the overall goal of this cumulative dissertation is to investigate the role of employees within the organizational information security chain and to provide empirical results and theoretically grounded implications for both, researchers and practitioners. The dissertation contains two main parts. The first part (cf. chapter 4) focusses directly on employees' information security awareness and behavior. The second part (cf. chapter 5) aims at investigating the consumerization of IT in the context of organizational information security. The first part of this dissertation addresses researchers in the field of employees' information security awareness and behavior as well as for practitioners that aim at establishing efficient and a sustainable information security management and security, education, training and awareness (SETA) programs within organizations. In order to provide a theoretical basis and to identify new areas of research, an in-depth analysis of the current state of academic research was initially performed. For this purpose, a structured literature review was conducted that followed several renowned academic guidelines (cf. chapter 4.1.2). This review was first conducted in 2012 and was later updated in 2013 in order to provide a current literature base. Overall ten academic databases were searched and a total of 144 relevant publications were identified. After a structured analysis of these studies, several findings were obtained (cf. chapter 4.1.3). As depicted in Figure I, the research field of employees' information security awareness and behavior is characterized by a majority of quantitative empirical studies. These studies are predominantly based on four behavioral theories that were adopted from psychology and criminology, namely Theory of Reasoned Action (TRA) / Theory of Planned Behavior (TPB), General Deterrence Theory (GDT), Protection Motivation Theory (PMT) and Technology Acceptance Model (TAM). Contextual analysis of studies that applied one or more of these four theories revealed that several researchers discussed nume-



rous factors that affect employees' information security behavior, but with partly divergent results. However, a solid confirmation of existing construct relationships in the context of employees' security behavior is provided by existing literature. Employees' information security behavior is commonly operationalized by employees' behavioral intention to comply with organizational information security policies. The assessment of employees' compliance intention rather than employees' actual security behavior is a controversial topic in the research field, but technically and theoretically justified by several authors. Furthermore, researchers mostly relied on employees' self-reports in order to measure their compliance intention. Though, the use of self-reports are prone to the problems of common method variance, consistency motif and social desirability the results may be biased. The findings of the comprehensive literature review provided major input for the further research process. Employees' compliance with information security policies has been widely recognized by researchers and practitioners as a key socio-organizational resource. Consequently, organizations face the challenge how to effectively and efficiently promote security policies to their employees. This includes the design of information security policies and measures to motivate employees to follow those policies. Although the capabilities of leaders to motivate their followers have previously been demonstrated in other management areas, the role of managerial leadership in the special context of information security has been considered only by few studies.



In order to address this gap and to extend the spectrum of applied theories, the concept of transformational leadership was adapted to the contemplated research field. This concept postulates that followers feel trust, respect, loyalty and admiration for their managers or supervisors and therefore perform above the average (cf. chapter 2.2.3). Within this dissertation it was investigated whether transformational leaders are capable of improving employees' perception of security climate and employees' security motivation and thereby enhance employees' intention to comply with organizational information security policies and employees' intention to actively participate in organizational information security, e.g. voluntarily participating in security trainings (cf. chapter 4.2.2). A research model was developed and empirically tested by means of structural equation modeling (SEM) with 208 employees from different international companies and branches (cf. chapter 4.2.3). Results show that transformational leaders have a significant positive influence on employees' participation intention, but no significant influence on employees' compliance intention (see Figure II). However, the research model provides strong evidence that employees' perception of security climate and their intrinsic security motivation mediate the influence of transformational leaders on both, employees' compliance and participation intention (Figure II). Findings of this study emphasize the importance of leadership with regard to employees' information security behavior (cf. chapter 4.2.4). Accordingly, organizations can sustainably improve information security if they promote transformational leadership by enhancing supervisors' awareness and abilities to promote and convey the value and necessity of information security among employees. By stimulating employees' intrinsic motivation and

enhancing organization security climate, transformational leaders help organizations to reduce formal control measures and to save costs.

An already common method for enhancing employees' knowledge and skills for coping with threats regarding to information security is the implementation of SETA programs. However, in this context the organizations face the challenge of how to assess the current state of employees' information security awareness and behavior. To ensure that SETA programs are efficiently aligned to organization's objectives, it is essential to identify the most important areas on which to concentrate. The initial literature review revealed that only few studies addressed this topic and research is lacking of a generic process models for conducting SETA needs assessments. To close this gap systematic approach was developed for capturing, evaluating and depicting the current state of employees' security awareness and behavior. In order to provide practical relevance while accounting for methodological rigor, an action design research (ADR) approach was used to draw general design principles from organizational intervention (cf. chapters 3.2; 4.3.2). The study emerged from a project within a German engineering company that operates in 60 countries with a total of 3,200 employees. The resulting proposal for a needs assessment process is shown in Figure III. It consists of four phases: (1) definition of target values, (2) measurement of actual values and (3) Comparison actual and target values and visualization of needs (cf. chapter 4.3.3).

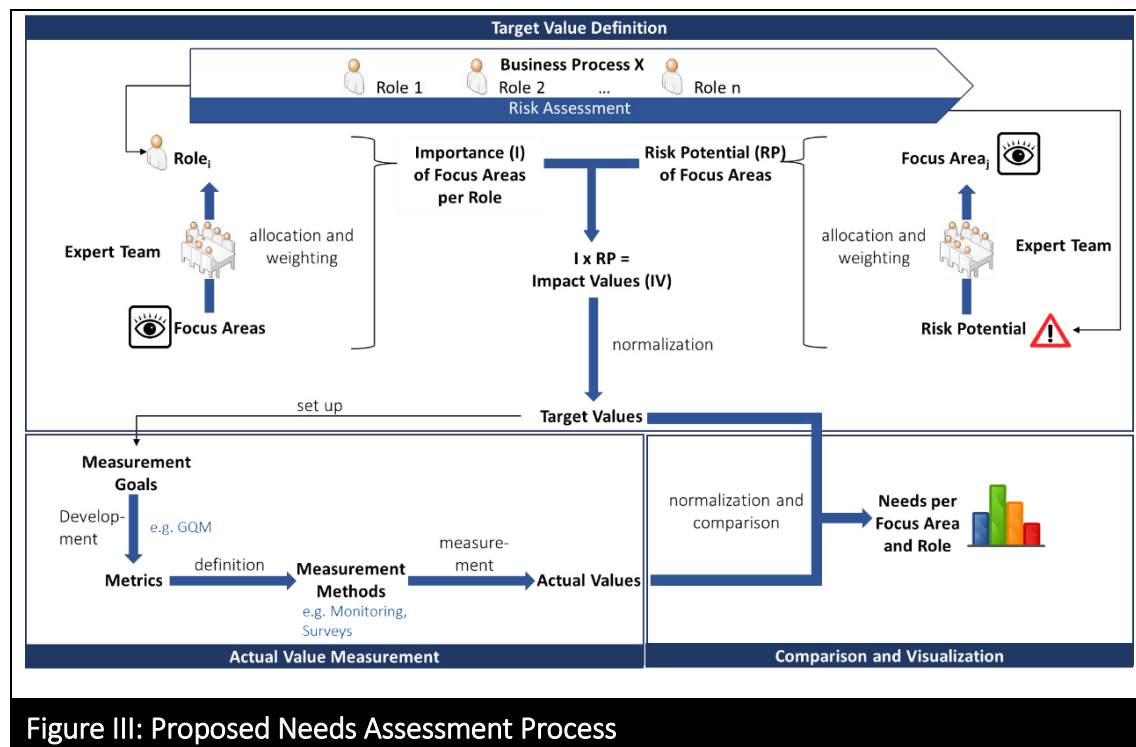
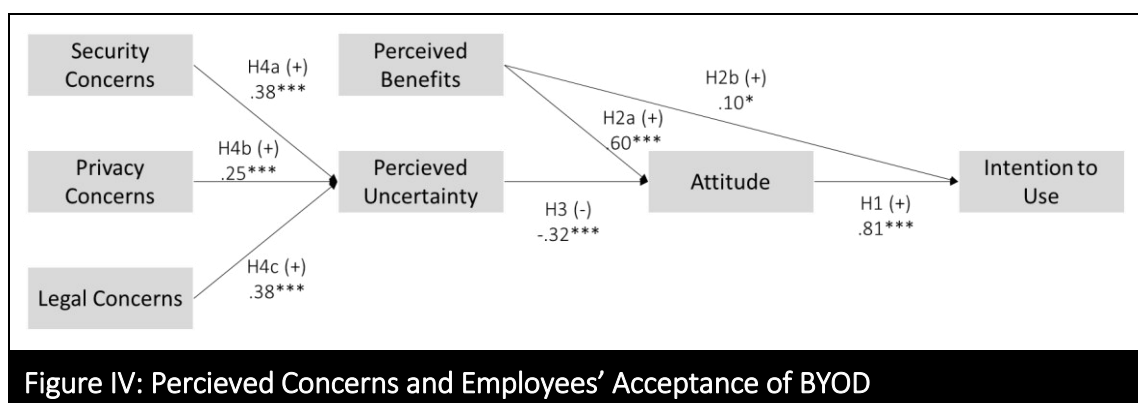


Figure III: Proposed Needs Assessment Process

In the first phase, different observation levels (i.e. roles, focus areas) are considered. Each focus area is weighted by its inherent risk potential and the importance for each role. In phase two, applicable metrics are developed based on previously measurement goals. Reliable data sources are selected (e.g. system monitoring data, incident reports). For the evaluation of the gap between actual and target values in phase three, normalization of the values must be performed in order to establish comparability. A points-based system is established to facilitate the evaluation of the gap. Results are depicted in an awareness map. Following the ADR approach, each step during the problem formulation and BIE stages were reflected in order to learn from the practical intervention. Through formalization, the learning was transformed into general design principles (cf. chapter 4.3.4) with the purpose of contributing academic knowledge to the respective research field (Table I).

Table I: Design Principles for a SETA Needs Assessment Process	
Design principle	Description
Stakeholder Integration	It is necessary to consider relevant stakeholders (i.e. management, experts, key-users) to reduce barriers within the organization and understand the purpose. Experts and key-users provide valuable experiences that complement measured data.
Perspectives	Different observation levels should be integrated to enable a selective analysis of the current state of employees' security behavior. The selection and combination of observation levels depends on the organizational context.
Weighted Focus Areas	Focus areas are critical risk areas of employees' security behavior. To determine adequate target values, the risk potential and importance of each focus area has to be evaluated.
Applicable 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 behavior.
Reliable Data Sources	Instead of relying completely on employees' self reports, the use of reliable data sources such as system monitoring should be aspired to. However, the integration of system monitoring data requires the establishment of a mature and detailed monitoring process.
Normalization	To make metrics comparable, normalization of data is needed.
Awareness Map	By depicting results from the evaluation process in an awareness map, needs for training and awareness measures can easily be identified. However, proper documentation of the measurement process is necessary to develop concrete measures.

The second part of this cumulative dissertation focuses on information security within the context of IT consumerization and encompasses two studies. The first study addresses Bring-Your-Own-Device (BYOD) as a special form of IT consumerization. At the intersection between private and organizational use of mobile computing devices (i.e. smartphone and/or tablet), the concept of BYOD emerged over the past several years and challenges the relationship between organizations and employees. In this regard, practical literature frequently emphasizes and discusses concerns regarding security, privacy and legal aspects. The question arises, to which degree these concerns do affect employees' intention to use BYOD mobile devices. In order to investigate this question a research model was developed that is based on the technology acceptance model and the theory of reasoned action (cf. chapters 5.1.2; 2.1.1; 2.1.2) as depicted in Figure IV. The proposed research model was empirically tested by means of structural equation modeling (SEM) (cf. chapter 5.1.3). A total of 151 employees from various German companies and branches completed an online survey. The theoretical model is strongly supported by the results of empirical investigation as all hypotheses were supported with high significance (cf. chapter 5.1.4). Findings show that perceived benefits and perceived uncertainty have a significant influence on employees' acceptance of BYOD. All three dimensions of concerns were proven to be major antecedents for employees' perception of uncertainty. It is notable that the influence of privacy concerns is considerably lower than the influences of security and legal concerns. Moreover, results suggest that employees have a slightly negative attitude towards BYOD. Since this study reveals that an increase in employee perception of the benefits of using BYOD mobile devices will have the greatest impact on their attitudes, it can be suggested that organizations should aim at communicating and emphasizing the advantages to their employees when planning to adopt the concept of BYOD.



The second study within part two of this dissertation is motivated by the emergence of IT consumerization as the main driver for social, mobile and cloud computing within organizations. These global trends in connection with the steadily increasing amount of information evolved independently, however, by mutual reinforcement these trends confront organizations with novel and unique challenges, especially with regard to their governance structure as the framework for the organizational information security strategy. The goal of this study is to develop a general valid and applicable reference model that addresses the new challenges and requirements presented by the Nexus of Forces. For this purpose, a three staged research approach was applied that is based on a Delphi-study (cf. chapter 5.2.2). In the first stage an initial conceptual model was developed on the basis of a literature analysis in the field of IS governance. In the second stage, this conceptual model was discussed and enhanced within a two-round Delphi approach (cf. chapter 3.4) incorporating 18 top experts in the field of IS governance and new technologies. In the last stage, the expert opinions were summarized and a reference model was created (Figure V).

Several findings were implemented within the proposed IS governance reference model (cf. chapters 5.2.3; 5.2.4). With regard to internal contingencies, the impact of the forces depends on the role of IS within the organizations. Accordingly, organizations that manage IS as an innovator are exposed more to the impact of the Nexus of Forces than organizations that have a rather conservative IS strategy. The Nexus of Forces challenges the separation of centralized or decentralized governance designs as it requires flexible adjustments to cultural, social, and regional aspects with regard to employees' and business requirements on the one hand and the definition general and sustainable IT infrastructures on the other hand. The separation of IS governance that focusses on mere technical aspects and the information governance is gaining more importance. Since consumerization affects organizations mainly on the business level, the handling of the Nexus of Forces is not primary an IS responsibility. Corporate governance has to set structures concerning IT investments, business applications and IT principles in the first instance. The IS governance is subordinated to the corporate governance and provides consulting functions regarding IS related decisions. IS management is responsible for operational implementation of IS decisions.

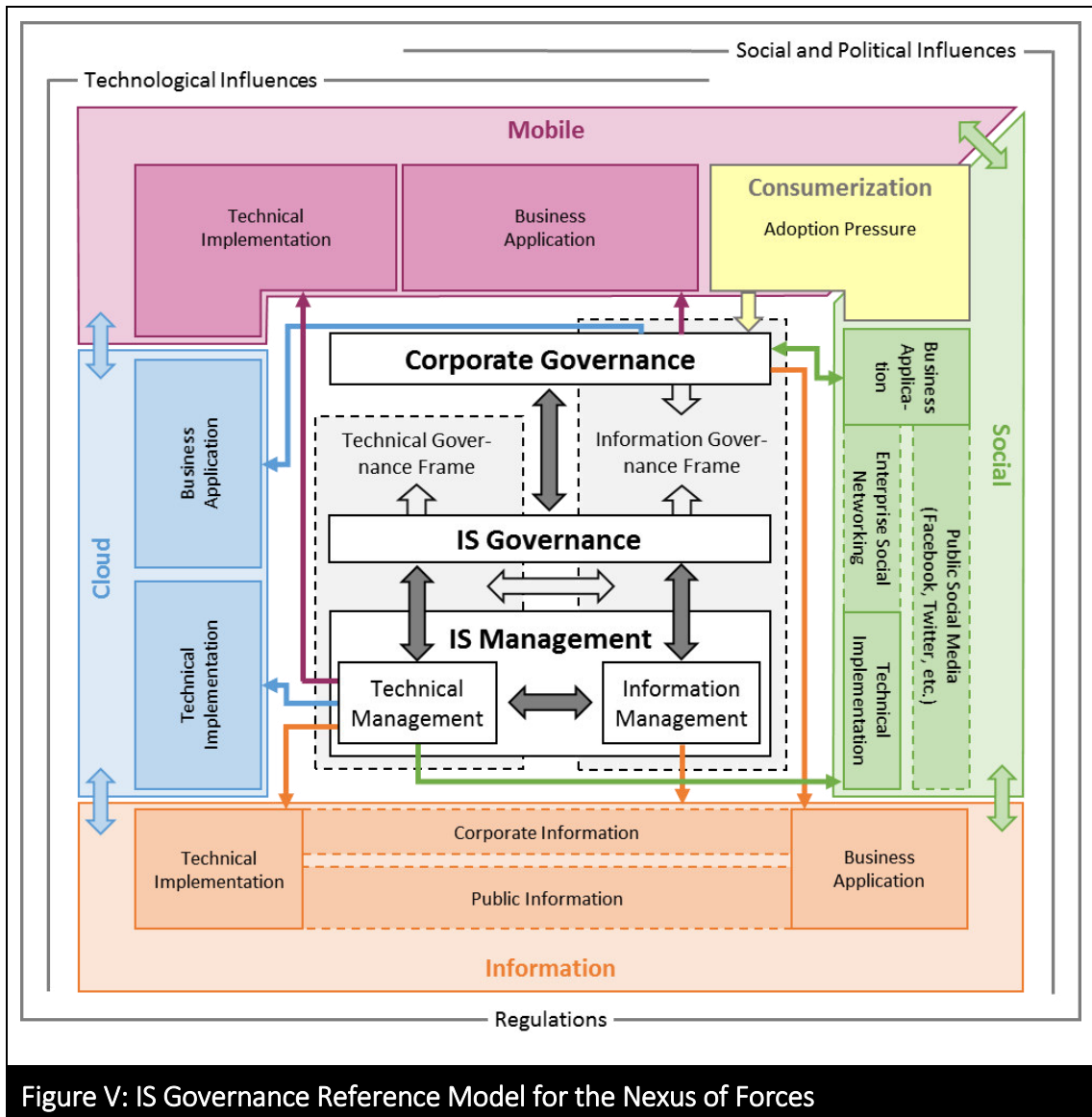


Figure V: IS Governance Reference Model for the Nexus of Forces

The results of this cumulative dissertation address two objectives. On the one hand these results contribute to research in the area of employees' information security awareness and behavior. On the other hand, findings of this dissertation provide guidance for practitioners in the context of implementing sustainable information security measures that take the role of employees' into account. Various research methods were applied in order to investigate several fields in the area of employees' information security awareness and behavior as well as the impact of consumerization of IT in the context of organizational information security. A multi-method research process was applied, incorporating qualitative and quantitative research methods that aimed at producing reliable results within the complex and multidimensional field of information security. Moreover, the research process included both main criteria of high quality IS research: rigor and relevance. In order to ensure methodological rigor, research methods that are

established in the field of IS research were selected and executed by considering general accepted guidelines. The focus on topics that are inspired from practical problems aimed at enhancing the practical relevance. This was accomplished by by identifying research gaps not only by reviewing academic literature but also by considering practical literature, e.g. market research studies.

III. Table of Contents

I. ABSTRACT	2
II. MANAGEMENT SUMMARY	3
III. TABLE OF CONTENTS	12
IV. TABLE OF FIGURES	15
V. LIST OF TABLES.....	16
VI. LIST OF ABBREVIATIONS.....	17
0. OVERVIEW OF PUBLICATIONS.....	20
1. INTRODUCTION	1
1.1 MOTIVATION AND PROBLEM DEFINITION.....	1
1.2 RESEARCH QUESTIONS	4
1.3 STRUCTURE OF THE DISSERTATION.....	7
2. THEORETICAL BACKGROUND	9
2.1 BEHAVIORAL THEORIES.....	9
2.1.1 <i>Theory of Reasoned Action / Theory of Planned Behavior</i>	9
2.1.2 <i>Technology Acceptance Model</i>	10
2.1.3 <i>Protection Motivation Theory</i>	10
2.1.4 <i>General Deterrence Theory</i>	11
2.2 LEADERSHIP THEORIES.....	12
2.2.1 <i>Leadership in IS Security Research</i>	12
2.2.2 <i>Transactional Leadership</i>	14
2.2.3 <i>Transformational Leadership</i>	15
2.3 IS GOVERNANCE	16
2.3.1 <i>Definition and Scope of IS Governance</i>	16
2.3.2 <i>IS Governance Forms and Contingencies</i>	18

3. RESEARCH METHODOLOGY.....	20
3.1 RESEARCH METHODS IN INFORMATION SYSTEMS	20
3.2 ACTION (DESIGN) RESEARCH	21
3.3 SURVEYS.....	23
3.3.1 <i>Exploratory Factor Analysis and Principle Component Analysis</i>	24
3.3.1 <i>Structural Equation Modeling</i>	24
3.3.2 <i>Partial Least Squares</i>	26
3.4 DELPHI METHOD	27
3.4.1 <i>Qualitative Interviews</i>	28
3.4.2 <i>Qualitative Content Analysis</i>	29
4. EMPLOYEES' INFORMATION SECURITY AWARENESS AND BEHAVIOR.....	30
4.1 LITERATURE ANALYSIS	30
4.1.1 <i>Motivation and Purpose</i>	31
4.1.2 <i>Research Design</i>	32
4.1.3 <i>Findings</i>	34
4.1.4 <i>Limitations</i>	37
4.1.5 <i>Conclusion</i>	38
4.2 TRANSFORMATIONAL LEADERSHIP AND EMPLOYEES' SECURITY PERFORMANCE	39
4.2.1 <i>Motivation and Purpose</i>	39
4.2.2 <i>Theoretical Background</i>	40
4.2.3 <i>Research Design and Data Collection</i>	42
4.2.4 <i>Discussion of Results and Implications</i>	44
4.2.5 <i>Limitations</i>	45
4.2.6 <i>Conclusion</i>	46
4.3 A NEEDS ASSESSMENT PROCESS FOR SETA PROGRAMS	47
4.3.1 <i>Motivation and Purpose</i>	47
4.3.2 <i>Research Design</i>	48
4.3.3 <i>Results</i>	50
4.3.4 <i>Discussion</i>	51
4.3.5 <i>Limitations</i>	53
4.3.6 <i>Conclusion</i>	54

5.	CONSUMERIZATION OF IT AND ORGANIZATIONAL INFORMATION SECURITY ..	56
5.1	EMPLOYEES' ACCEPTANCE OF BYOD MOBILE DEVICES.....	56
5.1.1	<i>Motivation and Purpose</i>	<i>56</i>
5.1.2	<i>Theoretical Background</i>	<i>57</i>
5.1.3	<i>Research Design and Data Collection</i>	<i>59</i>
5.1.4	<i>Discussion of Results and Implications</i>	<i>60</i>
5.1.5	<i>Limitations</i>	<i>62</i>
5.1.6	<i>Conclusion</i>	<i>62</i>
5.2	AN IS GOVERNANCE REFERENCE MODEL FOR THE NEXUS OF FORCES.....	64
5.2.1	<i>Motivation and Purpose</i>	<i>64</i>
5.2.2	<i>Research Design</i>	<i>65</i>
5.2.3	<i>Findings</i>	<i>67</i>
5.2.4	<i>Discussion.....</i>	<i>69</i>
5.2.5	<i>Limitations</i>	<i>71</i>
5.2.6	<i>Conclusion</i>	<i>72</i>
6.	OVERALL CONCLUSION	73
6.1	SUMMARY OF RESULTS AND IMPLICATIONS	73
6.1.1	<i>Employees' Information Security Awareness and Behavior</i>	<i>73</i>
6.1.2	<i>Consumerization of IT and Organizational Information Security</i>	<i>75</i>
6.2	OVERALL LIMITATIONS	77
6.2.1	<i>Application of Various Research Methods.....</i>	<i>77</i>
6.2.2	<i>Rigor and Relevance.....</i>	<i>78</i>
6.3	OUTLOOK	81
	REFERENCES.....	84
	APPENDICES.....	104