Contributions to Organizational Information Security

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 Benedikt Lebek
geboren am 01. August 1985 in Peine

2015

Betreuer und Gutachter:	Prof. Dr. Michael H. Breitner
Weiterer Gutachter:	Prof. Dr. Jan Muntermann
Vorsitzender der Prüfungskommission:	Prof. Dr. Hans-Jörg von Mettenheim
Weiteres Mitglied (beratend):	Dr. Ute Lohse
Tag der Promotion:	07.05.2015

Meiner Familie.

I. Abstract/Abstrakt

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 adresses 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 persue 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.

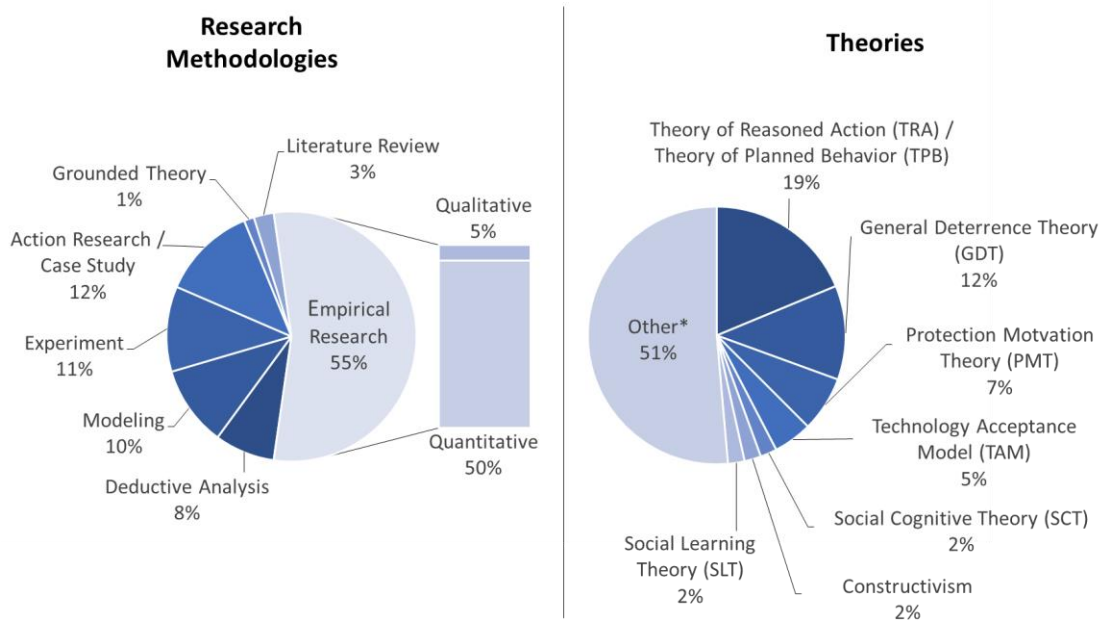
Keywords: *Employees' Information Security Awareness and Behavior* | *Security Education, Training and Awareness* | *Consumerization of IT* | *Bring Your Own Device* | *IT Governance* | *Nexus of Forces*

Aufgrund der Zunahme von komplexen und multinationalen Bedrohungen für die Informationssicherheit, stehen Unternehmen vor der Herausforderung, effiziente und nachhaltige Informationssicherheitsprogramme zu etablieren. Ziel dieser kumulativen Dissertation ist es einen Beitrag zur Informationssicherheits-Forschung zu leisten. Sie fokussiert vor allem das Informationssicherheitsbewusstsein und -verhalten von Mitarbeitern in Bezug auf Informationssicherheit. Zwei Forschungsziele werden in dieser Arbeit verfolgt. Das erste Ziel bezieht sich auf das Informationssicherheitsbewusstsein und -verhalten von Mitarbeiter im Allgemeinen und basiert auf einer umfassenden Überprüfung und Analyse bisherigerer Studien im betrachteten Forschungsfeld innerhalb der letzten zehn Jahre. Durch die Integration des Konzepts der transformationalen Führung, wird der Einfluss von Vorgesetzten und Managern auf Sicherheitsbewusstsein und -verhalten von Mitarbeitern untersucht. Darüber hinaus wird ein systematischer Ansatz für die Erfassung, Bewertung und Darstellung des tatsächlichen Informationssicherheitsverhaltens von Mitarbeitern in realen Arbeitsumgebungen präsentiert. Das zweite Ziel betrachtet die Auswirkungen der “Consumerization” der IT auf die Organisation der Informationssicherheit in Unternehmen. In diesem Zusammenhang wird zunächst der Einfluss von Sicherheits-, Datenschutz- und rechtlichen Bedenken auf die Akzeptanz des Bring-Your-Own-Device Konzepts durch Mitarbeiter untersucht. Anschließend wird das übergreifende Konzept der “Consumerization” der IT betrachtet. Es werden die Auswirkungen der neuen Technologien Mobile-, Social- und Cloud-Computing sowie Big Data auf IS Governance als Rahmen für die Organisation der Informationssicherheit in Unternehmen untersucht. Um die Forschungsziele zu verfolgen wurde ein Multi-Methoden Forschungsansatz gewählt, der Methoden aus den quantitativen und der qualitativen Forschungsparadigmen enthält. Durch die Anwendung von Forschungsmethoden, die auf dem Gebiet der Informationssystem-Forschung etabliert sind, wird akademische rigorosität sichergestellt. Durch die Konzentration auf Themen, die von praktischen Problemen inspiriert sind wird die praktische Relevanz dieser Arbeit verstärkt.

Schlagworte: *Informationssicherheitsbewusstsein und -verhalten von Mitarbeitern | Informationssicherheits-Bildung, -Training und Bewusstsein | Consumerization der 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 form 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-



* theories applied in only one study (incl. studies that applied no theories)

Figure I: Application of Research Methods and Theories within Analyzed Literature

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.

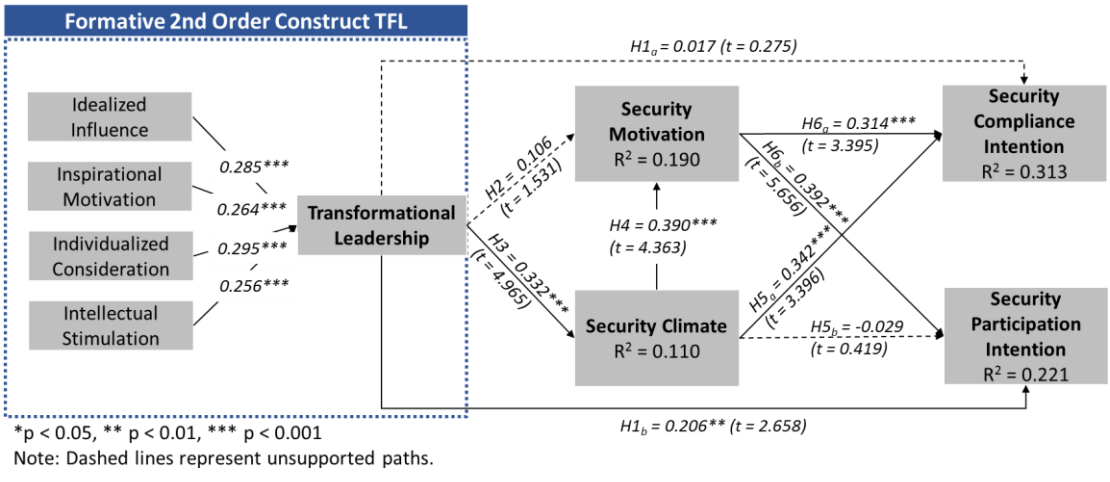


Figure II: Transformational Leadership and Employees' Security Performance

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 safe 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).

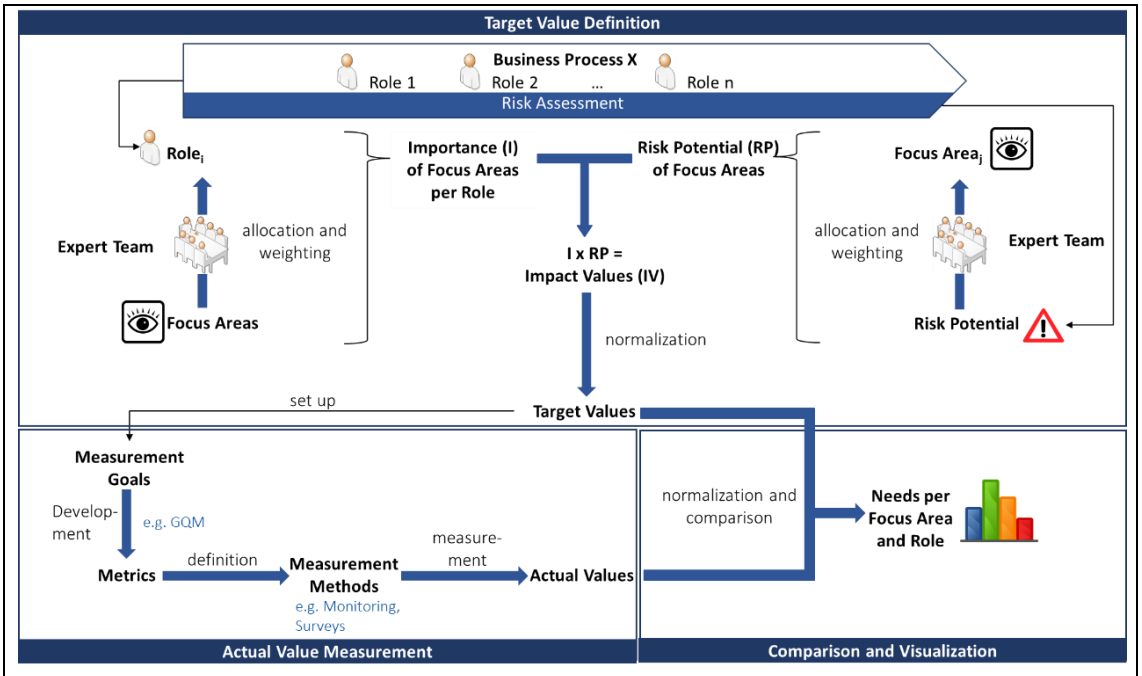


Figure III: Proposed Needs Assessment Process

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 Asessment 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.

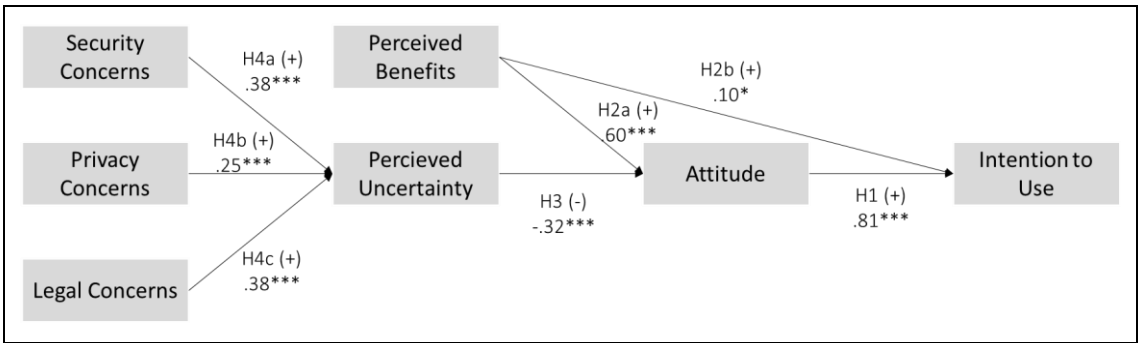


Figure IV: Percieved Concerns and Employees' Acceptance of BYOD

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.

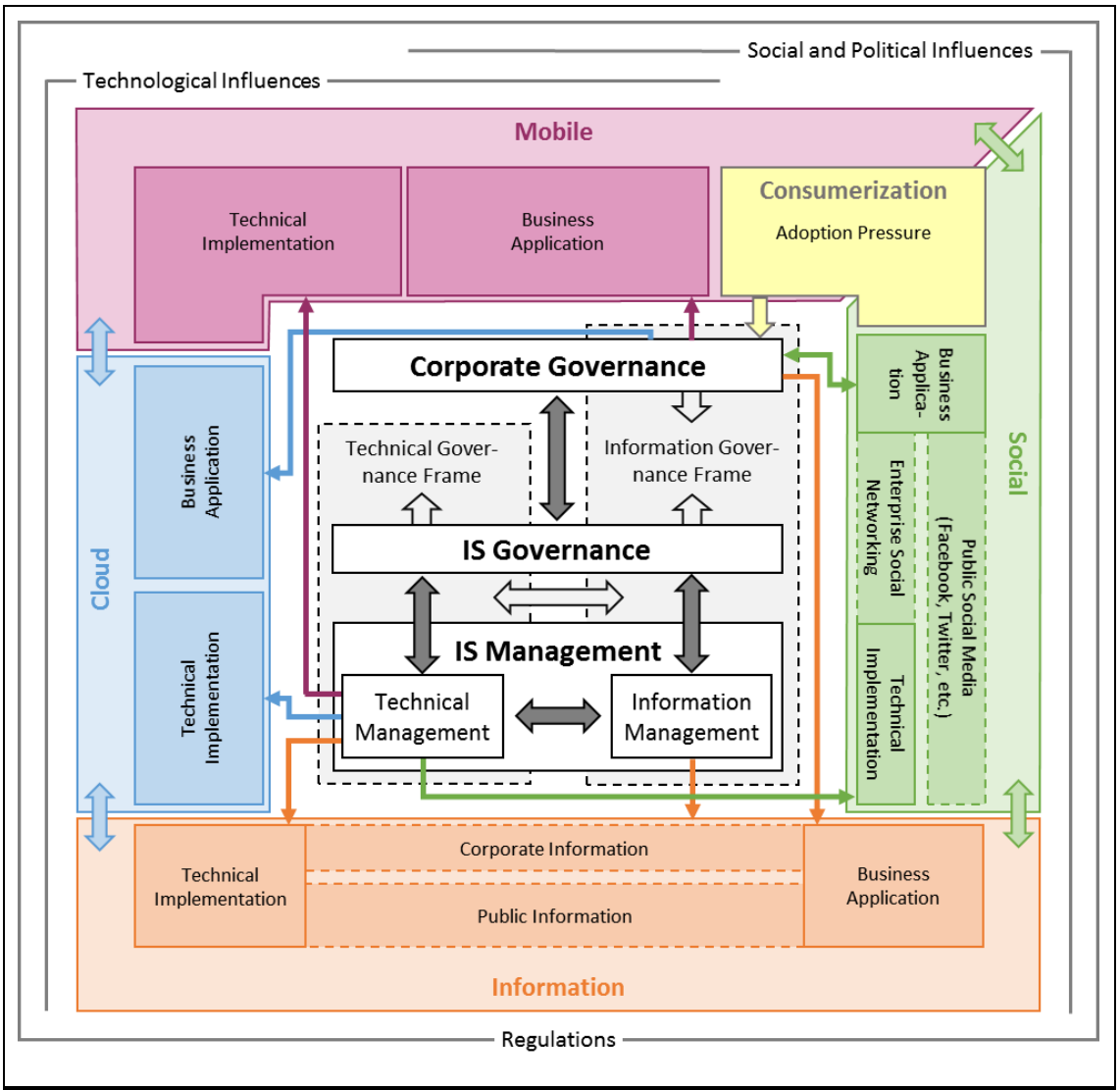


Figure V: IS Governance Reference Model for the Nexus of Forces

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

IV. Table of Figures

V. List of Tables

VI. List of Abbreviations

ADR	Action Design Research
AMCIS	Americas Conference on Information Systems
AR	Action Research
ATT	Attitude
AVE	Average Variance Extracted
BYOD	Bring Your Own Device
CA	Coping Appraisal
cf.	compare
CFA	Confirmatory Factor Analysis
CIO	Chief Information Officer
COBIT	Control Objectives for Information and Related Technology
CR	Composite Reliability
DSR	Design Science Research
e.g.	exempliy gratia / for example
ECIS	European Conference on Information Systems
EFA	Exploratory Factor Analysis
et al.	et alia
GDT	General Deterrence Theory
GI-FB WI	Gesellschaft für Informatik –Fachbreich Wirtschaftsinformatik
HICSS	Hawaii International Conference on System Sciences

i.e.	id est / that is to say
ICIS	International Conference on Information Systems
Inc.	Incorporated.
IS	Information Systems
ISO	International Organization for Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library
MKWI	Multikonferenz Wirtschaftsinformatik
PBC	Perceived Behavioral Control
PBC	Perceived Behavioral Control
PCA	Principal Component Analysis
PCOS	Percieved Certainty of Sanctions
PEOU	Perceived Ease of Use
PLS	Partial Least Squares
PMT	Protection Motivation Theory
PSOS	Percieved Severity of Sanctions
PSOT	Perceived Severity of Threats
PU	Perceived Usefulness
PV	Perceived Vulnerability
RC	Response Costs
RE	Response Efficacy
S	Sanctions
SEM	Structural Equation Modeling
SETA	Security Education, Training and Awareness
SN	Subjective Norm

TA	Threat Appraisal
TAM	Technology Acceptance Model
TPB	Theory of Planned Behavior
TRA	Theory of Reasoned Actions
VHB	Verband der Hochschullehrer für Betriebswirtschaft
WKWI	Wissenschaftliche Kommission Wirtschaftsinformatik

0. Overview of Publications

The author began to examine the role of employees in the context of organizational information security during the preparation of his diploma thesis at the Institute for Information Systems Research at the Gottfried Wilhelm Leibniz Universität Hannover in, 2011. It was entitled “Rechtliche Grenzen und ethische sowie moralische Bedenken der automatischen Identifikation unternehmensschädlicher Handlungen” (Engl.: “Legal and ethical boundaries as well as moral issues of automatic insider threat identification and prediction”). With a focus on legal compliance of the (IT) risk management, in this work a conceptual model for the automated identification and prevention malicious actions by employees is presented, that takes the German data protection law and employee participation rights as well as ethical and moral concerns into account. The work was refinded and published in the proceedings of the “Multikonferenz Wirtschaftsinformatik (MKWI)” in 2012 (cf. Appendix A1).

In the next step, a systemeatic and comprehensive literature search and analysis in the research field of employees’ information security awareness and behavior was conducted to provide a solid basis for the further reaserach process and the resulting publications. The results of the literature review were initailly presented at the “Hawaii International Conference on System Sciences (HICSS)” and published in the proceedings in 2013 with the title “Employees’ Information Security Awareness and Behavior: A Literature Review” (cf. Appendix A2). Subsequently, the work was extended, updated and refined for the publication in the journal “Management Research Review (MRR)” in, 2014 (cf. Appendix A6). In this work, four multidisciplinary behavioral theories form psychology, sociology, and criminology were identified to be mainly used within the research domain of employees’ information security awareness and behavior. Grounded on indepth analyses, gaps in existing research were uncovered and implications for further research were worked out. As a result the following two major findings became appearant.

First of all, the contemplated research domain is strongly focused on theoretically grounded explanations for employees' information security awareness and behavior. Consequently, a generally accepted approach that adresses organizational requirements is missing. Practitioners face the problem of how to adapt theoretical explanations for employees' behavior in order to establish and manage efficient and sustainable security education, training and awareness (SETA) programs within organizations. To adress this gap, a systematic approach to capturing, evaluating, and depicting the current state of employees' security awareness and behavior within organizations was developed. The results of this work, entiteled "Towards a Needs Assessment Process Model for Security, Education, Training and Awareness Programs - An Action Design Research Study" were presented at the "European Conference on Information Systems (ECIS)" and published in the proceedings in 2013 (cf. Appendix A4).

Secondly, most research in the area of employees' information security awareness and behavior is solely focused on the employees' perpective and does not consider the influence of leadership. Therefore, the potential impact of transformational leadership as a form of management leadership on employees' information security behavior was found worthy to investigation. A research model was developed and empirically tested by means of structural equation modeling (SEM). The findings presented under the title "Transformational Leadership and Employees' Information Security Performance: The Mediating Role of Motivation and Climate" at the "Internation Conference on Information Systems (ICIS)" in 2014 and are published in the conference proceedings (cf. Appendix A8).

As the continuing consumerization of IT leads to a paradigm shift with regard to organizational information security and is strongly influencing employees' role within the information security chain, this aspect was also considered within the herein described research process. At first, the influence of security, privacy and legal concerns on employees' willingness to adapt to the Bring-Your-Own-Device (BYOD) concept was examined. Therefore, a research model based on the Technology Acceptance Model (TAM) and the Theory of Reasoned Action (TRA) was developed and empirically tested using SEM. The results of this study, entiteled "Investigating the Influence of Security, Privacy, and Legal Concerns on Employees' Intention to Use BYOD Mobile Devices" was presented at the "Americas Conference on Information Systems (AMCIS)" and published in

the Proceeedings in 2013. The paper is one of five papers that were awarded with the "Best Conference Paper Award" (cf. Appendix A3).

Based on this work, a qualitative interview study was conducted in order to examine employees' perception of advantages and disadvantages of the BYOD concept. This paper was entiteled "Vor- und Nachteile von Bring Your Own Device (BYOD) aus Mitarbeitersicht: Eine qualitative Analyse von Interviews" (Engl.: "Advantages and disadvantages of Bring Your Own Device (BYOD) from employees' perspective: A qualitative analysis of interviews") and was presented at the "Multikonferenz Wirtschaftsinformatik" and published in the proceedings in 2014 (cf. Appendix A5).

In strong context to BYOD is the concept of consumerization. Consumerization describes the use technologies for working purposes that were primarily designed for private use. This includes in addition to mobile devices, technologies and services like social media and cloud services. The pressure that is exerted by the consumerization trend forces organizations to adopt these new technologies. Adding information as a fourth component, mobile, cloud and social computing are reffered to as the Nexus of Forces by Gartner (2012) and are expected to have a novel and lasting impact not only on organzations but also on IS governance as the framework for organizational information security strategies. In order to investigate this impact a qualitative study was conducted and submitted to the "Journal of the Association for Information Systems" (JAIS) in 2014 with the title "An IS Governance Reference Model for the Nexus of Forces" (cf. Appendix A7).

Table 1: Overview of Publications

Publication Date	Titel	Authors	Conference/Journal	VHB / WKWI*	VHB / JQ2.1**	JQ2.1** Index value	Chapter	Appen-dix
2012	Rechts- und ethikkonforme Identifikation von unternehmensschädlichen Handlungen durch semiautomatisierte Prozesse	B. Lebek, S. Hoyer, H. Zakhariya, M.H. Breitner	Tagungsband Multikonferenz Wirtschaftsinformatik (MKWI 2012), Braunschweig, Deutschland, pp. 971-982.	C	D	5,44	-	A1
2013	Employees' Information Security Awareness and Behavior: A Literature Review	B. Lebek, J. Uffen, M. Neumann, B. Hohler, M.H. Breitner	Proceedings of the Hawaii International Conference on System Sciences (HICSS 2013), Maui, HI, USA, pp. 2978 - 2987	B	C	6,44	4.1	A2
2013	Investigating the Influence of Security, Privacy, and Legal Concerns on Employees' Intention to Use BYOD Mobile Devices	B. Lebek, K. Degirmenci, M.H. Breitner	Proceedings of the Americas Conference on Information Systems (AMCIS 2013), Chicago, IL, USA, Paper 8. (Winner of Best Conference Paper Award)	B	D	5,92	5.1	A3
2013	Towards a Needs Assessment Process Model for Security, Education, Training and Awareness Programs - An Action Design Research Study	B. Lebek, J. Uffen, M. Neumann, B. Hohler	Proceedings of the European Conference on Information Systems (ECIS 2013), Utrecht, Netherlands, Paper 110.	A	B	7,37	4.3	A4
2014	Vor- und Nachteile von Bring Your Own Device (BYOD) aus Mitarbeitersicht: Eine qualitative Analyse von Interviews	B. Lebek, V. Vogel, M.H. Breitner	Tagungsband Multikonferenz Wirtschaftsinformatik (MKWI 2014), Paderborn, Deutschland, pp. 1234-1246.	C	D	5,44	-	A5
2014	Information Security Awareness and Behavior: A Theory-based Literature Review	B. Lebek, J. Uffen, M. Neumann, B. Hohler, M.H. Breitner	Management Research Review, Vol. 37, No. 11.	-	C	6,69	4.1	A6
2014	Big Data, Social, Mobile, and Cloud Computing: A Reference Model for IS Governance and the Nexus of Forces	B. Lebek, T.A. Rickenberg, M.H. Breitner	Submitted to: Journal of the Association for Information Systems (JAIS).	B	B	7,96	5.2	A7
2014	Transformational Leadership and Employees' Information Security Performance: The Mediating Role of Motivation and Climate	B. Lebek, N. Guhr, M.H. Breitner	International Conference on Information Systems (ICIS 2014), Auckland, New Zealand.	A	A	8,48	4.2	A8

* Assignment by the "Wissenschaftliche Kommission Wirtschaftsinformatik im Verband der Hochschulllehrer für Betriebswirtschaft e. V." and the "Fachbereich Wirtschaftsinformatik der Gesellschaft für Informatik" in the WI-Orientationlists, cf. WKWI and GI-FB WI (2008)
** cf. VHB-JOURQUAL 2.1 (2011)

1. Introduction

1.1 Motivation and Problem Definition

Today's organizations operate in an electronically interconnected world that allows to execute global business transactions around the clock. Although organizations benefit from technological advances, fast communication, unlimited information and the extremely fast execution of business processes and financial transactions also provide new challenges for information security. Since breaches to information security cause hundreds of billions US Dollars in of annual worldwide economic damage (D'Arcy et al. 2009; D'Arcy and Hovav 2011), information sytstems (IS) security has become critically important and is considered to be one of the top management priorities (Kirsch and Boss 2007; Bulgurcu et al. 2010; D'Arcy and Herath 2011; Herath and Rao 2009b). Organizations commonly focus on external threats to information security, like hacking and cyber-espionage. Consequently, organizations mainly rely on technical solutions like firewalls, anti-virus software, and data loss prevention (DLP) tools in order to mitigate these threats to information security (Boss et al. 2009; Bulgurcu et al. 2010). However, many serious IS security breaches originate from the inside of organizations due to employees' failure or unwillingness to comply with basic security procedures (Siponen and Vance 2010; Karjalainen and Siponen 2011). This includes the misuse of priveleges by insiders, the loss of hardware and miscellaneous errors by endusers (Verizon, 2014). According to a market study by IDC (2011), employees are considered to be the weakest link in the information security chain by 50% of the surveyed organizations (Figure 1). On the one hand, security breaches by insiders are monetarily costly since legal actions and fines may ensue. On the other hand, organizations also face damages that can not be monetarily quantified (CSO magazine, 2011). For example, the reputation of an organization may be negatively affected since customers and business partners lose

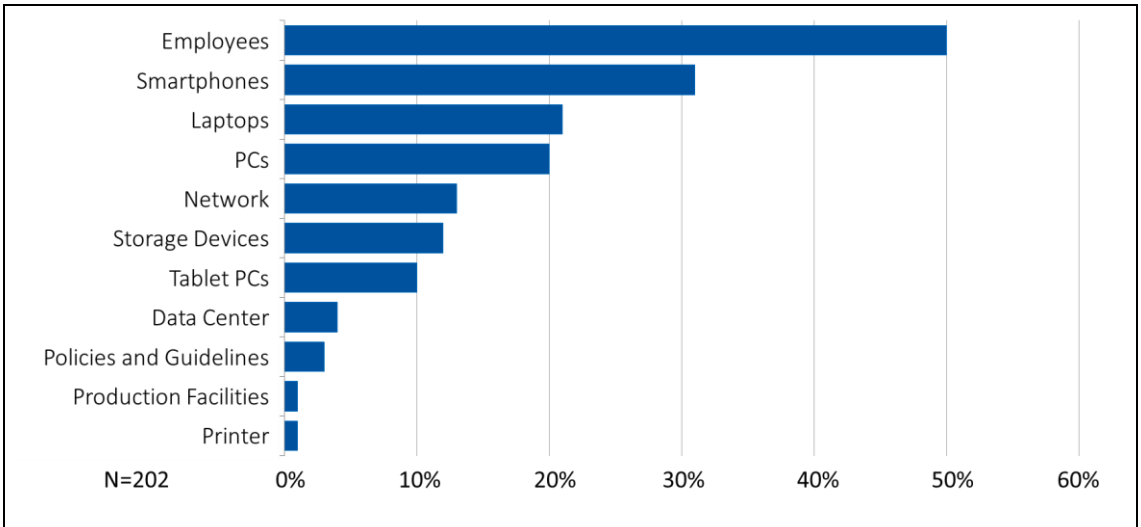


Figure 1: The Weakest Link in the Information Security Chain (IDC, 2011)

the confidence in an organizations ability to protect confidential or proprietary information (Verizon, 2014). By considering the human component technological measures alone are insufficient in order to guarantee information security. Therefore organizations also establish "other formal and informal control mechanisms, including policies, procedures, organizational culture, and the role individuals play in security" (Herath and Rao 2009b). Information security policies aim to provide employees with guidelines on how to ensure information security in the course of performing their jobs (Bulgurcu et al. 2010). However, the existence of such policies is not sufficient to ensure an adequate level of information security. The lack of employees' awareness of the importance of security practices and noncompliant behavior due to employees' ignorance of security policies, constitutes a major problem for organizations as it can render security efforts ineffective (Herath and Rao 2009b). In this context, not only the design of security policies, but also the motivation of individuals to follow those policies is of high importance (Boss et al. 2009). In order to promote security policies to employees, security education, training, and awareness (SETA) programs have garnered increasing attention. Not only market research studies, but also academic research studies emphasize the importance and the role of employees within the context of organizational information security (e.g., Spears and Barki 2010; Siponen et al. 2006). In order to explain and predict employees' security-related behavior and awareness, academic studies have adopted diverse theories from e.g. social psychology and criminology to a research field that is characterized by quantitative empirical research. However, practitioners face the problem of how the theoretical constructs that were found to be determining employees'

behavior can be used for ensuring efficient and sustainable information security within organizations. As a result, and due to the complex nature of the information security domain a gap between theoretically founded explanation of employees' security behavior and the need of practitioners to know which interventions to apply can be identified (Workman et al. 2008).

Advances in technology provide constantly changing challenges for organizational information security. For example, the advantages of recent trends like mobile, social and cloud computing are accompanied by various new threats to information security. The increasing use of mobile computing devices (e.g. smartphones, tablets PCs) within organizations entails a steadily growing risk for information security. According to IDC (2011), smartphones provide the second highest threat to organizational information security next to employees (Figure 1). In a recent study by KPMG (2013), the use of mobile communication was identified as the top threat to information security (64%) by the surveyed organizations. This is attributed to the fact that smartphones and other mobile devices are permanently connected to the internet, are storing a large amount of data and are linked to social media. The risks entailed by the use of smartphones and the associated mobilization of the workplace underline the importance of emplyoees' information security awareness and behavior. This is amplified when it comes to the use of privately owned mobile devices for working purposes. This concept, known as Bring-Your-Own-Device (BYOD) challenges organizations as legal and technical restrictions impede the effective and sustainable protection of organizational data.

Looking at the mentioned trends as a whole, it becomes apparent that the associated proliferation of threats to organizational information security demands for an augmentation of risk management. In this context IS governance as the paramount framework for information security management becomes a focal point in order to "create means of recognizing capturing, assessing and testing human factor implications" (Colwill, 2010). However, organizational governance structures and especially IS governance is challenged by the advancing consumerization of IT and the inherent emancipation of and a shift of power towards the employees as users of information systems. Moreover, new technological developments in the areas of mobile, social and cloud computing as

well as advances regarding the analysis of big amounts of data represent an interconnected set of current trends ("the Nexus of Forces", Gartner Inc., 2013) that provide novel and unique challenges for IS governance and organizations as a whole. As a result, organizational information security strategies must be flexible and agile in order to adapt the constantly evolving risk environment (KPMG, 2011). The research process described in the dissertation mainly focuses on employees' behavior in the context of organizational information security. Morover, the influences of the new trends BYOD and the Nexus of Forces are considered to broaden the scope of the research.

1.2 Research Questions

In order to contribute to the research field and to provide implications for practitioners the herein described cumulative research process approaches five research questions that deal with the role of employees' within the organizational information security chain. To provide a solid basis for the research project presented in this dissertation, a structured literature review was conducted in the first place with the purpose to uncover areas where research is needed (Webster and Watson, 2002). A literature review is considered to be a fundamental and essential first step for every research project (Hart, 1999; Webster and Watson, 2002; vom Brocke et al., 2009). It helps to assure relevance and rigor of research as it helps to avoid to reinvestigate what is already known and facilitates the effective usage of an existing knowledge base (vom Brocke et al., 2009). Aditionally, a literature review does not only uncover research gaps, but "will provide the researcher with the framework for their own work; this includes methodological assumptions, data-collection techniques, key concepts and structuring the research into a conventional academic dissertation" (Hart, 1999). Levy and Ellis (2006) defined four characteristics that are neccesarry for an effective literature review: (1) methodological analysis and synthetisis of quality literature, (2) provision of a foundation for a certain research topic, (3) justification for the selection of the research methodology and (4) demonstration of the research contribution. In order to fullfill these requirements and since literature reviews are important in any scholarship and in IS in particular (vom Brocke et al., 2009), the following first research question is proposed:

RQ1: Which theories have been recently used in IS literature to explain employees' security related awareness and behavior?

In the course of the literature review it became apparent, that although organizations mainly focus on technology-based solutions in otder to mitigate threats to information security (Boss et al. 2009, Bulgurcu et al., 2010), "other formal and informal control mechanisms, including policies, procedures, organizational culture, and the role individuals play in security" (Herath and Rao 2009b) become more and more important. IS researchers focused on employees' compliance to organizational information security policies and aimed to identify ways to motivate employees' to follow those policies (Boss et al., 2009). For this purpose, theories from social psychology and criminology were adopted to IS literature (Mishra and Dhillon, 2005). In addition to focusing on employees' perspective within the context of information security, IS security researchers also began to investigate the impact of differences in management (Uffen et al. 2012). However, the results of the literature review revealed lack of studies considering established leadership theories in the context of employees' information security behavior. Therefore, in the second step of this dissertation, the concept of transformational leadership was adopted to the contemplated research field and the following research question proposed:

RQ2: How does transformational leadership influence employees' information security performance?

Research in the field of employees' information security behavior is primarily focused on the assessment and prediction of employees' information security policy compliance by using behavioral theories. However, in academic literature it has been debated for a long time how to enhance the relevance of the output of IS research while mainaining a high standard of methodological rigor (e.g. Davenport and Markus, 1999, Lee 1999). In this context, Benbasat and Zmud (1999) state that "IS researchers should look to practice to identify research topics and look to IS literature only after a commitment has been made to a specific topic". According to the authors, this would help enhance value for practitioners while conducting applied theoretical research. Davenport and Markus (1999) underline the suitability of evaluation research as an alternative for ap-

plied theory research. Within a research project in cooperation with a German engineering company, it was discoverd, that a generally accepted approach to capture the actual level of employees' security awareness and behavior is missing. This is of importance especially in the context of the development and implementation of security education, traning, and awareness (SETA) programms, which demands for the execution of a needs assessment (cf. NIST SP-800-50). In order to adress this practical gap with a rigorous academical approach, the third research question is proposed:

> *RQ3: What are the design principles for developing and implementing a needs assessment process for SETA programs that considers an organization's individual context?*

One of the most disruptive trends that occurred in field of information systems within the past decade is the consumerization of IT. Consequently, this dissertation addresses this important topic in the second section of the main part. Information security issues in the context of consumerization are a major concern for organizations, since organizations face the problem of establishing effective security guidelines for employee owned hardware (Niehaves et al., 2012). The concept of bring your own device (BYOD) is a particular form of consumerization of IT (Niehaves et al., 2012) that is often linked to advantages for employees and organizations. These advantages encourage organizations to adopt the BYOD concept. A precondition for a successful BYOD implementation is employees' acceptance, because an implementation usually depends on employees' voluntary participation. However, employees' acceptance is not only dependent on employees' perceived benefits, but is also impacted by employees' perceived concerns (Oliver and Bearden, 1985). In practice, concerns regarding security, privacy, and legal aspects of BYOD are discussed (e.g. Miller et al., 2012; Osterman Research, 2012; Silvergate and Salner, 2011). Since the examination of these concerns found little attention in previous studies (Niehaves et al., 2012) the following research question is proposed:

> *RQ4: To which degree do security, privacy, and lega concerns affect employees' intention to use BYOD mobile devices?*

By empowering indiciduals in their interaction with each other and the associated information, the interconnected trends of mobile, social and cloud computing impact organizations through consumerization pressure. These trends in combination with big data are referred to as the 'Nexus of Forces' (Gartner, 2013). Through a shift of power towards and emancipation of the user, organizational control mechanisms such as IS governance are challenged. Organizations aim to maximize the Nexus' benefits while mitigating the associated risks. A demand for a robust framework to govern these technologies arises. Although, several recent studies addressed IS governance in the context of one of the trends social, mobile, and cloud computing or big data analytics (e.g. van Osch and Coursaris 2013; Heier et al. 2012), the interconnections among the four individual forces provide novel challenges for IS governance. To address this gap the following research question is proposed:

> *RQ5: How do the new challenges of big data, social, mobile, and cloud computing influence IS governance?*

1.3 Structure of the Dissertation

The prupose of this cumulative dissertation is to investigate the role of employees within the organizational information security chain. The dissertation is structured as depicted in Figure 2. Chapter 0 provides an initial overview of the single publications that constitute this dissertation. The introduction in chapter one motivates the overall goal of the described research and defines the underlying research problem. Furthermore, the central research questions that are addressed within the single publications of this cummulaitive research are derived within the first chapter.

The second chapter provides the theoretical background for the main part of this dissertation in order to guarantee a common understanding and terminology. This includes the introduction and explanation of underlying behavioral theories, leadership theories and as brief definition of IS governance. Since various research methods are applied within the course of this dissertation, chapter three provides an overview and describtion of the used design oriented (action design research), quantitative (survey), and qualitative (Delphi) approaches.

The chapters four and five constitute the main part of the dissertation and discuss the results of five major publicatons. Chapter four refers to studies within the context of employees' information security awareness and behavior, whereas chapter five examines information security within the context of consumerization. In chapter six the overall limitations of this dissertation are outlined before chapter seven summarizes the overall results and presents directions for future research.

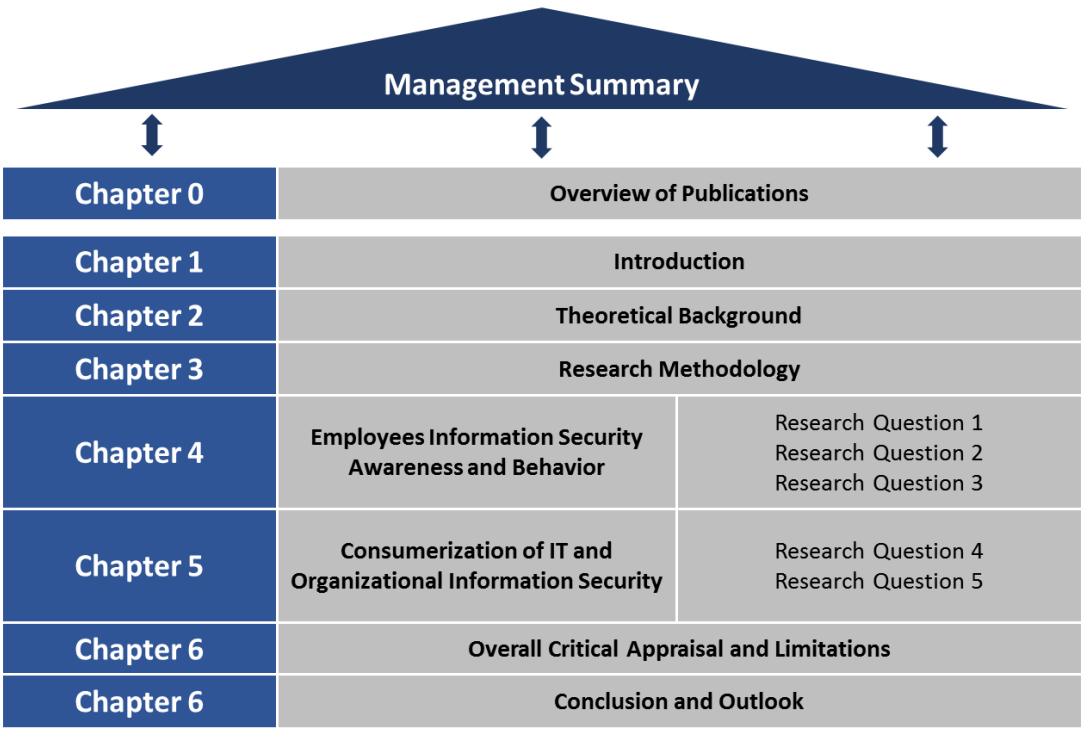


Figure 2: Structure of the Dissertation

2. Theoretical Background

2.1 Behavioral Theories

2.1.1 Theory of Reasoned Action / Theory of Planned Behavior

Founded by Fishbein and Ajzen (1975), the theory of reasoned action postulates, that a person's behavioral intention depends on his or her subjective norm and attitude towards a certain behavior. Subjective norm consists of the beliefs about the normative expectations of other people regarding a certain behavior. The attitude construct reflects the outcome of the evaluation of expected consequences of performing a certain behavior. By adding the construct of perceived behavioral control, the theory of planned behavior (Ajzen, 1985 & 1991) expands the theory of reasoned action in order to improve its predictive power. The perceived behavioral control construct originates from Bandura's (1982) work on self-efficacy. Self-efficacy is defined as a person's subjective conviction of possessing the skills and knowledge to perform a certain behavior (Ajzen, 1988).

In the context of employees' information security awareness and behavior, researchers emphasize the use of employees' behavioral intention to comply with organizational information security policies as a predictor of employees' actual behavior (e.g., Limayem and Hirt, 2003; Siponen et al., 2007; Ifinedo, 2012) due to certain difficulties with observing actual security compliant behavior (Vroom and von Solms, 2004). The use of behavioral intention as a proximal cognitive antecedents of actual behavior in information security research is mainly justified as researchers demonstrated a strong and consistent relationship between the two constructs in non-information security context (e.g. Venkatesh et al., 2003; Webb and Sheeran, 2006).

2.1.2 Technology Acceptance Model

Based on the Theory of Reasoned Action, the Technology Acceptance Model was originally introduced by Davis (1989). It applies intention to use as the key dependent varialble to describe users' assceptance of IT. The most immediate of intention to use is attitude, which is defined as a subjective evaluation of an individuals' positive or negative feelings about the adoption of a technology (Davis et al, 1989). Moreover, the TAM postulates that perceived usefulness and perceived ease of use are antecedents of technology acceptance. Perceived usefulness is defined as the subjective perception that a specific technology or system is capable of of being advantageous with regard to job performance (Davis et al., 1989). Perceived ease of use measures the degree to which users' expect that learning the use of new technology requires effort (Venkatesh et al., 2003).

With regard to employees' information security awareness and behavior, TAM determines the employees' intention to comply with information security policies (ISPs). Studies examined the employees' perception of the usefulness of organizational security measeures as well as the perceived ease of use in order to predict employees' intention to use (e.g. Dinev et al., 2009; Hu and Dinev, 2007; Xue et al., 2011). Whereas the importance of the relationship of attitude and intention is generally empohasized, in the information security context authors often examined a direct relationship between perceived ease of use and perceived usefulness and behavioral intention (e.g. Hu and Dinev, 2007; Xue et al., 2011). 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).

2.1.3 Protection Motivation Theory

Originating from health psychology, the protection motivation theory was introduced by Rogers (1975) and later revised by Rogers (1983) by emphasizing the cognitive process that mediates behavioral change (Boer and Seydel, 1996). The theory aims to explain whether a person's attitude and behavior are influenced directly or indirectly by fear appeals. The process of coping with potential threats leads to protection motivation and is the result of two independent appraisal processes: threat appraisal and coping appraisal (Norman et al., 2005). Within the threat appraisal process, the degree of harm

a potential threat can cause (perceived severity) and the probability that one will experience harm (perceived vulnerability) are evaluated (Boer and Seydel, 1996). Coping appraisal consist of three components: response efficacy, self-efficacy and response costs. Response efficacy refers to a person's expectancy that a certain (recommended) behavior leads to threat prevention. Related to this is the construct of self-efficacy (Bandura, 1982), as already mentioned in the context of the theory of reasoned action, referring to a person's belief in his/her ability to carry out a certain behavior. The construct of response costs represent any physical or psychological costs related to the protective behavior and has negative influence on protection motivation (Norman et al., 2005).

Studies using the Protection Motivation Theory with regard to employees' information security awareness and behavior incorporated a plethora of different constructs (Herath and Rao, 2009b). A significant relationship of the theory's core constructs to employees' behavioral intention was demonstrated by the majority of the studies. It is shown that threat appraisal is a predictor of employees' intention to comply with organization security policies (e.g. Pahnila et al., 2007a; Siponen et al., 2010). Response efficacy and self-efficacy have been proven to be significant for employees' compliance intention (e.g. Ifinedo, 2012; Johnston and Warkentin, 2010; Siponen et al., 2007).

2.1.4 General Deterrence Theory

Adapted from criminal justice research, deterrence theory states that persons are deterred from committing criminal behavior if they perceive sanctions as certain as well as severe and has been utilized to investigate the efficacy of legal sanctions in the context of crime prevention (Williams and Hawkins, 1986). It can be distinguished between specific and general deterrence theory. Whereas specific deterrence theory posits that persons are deterred from committing crimes by actual experience of punishment, general deterrence theory implies that the demonstration of sanctions as a result of criminal behavior discourages the public to commit criminal acts (McShane and Williams, 1997). Classic deterrence theory focused on formal sanctions (i.e. legal sanctions) and was later extended by informal sanctions (e.g. social disapproval, shame etc.) (D'Arcy and Herath, 2011).

Employees' information security awareness and behavior research mainly utilizes general deterrence theory including formal sanctions. Employees' decision regarding information security policy compliance intention is the result of balancing the possible cost and benefits of different behavioral alternatives (Bulgurcu et al., 2010; D'Arcy et al., 2009). The constructs of perceived severity of sanctions and perceived certainty of sanctions were related to behavioral intention (e.g. Herath and Rao, 2009a; Hovav and D'Arcy, 2012; Xue et al., 2011). Employees' behavioral intentions are measured as users' perception as to whether a violation of specific parts of information security policy may increase his or her general utility. Some studies incorporated additional constructs to the core constructs of general deterrence theory (e.g. Pahnila et al., 2007b; Siponen and Vance, 2010). However, the role of deterrence in the field of information security is controversial as studies produced disparate and often controversial findings (D'Arcy and Herath, 2011).

2.2 Leadership Theories

2.2.1 Leadership in IS Security Research[1]

Since IS literature is more and more focused on the employee perspective in the context of information security research, the role of managers in the in the information security chain found little attention (Uffen et al., 2013). However, with regard to management involvement in the context of information security, literature emphasizes the importance of CIOs and IT executives for developing and maintaining a culture of compliance in order to achieve information security effectiveness (Stewart and Thelander, 2005). For example, Broadbent and Kitzis (2004) pointed out, that success of CIOs depends on their ability to go beyond pure management and lead by setting expectations and to influence others to change. The main challenges for IT leaders is to balance in terms of cutting costs and promote innovation, and to develop trust and relationships. Therefore interpersonal skills are critical factors for CIOs in order to be well in alliances and partnerships, with the business leaders and other functional leaders (Stewart and

[1] This section is adapted from Lebek et al. (2014, pp. 3 ff).

Thelander, 2005). Beginning with senior management, organizations have to aim for establishing a leadership style that understands information security as an important issue and forms a security culture throughout the organizational levels (Dutta and McCrohan, 2002). Focusing on small and medium enterprises, Dojkovski et al. (2007) identified several attributes of managerial leadership that influence organizational information security outcomes. Accordingly, leaders must act as role models with regard to information security and take initiative in order to be informed about information security topics and develop governance structures for maintaining adequate information security. Mishra and Dhillon (2005) emphasize that top management accountability is a crucial factor for effective information security. The authors split managerial information security responsibilities into formal and informal measures. Formal measures are e.g. the creation and implementation of security policies, the assessment of internal control mechanisms, the promotion of group behavior as well as the development of a leadership style that promotes compliant behavior and carries out strong measures against non-compliant behavior. Research on leadership style has demonstrated that using punishment as a negative stimulus is an effective way to enhance employees' job performance and to reduce undesired behavior when a punishment expectancy has developed among employees (Xue et al., 2011). The informal side of managerial information security measures is about the creation of an organizational culture that recognizes the importance of information security by considering prevalent norms, individual believes and personal values of employees (Mishra and Dhillon, 2005).

Referring to the behavioral theories previously mentioned in this chapter, it can be assumed that a laissez-faire style of leadership and management attitude with regard to employees' security awareness and behavior would not effective. Studies demonstrate that this type of leadership style does not cause that guidelines are being followed properly due to a lack of employees' motivation. (Siponen and Kajava, 1998). To increase employees' in intrinsic motivation and intention to comply with information security policies, certain leadership soft skills and a healthy organizational culture are imperative factors and a basic precondition (Siponen, 2000). This is consistent with Collins (2001), who identified key strategies for successful leaders: "a focus on natural talent; passionate interest and well rewarded activity [and] a culture of discipline. People come first and their efforts good or bad are amplified" (Stewart and Thelander, 2005).

2.2.2 Transactional Leadership

Burns (1978) stated that two forms of leadership styles exist. Accordingly the leadership process can occur in a transactional way or a transformational way (Bass et al., 1987). Both kinds of leadership styles differ in the relationship between leaders and followers. Transactional leadership aims to motivate followers by helping them to fulfill their own self-interests (Sadgehi and Lope Pihie , 2012) by using rewards as exchange for achieving previously defined performance goals (Jung and Sosik, 2002; Rafferty and Griffin, 2004, Yukl, 2006). Therefore, transactional leaders define and clarify desired outcomes, objectives as well as required tasks to their followers and are creating the necessary confidence to accomplish the desired effort. Furthermore, transactional leaders identify the needs and desires of their followers and clarify how these needs and desires will be satisfied if the required goals are fulfilled (Avolio and Bass, 2004). Consequently, the relationship between leaders and followers is based on an inherent contract of mutual reinforcement in order to achieve higher performance (Jung and Sosik, 2002). As shown in Figure 3, transactional leadership can consist of three dimensions of behavior: contingent reward, management-by-exception and laissez-faire leadership (Avolio et al., 1999; Bono and Judge, 2004; Stewart, 2006).

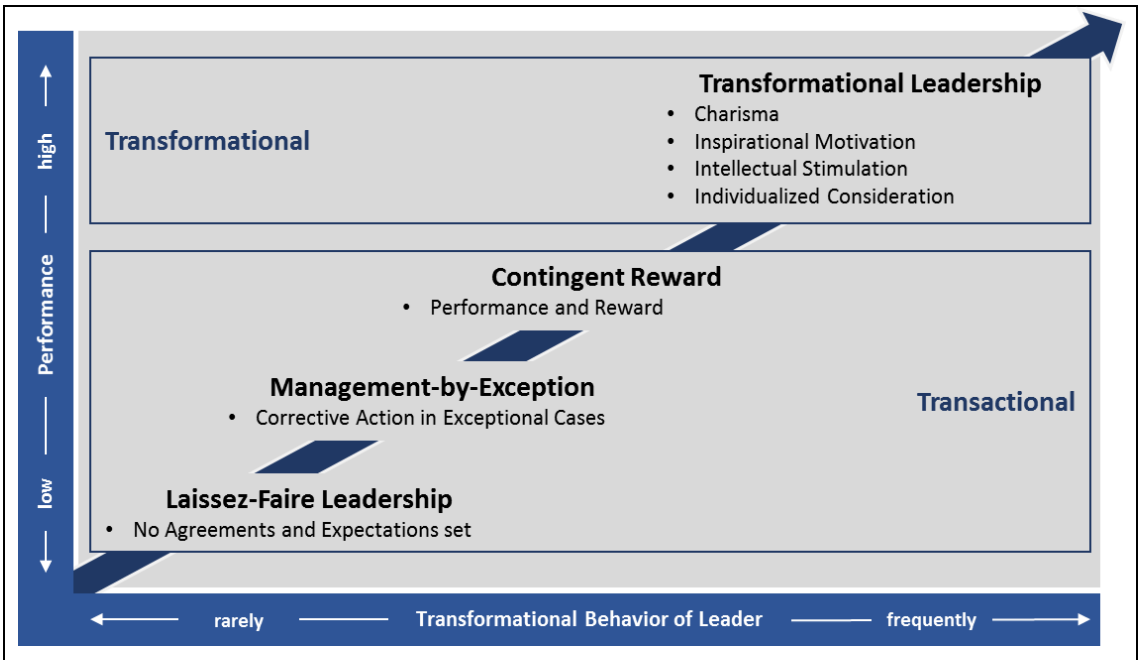


Figure 3: Leadership Continuum

Contingent reward encompasses the degree of using rewards that followers receive (e.g. wages or prestige) in exchange for meeting defined performance standards (Bass et al., 1987; Bono, 2004; Sadgehi and Lope Pihie, 2012). Prior research has demonstrated a positive relation between contingent rewards and followers' performance and commitment (Bass et al., 2003). Management-by-exception can occur in a passive or an active form. The active management-by-exception leader watches follower behavior for mistakes and rule violations and corrects errors and problems before they become severe (Sadgehi and Lope Pihie, 2012). The passive management-by-exception leader tends to avoid corrective actions (Bass et al., 1987) and waits until deviations and errors occur before taking actions (Stewart, 2006). This type of leader also avoids to ex-ante clarify agreements and expectations to his followers (Sadgehi and Lope Pihie, 2012) and is also labeled as laissez-faire leadership (Bass et al., 2003). Although, laissez-faire leadership is also referred to as non-leadership, it can be included into transactional leadership theory (Bass, 1985; Bono, 2004). Laissez-faire leaders avoid to influence as they do not clarify goals, objectives or expectations to followers (Bass et al., 2003). Transactional leadership is sufficient for maintaining the current situation in organizations (Geijsel et al., 2003; Sadgehi and Lope Pihie, 2012).

2.2.3 Transformational Leadership[2]

In contrast to transactional leaders, transformational leaders encourage change and innovations (Geijsel et al., 2003). The concept of transformational leadership goes back to the theoretical ideas of Burns (1978) in the context of political leadership. Based on Burns' work, Bass (1985) introduced a model of transformational leadership that was later adopted to organizational psychology research. Transformational leadership is not seen as a substitute for transactional leadership, but as an extension as it augments transactional leadership in achieving goals of leaders, followers and organizations. Using transactional leadership as a basis for effective leadership, transformational leadership results in a higher willingness of employees to show a greater commitment and a higher employee satisfaction (Avolio and Bass, 2004). Transformational leaders convey the

[2] This section is adapted from Lebek et al. (2014, pp. 4ff).

value and importance of desired outcomes to their followers, stimulate them to transcend their self-interest for the interests of their groups or organizations and thus facilitate a collective motivation (Jung and Sosik, 2002). Four specific components of transformational leadership have been identified: (1) idealized influence, (2) inspirational motivation, (3) intellectual stimulation, and (4) individualized consideration (Geijsel et al., 2002; Jung and Sosik, 2002; Bass et al., 2003). Idealized influence refers to the degree to which a leader displays behavior that causes followers to identify with the leader. Leaders possess a clear set of values like high ethical and moral standards (Bono, 2004) and consider the needs of their followers over their own (Bass et al., 2003). Inspirational motivation deals with ways leaders motivate followers and generate optimism (Stewart, 2006). Leaders with inspirational motivation challenge followers with high standards, communicate an optimistic vision and speaks optimistic about the future. Leaders attract enthusiasm and energize their followers (Rafferty and Griffin, 2004). Through intellectual stimulation, leaders encourage followers to question established methods and organizational norms and to get a new perspective on a problem (Bass, 1987; Avolio et al., 1999). Thereby leaders push followers to develop innovative strategies and to improve existing methods (Bono, 2004). Individualized consideration refers to the degree of leaders concerning about their followers needs and interests. By establishing a supportive climate and providing coaching and mentoring, leaders help followers to raise their personal abilities and potential (Stewart, 2006; Geijsel et al., 2002). Hence, transformational leaders do not only recognize and satisfy followers' current needs but also elevate those needs in order to personally develop followers (Bass, 1987).

2.3 IS Governance

2.3.1 Definition and Scope of IS Governance

As mentioned in chapter 1, IS governance constitutes the paramount framework for organizational information security and is challenged by threats that are associated by new trends that shift power towards employees. IS governance is commonly referred to as an integral part of corporate governance (Webb et al., 2006; Burtscher et al., 2009). IS governance draws from corporate governance principles and focuses on the management and use of IT in order to achieve corporate performance goals (Weill and Ross,

2004b). Both, corporate and IS governance aim for value delivery and risk management. Corporate governance defines the strategic direction of an organization, whereas IS governance specifies the leadership and organizational structures, processes and relational mechanisms to ensure that IT is properly aligned to the business strategies and objectives (De Haes and van Grembergen, 2005; Burtscher et al., 2009; Zarvic, 2012; Urbach, 2013). By specifying the decision rights and accountability standards, IS governance concentrates on performing and transforming IT to meet present and future demands of business. While the main purpose of IS governance is to ensure that IT decisions are consistent with organizational objectives (Burtscher, 2009), five goals of IS governance (Figure 4) are generally distinguished in academic literature: strategic alignment, value delivery, risk management, resource management, and performance measurement (e.g.: Dahlberg, 2006; Webb et al., 2006, Börner et al., 2009). Strategic alignment focuses on fitting the IT strategy to the business strategy in order to achieve maximum business value (Webb et al., 2006; Liang et al., 2011), as well as validating and specifying the value proposition of IT (Burtscher et al., 2009). Driven by strategic alignment, value delivery ensures that IT makes substantial and verifiable contributions to organizational success and aims at the realization of business value (van Grembergen et al., 2004). This includes the development and delivery of value-oriented IT services that meet customer demands and thus establish a „relationship between the degree of strategic alignment and the value added by IT" (Börner et al., 2009). The main objective of risk management is to protect IT assets and to recover from disasters (van Grembergen et al., 2004). Its purpose is to analyze risks regarding the use of IT and to treat those risks in accordance with the organization's risk preferences and attitude (Börner et al., 2009; Novotny, 2012). Resource management focuses on „the proper management of critical IT resources: applications, information, infrastructure, and people" (Burtscher et al., 2009).

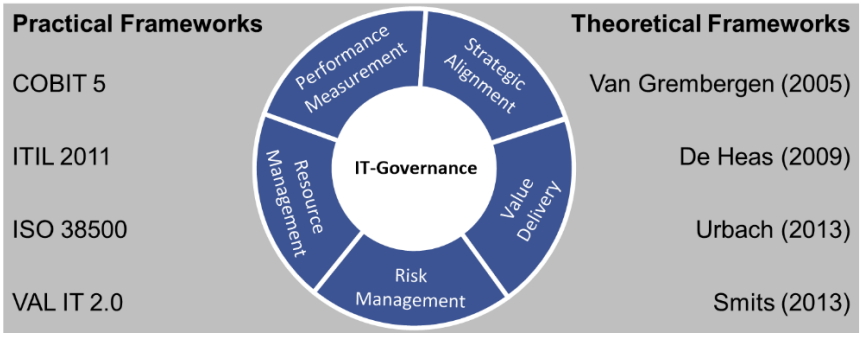


Figure 4: IT Governance Goals and Frameworks

Performance measurement aims to secure the level of quality within the IT organization (Ask et al., 2007). Therefore it „tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery" (Burtscher et al., 2009). Strategic alignment, resource management, and performance measurement are preconditions for successful value delivery and risk management. The first three goals are referred to as 'drivers,' whereas the latter two are referred to as 'outcomes' (Burtscher et al., 2009).IS governance is closely related to the subjects of IT management, information governance, strategic information systems planning (SISP) and related practitioners' frameworks such as COBIT, ITIL, CMMI, VAL IT, and ISO/IEC, 17799 (Burtscher et al., 2009). IT management can be distinguished from IS governance with regard to the time dimension and the business orientation. By specifying decision rights and accountability standards, IS governance concentrates on performing and transforming IT to meet present and future demands of business. In contrast, IT management is focused on the process of making and implementing decisions in the present in order to ensure the effective and efficient supply of IT services and IT operations (Weill, 2004; van Grembergen and De Haes, 2005). Information governance differs from IS governance in scope, as it emphasizes the quality of information in the context of governance. Information governance considers the search, creation, use, and exchange of information (Kooper et al., 2011). IS governance has several links and overlapping areas with SISP, as is shown by the four objectives of SISP: aligning IT with business goals, exploiting IT for competitive advantage, directing efficient and effective management of IT resources, and developing technology policies and architectures (van Grembergen and De Haes, 2005; Webb et al., 2006). IS governance expands the scope of SISP by adding the aspect of managing risks. Whereas SISP is internally oriented, IS governance is considered to be part of corporate governance (Burtscher et al., 2009).

2.3.2 IS Governance Forms and Contingencies

IS governance forms refer to the placement of decision-making structures within organizations. Literature typically distinguishes between two basic governance designs: centralized and decentralized IS governance (Peterson, 2004; Brown and Grant, 2005). In centralized IS governance designs, all decision-making authorities are located within a central IS department, whereas in decentralized IS governance designs, decision-making

is grounded in divisional IT departments and line management has the authority to make decisions (Brown et al., 2005; Burtscher et al., 2009). Centralized IS governance allows more control over IT standards and the realization of economics of scale. Decentralized IS governance provides greater flexibility and responsiveness to business needs, as it allows an increase in customization (Brown et al., 2005). Weill and Ross (2004b) introduced six governance classifications based on the ideal of political archetypes (see Table 1). The business monarchy and the IT monarchy reflect the concept of a strict centralized IS governance design, whereas the feudal archetype draws parallels to a strict decentralized decision-making structure. The federal archetype presents the middle ground between the two strict IS governance orientations. IT duopoly refers to a relationship between a business and a technical partner and has been considered less frequently in research literature, as has as the anarchy archetype (Brown et al., 2005). IS governance and its outcomes are impacted by multiple contingencies (Sambamurthy and Zmud, 1999; van Grembergen et al., 2004; Brown et al., 2005; Dahlberg and Kivijarvi, 2006; De Haes and van Grembergen, 2006), which can be divided into internal and external influence factors (Burtscher et al., 2009). Brown et al. (2005) identified four main contingencies regarded by academic literature: organizational structure, business strategy, industry and organization size. Moreover, the authors note the absence of technology and technology-adoption within existing consistency research. Further determinants of organizational governance arrangement considered by research include geography, regulatory influence factors, corporate governance, organizational culture, and role of IT within the organization (Burtscher et al., 2009).

Table 2: IS Governance Archetypes (Based on Weill and Ross, 2004b)

Archetype	Design	Decision-Making Structure
Business Monarchy	Centralized	IT Decisions Are Made by Chief Officers
IT Monarchy	Centralized	Corporate IT Professionals Make IT Decisions
IT Duopoly	Centralized	IT Executives and One Business Group Decide Together
Federal	Hybrid	Hybrid Decision Making
Feudal	Decentralized	Decision by Autonomous Business Units
Anarchy	Decentralized	Each Small Group Makes Decisions

3. Research Methodology

3.1 Research Methods in Information Systems

The German academic literature commonly differentiates between the the German "Wirtschaftsinformatik (WI)" and the Anglo-Saxon "Information Systems Research (ISR)". WI mostly draws from natural sciences, formal sciences, engineering sciences, and design-oriented science. In contrast ISR has a stronger orientation towards behavioral sciences (Wilde and Hess, 2006). Due to the similar orientation and direction of the two research streams (Wilde and Hess, 2007), these are considered together and referred to as ISR in the following. The ISR domain is, similar to other domains of management research, characterized by a plethora of research methods (Mingers, 2001).

Table 3: Scientific Methods in ISR (Wilde and Hess, 2006)

Name	Chapter/ Appendix	Name	Chapter/ Appendix
Development / Testing of Prototypes	-	Content Analysis	3.4.2; 5.2; A5; A7
Simulation	-	Case Studies / Field Studies	-
Modeling	A1	Laboratory Experiments	-
Subjective, Argumentative Research	-	Field Experiments	-
Deduction	-	Survey	3.3; 4.2; 5.1; A3; A8
Learning By Doing	-	Interviews	3.4.1; 5.2; A5; A7
Research By Developing	-	Observation	-
Action Research	3.2; 4.3; A4	Reference Modeling	5.2; A7
Forecasting	-	Description And Interpretation	-
Grounded Theory	-	Ethnography	-

A method is generally defined as a procedure which is characterized by a certain set of tools as a means of goal attainment (Chmielewicz, 1994). A method is referred to as a scientific method if it is described by intersubjectively comprehensible and verifiable rules (Wilde and Hess, 2006). In ISR, scientific methods are used to fulfill two kinds of scientific interests. First, corresponding to natural sciences, descriptive research aims to derive knowledge in order to gain a better understanding of IS. Second, prescriptive research is a design science that uses knowledge in order to enhance performance of IS (March and Smith, 1995). Based on König et al. (1996) and Lange (2006), Wilde and Hess (2006) provide a list of scientific methods used wirthin the ISR domain (Table 3). In the following, the research methods that were used within the research process described in this dissertation are presented.

3.2 Action (Design) Research

Action design research, as a form of action research was applied in the context of developing and testing a needs assessment process for SETA programs (cf. Chapter 4.3). According to Rapoport (1970), who defines the aim of Action Research (AR) as „to contribute to the practical concerns of people in an immediate problematic situation and to the goals of social science by joint collaboration within a mutually acceptable ethical framework", AR has the dual task of solving a practical problem and expanding scientific knowledge (Anaman et al., 2008). However, in the course of debating practical relevance and scientific rigor in IS research, the state of AR as a proper research methodology has been questioned (Goldkuhl, 2008) and AR was criticized as „mostly glorified consulting" (Anaman, 2008). Since AR specifically aims at solving a specific practical problem, it does not explicitly consider general practical relevance and takes scientific contribution for granted (Goldkuhl, 2008). In order to avoid the criticism passed on AR, design science research (DSR) seems to be applicable to address both of the objectives described above. Design science research aims for developing abstract design knowledge that intends to solve a class of problems rather than solving a problem in a specific organizational setting (Hevner et al., 2004, Hrastinski et al., 2008). Therefore Iivari and Venable (2009) define DSR as „a research activity that invents or builds new, innovative artifacts or solving problems or achieving improvements, i.e. DSR creates new means for achieving some general (unsituated) goal, as its major research contributions." In recent years,

a discussion on the (dis)similarities of AR and DSR arose in IS research literature (e.g. Järvinen, 2007, Iivari and Venable, 2009, Papas et al., 2012). Based on this debate, also combinations of the two research methods were discussed in order to close the gap between organizational relevance and methodological rigor (e.g. Lindgren, 2004; Iivari, 2007, Sein et al., 2011).

The term 'action design research' (ADR) was first mentioned by Iivari (2007) to describe the combination of action research and design research (DR). Building on that, Sein et al. (2011) introduced the ADR approach as "a new design research method that draws from action research". That ADR approach incorporates the two challenges mentioned above: (1) by addressing a problem in a specific organizational setting, ADR takes the influence of practitioners and the ongoing use within the specific organizational context into account, (2) to meet the requirement of academicals contributions, ADR constructs and evaluates generalized artifacts that address a class of problems through formalized learning from the organizational intervention. Although Sein et al. (2011) primarily see technical products as the outcome of DR by specifically referring to artifacts as „bundles of hardware and/or software", it can be argued, that the ADR approach is also applicable for a extended definition of the term artifact that includes organizational and social aspects of IS (Hrastinski et al., 2008) as well as concepts (Järvinen, 2007), models, methods and instantiations (March and Smith, 1995; Hevner et al., 2004).

According to Sein et al. (2011), ADR consists of four stages: (1) problem formulation; (2) building, intervention and evaluation (BIE); (3) reflection and learning; (4) formalization of learning (Figure 5). The first stage is triggered by a problem perceived in the specific practical setting and conceptualizes it as an instantation of a broader class of problems in order to provide a research opportunity. The BIE is consisting of several iterative cycles which are carried out in a real-world environment in order to build and continuously evaluate an artifact. The reflection and learning stage is carried out simultaneously to the BIE stage. It allows to gain a clear understanding of the problem due to early evaluation and to generate experiences from the specific problem solution by obtaining continuous feedback from the several BIE cycles. The fourth stage aims at providing a general solution for the broad class of problems as it outlines the results as design principles and transfers experiences form a specific problem solution into knowledge that addresses the broad class of problems.

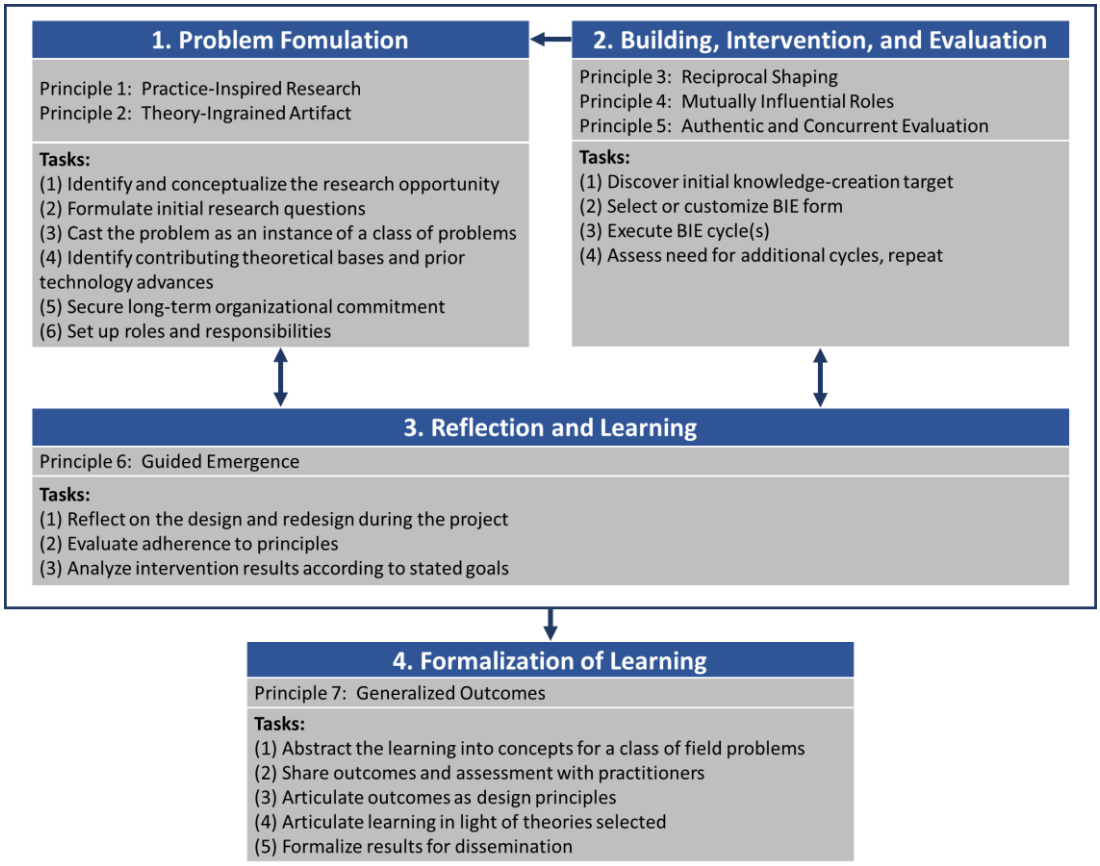


Figure 5: ADR Method - Stages, Principles and Tasks (Sein et al., 2011)

3.3 Surveys

Surveys are method for collecting data and therefore do no constitute a complete scientific method. Accordingly, surveys are referred to as a method, in the context of collecting a great amount of data for the purpose of quantitative analyses (Fettke and Loss, 2007). The survey method aims at empirically testing of theoretical models concepts and prepositions (Creswell, 2008; Forza, 2002). Quantitative research aims at producing generally applicable results in the form of objectively measurable quantities (Flick, 2006; Altobelli, 2007). The data obtained are usually evaluated by means of statistical methods (Altobelli, 2007). In the context of this dissertation, surveys were applied in order to gather structured empirical data (cf. Chapters 4.2 and 5.1). Data analyzing techniques of multivariate statistics are applied and described in the following.

3.3.1 Exploratory Factor Analysis and Principle Component Analysis

Factor analysis is a method of multivariate statistics that is used to determine factors (latent variables) from empirical examination of several observable variables (manifest variables) (Sedlmaier and Renkewitz, 2013). Two types of factor analyses exist, namely confirmatory factor analysis (CFA) and exploratory factoranalysis (EFA) (Williams et al., 2010). In the context of this dissertation, EFA was applied within two quantitative empirical studies (cf. Chapters 4.2 and 5.1) in order to set up structural equation modeling (cf. Chapter 3.3.1). Contrasting CFA, EFA is not used in order to test hypotheses. EFA is used to analyze interrelationships among items in order to reduce the number of items used within a model (Stewart, 1981; Williams et al., 2010). While reducing the number of items, EFA aims at accurately and comprehensively expressing the same amount of information that contained within the initial set of items (Sedlmaier and Renkewitz, 2013). A precondition for conducting EFA is the suitability of the data. In the context of this dissertation suitability of the data was determined according to the Kaiser-Meyer-Olkin (KMO) criterion. This measure indicates the extent to which the variables belong together and serves as an indication of whether a factor analysis is appropriate. The KMO criterion should be at least 0.5 (Chin, 1998; Fishbein and Ajzen, 1975, Williams et al, 2010). In order to extract factors, principle component analysis (PCA) was applied. The number of components were determined using the Kaiser criterion. Accordingly, factors with eigenvalues larger than 1 were extracted (Hayton et al., 2012; Williams et al., 2010). Since this procedure leads to high correltations of most items with all determined factors, varimax rotation is used in order to allow for interpretation of the factors (Williams et al., 2010).

3.3.1 Structural Equation Modeling

Structural equation modeling (SEM) is a statistical procedure to test and estimate correltations between endogenous and exogenous variables within a causal model. Whereas first generation statistical techniques are only applicable if the data set is free from random error and systematic error (i.e. method variance), SEM presents a second generation technique that avoids the restrictions of first generation techniques (Chin, 1998; Lowry and Gaskin, 2014). Most empirical studies focus on the investigation of latent variables, which are interconnected by a network of hypotheses. SEM allows to

measure these latent variables, which are not directly observable. Due to unobservability, latent variables are operationalized by identifying indicators that empirically represent each latent variable. By using multivariate analyses, effect relationships of latent variables are tested. (Nitzl, 2010; Roy et al., 2012). A structural model consist of exogenous and endogenous constructs (Figure 6). The endogenous variables (i.e. η_1) is the outcome from at least one casual relationship. The exogenous variables (i.e. ξ_1 & ξ_2) are the predictors of the other variable in the model (Gefen et al., 2000). Two types of measurement models exist, namely formative and reflective. The differentiation between reflective and formative measurement models depends on the causal relationship of the latent and manifest variables (Nitzil, 2010) and impacts the estimation procedure (Fornell and Bookstein, 1982). Reflective indicators represent observable measures that are affected by unobservable latent constructs (Maccallum and Browne, 1993) and are determined by the latent construct (Edwards et al., 2000; Jahn, 2007). Since reflective indicators are interchangeable, the elimination of an indicator does not lead to contextual changes within the construct (Diamantopolous and Winklhofer, 2001; Jahn, 2007). In contrast, formative indicators determine the latent construct (Chin, 1998; Edwards et al. 2000). Since formative indicators are not correltated they are not interchangeable. Consequently, the elimination of a formative indicator substantially changes the characteristics of the latent variable (Jahns and Moser, 2007; Nitzl, 2010).

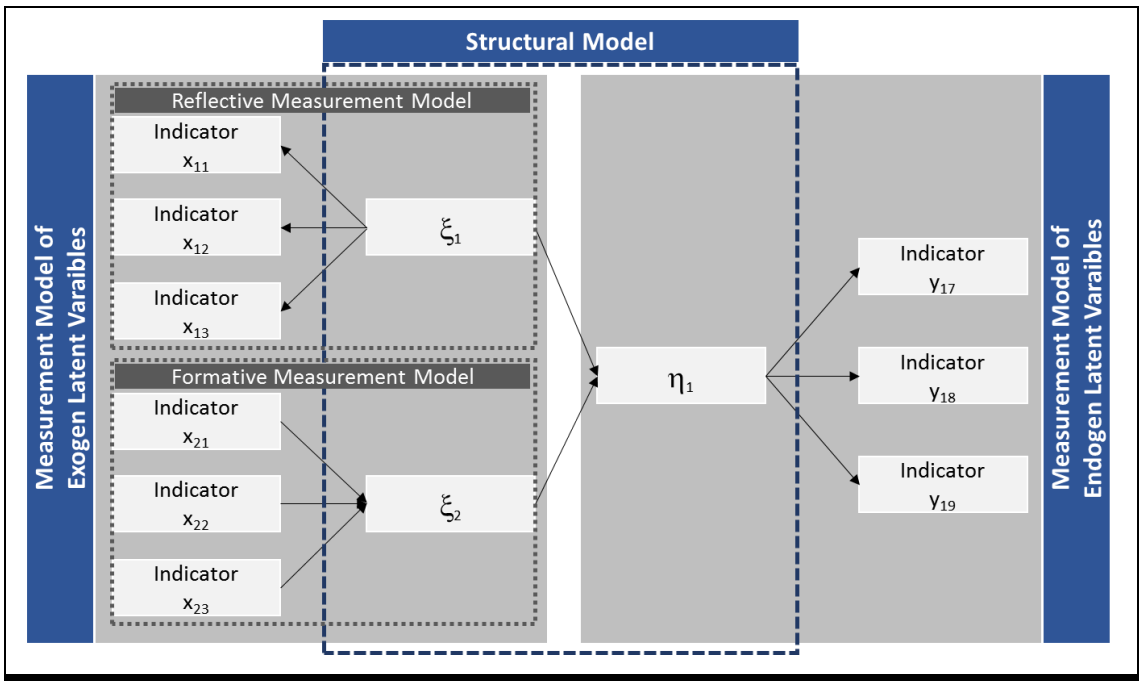


Figure 6: Construction of a Causal Model (adapted from Nitzl, 2010)

3.3.2 Partial Least Squares

In general, two approaches for SEM, namely covariance-based SEM and variance-based SEM exist (Nitzl, 2010, Lehner et al., 2009). The analysis of covariances aims at fiting the parameter estimates as precisely to the to the empirical covariance matrix as possible. For this purpose, LISREL is the most frequently used softwaretool (Nitzl, 2010). For the analyses of variance, the most common method is partial least squares (PLS). This method aims at maximizing the share of the dependent variables in order to estimate the parameters of the theoretical model (Haenlein and Kaplan, 2004; Nitzl, 2010; Hair et al., 2010). SmartPLS is the most popular software application for conducting the PLS method. PLS decomposes the overall model and uses multiple regression in order to estimate the parameters for each partial model as the remaining partial models stay constant (Fornell and Bookstein, 1982; Jahn, 2007; Nitzl, 2010). The PLS method is suitable mainly for exploratory studies and theory development (Chin, 1998; Reinartz et al., 2009). An overview of criteria to decide whether variance-based (PLS) or covariance-bases (LISREL) is applicable is provided in Table 4. Several quality criteria must be fulfilled for the application of PLS. There are different quality criteria for the measurement models and the structural model discussed in literature (see e.g. Chin, 1998; Hair et al., 2011).

Table 4: Decision Criteria Variance-based vs. Covariance-based PLS (Nitzl, 2010)

Criterion	Variance-based (PLS)	Covariance-based (LISREL)
Objective	Based on prediction	Based on parameters
Estimate principle	Iterative and non-iterative least squares estimation	Minimisation of the distance between model-theoretical and empirical covariance
Distributional assumptions	No statistical assumptions about distribution	Multivariate normal distribution of the data
Consistency of the estimator	Consistent, if number of cases and number of indicators are high	Consistent
Estimator on model level	Conservative	Inflationary, if indicator loading is low
Formative construct operationalisation	Possible without difficulty	Possible under certain conditions
Applicable quality criteria	Only partial qality criteria possible	Both global and partial quality criteria possible
Sample size	Mostly, small sample size is sufficient	Sample size from, 200 to 800
Level of measurement	No restrictions	At least interval scaled
Applications	PLSGraph, SmartPLS, LVPLS	LISREL, AMOS, EQS, M-Plus

3.4 Delphi Method

In the context of this dissertation, the Delphi Method was used to obtain expert opinions concerning the impact of the Nexus of Forces on IS governance (cf. chaper 5.2 and Appendix A7). The Delphi method was originally developed in the, 1950s by employees of the RAND Cooperation in the context of a U.S. Air Force project and was used as a procedure to obtain a reliable consensus of experts' opinions for the purpose of decision support with regard to strategic weapons systems (Rowe and Wright, 1999). Over time, the Delphi method was adopted to other areas like social sciences and technology development (Häder and Häder, 2000). Today, the Delphi method is an "established systematic interactive research method that relies on a panel of independent experts" (Olbrich et al., 2011). Since diverse forms of the Delphi method offer a high degree of flexibility, this approach is suitable in order to explore new issues based on subjective and complex judgments of experts (Kendall, 1977). Despite of the diversification of different types of the Delphi method, in literature it is agreed, that the "Delphi method is a method forinterviewing experts in two or more rounds, in which the results of the previous round are presented in the second or later rounds of interviews. Thus, the expert judging from the second interview round is influenced of the opinions of their peers from previous rounds" (translated from: Häder and Häder, 1995). Accordingly, this method is a highly structured group communication process in order to gain expert evaluation of issues and topics under uncertain and incomplete knowledge (Cuhls, 2009). Consequently, it can be argued, that the purpose Delphi method can be viewed in two ways: (1) as a method to explore certain topics and (2) as a method for the control of group communication (Häder, 2009). The following components of a Delphi study are commonly named in the literature (e.g. Häder and Häder, 2000; Ammon, 2009; Häder, 2009):

- Using a formalized questionnaire
- Interviews of experts
- Anonymity of individual responses and participants
- Determining a statistical group response and given justifications
- Information of participants about (statistical and verbal) group response
- (Multiple) Repetition(s) of the interview

3.4.1 Qualitative Interviews

Generally, three forms of data collection are distinguished within qualitative research: (1) interviews, (2) observation and (3) content analysis. Within this dissertation, qualitative interviews were used for systematic data collection within the Delphi approach. Similar to surveys, interviews are not considered a complete research method but a method for collecting data in order to provide the basis for qualitative content analyses (Fettke and Loos, 2007). In contrast to the deductive approach of the previously described quantitative survey method, qualitative interviews constitute an inductive approach for the purpose of theory development on the basis of empirical data. The goal of qualitative research is to uncover and identify new aspects rather than confirming (or disprove) existing theories as quantitative research does (Flick, 2006). Characteristic of qualitative research is the small size of the sample as well as the interaction between the interviewee and the researcher (Altobelli, 2007). Through the reflection of the researcher on the research topic, the communication of the researcher with the participants constututes an explicit part of resulting knowledge (Flick, 2006). Accordingly, qualitative studies do not primarily aim at a high degree of representativeness, but to generate insights into the characteresitics of a research topic. In the context of the article described in chapter 5.2 expert interviews, a special from the qualitative interviews, were used. The characteristics of this interview method are summarized in table.

Table 5: Characteristics of Qualitative Expert Interviews (Neumann, 2011)

Characteristic	Occurence	Description
Execution	Personal Interview	The Interviewer can immediately react to answers and influence the course of the interview and ask further questions.
Purpose	Compilation of Expert Knowledge	The interviewee is encouraged to reveal his expert knowledge.
Degree of Freedom	Open Interview	The interviewee can answer freely and state what he finds relevant as no predefined answers are given.
Structuring	Unstructured Interview	The interviewer can adopt his questions and topics to the specific situaton as no catalog of questions exists.
Analysis	Qualitative Interview	Answers are analyszed by means of qualitative content analysis.

3.4.2 Qualitative Content Analysis

For the evaluation of data material from expert interviews, the qualitative content analysis is recommended (e.g. Gläser and Laudel, 2009). The goal of the analysis of qualitative data is to systematically and objectively reduce the complexity of the empirical material with regard to the defined research question (Neumann, 2011) in order to "to attain a condensed and broad description of the phenomenon" (Elo and Kyngäs, 2007). Therefore, content analysis helps to summarize words and phrases that share the same meaning under fewer content-related categories. In general, qualitative data can be analyzed using quantitative or qualitative procedures. Following a quantitative analysis approach, text passages are assigned to predefined categories and analyzed with regard to absolute and relative frequencies. However, this approach is critized as the analysis of frequencies falls short to describe the complete meaning of texts as it does not consider latent contexts and only focusses on quantifiable content (Mayring, 2010; Neumann, 2011). Qualitative content analysis aims to reduce these limitations by interpreting the manifest and latent context of texts and phrases. According to Gläser and Laudel (2009), the process of the qualitative content analysis consist uf the three steps extraction, analysis, and interpretation as shown in Figure 7. By extracting relevant information from the original texts, qualitative content analysis saparates from the original texts as the mass of data is reduced and structured with regard to the research question. For this purpose, serach grids are ex-ante defined based on theoretical reasoning. Extraction in this context means to read the text and to decide wether contained informations are relevant for the purpose of the study. If informations are relevant they are assigned to the categoried of the search grid. The categorized results of the extraction are available for analysis and interpretation (Gläser and Laudel, 2009).

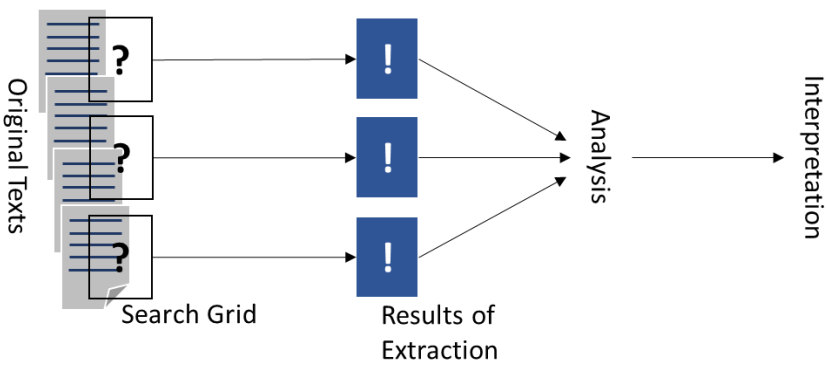


Figure 7: Process of the Qualitative Content Analysis (Gläser and Laudel, 2009)

4. Employees' Information Security Awareness and Behavior

4.1 Literature Analysis

This section is based on the research paper with the title "Information Security Awareness and Behavior: A Theory-based Literature Review" (cf. Appendix A6). The work was submitted and accepted for publication in the international journal "Management Research Review (MRR)" (Lebek et al., 2014). The journal, previously named "Management Research News", publishes latest research results in general management, including information and knowledge management. The VHB-Jourqual, 2.1 ranking based on Schrader and Hennig-Thurau (2009) rated the journal with a "C". The WKWI and GI-FB WI did not rate the journal, as it is does not exclusively focus on IS topics (WKWI, 2008).

By including concrete definitions of the behavioral determinants and updating the reviewed literature database throughout the year, 2013, this paper is an extended and updated version of a paper that was previously published at the "Hawaii International Conference on System Science (HICSS)" in Maui, HI, USA (January 07 – January, 10, 2013). The HICSS is one of the worlds longest-standing and continuous running research conferences and is ranked second in citation ranking among, 18 IS conferences (Hock et al., 2006) and ranked third in value among, 13 Management Information Systems (MIS) conferences (Kent et al., 2001). The paper, entitled "Employees' Information Security Awareness and Behavior: A Literature Review", was presented in the Mini-Track "Emerging Risks and Systemic Concerns in Information Security Research and Applications" which is part of the global track "Internet and the Digital Economy".

4.1.1 Motivation and Purpose

The research domain of employees' information security awareness and behavior is characterized by a high degree of multidisciplinarity as theories from e.g. social psychology pedagogy, education and criminology were adopted to IS literature in order to explain and predict security-related behavior (Mishra and Dhillon, 2005). Due to the importance of the topic, numerous studies have been conducted throughout the past years. An up-to-date overview of used theories and main results was needed in order to provide a solid basis for the research process described within this dissertation by identifying gaps in existing research. As Webster and Watson (2002) state, "a review of prior, relevant literature is an essential feature of any academic project. An effective review creates a firm foundation for advancing knowledge. It facilitates theory development, closes areas where a plethora of research exists, and uncovers areas where research is needed."

Although prior literature studies were conducted, these did not provide the necessary basis for the purpose of the present dissertation. For example, Siponen (2000) conducted a literature review focused on different approaches for minimizing user-related faults in information security, rather than on the underlying theories. Moreover, since this study was published 14 years ago it does not provide a current overview of the research field and therefore was not suitable as a basis for further research. In a more recent study, Abraham (2011) identified factors that influence security behavior (i.e., policies, communication practices, peer influences, etc.) but likewise not on behavioral theories. In addition, several studies included literature reviews that were target-oriented in order to provide the theoretical basis for further research within the same article. As the reviews were not the focal point of the respective articles, these were not comprehensive (e.g. Mishra and Dhillon, 2005; Aurigemma and Panko, 2012). Consequently, a comprehensive up-to-date literature review was conducted in order to analyze and define the status quo for the ongoing research process.

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

4.1.2 Research Design

The aim of a literature review is to accumulate a comprehensive body of relevant literature (Webster and Watson, 2002) in order to provide a "foundation upon which new research can be build" (Levy and Ellis, 2006). The quality of a literature review strongly depends on the search process (vom Brocke et al., 2009). Therefore the underlying process follows a two-step approach. First of all, a systematic literature search through renowned scientific databases was conducted by using well established guidelines. Secondly, the concept-centric literature analysis process was independently conducted by two researchers in order to minimize biases. An overview of the entire research process is provided by Figure 8.

In order to ensure methodological rigor of the literature review process, the structured approach by Webster and Watson (2002) and guidelines by vom Brocke et al. (2009) were adopted. To guarantee the replicability and therefore the reliability of the literature search process, the search process was documented comprehensively. The validity of the literature search process is ensured by adhering to following points: (1) Established academic databases were selected, that contain renowned journals outlets in the area of IS research (e.g. European Journal of Information Systems, MIS Quarterly, Information Systems Journal) and the proceedings of widely recognized IS conferences (e.g. International Conference on Information Systems, European Conference on Information Systems, Hawaii International Conference on System Sciences). Therefore, ten databases were searched: AISeL, ScienceDirect, IEEEXplore, JSTOR, SpringerLink, ACM, Wiley,

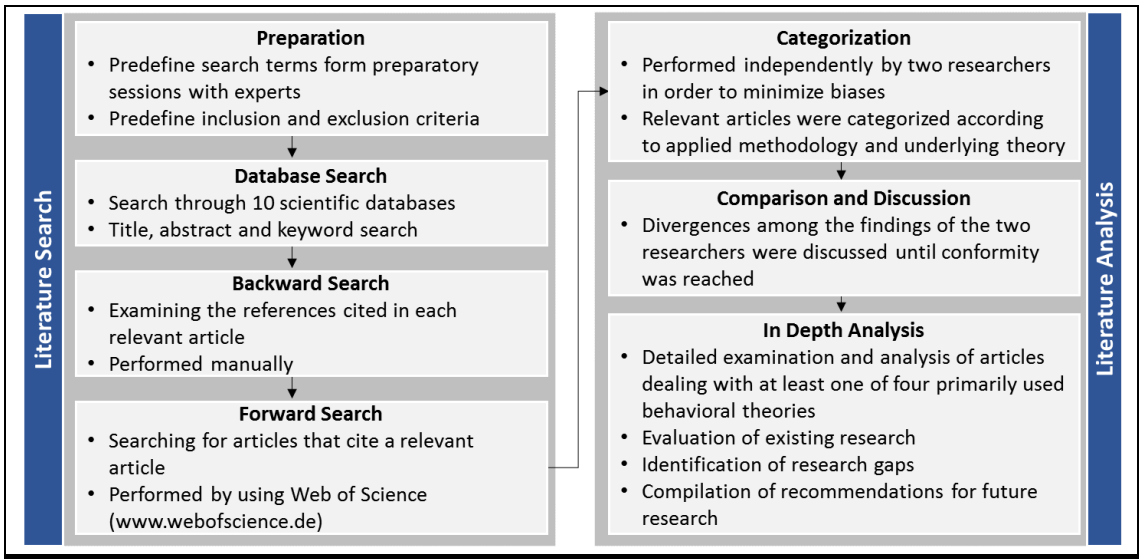


Figure 8: Literature Review Process

Emerald, InformsOnline, and Palgrave Macmillan. (2) Appropriate search terms were defined during a group discussion with four experts in the field of employees' information security awareness and behavior research. The resulting list included the terms security awareness, awareness training, awareness program, awareness campaign, security education, security motivation, security behavior, and personnel security. (3) Inclusion and exclusion criteria were defined in order to determine whether a publication is releveant in the contemplated research context. This was also done during the expert-group discussion. (4) A forward and a backward search based on publications that were found to be relevant were carried out in order to identify further relevant publications that were not uncovered by means of the prior keyword search. (5) By selecting a broad period of, 14 years to be searched, it was possible to gain a comprehensive overview of the contemplated research field and its evolution over the last decade.Contrary to the recommendations of Webster and Watson (2002) and vom Brocke et al. (2009) to focus on high-quality literature, outlets from conferences or journals that are not highly rated in international conference or journal rankings (e.g. AIS, Walstrom and Hardgrave, 2001, Willcocks et al., 2008) were considered since some of these conferences or journals specialize in the field of IS security (e.g. Computers & Security, Information Management & Computer Security) and therefore contain numerous publications dealing with topics that are relevant for the underlying research projects. The search process resulted in 4,168 publications that were potentially relevant in the context of employees' information security awareness and behavior research. After manually screening all 4,168 potentially relevant publications with regard to prior defined inclusion and exclusion criteria, 95 articles were identified to be relevant. Afterwards a backward and a forward search was carried out as recommended by Webster and Watson (2002). Finally, a total of 144 articles were identified and provides a basis for further analyses. In order to summarize literature and to provide readers a quick overview of previous studies in the research field of employees' information security awareness and behavior, the identified research papers were analyzed with regard to applied theories and research methodologies. In the context of identifying theories, the broad definition of presented by Karjalainen and Siponen (2011) was utilized. According tot he authors any application of a model, a framework or a concept was considered to be a theory-based approach. A list of theories was developed inductively while reviewing the articles resulting in a total of

54 identified theories that were applied in the contemplated research field. Since the majority of the identified theories were used in two or fewer publications, the further analysis was focused on four primarily used theories, namely the Theory of Reasoned Action (TRA) / Theory of Planned Behavior (TPB), the General Deterrence Theory (GDT), the Protection Motvation Theory (PMT), and the Technology Acceptance Model (TAM). In addition to the list of applied theories, a list of research methodologies was defined prior reading the publications in detail. With reference to the methodology spectrum in IS research presented by Wilde and Hess (2007), it was distinguished between seven different research methodologies: deductive analysis, modeling, experiment, action research / case study, grounded theory, literature review, empirical research (qualitative / quantitative). To limit mistakes and subjective biases, the analysis process was performed by two researchers. In the first step each researcher independently determined the applied theory and used research methodology for every single paper. Subsequently the results of the individual categorization of theory and methodology were compared. The results of both researchers were consistent for the most part. In case divergences occurred, the points in question were discussed until conformity was reached.

4.1.3 Findings

Due to the dominance of four behavioral theories within the contemplated research field it was chosen to focus on an in-depth analysis of those theories in the further analysis process. A meta-model that synthesizes the core constructs of the aforementioned theories is introduced in order to explain employees' information security behavior (see Figure 9; Table 6). Based on this, results of prior empirically tested models are summarized and discussed in order to identify gaps in existing research and to provide a solid foundation for the further research process that is described within this dissertation. Each behavioral factor has been tested and evaluated in multiple studies. 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 as described in detail in Lebek et al. (2014) (cf. Appendix A6).

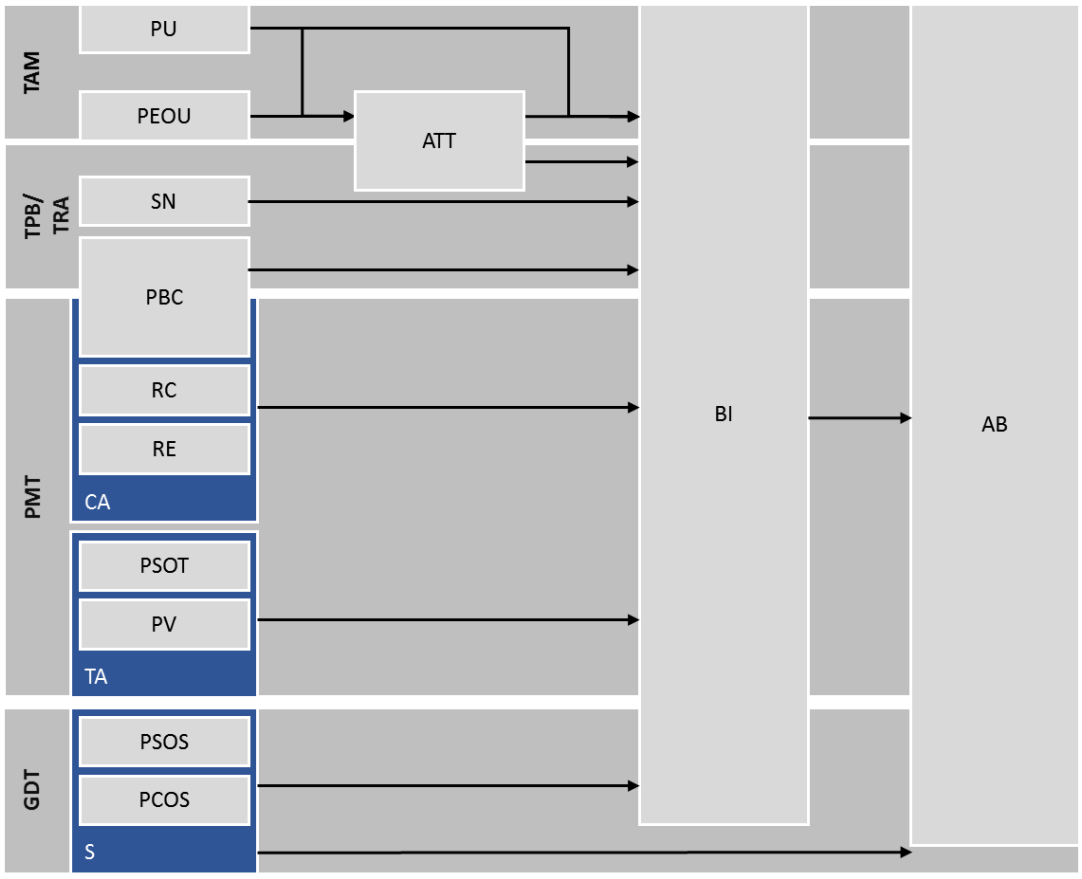


Figure 9: Meta-Model of Theories Primarily Used in Literature

Table 6: List of Theories, Constructs and the Respective Abbreviations

Theory	Abbr.	Construct	Abbr.
Technology Acceptance Model	TAM	Perceived Usefulness	PU
		Perceived Ease of Use	PEOU
		Attitude	ATT
Theory of Reasoned Action / Theory of Planned Behavior	TRA / TPB	Subjective Norm	SN
		Perceived Behavioral Control	PBC
Protection Motivation Theory	PMT	Coping Appraisal	CA
		Perceived Behavioral Control	PBC
		Response Costs	RC
		Response Efficacy	RE
		Threat Appraisal	TA
		Perceived Severity of Threats	PSOT
		Perceived Vulnerability	PV
General Deterrence Theory	GDT	Sanctions	S
		Percieved Severity of Sanctions	PSOS
		Percieved Certainty of Sanctions	PCOS

One major finding of the literature analysis is, that most studies assess employees' behavioral intention to comply with organizational information security policies rather than employees' actual security behavior (e.g. Limayem and Hirt, 2003; Siponen et al., 2007; Ifinedo, 2012; Pahnila et al., 2007a; Zhang et al., 2009a). This is grounded technically and theoretically. From a technical point of view, measurement of actual security compliant 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&b), 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). Several researchers demonstrated a strong and consistent relationship between the two constructs in non-information security context (Venkatesh et al., 2003; Webb and Sheeran, 2006). 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).

According to Podsakoff and Organ (1986) who stated, that factors like employees' intentions, attitudes, motivations or satisfaction are not verifiable by means other than self-reporting, the majority of reviewed studies used questionnaires in order 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, and results may be biased. Moreover, since employees' self-reported perceptions of security behavior are not necessarily in line with their actual behavior, the application of self-reports as predictors of employees' actual behavior can be questioned (Workmann et al., 2008). Although observation seems to be an instrument for gathering more objective data, the sensitive nature of security-related data prohibits a more frequent application of this data collection method. Organizations are unwilling to reveal information that provides insights into a company's current information security status (Kotulic and Clark, 2004). Workman et al.

(2008) proposed a combination of self-reporting and observational sampling in triangulation is an appropriate means of reducing the lack of qualitative and interpretive studies in this research field. Although, previous quantitative empirical research mainly used employees as a sample (in contrast to e.g. students), studies that provide insight into actual working environments are the minority. Inorder to reduce this gap, case studies including employees from one or more companies would be useful for further research and to extend the body of knowledge (Bulgrucu et al., 2009b). Additionally, experimental studies, as used by Johnston and Warkentin (2010), for example, are also a good method for 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.

4.1.4 Limitations

Although a systematic literature search was conducted in order to ensure that a relatively complete census of relevant literature was accumulated, a major challenge was the proliferation of terms that describe similar concepts within IT research. Consequently, due to the search process based on predefined keywords, it is possible, that valuable research papers are missing within the database that was used for further analysis. Webster and Watson (2002) already recognized the existence of this problem, but also stated that it is impossible to avoid. Nevertheless, the application of latent semantic analysis to our dataset could be a useful addition by discovering more coherent concepts. For example, Koukal et al. (2014) describe a way to enhance literature reviews through latent semantic indexing. A manual approach was used for identifying applied theories and research methodologies. Manual categorization processes are generally prone to mistakes, e.g. subjective biases. In order to mitigate these biases, the categorization process was conducted independently by two researchers and the results were compared subsequently and discussed until consensus was reached. However, the identification of the applied research methodology was not always clear as sometimes one

or more methodological approaches were used in combination, involving the combination of qualitative and quantitative elements. Following Rowley and Slack (2004) literature reviews should focus on research articles of high quality. Nevertheless, in IS research a vast amount of potentially relevant articles exist that are of diverse quality, leading to complications with regard to the identification of high quality research sources (Levy and Ellis, 2006, vom Brocke, 2009). Consequently, on the one hand, also outlets from conferences and journals of minor rankings were included which might have slightly negative effects on the review quality. On the other hand, only publications of controlled quality were included in the analysis process. Non-peer-reviewed publications (e.g. books, whitepapers) for example were not considered. This leads to the effect that some contributions might be missing in this literature review as one can assume that books might also include valuable contributions to the contemplated research field.

4.1.5 Conclusion

The analysis of, 144 publication showed that quantitavie empirical studies are the majority within the area of employees' information security awareness and behavior research. These studies mainly utilized TPB/TRA, TAM, GDT and PMT in order to explain and predict employees' security-related behavior. Since existing research provides solid evidence for the relationships between the main constructs of these four theories, future studies have to focus on additional factors that influence employees' information security awareness and behavior. It should be the aim of academic literature not only to focus on theory, but also to provide relevance for practitioners in order to prevent research from becoming an end unto itself (Rosemann and Vessey, 2008). In the context of this study key question for practitioners is how to influence employees' behavior to reduce information security risks. A gap between theory and practice threatens to arise, since literature analyses showed, that only few studies exist which focus on developing and testing procedures, measures and tool that address the problem of measuring and manipulating employees' behavior within actual work environments (Workman et al., 2008). In order to prevent this gap, it is necessary to build on the theoretical foundation that already exists, while focusing on the development of procedures that equip practitioners with tools to define effective security measures and information security awareness programs.

4.2 Transformational Leadership and Employees' Security Performance

This chapter is based on the research paper entitled "Transformational Leadership and Employees' Information Security Performance: The Mediating Role of Motivation and Climate" (cf. Appendix A8). The paper was presented at the "International Conference on Information Systems (ICIS)" in Auckland, New Zealand (December, 14 – December, 17, 2014) and and is published in the conference proceedings. The ICIS the anual meeting of the Association for Information Systems (AIS) which represents 4,000 members from more than 95 universities worldwide. It is the most prestigious and biggest conference in the IS research discipline worldwide and provides a platform for researchers to present and discuss highly significant scientific work. The conference guarantees high quality and professional focus of published research papers. The paper was submitted to the Track "IS Security and Privacy".

4.2.1 Motivation and Purpose

The results from the literature review show that employees' information security awareness and behavior as well as the resulting (non-)compliance with information security policies is considered to be a key socio-organizational resource (Bulgurcu et al., 2010; Siponen and Vance, 2010) that has garnered increasing academic attention over the last ten years. While referring to employees' as the weakest link in the information security chain, researchers have focused on employees' individual perspectives. A major challenge for organizations is to find an effective way to promote security policies to individual employees. In this context, not only the design of security policies, but also the motivation of individuals to follow those policies is of high importance (Boss et al., 2009). In this context, the role of managerial leadership has been considered only by few studies. Ashenden (2008) emphasized that a change in organizational culture towards a higher emphasis of information security can only be accomplished if managers possess certain soft skills.

In order to examine the role of leadership with regard to employees' imformation security behavior and to contribute to the contemplated research field, the aim of this study

is to investigate the influence of leadership on employees' information security behavior. Reffering to the behavioral theories that were primarily used within employees' information security behavior research (cf. Chapters 2.1 and 4.1) studies provide evidence that a laissez-faire style of leadership (as a dimension of transactional leadership) does not motivate employees' to follow organizational information security policies (Siponen and Kajava, 1998). In general, transactional leadership is merely capable of maintining the current state of employees' information security (Geijsel et al., 2003; Sadgehi and Lope Pihie, 2012). However, as organizations aim to constantly improve information security, this study investigates the influence of transformational leadership which has been proven to positively influence employee attitudes, behavior, and performance (Walumbwa et al., 2008) and to encourage employees to perform beyond expectations (Rafferty and Griffin, 2004). The goal of this study is to investigate how transformational leadership influences employees' intention to meet minimum information security standards, and employees' intention to actively support information security. These two characteristics of employees' behavioral intention compromise the construct of employees' information security performance. This results in the following underlying research question:

> *RQ: How does transformational leadership influence employees' information security performance?*

4.2.2 Theoretical Background

Employees' security compliance intention refers to in-role behaviors which are defined as "the behaviors that are necessary for the completion of the responsible work" (Zhu 2013) and are described in the formal job description. In the information security context, in-role behaviors tend to be non-malicious while focusing on the adherence to organizational information security policies in order to meet minimum information security standards at work (Innes et al., 2010). Employees' behavioral intention represents the key dependent variable utilized in most of previous studies within the contemplated research field (Lebek et al., 2013). In order to extend prior research, this study also put

extra-role behaviors[3] into the focus by introducing employees' security participation intention as the second dimension of employees' information security performance. The construct of employees' participation intention includes a greater voluntary element and aims to improve organizational information security in contrast to merely adhering to minimum information security standards. Since transformational leaders are able to stimulate employees' to perform beyond expectations, this leadership style is positively correlated with extra-role behaviors (Podsakoff et al., 1990; Podsakoff, 2000).

Referring to results from previous studies in the field of leadership research, this study also aims to investigate the mediating effects of intrinsic motivation and organizational climate within the context of information security. Intrinsic motivation is defined by Brown (2007) as a behavior that leads to inherent satisfaction and is not depending on external rewards. Intrinsic motivation is similar to the construct of attitude that has been utilized by numerous studies in the contemplated research field (e.g. Bulgurcu, 2009; Herath and Rao 2009b) but differs in an important aspect: Whereas attitude refers to the quality of actions, (i.e., the perception as to whether a behavior is positive or negative), motivation refers to activity levels (i.e., the perceived importance of performing a behavior) (Siponen, 2000). It is assumed that transformational leaders enhance employees' intrinsic motivation by promoting their autonomy.

Numerous studies utilized subjective norms in order to explain employees' information security behavior (e.g. Herath and Rao 2009b, Bulgurcu 2010). Subjective norms reflect employees' perceived social pressure (i.e. by supervisors or coworkers) to perform a certain behavior (Ifinedo 2012). In contrast, in this study the construct of security climate is used. Security climate reflects employees' perception of management values and organizational practices towards information security. Security climate is defined as employees' perceptions of management and organizational approaches to information security, which helps employees to make sense of the priority accorded to information security within the organization. Accordingly, employees' adhere to information security policies since they assign a high value to organization information security themselves rather than merely try to meet the expectations of their peer. It is assumed that trans-

[3] Also known as: Organizational Citizienship Behavior (OCB)

formational leaders are capable of conveying the purpose and value of information security to their followers and thus enhance information security climate within organizations.

4.2.3 Research Design and Data Collection

To investigate the research question as presented above, the survey method was utilized in combination with partial least squares structural equation modeling for the statistical analysis of empirical data (see Chapter 3.3). An online survey was created and pre-tested in order to increase the studies validity. To assess clarity of the survey questions and instructions and to evaluate the overall measurement model, in the first step the initial set of items was reviewed by 12 information systems faculty members and students. In a second step, people of different age groups, as well as undergraduate and graduate students, were interviewed and asked for their feedback. The initial questionnaire was slightly modified based on the gained feedback.

For the final study, a simple randomized sample was used for the purpose of providing an unbiased random selection of participants. An overview of the demographic profile of the sample is provided in Figure 10. The questionnaire was distributed over social networks (e.g. Xing, LinkedIn, Facebook) and email addresses that were gathered from company websites. The first question of the survey eliminated those participants who were not employed. A total of 440 employees participated in the study of which 208 (47.27 %) produced usable data for statistical analysis. The response rate is acceptable given the nature of the study.

The questionnaire consists of two parts. In the first part, participants were asked to rate their subjective perception of transformational leadership by their respective supervisors. For this purpose, the multifactor leadership questionnaire (MLQ) form 5x-short was used. The MLQ constitutes a well-established measurement instrument for assessing leadership behavior that has been utilized by various studies (e.g. Antonakis et al., 2003; Avolio and Bass, 2004; Erkutlu, 2008; Sadeghi and Lope Pihie, 2012). In the second part, security climate, security motivation, and employees' security performance intention were assessed using multi item scales that were adopted from previous validated studies.

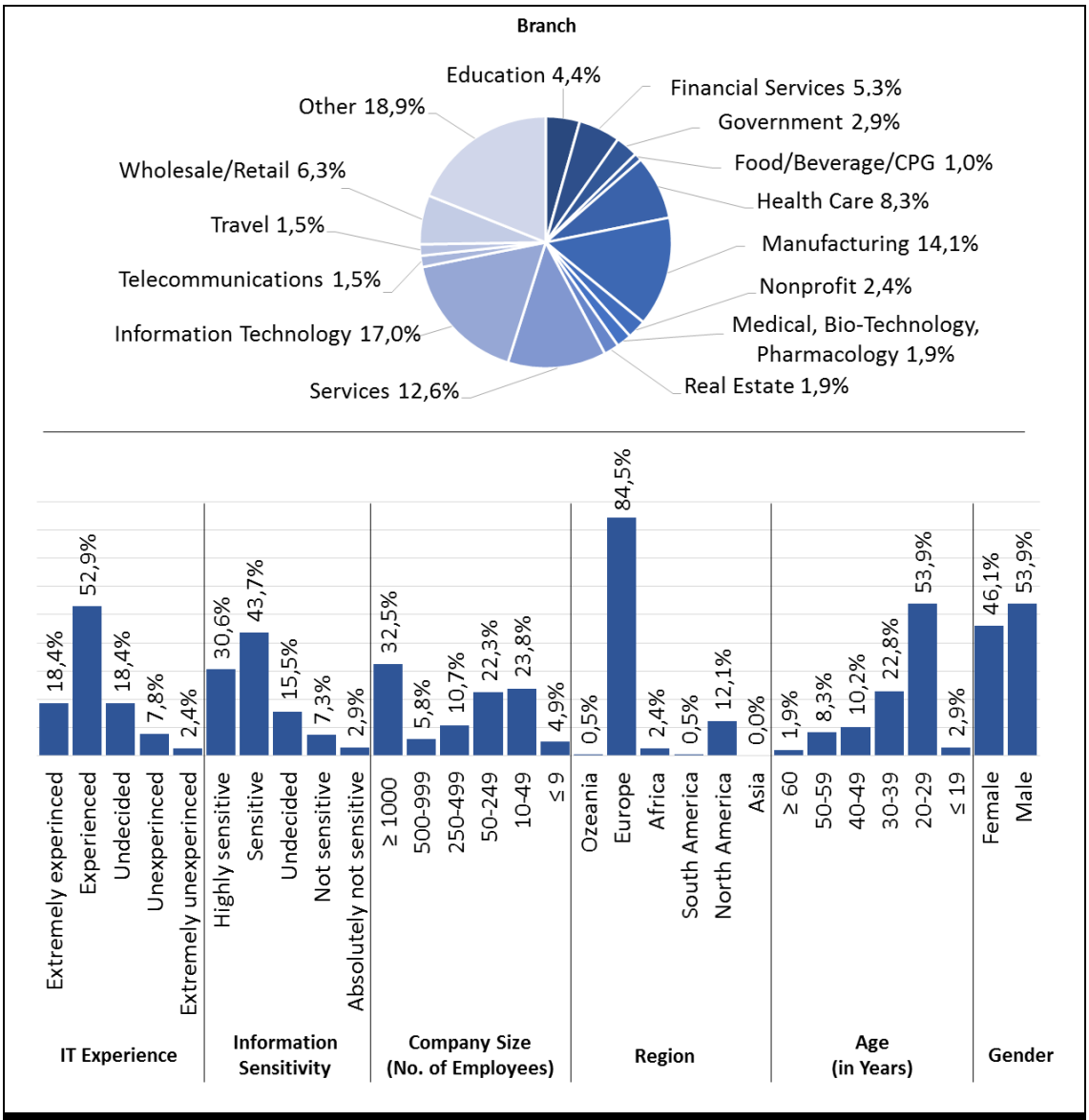


Figure 10: Demographic Profile of the Sample

The overall information security constructs were modeled with reflective indicators, because of the direction of the causality, the interchangeability of the indicators, the covariation among the indicators and the nomological net of the constructs (Petter et al. 2007). In contrast, transformational leadership is modeled as a second-order latent construct with first-order subdimensions as formative indicators. Although, this construct has been mainly modeled with reflective indicators in previous literature, MacKenzie et al. (2005) argue that modeling with second-order formative constructs would be more appropriate. Transformational leadership is conceptualized as having multiple behavioral sub-dimensions, namely: (1) Idealized Influence, which is divided into Idealized Influence (Behavior), and Idealized Influence (Attributed), (2) Individualized Consideration, (3) Inspirational Motivation, and (4) Intellectual Stimulation.

4.2.4 Discussion of Results and Implications

The results from structural model testing support the proposed research model in most parts. The major findings are summarized in Figure 11. Whereas results confirm a direct influence of transformation leadership on employees' security participation intention, no direct influnce of transformational leadership on employees' security compliance intention was found. Previous studies demonstrated that compliance intention depends on formal control measures. The exertion of formal control measures (i.e. rewards or sanctions) is closely related to transactional leadership (Avolio and Bass, 2004; Podsakoff et al., 2006). Transformational leadership is an extension of transactional leadership, meaning that transformational leaders are also capable of using transactional behavior in the form of contingent rewards or punishment. However, in the context of this study, only transformational leadership attributes were assessed. In order to completely explain the influence of leadership on compliance intention the examination of the full range leadership continuum is necessary.

The results of this study show a positive influence of transformational leadership on employees' perception of security climate. This finding is of importance, as security climate mediates the effects transformational leadership on employees' security compliance intention. By forming a positive organizational climate towards information security, transformational leaders ensure that employees' adhere to information security policies. Moreover, a positive security climate enhances employees' motivation towards information security. As results do not confirm a direct relationship between transformational leadership and employees' security motivation, the mediating effects of climate are emphasized. In addition the results also show that both, security motivation and security climate positively influence security compliance intention. Whereas results confirmed a positive relationship between security motivation and participation intention, findings do not confirm a positive relationship between security climate and participation intention. This finding contradicts studies from the field of employees' safety behavior research (e.g., Neal and Griffin 2006; Clarke 2006). It is argued, that a positive

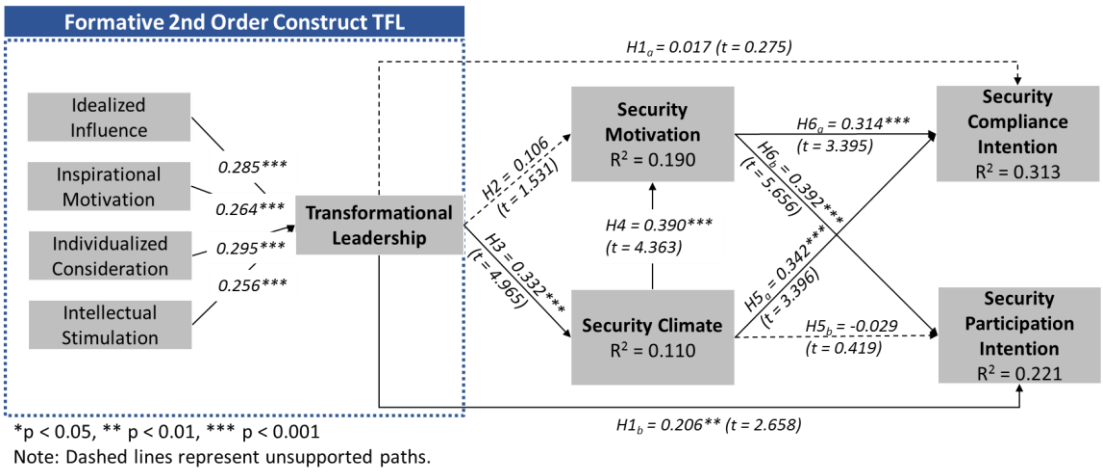


Figure 11: Results of the Structural Equation Modeling (SEM)

safety climate represents a leader that cares for employees' wellbeing (Clarke, 2006) However, this argument cannot be transferred to the context of information security as management commitment to information security does not primarily benefit employees' self-interests, but instead organizational group-interest.

Findings of this study provides several implications for practice. First of all, findings underline the importance of supervisor and managerial leadership behavior within the context of organizational information security. Consequently, in order to implement information security training and awareness (SETA) programs and to s sustainably improve information security, organizations must not only consider formal measures. Next to addressing employees' knowledge and skills for coping with threats to information security, they must also enhance supervisors' awareness and abilities to promote and convey the value and necessity of information security among employees by means of transformational leadership behavior. By stimulating employees' intrinsic motivation and enhancing organization security climate, transformational leaders help organizations to reduce formal control measures and to safe costs.

4.2.5 Limitations

One major limitation of this study is the assessment of employees' behavioral intettion by using self-reported data rather than measuring employees' actual information security behavior. As already discussed within section 4.1.3, the use of self-reported data referring to employees' behavioral intentions in the context of studies on employees' information security behavior is highly debated within academic literature. Due to the

lack of applicable, efficient and reliable means to measure employees' actual security behavior, the use of self-reported behavioral intentions is an established practice within this research area. Hence, this approach was chosen as a suitable method for this study. Nevertheless, when interpreting the results of this study, the argumentation of Workmann et al. (2008) has to be considered, that behavioral intentions are not necessarily bound to be in line with actual behaviors.

Siponen and Vance (2014) state that the use of generic questions distorts empirical results since "respondents need to use their memory and imagination" while responding. The authors advocate for the use of sprecific question in order to enhance the quality and relevance of empirical studies. However, there are mainly two reasons for using generic questions within the context of this study. In order to develop specific questions, it is necessary to have insight into the work environment of the participants and especially into the information security topics the participants have to deal with. For this study, a simple random sample was used and was not limited to countries, companies, branches, or job functions. Consequently, and due to the fact that all participants are unknown to the researchers, it was not possible to investigate a specific yet common and relevant issue. Furthermore, in order to increase the validity of the study, all items were adopted from previously tested, renowned and frequently cited studies in the research fields of employees' information security behavior or transformation leadership.

4.2.6 Conclusion

As shown in section 4.1, the research field of employees' information security awareness and behavior is replete with studies that discuss explanations for employees' security behavior by adopting behavioral theories from the fields of psychology, sociology and criminology. While these theories mainly focus on the employees' perspective, the role of managers and supervisors in the organizational information security chain has received only little attention within academic research. Introducing the concept of transformational leadership to the contemplated research field, this study presents several implications for research and practice. The results demonstrated the capabilities of transformational leaders to enhance the information security performance of their followers. Although previous studies showed that transformational leadership positively influences organizational and IT effectiveness (Cho and Park, 2007) this study is the first

to prove this connection in the specific context of information security. This is necessary since information security differentiates from other organizational contexts mainly due to two reasons: First, information security is mainly seen as inconvenient and hindering with regard to work productivity and efficiency. Second, information security does not primarily generate business value (Chan et al., 2005). This study shows that transformational leaders are capable of enhancing employees' information security performance and thereby complement or even supersede external influences like punishment. It would be interesting for future research to compare the effects of transformational leadership to other leadership styles, like transactional leadership and management-by-exception that utilize more external measures. An analysis of the whole leadership continuum as shown in section 2.2.2 will assists organizations in promoting and implementing information security measures. By addressing especially managers and supervisors within SETA programs, organization can enhance the training effects and reduce costs as the attitude and intetntions pass down to employees.

4.3 A Needs Assessment Process for SETA Programs

This section refers to the article entitled "Towards a Needs Assessment Process Model for Security, Education, Training and Awareness Programs - An Action Design Research Study" (cf. Appendix A4). The paper was presented at the, 21st European Conference on Information Systems (ECIS) in Utrecht, Netherlands (June 5 - June 8, 2013) and published in the conference proceedings. The ECIS is affiliated to the Association for Information Systems (AIS) and is considered to be the most prestigious platform for IS academics and professionals in Europe and the second most important IS conference worldwide. With recent acceptance rates in the low 30% range[4] and peer-reviewing information systems research papers, the conference guarantees high quality output. The paper discussed in this section was presented at the track "IS Security and Privacy".

4.3.1 Motivation and Purpose

One major finding discussed within the literature review section is that there are technical restrictions when it comes to measure and evaluate employees' actual information

[4] http://is2.lse.ac.uk/asp/aspecis/AcceptanceRates.htm

security behavior. This represents a problem not only for researchers but also for practitioners. Organizations started to implement security education, training and awareness (SETA) programs to provide their employees with awareness of information security risks and the necessary skills to protect organizational information assets. However, during the SETA program development and implementation process, it is necessary to evaluate the actual state of employees' security related behavior within needs assessment in order to ensure that those programs are efficiently aligned with organizational objectives. Organizations often face difficulties in managing an efficient and sustainable SETA approach when considering personnel security, user access control, and network security (Eloff and Eloff, 2005). Results of the literature review showed, that a generally accepted approach that focuses on basic organizational requirements does not exist as a gap between behavioral approaches in order to explain employees' adherence of security policies and the need of security managers to know which interventions to apply has evolved (Workman et al., 2008). In order to close this gap, in this research step a systematic and customizable approach is developed, that does not only capture and evaluate the actual state of employees' security awareness and behavior, but also assists organizations in determining a risk and priority measurement. Therefore the following reseachr Question is proposed:

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

4.3.2 Research Design

The objective of this research step is to develop a needs assessment process for SETA programs that can be applied within multiple organizations. In order to ensure methodological rigor while aiming at organizational relevance, the action design research (ADR) approach by Sein et al. (2011) was chosen as the underlying research methodology. As discussed within the first chapter of this dissertation, ADR addresses these two challenges by taking the influence of practitioners and the ongoing interaction with researchers within the specific organizational context into account and evaluates generalized IS artifacts through formalized learning that address a class of problems. Extending the narrow definition of IS artifacts as merely technical products (Sein et al., 2011), IS

artifacts can also encompass concepts (Järvinen, 2007), models, methods and instantiations (March and Smith, 1995; Hevner et al., 2004). Therfore ADR is applicable for this research step.

A German engineering company was the partner company for this research project. The company was suitable for this study for several reaons. First of all, employing 3,200 people in 60 countries (including Europe, America and Asia), the company provides international experience which helps to generalize findings for the worldwide IS community. Moreover, all IS activities, including information security, are centrally managed from its headquarters in Germany which allows unbureaucratic involvement of the researchers during the whole project. Last, the geographical proximity of the research facility and the companies headquarter facilitates the communication between the reseearchers and the involved project partners as personal meetings were possible at each time. The conducted ADR process consists of four stages (1) problem formulation, (2) building, intervention and evaluation (BIE), (3) reflection and learning, and (4) formalization of learning (Figure 12).

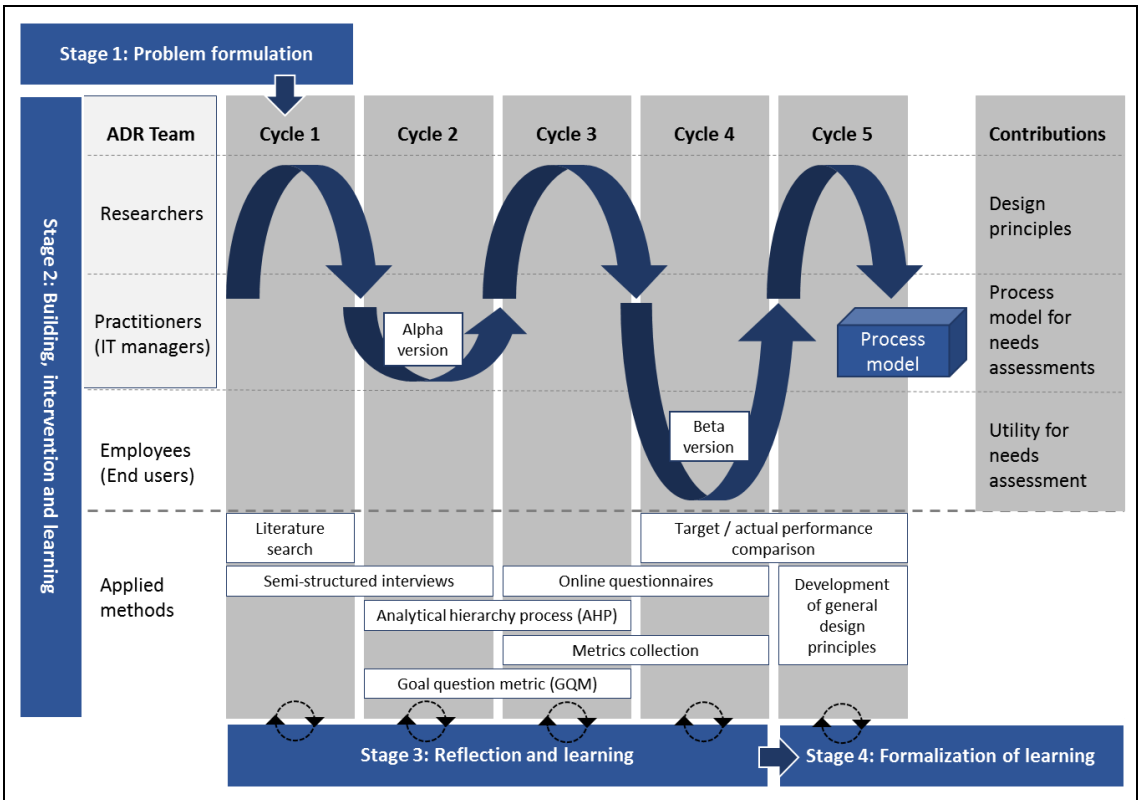


Figure 12: Reserach Design Based on ADR Approach by Sein et al., 2011

Stage 1: The target company faced the problem of how to capture the actual level of employees' security awareness and behavior in terms of a SETA needs assessment. The initial literature review facilitated to transfer the specific practical problem into an instance of a broader class of problems. An ADR team was formed, made up of researchers and members of the SETA project team within the target company, including the company's CIO and the security project manager.

Stage 2: The BIE stage consists of five cycles. In the first cycle, an initial process model was developed on the basis of literature analyses and the results of semi-structured interviews with experts from the target company. The continuous testing of the initial model throughout the following cycles within a real-world environment allowed for incremental shaping of the IS artifact. The gradually inclusion of IT managers and later end users provided sound feedback within the respective research phase.

Stage 3: The artifact evaluation was carried out parallel to stage two and was based on semi-structured interviews with practitioners and employees as well as comparison to existing literature.

Stage 4: The fourth stage aims at providing a general solution for the broad class of problems as it outlines the results of this study as design principles.

4.3.3 Results

The proposed process model for evaluating information security training and awareness needs (Figure 13) is based on the consideration of different perspectives on employees' security behavior. Due to the assumption that employees in different roles and positions display different security related behavior in certain areas, roles and focus areas are considered within the needs assessment process. The concept of focus areas is adapted from Kruger and Kearney (2006). Focus areas constitute critical risk areas in which the behavior of the employees is evaluated (e.g. 'use of mobile devices'). Since each focus area contains a different risk potential is of differt importance for each role, the inherent riskpotetial and importance are considered during the target value determination.

In order to measure employees' actual security behavior, security metrics have to be identified. The use of self-reported data to measure security-related behavior is prone to the problems of common method variance, consistency motif, and social desirability,

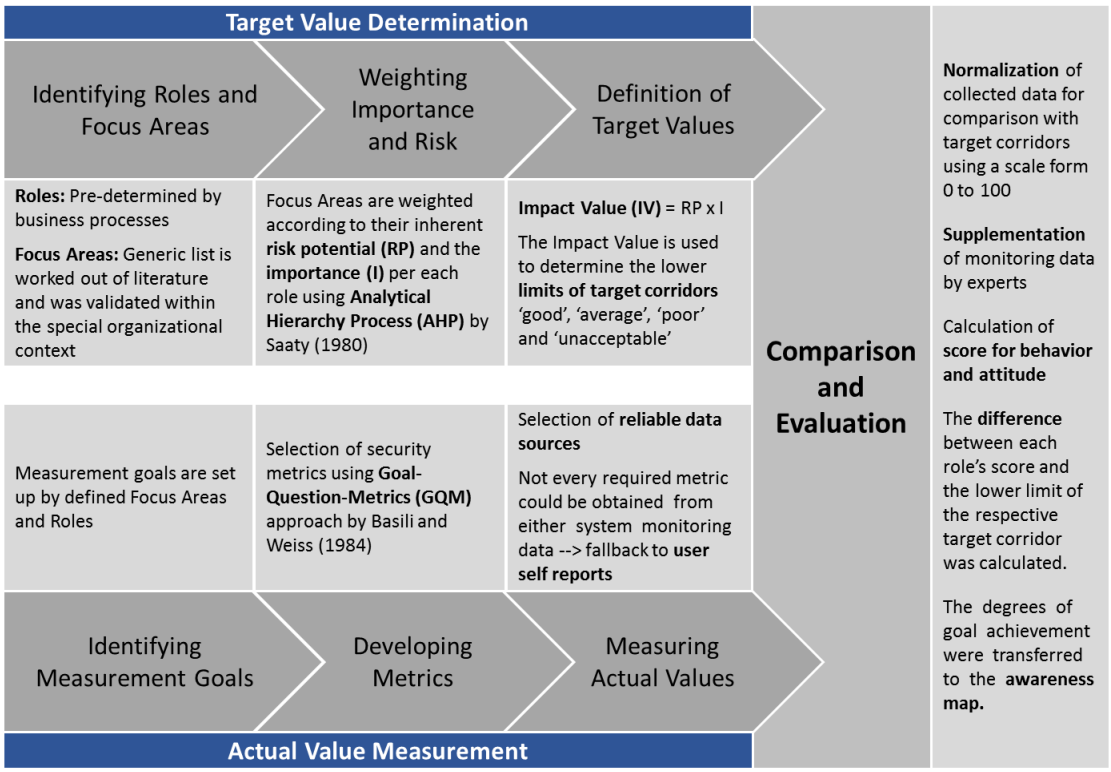


Figure 13: Process Model for SETA Needs Assessments

and results may be biased (Workman et al., 2008). Therefore, the integration of empirical data that determines actual behavior (e.g. system monitoring data, incident records) into the measurement process is preferable. To evaluate the gap between actual and desired behavior, a normalization process is needed to ensure that target and actual values are comparable.

4.3.4 Discussion

To provide a basis for determining and developing efficient training and awareness measures, the proposed needs assessment process demands for the considerisation of different perspectives on employees' information security related behavior. In the context of testing and evaluating the process model within an engineering company, roles and focus areas were selected as suitable filters. However, those perspectives can be adjusted to specific organizational requirements and can be e.g. business units, departments, or business processes. The combination of several perspectives facilitates a variable and detailed consideration of employees' security behavior within a company (Figure 14) in order to efficiently align SETA programs with specific organizational objectives.

With regard to the focus areas, several propositions exist in academic and specialist literature. However, organization-specific customization is neccessary. This requires a standardized approach (e.g. expert interviews, group discussions). The adoption of the AHP approach (Saaty, 1980) for weighting the focus areas led to the desired results but entailed unanticipated difficulties. Even though a definition of each focus area was sent to the participants, they struggled to understand the focus areas. The online questionnaire used for conducting the AHP consisted of, 180 pair wise comparisons, which meant a high workload for each participant. This led to a high number of questionnaires being incomplete. To prevent these difficulties, the use of a method that allows interaction with the participants (e.g. group discussions) to perform the AHP process is recommended. Alternatively, a simpler weighting process can be applied (e.g. absolute weighting), under the premise that less accurate results can be tollerated.Self reported data are considered less reliable than data from incident records or monitoring sytstems. However, since several aspects of employees' behavior and especialy employees' attitudes cannot be obtained from monitoring data or incident reports, the use of questionnaires is inevitable. Additionally, questionnaires are better for subsequent analyses, because results can be compared by using homogeneous scales. A major challenge emerged with regard to the inclusion of system monitoring data. During the study it became apparent that available data was not sufficiently detailed, demanding for manual adjustments. A mature system monitoring process is a necessary precondition for successfully integrating system monitoring data into a SETA needs assessment process.

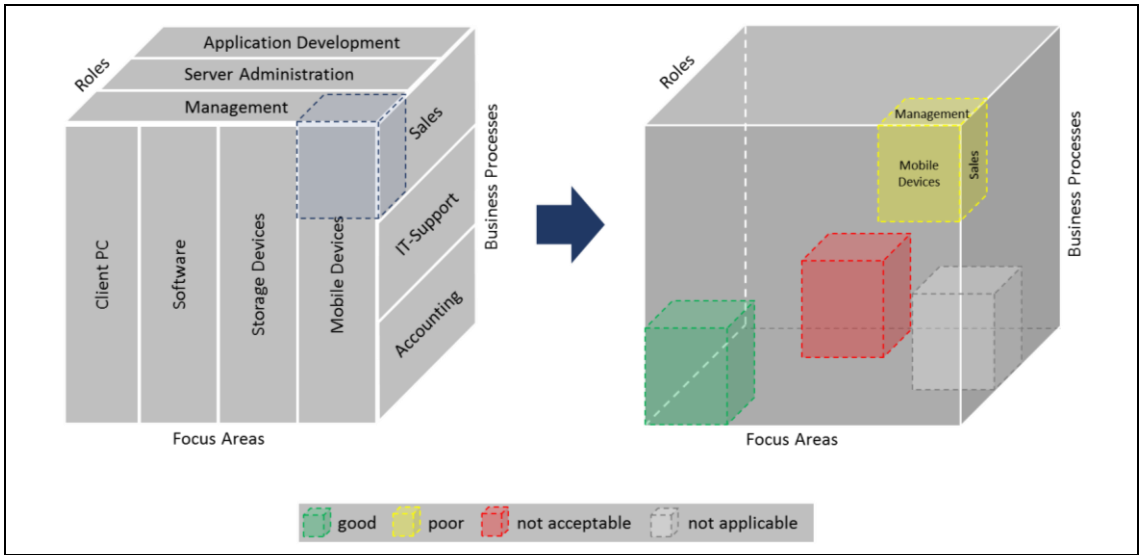


Figure 14: Considering Roles, Processes and Focus Areas for Assessing SETA Needs

4.3.5 Limitations

Following the ADR approach, the proposed model was developed and evaluated within the specific organizational context of a single company. Although, design principles that address a class of problems were derived through formalization of learning, it can be argued, that the generalizability of the study's findings are challenged by this fact. Lee and Baskerville (2003) argue, that IS research literature has "transferred, from statistical research to qualitative research, both the notion of sampling and the associated notion that a small sample size (e.g., only one organization) limits generalizability." However, the authors state that the adoption of statistical generalizability is an inappropriate measure for qualitative studies. According to Lee and Baskerville (2003), the design principles derived in the course of the development of the needs assessment process model are generalizable as they constitute "well-founded but as-yet untested hypotheses". However, this also implies that further testing, evaluation and refinement is needed in order to enhance the quality of the artifact and to enhance relevance of the proposed model. For example, case studies (e.g.Walsham, 1995) or applicability checks (e.g. Rosemann and Vessey, 2008) are suitable and well-established research methods that are suitable for this purpose.Moreover, future studies could investigate differences in branch or company size in order to uncover cross-organizational differences. For example, regarding the questions if information security requirements are much stricter in the financial or health care sector. Based on such further research it would be possible to identify neccessary adjustments of the proposed needs assessment process for different organizations or branches.

A further limitation is, that the suggested process was applied to one business process within the target company and measured employees' security behavior in two out of nine focus areas. Since the suggested approach is repetitive for each business process and focus area, it is not expected that substantial changes to the general design principles occur when more processes and focus areas are included. However, the design principles can be refined through experience from practitioners and through employee feedback during an organization wide roll-out of the needs assessment process. The focus of this study was to develop and validate an approach for needs assessments which represents the first step in the overall process of implementing a SETA program. It would be

interesting for future research to investigate the long term experiences of the application of the proposed needs assessment approach. Particularly in the context of developing concrete information security awareness and training measures, the suggested approach has to prove its utility, which is part of an ongoing research process as mentioned in the problem formulation stage. In the course of this study, an organization specific list of security metrics was developed. It would be valuable if future research provides a generic list of security metrics in order to complement the proposed process model.

4.3.6 Conclusion

This study contributes to scientific literature as it focuses on reducing the lack of generic process models in the context of employees' security behavior. As the initial literature review showed, previous research mainly addressed the theoretical explanation and prediction of employees' information security behavior by adopting different cognitive factors (see Chapter 2.1). The proposed needs assessment process model aims to measure and evaluate employees' security awareness and behavior in a real work environment and facilitates the development of concrete training and awareness measures. IT enables dynamic depiction of the current state of employees' security behavior within organizations and its changes over time.

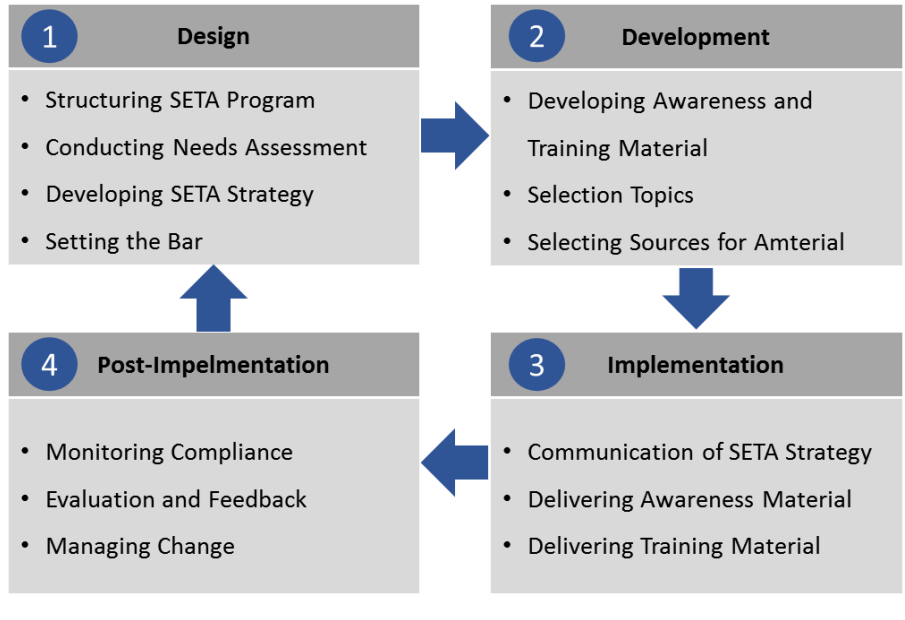


Figure 15: Life-Cycle of a SETA Program According to NIST-SP-800-50

The presented process can also be used for future research to test and evaluate the efficiency of different SETA measures in the organizational context, e.g. in field-experimental settings. Addressing a practical point of view, the developed process model builds directly on the NIST-SP-800-50 standard. This standard provides guidelines for developing and implementing a comprehensive SETA program within organizations, encompassing four sub-processes, namely Design, Development, Implementation and Post-Implementation (Figure 15). The process model developed and tested in the context of this study mainly addresses the needs assessment within the first sub-process. However, due to the generic design the process is also applicable for the compliance monitoring within the post-implementaion phase as it can be executed continuously. The proposed needs assessment process presents only a small part of SETA program lifecycle. Since standards like NIST-SP-800-50 only provide guidelienes but no detailed process description, further work is needed in order to develop a comprehensive process model that encompasses all four sub-processes.

5. Consumerization of IT and Organizational Information Security

5.1 Employees' Acceptance of BYOD Mobile Devices

This section refers to the sesearch article entiteled "The Influence of Security, Privacy, and Legal Concerns on Employees' Intention to Use BYOD Mobile Devices" that was presented at the, 19th Americas Conference on Information Systems (AMCIS), in Chicago Illinois, USA (August, 15 -, 17, 2013) and published in the conference proceedings. The AMCIS is the international conference of the Association for Information Systems (AIS) which is annually held in North, Central or South America. The conference provides a platform for presenting and discussing quality research and pedagogical development within the information systems domain[5]. The paper was submitted to the track „Information Systems Security, Assurance and Privacy". The paper was awarded with one of five „Best Conference Paper" awards from 15 nominees out of 250 accepted submissions.

5.1.1 Motivation and Purpose

The importance of mobile computing devices, such as smartphones and tablet PCs, is constantly increasing (Aldhaban, 2012). Recent studies show, that the global mobile penetration reached 87% with a total number of almost 6 Billion mobile subscriptions by the end of, 2011 (ICT, 2011). This was facilitated by an evolution in technology over the past decade (Moreno, et al. 2012), like innovations in form and usability of mobile devices and a wide-spread adoption of mobile data networks (Tu and Yuan, 2012). As a result, mobile computing devices became a part of daily life for many users (Moreno et

[5] http://ais.site-ym.com/?AMCISPage

al., 2012). Mobility is also a main driving factor of modern service society (Zaplata et al., 2009). Due to increased convenience, efficiency and productivity of mobile devices, more and more organizations are considering ways to implement mobile devices into their information technology (IT) infrastructure in order to use the advantages of flexibility these devices offer (Scheepers and Scheepers, 2004; Vershney, 2003). Consequently, scholars turn their attention on the impact of mobile technology on individuals and organizations (Scheepers and Scheepers, 2004; Kietzmann, 2008). At the intersection between private and organizational use of mobile computing devices, the concept of Bring-Your-Own-Device (BYOD) emerged over the past several years and is already common in organizations of all sizes (Johnson and Joshi, 2012; Miller et al., 2012). According to a study by Osterman Research (2012), 65% of organizations worldwide have adopted BYOD to some extend by the end of, 2012. Moreover, the study identified three main benefits that drive BYOD: Increased employee efficiency, improved employee satisfaction and reduced corporate costs. Nevertheless, this emerging trend is creating a "unique set of set of challenges for IT professionals" (Johnson and Joshi, 2012) as it "redefines the relationship between employees and the IT organization" (Niehaves et al., 2012). Consequently, concerns regarding security, privacy and legal aspects of BYOD are discussed in mostly practical literature (e.g. Osterman Research, 2012; Miller et al., 2012; Silvergate and Salner, 2011). According to Nievhaves et al. (2012) academic IS research literature is currently missing "a clear theoretical understanding" of the BYOD phenomenon as especially the negative effects of concerns on employees' acceptance of BYOD have been considered inadequate (Nievhaves et al., 2012). As the BYOD concept usually depends on employees' voluntary participation, employees' acceptance necessary precondition for a successful imlementation. To assist practitioners to mitigate barriers in the context of BYOD imlementation and to extend the theoretical understandig of employees' BYOD acceptance, the following question ins investigated:

> *RQ: To which degree do security, privacy, and legal concerns affect employees' intention to use BYOD mobile devices?*

5.1.2 Theoretical Background

A research model based on the theory of reasoned action (TRA) and the technology acceptance model (TAM) was developed. According to the TAM, behavioral intention is

the key dependent variable to describe users' acceptance of IT and has been utilized in numerous studies (e.g. Taylor and Todd, 1995; Venkatesh and Davis, 1996; Nysveen et al., 2005). In the context of this study, users' acceptance is employees' intention to adopt the BYOD concept by using privately owned mobile devices for working purposes. As proposed by the TAM and TRA, employees' intention to use BYOD mobile devices is significantly influenced by their attitude towards BYOD. Attitude results from the evaluation of the believed outcomes of a certain behavior (Fishbein and Ajzen, 1975). Oliver and Bearden (1985), referred to possible outcomes as benefits or problems. Employees regard IT at the workplace to be beneficial if it helps them to perform their jobs. These benedfits are indicated as perceived usefulness (Davis et al., 1989). According to the TAM, perceived usefulness affects attitude and also has a direct influence on intention. In the context of BYOD, several studies revealed benefits for both, employees and organizations. For example, the use of the privately owned mobile devices at the workplace can raise the satisfaction of employees and therefore increase their motivation (Niehaves et al., 2012). Moreover, the use of BYOD mobile devices increases overall productivity and efficiency (Osterman Research, 2012). With regard to problems of organizational IT adoption, several studiesfocused on perceived uncertainty (e.g. Harnesk and Lindström, 2011; Spears and Barki, 2010). Considering the usage of BYOD mobile devices, we define perceived usefulness as perceived benefits and problems as perceived uncertainty and adapt these constructs to our research model.Following Pavlou et al. (2007) security concerns and privacy concerns affect perceived uncertainty. Additionally, several studies emphasized the importance of legal concerns in the context of BYOD (Miller et al., 2012; Osterman Research, 2012; Silvergate and Salner, 2011). Consequently, legal concerns are considered to be a third factor influencing uncertainty within the proposed research model. With regard to security concerns, academic literature points out that the integration of mobile technology into the corporate IT infrastructure entails information security risk (e.g. Beulen and Streng, 2002; Giessmann et al., 2012; Scheepers and Scheepers, 2004). The use of BYOD mobile devices, corporate information security is exposed to new risks (Niehaves et al., 2012; Tu and Yuan, 2012) since privately owned devices provide a greater likelihood of potential violations of the corporate information security policies (Miller et al., 2012; Osterman Research, 2012). Privacy concerns in the context of BYOD originate from employees' apprehension that

private data (e.g. emails, photos, GPS data etc.) are exposed to the employer. It is difficult to differ between private and organizational data occur if employees use their privately owned devices for working purposes. Consequently, Miller et al. (2012) argue, that the privacy aspect is potentially more important than the security aspect. Several studies addressed end users' privacy concerns in the context of general mobile device usage (e.g. Figge, et al., 2003; Ho, 2009). Findings suggest that privacy concerns do affect an end user's acceptance of mobile services.In the context of BYOD, legal concerns refer to existing statutory regulations between employers and employees (Osterman Research, 2012; Silvergate and Salner, 2011). This affects mainly two aspects: First, BYOD mobile devices may cause violations of working hour regulations as employees "stay connected to their jobs on nights, weekends and even vacations" (Silvergate and Salner, 2011) and therefore demand compensation for their expanded working time. Second, employees are concerned about being hold liable if corporate information gets lost due to loss, theft or damage to their device.

5.1.3 Research Design and Data Collection

In order to empirically test the proposed hypotheses, an online survey was designed and distributed to employees of various German organizations. Only employees who privately own a mobile device (i.e. smartphone and/or tablet) were considered in order to accurately measure the hypothesized constructs. The questionnaire was pretested with employees and experts in the field of quantitative empirical research by means of intensive discussions. Multiple item constructs were chosen using a five-point Likert scale, which ranged from „strongly disagree" to „strongly agree". The survey was started by, 298 people, of which, 203 were employees (186 in possession of a mobile device). A total of, 151 persons completed the survey. The demographic profile of the sample is shown in Figure 16. The rotated exploratory factor analysis (EFA)[6] by means of a principal component analysis with varimax rotation showed that all factor loadings exceed 0.50 on their own construct which indicates convergent validity of the constructs. Moreover, results confirm discriminant validity as no cross loadings among the constructs that exceed 0.50 are existent (van der Heijden, 2003).

[6] Conducted with statistical software program IBM SPSS Statistics version 20

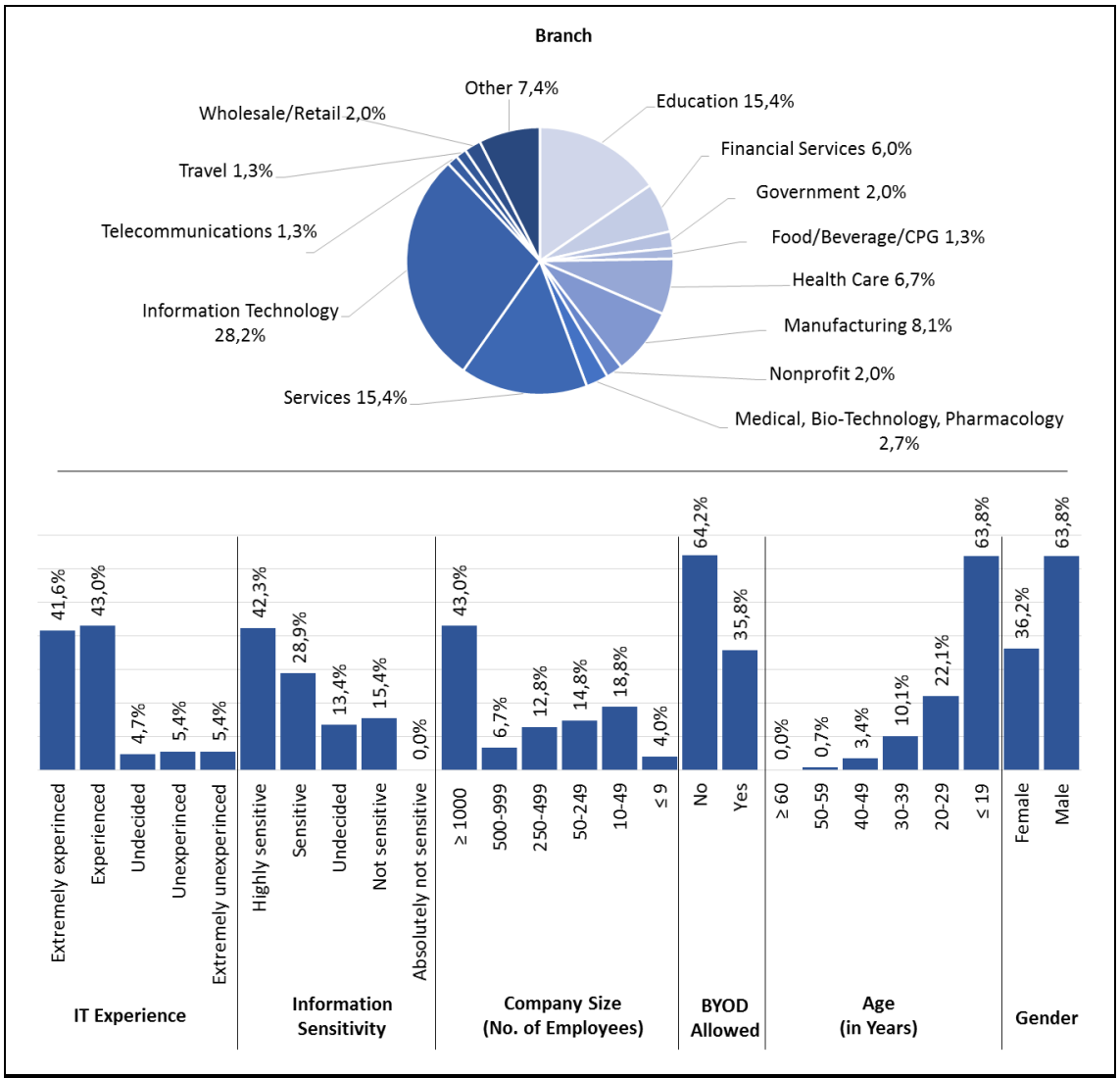


Figure 16: Demographic Profile of the Sample

In addition, internal consistency of the scales was further validated with the analysis of composite reliability (CR), which is similar to Cronbach's alphas. Results show, that CR values are ranging from 0.93 to 0.98 and therefore exeed the value of 0.70 as recommended by Gefen, et al. (2000). Furthermore, average variance extracted (AVE) as another indicator for convergent and discriminant validity ranges from 0.79 to 0.95 and clearly exceeds the lower limit of 0.50 as recommended by Fornell and Larcker (1981). Consequently, internal consistency of the scales as well as convergent and discriminant validity are demonstrated by means testing for CR and AVE.

5.1.4 Discussion of Results and Implications

The theoretical model is strongly supported by the results of empirical investigation as all hypotheses were supported with high significance (Figure 17). It was found that both,

perceived benefits and perceived uncertainty have significant influence on employees' attitude towards BYOD and therefore on employees' intention to use privately owned mobile devices for working purposes. However, the positive influence of perceived benefits clearly exceeds the negative impact of perceived uncertainty. Moreover, security, legal, and privacy concerns were proven to be major antecedents for employees' perception of uncertainty, explaining the majority of the construct's variances. In this context it is notable that the influence of privacy concerns is considerably lower than the influences of security concerns and legal concerns. With regards to Miller et al. (2012), who supposed that the privacy aspect is potentially more important than the security aspect, findings of this study reveal that employees have contradictory perceptions of this topic.

Furthermore, based on a 5 point Likert scale, all constructs' response mean values are within an interval of < .80 to the value of 3. These results show, that employees have a general indecision towards the use of privately owned mobile devices for working purposes. The majority of existing market research studies discovered increased job satisfaction through the effects of BYOD (Niehaves et al., 2012). On contrast, our theoretical study shows that employees are unsure as to whether using BYOD mobile devices would be beneficial or is related to security, legal, and privacy problems. The negative tending mean value of employees' attitude implies that employees have a slightly negative position towards BYOD, which is another contradiction to previous market research studies.

Since BYOD programs are usually not mandatory, employees' acceptance is crucial for a successful implementation. Consequently, organizations have to change the slightly negative attitude of employees towards BYOD, because attitude is the main driver of usage intention. Since this study reveals that an increase in employee perception of the

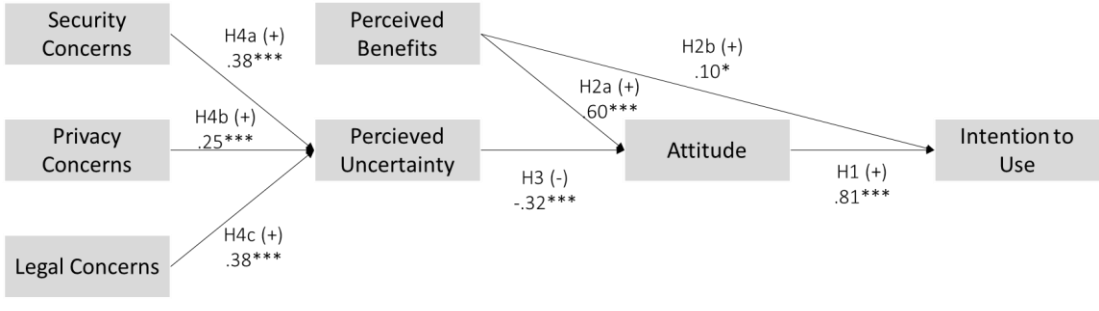


Figure 17: Results of the Structural Equation Modeling (SEM)

benefits of using BYOD mobile devices will have the greatest impact on their attitudes, it can be suggested that that organizations should aim at communicating the advantages to their employees when planning to adopt the concept of BYOD. Nevertheless, employees' perception of uncertainty cannot be neglected as it plays an important role. Therefore, a legal framework and privacy policies have to be established in order to mitigate employees' perceived uncertainty.

5.1.5 Limitations

This study shows a strong influence of privacy and legal concerns on employees' intention to use BYOD mobile devices. These two aspects strongly depend on specific laws and most likely vary from contry to country. Moreover, national cultures significantly impact IS studies (Leidner and Kayworth, 2006). Since only German employees' were considered within the context of this study, it was not controlled for cultural differences. Therefore, results can only be generalized to other cultures with caution. Future research is needed in order to uncover those cultural differences that influence employees' perceived benefits and perceived converns of BYOD among different cultures. Moreover, the sample size of N=151 completed questionnaires provides a relatively small sample size. However, according to Fornell and Larcker (1981) the partial least squares (PLS) analysis applied in this study has minimal demands for sample size.

The focus of this study was mainly to discover and analyze the impact of perceived uncertainties on employees' intention to use privately owned mobile devices for working purposes. Therefore, the questionnaire emphasized the disadvantages of the BYOD concept leading to a possible bias towards the negative side. Consequently, the findings that the positive influence of perceived benefits on employees' attitude is greater than the negative influence of employees' perceived uncertainty needs further evaluation. In addition, the possible benefits of the BYOD concept from an employees' point of view have demanded for further investigation.

5.1.6 Conclusion

The concept of Bring-Your-Own-Device and its advantages and disadvantages for both, employees' and organizations, is mainly discussed in practical literature and has received little academic attention (Niehaves et al., 2012). This study was among the first

to theoretically examine this topic within the IS research domain. Motivated by the increasing importance of the topic and the fact that consumerization of IT in general and BYOD in particular already impacted organizations of all sizes, this study provided implications for practitioners and future research.

The study aimed at analyzing the impact of perceived benefits and perceived concerns on employees' intention to use privately owned mobile devices for working purposes. In this context, the main focus was on employees' perception of concerns in the form of uncertainties with regard to privacy, security and legal issues. This focus was chosen in order to present new insights into the contemplated field, since practical literature commonly emphasized the benefits of the BYOD concept. The results of the study revealed several unexpected results that contradict most of the pratical literature. First, the results of the study show that employees' are indecisive towards their intentention to adopt BYOD. Second, it was shown that information security and legal issues are greater causes for employees' concerns than their individual privacy. The findings of this study provide several implications for practice as it is shown that organization also have to account for employees' concerns towards BYOD and can not only focus on the benefits. Furthermore, the findings that contradict assumptions within practical literature as disuccesd above provide input into academic discussion. The relevance of the research is shown in the increasing number of publications addressing BYDO since 2013 (e.g. Hopkins et al., 2014; Weeger and Gewald, 2014; Putri and Hovav 2014, Ortbach et al., 2014)

5.2 An IS Governance Reference Model for the Nexus of Forces

This section refers to the article “Big Data, Social, Mobile, and Cloud Computing: A Reference Model for IS Governance and the Nexus of Forces” that was submitted to the Journal of the Association for Information Systems (JAIS). The JAIS is the major journal of the Association for Information Systems, and publishes high quality articels in the field of information systems resreach. Especially it addresses topics with regard to global information systems. The journal promotes rigorously developed conceptual and empirical studies and encourages theory based multi- or inter-disciplinary research.[7]

5.2.1 Motivation and Purpose

The trends of social, mobile, and cloud computing, as well as big data analytics enable groundbreaking opportunities that impose far-reaching changes to business, economies, and societies. (Goes, 2013). Although the four trends have evolved independently, their convergence and mutual reinforcement provide unique challenges for organizations. Consequently, these trends are referred to as the ”Nexus of Forces”[8] by the IT research and advisory company Gartner and are predicted to have a lasting impact on the information systems (IS) domain and provide challenges and opportunities that go beyond mere technical aspects. Consumerization and and ubiquity of smart mobile devices resulted in a shift in power towards and emancipation of the users that will also impact traditional management and control mechanisms such as IS governance. As organizations aim to maximize opportunities from the Nexus of Forces while mitigating associated risks, a demand for a robust framework for governing these technologies arises. Focussing on the alignment of business and IT strategy, IS governance becomes a focal point (De Haes and van Grembergen, 2004; van Grembergen et al., 2004; Dahlberg and Kivijärvi, 2006). IS governance aims to design and implement effective IS structures and processes and consequently has a direct impact on the benefits generated by organizational IT investments (Webb et al., 2006). Previous research has confirmed a positive correlation between IS governance and organizational performance (Looso,

[7] http://aisel.aisnet.org/jais/
[8] For details see: http://www.gartner.com/technology/research/nexus-of-forces/

2010). Although recent studies addressed IS governance in the context of one of the trends social, mobile, and cloud computing or big data analytics (e.g. van Osch and Coursaris, 2013; Heier et al., 2012; Malik, 2013) none of these combine the forces within a comprehensive and integrated reference model. In order to address this gap, the aim of this study is to create a reference model that addresses the new requirements and challenges presented by the Nexus of Forces. Consequently the following research question is proposed:

> *RQ: How do the new challenges of big data, social, mobile, and cloud computing influence IS governance?*

5.2.2 Research Design

As the goal of this research is to develop a reference model, it is neccessary to define the construct 'reference models' at first. According to Goeken (2003) "a reference model is a recommendation that is useful for the development of specific models. It provides general solutions for a (abstract) class of problems that it is related to and supports the solution of specific tasks as it provides a starting point and serves as a model pattern for a class of modeling issues." From the perspective of information systems research, Fettke and Loos (2004) differ between reference models as a phenomenon in the object domain and reference models as a theoretical construct in the statement domain. Reference models in the object domain are existing phenomena, which are described and explained by the application of scientific methods. Reference models in the object domain, however, are theoretical constructs that have been defined by scientists. The content of reference models should be approtiate for the re-use in the design and construction of further specific models. Consequently, the recommendations contained in the reference models must fullfill the requirements of general validity and applicability. Reference modeling is typically folowing a structured approach, which involves the model constructor and the user of the model. The constructor is creating the model according to the requirements of the users (vom Brocke, 2003).

In order to obtain user requirements and to ensure the demands for general validity and applicability, a research approach consisting of three stages was applied (Figure 18). The

first stage builds the prepearation of the research by providing the theoretical grounding. After framing the problem, a literature search through renowned academic data bases (i.e. AISeL, IEEExplore, ScienceDirect, etc.) was conducted. In order to ensure rigor, the literature search and analysis process followed guidelines by Webster and Watson (2002), Levy and Ellis (2006), and vom Brocke et al. (2009). Based on analyses of identified relevant literature, an initial conceptual model was identified that served as a starting point for in depth examination in the further research process.

For the data collection pahse a Delphi approach was chosen as this flexible method is especially suitable to explore new issues with subjective and complex judgments of experts (Kendall, 1977). Therefore, experts in the field of IS governance with regard to the trends described by the Nexus of Forces were identified towards the end of the preparation stage. For this study, 18 participants from different branches were acquired. Finally an interview guideline was created. The second stage, was focused on conducting and interpreting expert interviews. In the first round, single interviews were conducted with each of the, 18 experts in order to explore the opinion of the experts and to evaluate the initial assumptions and conceptual model. Each interview was recorded and transcribed for analyzing purposes. Qualitative data analysis (Punch, 2005) and coding techniques were used to analyze and interpret the transcribed responses. Open coding was used to identify concepts and as initial labels were attached to the data. Within selective coding, higher level categories were generated from the descriptive open codes. Based on the coding results, an aggregated group response was generated and the initial conceptual model was refined. The results of the first round of interviews were presented to the participants in round two. Within the second round, seven experts participated in a focus group (Krueger and Casey, 2009) in order enable discussion among the experts. The other participants were again surveyed using qualitative interviews or written questionnaires. Overall, 14 out of, 18 experts (78%) participated in round two. While results from round one were essentially confirmed, the findings were significantly extended. Due to the homogeneity of the participants' responds, a saturation was observed and the Delphi process was finished after round two. In stage three, the results of the Delphi study were summarized and a reference model was created based on the expert opinions.

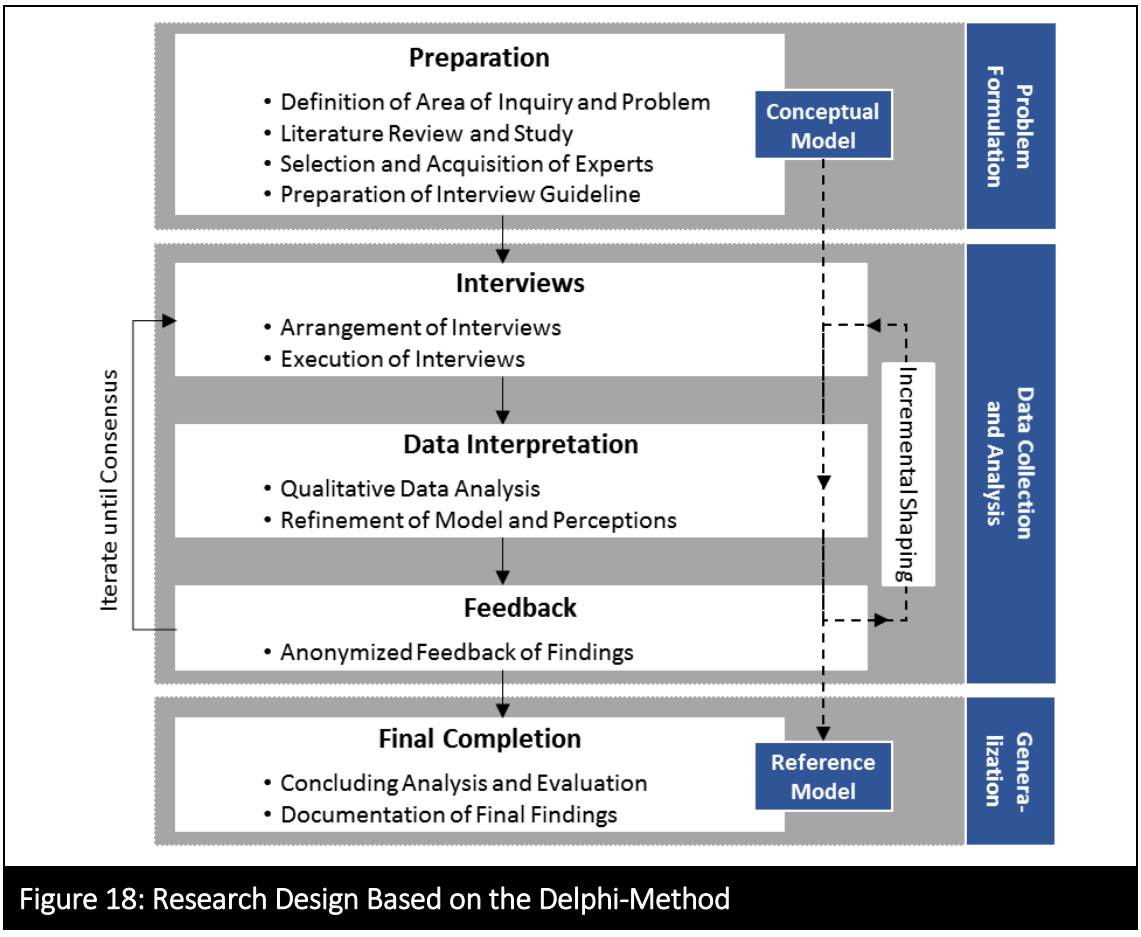


Figure 18: Research Design Based on the Delphi-Method

5.2.3 Findings

Based on the results of the initial analysis of existing governance literature and the findings by Gartner (2013) within the problem formulation stage, a conceptual model was created as depicted in Figure 19. Accordingly, each of the four forces (social, mobile, cloud, and information) as well as the four forces in combination are assumed to have an impact on organizational governance structures and organizations in general. This

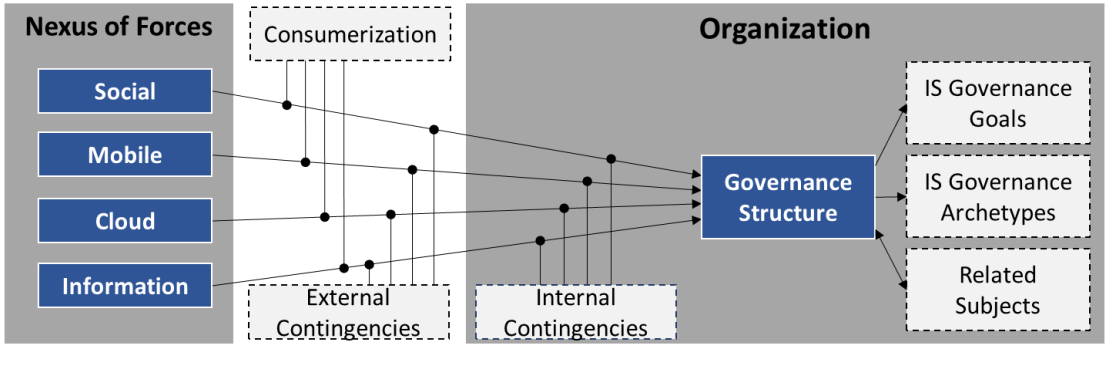


Figure 19: Conceptual Model of the Influence of Nexus of Forces on IS Governance

impact is moderated by the consumerization pressure, as well as by external and internal contingencies (for details on contingencies see chapter 2.3.2). Organiza-tional governance structures consist of the corporate governance and IS governance including their goals and archetypes as well as related subjects (for details see chap-ter 2.3.1). The proposed reference model (Figure 21) based on the results of the Delphi study presents a more detailed view of the initial assumptions from the con-ceptual model. Results show, that the environment of an organization provides sev-eral external contingencies that determine the impact that can be created by the Nexus of Forces. Regulations build an enclosing frame that describes legal guidelines for organizations. Within this frame, social and political influences as well as techno-logical influences affect the adoption of social, mobile, and cloud computing, as well as big data.

Consumerization has been identified as the main driver for the Nexus of Forces in organizations. The resulting adoption pressure affects organizations mainly on the business level. Therefore, the handling of the Nexus of forces is not a primary IS responsibility, as corporate governance has to set structures concerning IT investment, business application and IT principles in the first instance. The IS governance is subordinated to the corporate governance and can be devided in two major parts, information governance and technical governance. Due to increasing quantity and importance of information, information governance is gaining in significance. Basic rules and policies for processing, and storing information assets within an organization are described in the corporate governance frame, defined by corporate governance with expert input from IS governance. In this context, the information governance frame does not primarily address technical solutions. The main focus of IS governance decisions is on the implementation of technical solutions in accordance with strategies and guidelines defined on the corporate governance level. Therefore, it defines the technical governance frame which sets up guidelines with regard to IT architecture and infrastructure. The IS management is located below the IS governance and is responsible for the operative implementation of strategies and the adherence of guidelines.

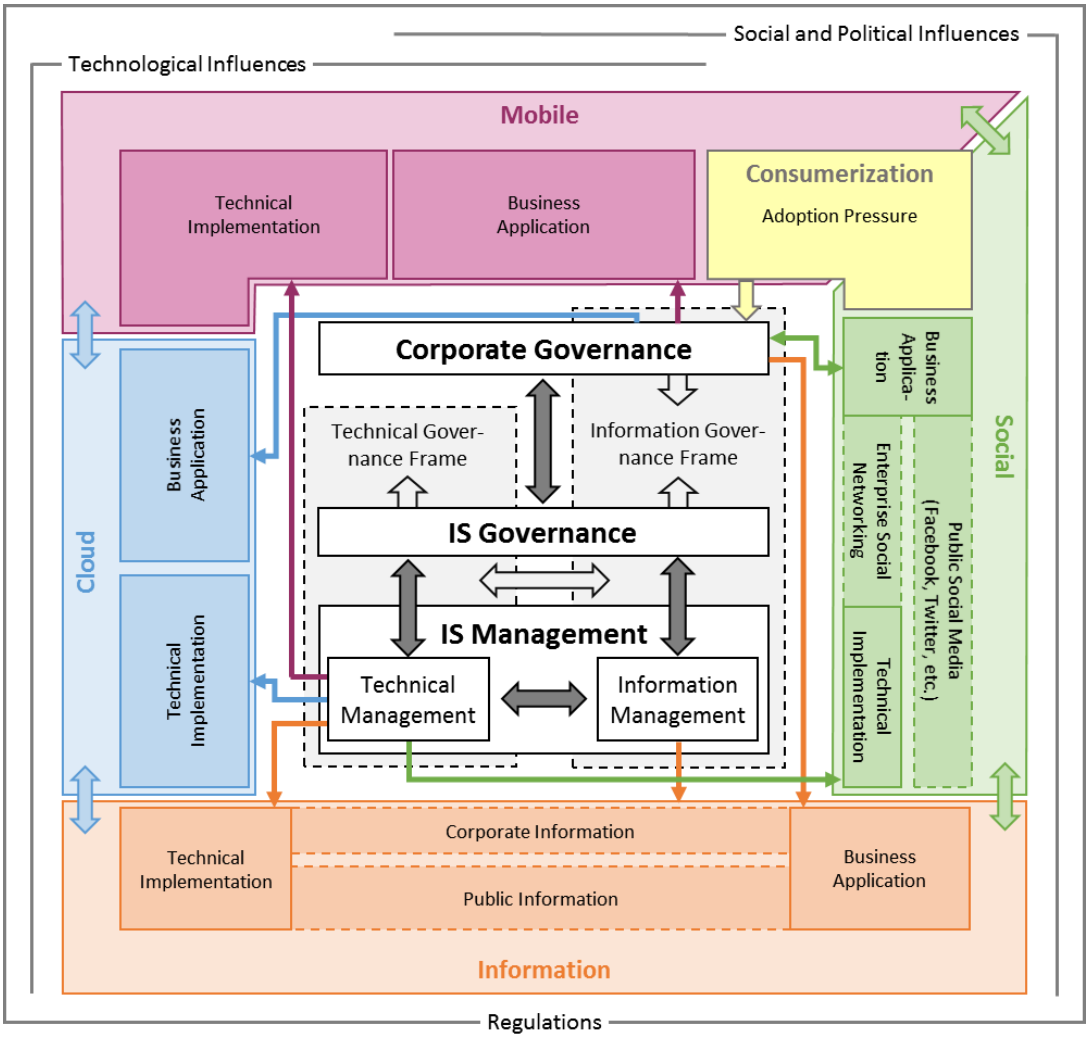


Figure 20: Proposed IS Governance Reference Model for the Nexus of Forces

5.2.4 Discussion

With regard to internal contingencies, the role and importance of IS within an organization is a major determinant of the impact that the Nexus of Forces is able to create on business and governance levels. Organizations can view IT and IS as innovators or from a rather conservative view (Chen et al., 2010; Leidner et al., 2010). Experts from organizations that regarded IS as an innovator rated the potential impact of the Nexus of Forces higher than participants with a rather conservative attitude towards IS. For instance, organizations that operate close to the consumer have experience with the new technologies and are steadily exploring new opportunities to add additional value. Organizations with a static business environment see no need to investigate cloud, mobile, and social computing or big data as they see more risks than benefits.

Furthermore, the Nexus of Forces impacts the governance archetypes within organizations. IS governance literature, generally distinguishes between centralized and decentralized structures. However, the Nexus of Forces continues to challenge this stringent separation of centralized or decentralized governance designs. On the one hand, consumerization pressure demands for flexible adjustments to cultural, social, and regional aspects with regard to employees' and business requirements. Centralized governance approaches tend to fail these demands due to inflexibility that results from extensive communication and coordination processes. On the other hand, the Nexus of Forces provides a multiplicity of new challenges and risks to organizations and especially IS governance as it, for example, shifts more power to the user. Therefore, decentralized approaches can fall short in defining stable and lasting infrastructures. Consequently, hybrid approaches will gain more importance (Andriole, 2012) as these attempt to balance the contrasts of standardization and innovation (Weill and Ross, 2004a).

As popular science mainly emphasize the benefits of the Nexus of Forces, this study also focuses on the accompanied doubts, concerns and risks. The trends of cloud, mobile, and social computing or big data provide an increased level of complexity for organizations and their established IT infrastructures. Consequently, as part of a cost-benefit analysis, organizations need to decide whether it is worthwhile or not to investigating in the new technologies. Organizations have to analyze the opportunities and threats of the Nexus of Forces diligently. Thereby they have to take in mind that an implementation or adaption will demand an adjustment of governance structures. Organizations face the challenge to react with foresight and not to adopt the Nexus of Forces too eraly, but also not to react too late to the upcoming adoption pressure. A possible consequence of disregarding the demand for new technologies is that shadow IT can emerge. If organizations fall short in implementing technologies that users know from private use, users might try to build their own solutions in terms of shadow IT. Organizations have to position themselves towards the Nexus of Forces, establish rulesas well as an appropriate strategy, and adjust governance structures. A well-implemented governance can help to keep the new technologies and opportunities manageable.

5.2.5 Limitations

This study is an initial attempt to explain the impact that the interconnected trends of social, mobile and cloud computing as well as big data have on organizations in general and on IS governance in particular. Consequently, the developed reference model does not raise the claim of being exhaustive. Future research is needed which should build on the suggestions developed in this study in order to refine and validate the implications. Due to the rise of the Nexus of Forces many organizations are currently in the midst of intense internal negotiations attempting to redefine the role of the IT function and the CIO. The question arises whether existing IS governance approaches can be adjustetd or the whole view on organization IS governance needs to be changed. As a result of the novelty of the topic, this question could not be sufficiently answered within the expert panel and demands for further in depth investigation. Moreover, since this study has a broad perspective on the Nexus of Forces and IS governance, future research can focus the discussion on just one aspect of governance that are highly impacted by the Nexus as identified within this study (e.g. governance archetypes). The experts that were interviewed in the context of this study were mainly from the industry branch. However, as stated in the discussion, it is likely that the impact of the Nexus of Forces varies between different organizations and branches. A further limitation arises from the use of qualitative expert interviews in order to collect empirical data. In general, qualitative methods for data collection raise concerns with regard to the inductive reasoning as subjective observations are used in order to develop generalized and verifiable theories. However, inductive assumptions are always uncertain assumptions as they are not based on concrete observable facts (Neumann, 2011). To mitigate these methodological limitations, a structured, intersubjective as well as comprehensible research approach was used, that was based on established research methods. Moreover, the mix of interview types (single interviews and group interviews) is uncommon for Delphi studies. The adoption of group interviews within the second round of the Delphi study aimed to enhance discussion among the expert panel members in order to get a deeper understanding of the subject matter. However, it was not possible to conduct focus groups with all members of the expert panel due to time restrictions of the members. The focus group provided evidence that was discussed with the remainder of the expert panel in personal or written interviews.

5.2.6 Conclusion

The study described within this section is based on a Delphi approach in order to collect qualitative empirical data from 18 top management experts of IS (governance) in two rounds of interviews. A conceptual model derived from a status quo literature analysis was uses as a starting point in order to develop a reference model for IS governance and the Nexus of Forces.Building on the assumptions from the reference model, it is argued, that the role of corporate governance concerning IS decisions is increasing due to the Nexus of Forces and the underlying consumerization pressure. The shift of responsibility and accountability towards the business management level and forces IS governance to focus on technical aspects of IS and provides consulting input into decisions made on the top management level within an organization. Consequently, organizations are required to rethink and redefine the role of IT/IS function and the role of the CIO. Furthermore, it is assumed that the Nexus of Forces challenges strict centralized or decentralized governance approaches and can lead to a change towards hybrid governance approaches and federal archetypes.

This study was carried out over a span of a year interviewing 18 top management experts in the field of IS governance. Although the participants revealed indepth expert knowledge within the lengthy interviews, the novelty and complexity of the topic made it difficult to elaborate concrete implications for each aspect. Therefore, future research and discussions are needed that focus on single aspects of the phenomenon. However, this study provides a comprehensive overview that facilitates to uncover important aspects. In this context, the presented reference model can serve as a guideline for future research. The global trends described by the Nexus of Forces are already impacting organizations and are gaining increasing attention from practitioners and outlets of popular science. To rise the relevance of IS research and to not fall behind popular science, it is necessary to investigate the impact of big data, social, mobile, and cloud computing on organizational IS.

6. Overall Conclusion

The research process described in this dissertation addresses two coherent research areas. The first area is directly focused on employees' information security awareness and behavior and constitutes the main focus of this dissertation. This area was addressed by overall four studies within the whole research process of which the three major publications are described in chapter 4. The second area deals with the influences of consumerization of IT on organizational information security and thereby focusses on a topic that is closely related to employees' security behavior. By considering the impact of consumerization and the resulting challenges organizational information security management is facing, chapter 5 broadens the scope of this dissertation. Overall four studies that address this topic were conducted, two of which are described chapter 5. After systematically displaying the results of the cumulative research process within the chapters 4 and 5, the purpose of this chapter is to reflect upon the gained insights. First, in this section the central results of the research are summarized. Building on that, implications concerning the role of employees within the organizational information security chain are worked out with regard to researchers' and practitioners' point of view. Furthermore, the overall research process is critically reviewed and limitations of the present dissertation are discussed. As a final point, issues and areas for future research are derived in the final section of this dissertation.

6.1 Summary of Results and Implications

6.1.1 Employees' Information Security Awareness and Behavior

The first step of the research process aimed at developing a theoretical foundation. Therefore, a structured literature review was performed. It was identified that the research field of employees' information security awareness and behavior is characterized by a majority of empirical studies that are mainly of quantitative nature. Addressing the

researchers' point of view, the literature review showed that the comtemplated research field is replete with studies dealing with TAM, TPB/TRA, GDT and/or PMT and therefore provides arguments to incorportate further theories in order to enhance the theoretical understanding of the subject matter. Moreover, results show that researchers mostly rely on employee self-reports in order to measure behavioral intention rather than actual behavior. Although being aware of the weaknesses of this approach, researchers argue that due a lack of an appropriate and applicable method of assessing employees' actual security behavior in a real work environment the use of self-reports cannot be avoided. From a practical point of view, results of the literature anlysis emphasize the importance of the design and the enforcement of information security policies. For example, employees' perception of the usefulness of security policies as well as employees' perception of sanctions in case of non-compliance with security policies are two determinantes that have direct influence on employees' security behavior and are controllable by organizational information security management.

Building on the findings from the literature analysis, a succeeding study was executed in order to expand the spectrum of theories used in the contemplated research field. While not losing the focus on employees' perspective on information security, the influence of the leadership style of management and supervisors was considered. For this purpose, the concept of transformational leadership was introduced to the research field. Results from empirical investigation confirmed a direct as well as a meditated influence of transformational leaders on employees' information security performance. This is mainly due to the capability of transformational leaders to enhance employees' perception of a positive security climate within organizations. The findings of this study underline the importance of the role of supervisors in the context of enhancing employees' information security behavior. Accordingly, organizations must not only establish SETA programs that address employees' knowledge and skills for coping with information security threats, but also improve supervisors' awareness and abilities to promote and convey the value of information security to employees in order to implement a holistic and sustainable information security approach. By fostering transformational leadership style within organizations, employees can be intrinsically motivated to comply with information security policies. Consequently organizations can reduce controlling leadership

measures like punishment in case of employees' non-compliance. Moreover, transformational leaders are capable of enhancing employees' intention to actively support information security which exceeds the mere compliance intention.

The next research step aimed at reducing the gap between theoretically founded explanation of employees' security behavior and the need of practitioners to know which intervention to apply. By using the ADR approach, a process model for measuring and evaluating employees' information security behavior with regard to a SETA needs assessment was developed and refined during several cycles of theoretical and practical intervention. As a result general design principles were defined. The proposed needs assessment process emphasized the development of organization specific target values. Feedback from practitioners that were involved in the research process revealed that the integration of stakeholders (i.e. experts, key users) is a necessary precondition as they provide valuable experiences that complements the measured data. In order to enable a selective analysis of the current state of employees' behavior, the different observation perspectives that take the specific organizational context into account has been found to be beneficial. Furthermore, it has been shown that the implementation of a SETA needs assessment process requires a mature and detailed monitoring process as well as a standardized process for developing security metrics that correspond to the specific observation levels. Although, the goal was pursued, that only reliable data sources such as system monitoring are used, results from the practical application check showed that the use of employee self-reports cannot be avoided completely. The presented process model enables practitioners to dynamically depict the current state of employees' security behavior. On the theoretical side, the process provides the basis for future research to test and evaluate the efficiency of different SETA measures in real work settings.

6.1.2 Consumerization of IT and Organizational Information Security

The following research step is not directly based on the initial literature review, but was inspired by the theories identified in the course of the literature review. The purpose of this step was to broaden the scope of this dissertation and investigating issues that are closely related to employees' role in organizational information security. The growing trend of BYOD shifts power towards the user. In this context, the question arises

whether users are aware of security, privacy and legal issues with regard to using their privately owned devices for working purposes and if possible concerns have influence on employees' intention to adopt BYOD. Results from empirical testing revealed a strong influence of perceived concerns on employees' intention to use BYOD mobile devices. These findings offer important implications for practitioners in two ways. On the one hand, results show that organizations have to address and to mitigate the above mentioned concerns when they plan to implement a BYOD program that is accepted by employees. On the other hand, results suggest that users are aware of the information security risks that are associated with BYOD. Consequently, since a basic awareness exists, organizations can build on that in order to establish information security measures in BYOD mobile devices that are accepted by end users.

Bring your own device is generally seen as a special form of the ongoing trend of IT consumerization. Consumerization of IT is the main driver of the four interconnected trends mobile, social, and cloud computing as well as big data. The combination of these forces, referred to as the Nexus of Forces, is expected to have a lasting impact on organizations and their IT infrastructure. In this context, the question arises how organizational and especially IS governance as the framework for organizational information security management have to be adjusted with regard to the new challenges. Results from a Delphi study indicate that the impact of the Nexus depends on the organization's environment and external contingencies. The consumerization pressure mainly impacts organizations on the business level. This shifts the responsibility of IT investment, business application and IT principles primarily towards the corporate governance. Consequently, IS governance focusses on rather technical aspects. Moreover, due to increasing quantity and importance of information, information governance is gaining in significance and will be separated from technological governance. It is supposed, that the Nexus of forces will redefine the role of IT management and the CIO within an organization as organizations face the challenge of whether existing IS governance approaches can be adjusted or the whole view on organization IS governance needs to be changed. In this context, it is likely that organization are turning away from strict centralized or decentralized governance approaches and will implement hybrid governance approaches and federal archetypes.

6.2 Overall Limitations

This cumulative dissertation encompasses five research studies that focus on the role of employees in the organizational information security chain, addressing both IS reserach paradigms, namely quantitative and qualitative research. Since the methodological and thematically limitations of the individual research studies that were discussed in detail within each publication and are revisited in chapter 4 and chapter 5 of this dissertation, the aim of this section is to critically review the overall research process and to identify general limitations.

6.2.1 Application of Various Research Methods

In order to pursue the overall goal of this dissertation, the underlying research process incorporates multiple quantitative and qualitative research methods. The multi-method approach, which is often also referred to as mixed-method research, assumes that quantitave and qualitative research are compatible and allows the combination of various method from both paradigms (Teddlie and Tashakkori, 2011). Multi-method research is defined by Johnston et al. (2007) as "the type of research in which a researcher or team of researchers combines elements of qualitative and quantitative research approaches (e.g., use of qualitative and quantitative viewpoints, data collection, analysis, inference techniques) for the broad purposes of breadth and depth of understanding and corroboration." The question which research methods are appropriate and applicable within the IS research domain has been debated for a long time. Although some researchers compared the IS domain to other management areas that are characterized by a plethora of research methods, others made statements towards the necessitiy of a single paradigm that allows for coherence in IS research (Mingers, 2001). However, the use of multi-method research approaches has been advocated by Mingers (2001) as the author states that "that research results will be richer and more reliable if different research methods, preferably from different (existing) paradigms, are routinely combined together". Accordingly, multi-method research is desirable in information systems research especially in research situations that are inherently complex and multidimensional so that a use of a wide range of methods is beneficial. Due to the complex nature

of the information security domain, the multi-method approach was found to be appropriate for the research process of this dissertation, because this approach considers "different dimensions of a real situation, material, social, and personal; to the tasks involved in the different stages of a research study" (Mingers, 2011). Therefore, multi-method research was applied within the research process of this dissertation in two ways as described by Johnston et al. (2007). First, multi-method research provides the underlying approach for the research process as a whole since methods were mixed across a set of closely related studies. Second, methods were mixed within single studies as described in chapters 4.3 and 5.2.

6.2.2 Rigor and Relevance

The proper selection and application of research methods that are established in the field of IS research aimed to ensure academic rigor, whereas the focus on topics that are inspired from practical problems aimed at enhancing the practical relevance of this dissertation. However, academic rigor versus practical relevance has been discussed in the IS research community for a long time and the discussion is still continuing (e.g. Benbasat and Zmud, 1999; Desouza et al., 2006; Straub and Ang, 2011). Due the application of various research methods from both, the qualitative and the quantitative research domain, this dissertation is exposed to several limitations concerning rigor and relevance. This section intends to position this dissertation within the academic rigor versus practical relevance discussion and to critically review the research process as a whole.

First, qualitative research methods as applied in chapter 4.3 are considered. Qualitative research methods offer the advantage of investigating and explaining insights of organizations with regard to managerial issues that are not suited for quantification (DeLuca et al., 2008). This is mainly due to the fact that qualitative research "fundamentally depends on watching people in their own territory and interacting with them in their own language, on their own terms" (Kirk and Miller, 1986 as cited in: Krefting, 1990). Design science studies commonly use qualitative methods for data collection in order to create artefacts that contribute to a general research filed by embodying a test of extant theory while addressing specific practical problem (Papas et al., 2012). However, studies that rely on qualitative methods often face the criticism of not being rigorous enough although they are dealing with topics that are practically relevant (DeLuca et al., 2008).

Due to this criticism, recent design science approaches (e.g. Hevner et al., 2007; Peffers et al., 2007) emphasize the rigor of the research process in terms of evaluating the designed artifact in subsequent and separated stages. Consequently, these approaches "value technological rigor at the cost of organizational relevance, and fail to recognize that the artifact emerges from interaction with the organizational context even when its initial design is guided by the researchers' intent" (Sein et al., 2011). In order to avoid this criticism while aiming at a similar research output, action research emphasizes the interaction of researchers and practitioners by addressing problems perceived in real-life environments (Goldkuhl, 2008). However, the strong involvement of practitioners in the research process (DeLuca et al., 2008) caused criticism as well (Anaman, 2008). It is questioned whether the specific problem that is investigated within an action research study is generally relevant and solutions are applied outside the context of the specific practice (Goldkuhl, 2008). To avoid the criticism to design science and action research, but to take advantage of the benefits of both approaches, a combined approach, namely action design research as recently proposed by Sein et al. (2011) was applied within this research. However, this approach is not free from limitations. Although action design research aims at defining general design principles that address a broad class of practical problems, the main input was obtained from the practical intervention within a single partner company. Consequently, the resulting principles are prone to subjective bias. Moreover, due to the novelty of this research method, only very few studies already applied action design research. Therefore, almost no experiences and knowledge with regard to this method exists within IS research.

Second, turning to quantitative studies as applied in chapter 4.2 and chapter 5.1, the other end of the rigor and relevance debate is of importance. Rigor in quantitative IS research is typified by "the stringent application of research methods, extensive theoretical support, and 'flawless' research designs" (Siponen and Vance, 2014). IS researchers have turned attention to rigor and produced a large number of methodological articles (Siponen and Vance, 2014). However, according to Benbasat and Zmud (1999) the IS research community has to critically review whether IS research produces knowledge that can be applied by IS professionals in their daily work and whether it addresses challenges and problems that are relevant in the business context. The authors emphasize

the importance of practical relevance within the field of applied sciences next to a rigorous approach that aims at theoretical advancement. One way to provide practical relevant research is to investigate themes that are of importance and useful from a practitioner's point of view (Straub and Ang, 2011). Theme-level relevance within this dissertation was addressed by identifying research gaps not only by reviewing academic literature but also by considering practical literature, e.g. market research studies. As described within chapter 1, recent information security studies (e.g. IDC, 2011; CSO magazine, 2011; Verizon RISK Team, 2011) demonstrated the importance of information security in general and employees' information security awareness and behavior in particular. Moreover, the research described in chapter 5.1 is largely based on themes and issues with regard to BYOD that were discussed in practitioners' literature. However, Siponen und Vance (2014) argue that theme-level relevance is not sufficient in order to ensure the practical relevance of academic studies. The authors call for more attention on contextual relevance, especially in the field of quantitative studies that investigate employees' information security awareness and behavior. The concept of contextual relevance goes beyond theme-level relevance and considers "whether the specific phenomenon under examination […] represents an important problem in practice" (Siponen und Vance, 2014). The authors outlined five guidelines that aim at enhancing contextual relevance in the field of survey research. Accordingly, researchers should use case examples from participants' actual work environment in order to ensure that participants must not rely on their memory and imagination while answering the survey questions as. However, there are restrictions with regard to the applicability, so that these guidelines were not used within the quantitative studies of this dissertation: The guidelines by Siponen and Vance (2014) call for the use of specific measures instead of generic measures. In order to develop specific measures, examples of information security policy violations have to be identified, that are relevant within the actual workin context of each participant. However, due to complexity of the information security domain and since the surveys were not limited to any company, branch, or country, it was not possible to develop a specific measure that is relevant accros various organizational contexts. To ensure validity of the measurement instrument despite the criticism towards the use of generic measures, the items used in dissertation were adopted from renowned and frequently cited validated studies.

6.3 Outlook

After summarizing the results of the individual research steps and outlining the overall limitations of the cumulative research process, this section aims at presenting an outlook in terms of providing directions for future research. The research process began with a coherent review of academic literature within the contemplated research field. The results show that this research field is replete with quantitative studies. As mentioned in the previous section, researchers began to critically review the practical relevance of this research stream. In this context, Siponen and Vance (2014) for example identified the common use of generic measurement models as a significant cause for the lack of contextual relevance and therefore advocate the use of specific measurements. Like discussed above, there are difficulties of replacing the common generic measures with more specific measures in quantitative empirical studies. Especially it would require a methodological change within the research stream. One way to utilize more specific measurements in quantitative research is to incorporate more experimental studies. Experiments have not yet found a frequent application within the contemplated research field, although this research method has been used in other scientific areas (e.g. social sciences) for decades. In this context, both forms of this method, namely laboratory and field experiments, provide the ability to generate new insights into employees information security behavior and contribute to the research field. The major advantage of laboratory experiments is that the environment can be completely controlled and therefore enables exact measurement of causal hypotheses by an academically validated process. The majority of existing experimental studies in employees' information security behavior research were performed in laboratory settings. However, laboratory experiments often face critics regarding the generalizability due to low sample sizes and participants that are not in a real work environment (e.g. students). Therefore, field experiments are necessary that focus on participants which are observed in real work environments. This would allow researchers to study the impact of different influential variables on employees' actual information security behavior during their daily work instead of assessing their behavioral intentions based on hypothetical assumptions. Since the implementation of field experiments needs a strong cooperation of researchers and practitioners, this research method provides the opportunity that

academics can obtain topics and issues that are importance in practice and thereby enhance the practical relevance of the research field.

Since employees' are widely recognized as the weakest link in the organizational information security chain, it is critically important for organizations to positively influence employees' compliance with effective security policies. In this context, the consideration of the influence of management and supervisors is a significant factor. By investigating the impact of transformational leadership tactics on employees' security behavior within this dissertation, it was shown that leaders are capable to enhance not only employees' intention to comply with organization information security policies, but also to actively support and enhance information security. As transformational leadership only represents a small part of the leadership spectrum it is necessary for future research to take the full range of leadership styles into consideration. The most obvious next step is to investigate the effects of transactional leadership on employees' information security awareness and behavior and to compare it to the impact of transformational leadership. Furthermore, with regard to previous studies in the contemplated research field that focused on cognitive antecedents of employees' security behavior, the consideration of interactive leadership theory would be an interesting next step. Accordingly, leadership is an interactive process, which is determined by the interaction of various factors. These include the personality traits of the participants (leaders and followers), the objective conditions of the situation and their subjective perception. Leadership is followed by a process of interaction between managers, employees and the individual situation. Due to the complexity of this topic, researchers should resort to field experiments rather than focusing on the survey method in order to investigate the interrelations of leader and follower behavior as well as situational influences in a differentiated approach

Observing employees' information security awareness and behavior within a real work environment demands for a structured approach that takes different dimensions of behavior into account. Within this dissertation a measurement process model was developed that focused on evaluating employees' security behavior within the context of a needs assessment for SETA programs. However, such a measurement process is not only relevant for practitioners, but also for researchers that are aiming at the measurement of employees' actual behavior within the organizational context. In order to enhance the quality and reliability of the presented measurement process, further validation is

needed, especially with regard to accuracy and completeness of measurement results. For the purpose of validating accuracy, one direction should be the integration of laboratory experiments to test the proposed measurement process within a group of participants that show a behavior that is ex-ante determined and evaluated by security experts. Afterwards the results of the measurement process can be compared to the ex-ante evaluation of the security experts. In order to enhance completeness, continuous development and verification of security metrics is needed. Although several institutions (e.g. ISO, BSI) provide metrics concerning the implementation of information security within organizations, only few metrics exist that address the multi-dimensional aspects of employees' security behavior. The development of these metrics is a field for further research in cooperation with practitioners. Also continuous verification of these metrics is needed due to rapid development in technologies.

Recent technology trends have various impacts on organizational information security. On the one hand, advances in mobile network bandwidth and performance of mobile devices lead to an increase in mobility of workplaces as employees are able to work anywhere and anytime. Consequently, more and more sensitive information are processed and stored outside of organizational premises exposing these information to various information security threats. On the other hand, trends like consumerization and BYOD shift more and more power to the end-user. As a result, technical measures alone are not sufficient to ensure information security and employees' have to accept more and more responsibilities for organizational data and information. Thus, these emerging trends emphasize the importance and necessity of employees' information security awareness and behavior research. As already mentioned above, also in this context it is a critically important task for IS research to investigate and develop measures that sustainably influence employees' compliance with information security policies. Futurer research has to investigate whether these technological developments challenge traditional approaches to organizational information security and demand novel orientation for information security management. Furthermore, although new technologies expose organizational information to new information security threats, the question arises if new technologies can also be used in order to help emplyoees to comply with security procedures. Future research could develop e.g. assistance systems or mobile learning scenarios that support employees with security tasks during their regular daily business.

References

Abraham, S. 2011. “Information security behavior: factors and research directions”, Proceedings of the Americas Conference on Information Systems, Paper 462.

Ajzen, I. 1985. “From intentions to actions: A theory of planned behavior,” in Action-control: From cognition to behavior, J. Kuhl and J. Beckman (eds.), Heidelberg: Springer-Verlag, pp. 11-39.

Ajzen, I. 1988. *Attitudes, Personality, and Behavior*, Chicago: The Dorsey Press.

Ajzen, I. 1991. “The theory of planned behavior,” *Organizational Behavior and Human Decision Processes* (50:2), pp. 179–211.

Aldhaban, F. 2012. “Exploring the Adoption of Smartphone Technology: Literature Review”, Technology Management for Emerging Technologies Proceedings, pp. 2758-2770.

Altobelli, C. F. 2007. “Qualitative und quantitative Marktforschung,” Das Wirtschaftsstudium, Vol. 36, No. 4, pp. 522-534.

Ammon, U. 2009. “Delphi-Befragung”, In: *Handbuch Methoden der Organisationsforschung,* VS Verlag für Sozialwissenschaften, pp. 458-476.

Anaman, M., Lycett, M., and Love, S. 2008. “Enhancing Customer Experience within the Mobile Telecommunications Industry,“ Proceedings of the European Conference on Information Systems, Paper 188.

Anderson, C.L. and Agarwal, R. 2010. “Practicing safe computing: a multimethod empirical examination of home computer user behavioral intentions”, MIS Quarterly, Vol. 34, No. 3, pp. 613-643.

Andriole, S. J. 2012. “Seven Indisputable Technology Trends That Will Define 2015,” Communications of the Association for Information Systems, pp. 61-72.

Antonakis, J., Avolio, B. J., and Sivasubramaniam, N. 2003. “Context and leadership: an examination of the nine-factor fullrange leadership theory using the Multifactor Leadership Questionnaire,” The Leadership Quarterly (13), pp. 261-295.

Ashenden, D. 2008. “Information Security management: A human challenge?,” Information Security Technical Report, Vol. 13, No. 4, pp. 195-201.

Ask, U., Björnson, H., Johansson, M., Magnusson, J. and Nilsson, A. 2007. “IT Governance in the light of Paradox - A Social Systems Theory Perspective,” Proceedings of the Hawaii International Conference on System Science.

Aurigemma, S. and Panko, R. 2007. “A composite framework for behavioral compliance with information security policies”, Proceedings of the Hawaii International Conference on System Sciences, pp. 3248-3257.

Avolio B. J., and Bass B. M. 2004. *Multifactor Leadership Questionnaire: Manual and Sample Set*. California: Mindgarden.

Avolio B. J., and Bass B. M. 2004. *Multifactor Leadership Questionnaire*: Manual and Sample Set. California: Mindgarden.

Avolio B. J., Bass B. M., and Jung D. I. 1999. “Re-examining the components of transformational and transactional leadership using the Multifactor Leadership Questionnaire,” Journal of Occupational and Organizational Psychology, Vol. 72, No. 4, pp. 441-462.

Bandura, A. 1982 "Self-efficacy mechanism in human agency," American Psychologist Vol. 37, No. 2, pp. 122-147.

Bass, B. M., Avolio, B. J., Jung, D. I. and Berson, Y. 2003. “Predicting unit performance by assessing transformational and transactional leadership”, Journal of Applied Psychology, Vol. 88, No. 2, pp. 207-218.

Bass, B. M., Waldman, D. A., Avolio B. J., and Bebb M. 1987. “Transformational Leadership and the Falling Dominoes Effect,” Group & Organization Management Vol. 73, No. 12, pp. 73-87.

Benbasat, I., and Zmud, R. 1999. “Empirial research in information systems: the practice of relevance,“ MIS Quarterly, Vol. 23, No. 1, pp. 3-16.

Beulen, E. and Streng, R.-J. 2002. “The Impact of Online Mobile Office Applications on the Effectiveness and Efficiency of Mobile Workers Behavior: A Field Experiment in the IT Services Sector”, Proceedings of the International Conference on Information Systems.

Boer, H., and Seydel, E. R. 1996. “Protection motivation theory”, in: Connor, M. and Norman, P. (Eds.) *Predicting Health Behavior*. Open University Press, Buckingham.

Bono J. E., and Judge T. A. 2004. “Personality and Transformational and Transactional Leadership: A Meta-Analysis,” Journal of Applied Psychology, Vol. 89, No. 5, pp. 901–910.

Börner, R., Looso, S., and Goeken, M. 2009. „Towards an operationalisation of governance and strategy for service identification and design,” Workshops Proceedings of the 12th IEEE International Enterprise Distributed Object Computing Conference, , Auckland, New Zealand, pp. 180-188.

Boss, S., Kirsch, L., Angermeier, I., Shingler, R. and Boss, R. 2009. "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.

Braodbent, M. and Kitzis, E. 2004. *The New CIO Leader: Setting the Agenda and Delivering Results,* Boston: Harvards Business School Press.

Brown, A. E., and Grant, G. G. 2005. „Framing the Frameworks: A Review of IT Governance Research," Communications of the Association for Information Systems, Vol. 15, pp. 696-712.

Brown, L. V. 2007. *Psychology of motivation*. New York: Nova Science Publishers.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. 2009a. "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, Vancouver, pp. 476-481.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. 2009b. "Roles of information security awareness and perceived fairness in information security policy compliance", Proceedings of the Americas Conference on Information Systems, San Francisco, Paper 419.

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

Burns, J. M. 1978. *Leadership*. New York: Harper & Row.

Burtscher, C., Manwani, S. and Remenyi, D. 2009. "Towards a conceptual map of IT governance: a Review of current academic and practitioner thinking," in Proceedings of the UK Academy for Information Systems Conference: Positive Information Systems, Oxford, UK.

Chan, M., Woon, I., and Kankanhalli, A. 2005. "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.

Chen, H., Chaing, R. H. L., and Storey V. C. 2013. „Business Intelligence and Analytics: From Big Data to Big Impact," MIS Quarterly, Vol. 36, No. 4, pp. 1165-1188.

Chin, W. W. 1998b. "The partial least squares approach to structural equation modeling," In: *Modern Methods for Business Research* (Marcoulides, G., Ed.), Lawrence Erlbaum Associates,Mahwah, NJ, pp. 295–336.

Chmielewicz, K. 1994. *Forschungskonzeptionen der Wirtschaftswissenschaft*, 3rd Edition, Stuttgart: Schäffer-Poeschel.

Cho, J., and Park, I. 2007. "Transformational Leadership and Information System Effectiveness," Proceedings of the International Conference on Information Systems, Paper 85.

Clarke, S., and Ward, K. 2006. “The role of leader influence tactics and safety climate in engaging employees' safety participation,” Risk Analysis (26:5), pp. 1175-1185.

Collins J., 2001. *Good To Great: Why Some Companies Make the Leap…and Others Don’t*, New York: HarperCollins.

Colwill, C. 2009. “Human factors in information security: The insider threat – Who can you trust these days?,“ Information Security Technical Report, Vol. 14, No. 4, pp. 186-196

CSO magazine 2011. “2011 Cybersecurity Watch Survey: Organizations Need More Skilled Cyber Professionals to Stay Secure,“ http://www.csoonline.com/.

Cuhls, K. 2009. “Delphi-Befragungen in der Zukunftsforschung,” In *Zukunftsforschung und Zukunftsgestaltung,* Springer Berlin Heidelberg, pp. 207-221.

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

D’Arcy, J. and Hovav, A. 2011. “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.

D’Arcy, J., Hovav, A., and Galletta, D. 2009. “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.

Dahlberg, T., and Kivijarvi, H. 2006. „An Integrated Framework for IT Governance and the Development and Validation of an Assessment Instrument,” in Proceedings of the 39th Annual Hawaii International Conference on System Sciences, HI, USA, p. 194b.

D'Arcy, J. and Herath, T. 2011. “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.

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

Davenport, T. H. and Markus, M. L. 1999. “Rigor vs. relevance revisited: response to Benbasat and Zmud”. MIS Quarterly, Vol. 23, No. 1, pp. 19-23.

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

Davis, F.D., 1989. “Perceived Usefullness, Perceived Ease of Use, and User Acceptance of Information Tchnology,” MIS Quarterly, Vol. 13, No. 3, pp 319-340.

De Haes, S. and Van Grembergen, W. 2008. „Analysing the Relationship between IT Governance and Business/IT Alignment Maturity," in Proceedings of the 41st Annual Hawaii International Conference on System Sciences, HI, USA, p. 428.

De Haes, S., and Van Grembergen, W. 2004. "IT Governance and Its Mechanisms," Information Systems Control Journal, Vol. 1, No. 1, pp. 27-33.

De Haes, S., and Van Grembergen, W. 2005. "IT Governance Structures, Processes and Relational Mechanisms: Achieving IT/Business Alignment in a Major Belgian Financial Group," in Proceedings of the 38th Annual Hawaii International Conference on System Sciences, HI, USA, p. 237b.

De Haes, S., and Van Grembergen, W. 2006. „Information Technology Governance Best Practices in Belgian Organisations," in Proceedings of the 39th Annual Hawaii International Conference on System Sciences, HI, USA, p. 195b.

DeLuca, D., Kock, N. and Gallivan, M. J. 2008. "Furthering information systems action research: a post-positivist synthesis of four dialectics," Journal of the Association for Information Systems, Vol. 9, No. 2, pp. 48-72.

Desouza, K. C., El Sawy, O. A., Galliers, R. D., Loebbecke, C., & Watson, R. T. (2006). Beyond rigor and relevance towards responsibility and reverberation: Information systems research that really matters. Communications of the Association for Information Systems, Vol. 17, No. 1, pp. 341-354.

Diamantopoulos A. and Winklhofer H. 2001. "Index construction with formative indicators: an alternative to scale development," Journal of Marketing Research, Vol. 38, No. 2, pp. 269-277.

Dinev, T., Goo, J., Hu, Q., and Nam, K. 2009. "User Behavior toward Protective Technologies - Cultural Differences between the United States and South Korea," Information Systems Journal, Vol. 19, No. 4, pp. 391-412.

Dojkovski, S., Lichtenstein, S., and Warren, M. J. 2007. "Fostering Information Security Culture in Small and Medium Size Enterprises: An Interpretive Study in Australia," in Proceedings of the 15th European Conference on Information Systems, St. Gallen, Switzerland, Paper 120.

Dutta, A., and McCrohan, K. 2002. "Management's role in information security in a cyber economy," California Management Review, Vol. 45, No. 1, pp. 67-87.

Edwards, J. R. and Bagozzi, R. P. 2000. "On the nature and Direction of relationships Between Constructs and Measures", Psychological Methods, Vol. 5, No. 2, pp. 155-174.

Elo, S., & Kyngäs, H. 2008. "The qualitative content analysis process," Journal of Advanced Nursing, Vol. 62, No. 1, pp. 107-115.

Eloff, J.H.P. and Eloff, M.M. 2005. "Information Security Architecture," Computer Fraud & Security, Vol. 11. No. 1, pp. 10-16.

Erkutlu, H. 2008. “The impact of transformational leadership on organizational and leadership effectiveness the Turkish case,” Journal of Management Development, Vol. 27, No. 7, pp. 708-726.

Fettke, D. W. I. P., & Loos, P. (2004). “Referenzmodellierungsforschung”, Wirtschaftsinformatik, Vol. 46, No. 5, pp. 331-340.

Fettke, P., and Loos, L. 2007. *Reference Modeling for Business Systems Analysis*, Hershey: Idea Group Publishing.

Figge, S., Schrott, G., Muntermann, J. and Rannenberg, K. 2003. Earning Money - A Situation Based Approach for Mobile Business Models,” Proceedings of the European Conference on Information Systems.

Fishbein, M., and Ajzen, I. 1975. *Belief, attitude, intention, and behavior: An introduction to theory and research,* Reading: Addison-Wesley.

Flick, U. 2006. *Qualitative Evaluationsforschung. Konzepte, Methoden, Umsetzungen*, Reinbek bei Hamburg: Rowohlt.

Fornell C. and Bookstein F. 1982. ”Two structural equation models: LISREL and PLS applied to consumer exit-voice theory,” Journal of Marketing Research, Vol. 19, pp. 440–452.

Fornell, C. and Larcker, D. 1981. “Evaluating Structural Equation Models with Unobservable Variables and Measurement Error,” Journal of Marketing Research, Vol. 18, No. 1, pp. 39-50.

Gartner Inc., 2013. „Examining the Depth of the Nexus of Forces,” Gartner Report ID: G00239390, (Plummer, D. C.and Sribar, V. T.).

Gartner. 2013. „Examining the Depth of the Nexus of Forces,” Gartner Report ID: G00239390, (Plummer, D. C.and Sribar, V. T.).

Gefen, D., Rigdon, E. E. and Straub, D. 2011. “An Update and Extension to SEM Guidelines for Administrative and Social Science Research,” MIS Quarterly, Vol. 35, No. 2, pp. iii–xiv.

Gefen, D., Straub, D.W. and Boudreau, M.-C. 2000. “Structural Equation Modeling and Regression: Guidelines for Research Practice,” Communications of AIS, Vol. 4, Article 7.

Geijsel, F., Sleegers, P., Leithwood, K., and Jantzi, D. 2003. “Transformational leadership effects on teachers’ commitment and effort toward school reform,” Journal of Educational Administration, Vol. 41, No. 3, pp.228-256.

Geijsel, F., Sleegers, P., Leithwood, K., and Jantzi, D. 2003. “Transformational leadership effects on teachers’ commitment and effort toward school reform,” Journal of Educational Administration, Vol. 41, No. 3, pp.228-256.

Giessmann, A.; Stanoevska-Slabeva, K. and de Visser, B. 2012. “Mobile Enterprise Applications - Current State and Future Directions,” Proceedings of the Hawaii International Conference on System Sciences.

Gläser, J., and Laudel, G. 2009. *Experteninterviews und qualitative Inhaltsanalyse als Instrumente rekonstruierender Untersuchungen*, 3. überarbeitete Auflage. Wiesbaden: VS-Verlag für Sozialwissenschaften.

Goeken, M. 2003. *Grundlagen und Ansätze einer Referenzmodellierung für Führungsinformationssysteme*, Philipps-Universität Marburg Institut für Wirtschaftsinformatik (Alpar/Hasenkamp Eds.) Fachbericht Nr. 03/02.

Goes, P. 2013. “Editor’s Comments,” MIS Quarterly, Vol. 37, No. 1, pp. iii-vii.

Goldkuhl, G. 2008. “Practical inquiry as action research and beyond,“ Proceedings of the European Conference on Information Systems.

Häder, M. 2009. *Delphi-Befragungen*, 2. Auflage, Wiesbaden: VS Verlag für Sozialwissenschaften.

Häder, M. and Häder, S. 2000. “Die Delphi-Methode als Gegenstand methodischer Forschungen. In: Häder et al. (Eds.) *Die Delphi-Technik in den Sozialwissenschaften,* VS Verlag für Sozialwissenschaften, pp. 11-31.

Haenlein, M. and Kaplan, A. M. 2004. “A Beginner’s Guide to Partial Least Squares Analysis,“ Understanding Statistics, Vol. 3, No. 4, pp. 283-297.

Hair, J. F., Ringle, C. M. and Sarstedt, M. 2011. ”PLS-SEM: Indeed a Silver Bullet,” Journal of Marketing Theory and Practice, Vol. 19, No. 2, pp. 139-151.

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

Hart, 1999. *Doing a Literature Review - Releasing the Social Science Research Imagination*, London: SAGE Publications.

Hayton, J. C., Allen, D. G. and Scarpello, V. 2004. ”Factor Retention Decisions in Exploratory Factor Analysis: A Tutorial on Parallel Analysis,“ Organizational Research Methods, Vol. 7, No. 2, pp. 191-205.

Heier, H., Borgman, H. P., and Bahli, B. 2012. “Cloudrise: Opportunities and Challenges for IT Governance at the Dawn of Cloud Computing,“ Proceedings of the 45th Hawaii International Conference on System Science, pp. 4982-4991.

Heier, H., Borgman, H. P., and Bahli, B. 2012. “Cloudrise: Opportunities and Challenges for IT Governance at the Dawn of Cloud Computing,“ Proceedings of the Hawaii International Conference on System Science, pp. 4982-4991.

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

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

Herath, T., and Rao, H. R. 2009a. “Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness,” Decision Support Systems, Vol. 47, No. 2, pp. 154-165.

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

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

Herath, T., and Rao, H. R. 2009b. “Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organizations,” European Journal on Information Systems (18:2), pp. 106-125

Hevner, A. R. 2007. “A three cycle view of design science research”, Scandinavian journal of information systems, Vol. 19, No. 2, Article 4.

Hevner, A., March, S., Park, J. and Ram, S. 2004. “Design science in information systems research,” MIS Quarterly, Vol. 28, No. 1, pp. 75-105.

Ho, S. Y. 2009. Opportunities and Challenges of Mobile Personalization: An Exploratory Study, Proceedings of the 17th European Conference on Information Systems.

Hock C., Hee-Woong K., and Weai C.T. 2006. “Information System Citation Patterns from ICIS Articles,“ Journal of the American Society for Information Science and Technology, Vol. 57, No. 9, pp. 1263-1274.

Hopkins, N., Sylvester, A., and Tate, M. 2013. “Motivations for BYOD: An Investigation of the Contents of a 21st Century School Bag,” Proceedings of the European Conference on Information Systems, Paper 183.

Hovav, A. and D’Arcy, J. 2012. “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.

Hrastinski, S.; Carlsson, S.; Henningsson, S. and Keller, C. 2008. “On How to Develop Design Theories for IS Use and Management,“ Proceedings of the European Conference on Information Systems, Paper 138.

Hu, Q., and Dinev, T. 2007. “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.

IDC 2011. “Pressemeldung: IDC-Studie: Abwehr neuer Angriffsszenarien, Cloud und Mobile Security sind die Top 3 Prioritäten deutscher IT Security Verantwortlicher”, www.idc.de/anwenderstudie_security2011.

Ifinedo, P. 2012. “Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory,” Computers & Security, (31:1), pp. 83-95.

Iivari, J. 2007. “A paradigmatic analysis of information systems as a design science”, Scandinavian Journal of Information Systems, Vol. 19, No. 2, pp. 39-63.

Iivari, J. and Venable, J. R. 2009. “Action research and design science research-seemingly similar but decisively dissimilar,“ Proceedings of the European Conference on Information Systems.

Inness, M., Turner, N., Barling, J., and Stride, C. B. 2010. “Transformational Leadership and Employee Safety Performance: A Within-Person, Between-Jobs Design,” Journal of Occupational Health Psychology, Vol. 15, No. 3, pp. 279-290.

Jahn, S. 2007. ”Strukturgleichungsmodellierung mit LISREL, AMOS und SmartPLS – Eine Einführung,“ Fakultät der Wirtschaftswissenschaften an der Technischen Universität Chemnitz.

Jahns, C. and Moser, R. 2007. ”Strategic Purchasing and Supply Management: A Strategy Based Selection of Suppliers”, Deutscher Universitätsverlag, Wiesbaden, Germany.

Järvinen, P. 2007. “Action Research is Similar to Design Science”, Quality and Quantity Vol. 41. No. 1, pp.37-54.

Johnson, N. and Joshi, K. D. 2012. “The Pathway to Enterprise Mobile Readiness: Analysis of Perceptions, Pressures, Preparedness, and Progression,” Proceedings of the Americas Conference on Information Systems, Paper 18.

Johnson, R. B., Onwuegbuzie, A. J. and Turner, L. A. 2007. “Toward a definition of mixed methods research,” Journal of Mixed Methods Research, Vol. 1, No. 2, pp. 112-133.

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

Jung, D. I., and Sosik J. J. 2002. “Transformational Leadership in Work Groups: The Role of Empowerment, Cohesiveness, and Collective-Efficacy on Perceived Group Performance,” Small Group Research, Vol. 33, No. 3, pp. 313-136.

Karjalainen, M. and Siponen, M. T. 2011. “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.

Kendall, J. W. 1977. “Variations of Delphi,“ Technological Forecasting and Social Change Vol. 11, No. 1, pp. 75-85.

Kendall, J. W. 1977. “Variations of Delphi,” Technological Forecasting and Social Change, Vol. 11, No. 1, pp. 75-85.

Kent A. W. and Hardgrave, B. C. 2001. “Forums for information systems scholars: III,” Information & Management, Vol. 39, pp. 117-124.

Kietzmann, J. 2008. “Interactive innovation of technology for mobile work,” European Journal of Information Systems, Vol. 17, No. 3, pp. 305-320.

Kirk, J. and Miller, M. 1986. *Reliability and Validity in Qualitative Research*. Beverly Hills: Sage.

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

König, W., Heinzl, A., Rumpf, M. and von Poblotzki, A. 1996. “Zur Entwicklung der Forschungsmethoden und Theoriekerne der Wirtschaftsinformatik in den nächsrten zehn Jahren. Eine kombinierte Delphi- und AHP-Untersuchung”, in: Heilmann, H. (Hrsg.): Information Engineering, München u.a., S. 35-66.

Kooper, M. N., Maes, R., and Roos Lindgreen, E. E .O. 2011. „On the governance of information: Introducing a new concept of governance to support the management of information,“ International Journal of Information Management, Vol. 31, No. 3, pp. 195–200.

Kotulic, A.G. and Clark, J.G. 2004. “Why there aren’t more information security research studies”, Information & Management, Vol. 41, No. 5, pp. 597-607.

Koukal, A., Gleue, C. and Breitner, M.H. 2014. “Enhancing Literature Review Methods-Towards More Efficient Literature Research with Latent Semantic Indexing,” Proceedings of the European Conference on Information Systems.

KPMG, 2011. “The e-Crime Report 2011,“ www.kpmg.de/forensic.

KPMG, 2013. “e-Crime,“ www.kpmg.de/forensic.

Krefting, L. 1991. “Rigor in Qualitative Research: The Assessment of Trustworthiness”, American Journal of Occupational Therapy, Vol. 45, No.3, pp. 214-222.

Krueger, R. A., Casey, M. A. 2009. *Focus Groups: A Practical Guide for Applied Research*, London: SAGE Publications.

Kruger, H.A. and Kearney, W.D. 2006. “A prototype for assessing information security awareness”, Computers & Security, Vol. 25, no. 4, pp. 289-296.

Lange, C. 2006. “Entwicklung und Stand der Disziplinen WI und IS,“ ICB Research Report Nr. 4, Institut für Informatik und Wirtschaftsinformatik der Universität Duis-burg-Essen.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., and Breitner M. H. 2014. “Information security awareness and behavior: a theory-based literature review,“ Management Research Review 2014, Vol. 37, No. 12, pp. 1049-1092.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., and Breitner, M. H. 2013. “Employees’ Information Security Awareness and Behavior: A Literature Review,” in Proceedings of the Hawaii International Conference on System Sciences, pp. 2978-2987.

Lee, A. S. 1999. “Rigor and relevance in MIS research: Beyond the approach of positivism alone.” MIS Quarterly, Vol. 23, No. 1, pp. 29-33.

Lee, A.S. and Baskerville, R.L. 2003. “Generalizing Generalizability in Information Systems Research”, Information Systems Research, Vol. 14, No. 3, pp. 221–243.

Lehner, F. and Haas, N. 2009. “Knowledge Management Success factors – Proposal of an Empirical Research,“ Proceedings of the European Conference on Knowledge Management, pp. 483-493.

Leidner, D. and Kayworth, T. 2006. “A Review of Culture in Information Systems Research: Toward a Theory of Information Technology Culture Conflict,” MIS Quarterly, Vol. 30, No. 2, pp. 357-399.

Levy, Y. and Ellis, T. J. 2006. “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.

Levy, Y. and Ellis, T.J. 2006. “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.

Liang, T-P, Chiu, Y-C., Wu, S., and Straub, D. 2011. „The Impact of IT Governance on Organizational Performance,“ in Proceedings of the Americas Conference on Information Systems, Detroit, MI, USA, pp. 107-142.

Limayem, M., and Hirt, S. G. 2003. “Force of Habit and Information Systems Usage: Theory and Initial Validation,” Journal of Association for Information Systems (4:1), pp. 65-97.

Lindgren, R., Henfridsson, O. and Schultze, U. 2004. “Design Principles for Competence Management Systems: A Synthesis of an Action Research Study”, MIS Quarterly, Vol.28, No. 3, pp. 435-472.

Looso, S., and Goeken, M. 2010. “Application of Best-Practice Reference Models of IT Governance,“ in Proceedings of the European Conference on Information Systems, Paper 129.

Lowry, P. B. and Gaskin, J. 2014. ”Partial Least Squares (PLS) Structural Equation Modeling (SEM) for Building and Testing Behavioral Causal Theory: When to Choose It and How to Use it,” IEEE Transactions on Professional Communication, Vol. 57, No. 2, pp. 123-146.

MacCallum, C. and Browne, M. W. 1993. “The Use of Causal Indicators in Covariance Structure Models: Some Practical Issues,” Psychological Bulletin. Vol. 114, No. 3, pp. 533–541, 1993.

MacKenzie, S. B., Podsakoff, P. M., and Jarvis, C. B. 2005. “The Problem of Measurement Model Misspecification in Behavioral and Organizational Research and Some Recommended Solutions,” Journal of Applied Science, Vol. 90, No. 4, pp. 710-730.

Malik, P. 2013. „Governing Big Data: Principles and practices,“ IBM Journal of Research and Development, Vol. 57, No. 3, pp. 11 - 13.

March, S. and Smith, G. 1995. “Design and natural science research on information technology,“ Decision Support Systems, Vol. 15, No. 4, pp. 251-266.

Mayring, P. 2010. “Qualitative Inhaltsanalyse” In: *Handbuch qualitative Forschung in der Psychologie*, Wiesbaden: VS Verlag für Sozialwissenschaften. pp. 601-613.

McShane, M. and Williams, F. P. 1997. *Criminal Justice*, New York & London: Garland Publishing,.

Miller, K.W., Voas, J. and Hulburt G.F. 2012. “BYOD: Security and Privacy Considerations,“ IT Professional, Vol. 14 No. 5, pp. 53-55.

Miller, K.W., Voas, J. and Hulburt G.F. 2012. “BYOD: Security and Privacy Considerations,” IT Professional, Vol. 14, No. 5, pp. 53-55.

Mingers, J. 2001. “Combining IS research methods: towards a pluralist methodology”, Information Systems Research, Vol. 12, No. 3, pp. 240-259.

Mingers, J. 2001. “Combining IS research methods: towards a pluralist methodology,” Information Systems Research, Vol. 12, No. 3, pp. 240-259.

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

Moreno, C., Tizon N. and Preda M. 2012. “Mobile Cloud Convergence in GaaS: A Business Model Proposition,” Proceedings of the Hawaii International Conference on System Sciences.

Neal, A., and Griffin, M. A. 2006. “A study of the lagged relationships among safety climate, safety motivation, safety behavior, and accidents at the individual and group levels,” Journal of Applied Psychology, Vol. 91, No. 4, pp. 946-953.

Neumann, M. 2011. *Wertorientiertes Informationsmanagement: Empirische Erkenntnisse und ein Referenzmodell zur Entscheidungsunterstützung*. Hamburg: Verlag Dr. Kovač.

Niehaves, B., Köffer, S. and Ortbach, K. 2012. "IT Consumerization – A Theory and Practice Review," Proceedings of the Eighteenth Americas Conference on Information Systems, Paper 18.

Nitzl, C. 2010. "Eine anwenderorientierte Einführung in die Partial Least Square (PLS)-Methode," Industrielles Management, Arbeitspapier Nr. 21.

Norman, P., Boer, H. and Seydel, E. R. 2005. "Protection motivation theory", in: Connor, M. and Norman, P. (Eds.) *Predicting Health Behaviour: Research and Practice with Social Cognition Models*, Maidenhead: Open University Press,.

Novotny, A., Bernroider, E. W. N., and Koch, S. 2012. „Dimensions and Operationalisation of IT Governance: A Literature Review and Meta-Case Study," in Proceedings of the 2012 International Conference on Information Resource Management, Vienna, Austria, pp. 1-13.

Nysveen, H., Pedersen, P.E. and Thorbjørnsen, H. 2005. "Intentions to Use Mobile Services: Antecedents and Cross-Service Comparisons," Journal of the Academy of Marketing Science, Vol. 33, No. 3, pp. 330-346.

Olbrich, S., Poeppelbuss, J. and Niehaves, B. 2011. "BI Systems Managers' Perception of Critical Contextual Success Factors: A Delphi Study," Proceedimgs of the International Conference on Information Systems.

Oliver, R.L. and Bearden, W.O. 1985. "Crossover Effects in the Theory of Reasoned Action: A Moderating Influence Attempt", Journal of Consumer Research, Vol. 12, No. 3, pp. 324-340.

Ortbach, K., Brockmann, T., and Stieglitz, S. 2014. Drivers for the adoption of mobile device management in organizations, Proceedings of the European Conference on Information Systems, Paper 10.

Osterman Research Inc. 2012. "Putting IT Back in Control of BYOD," Osterman Research White Paper.

Osterman Research Inc. 2012. "Putting IT Back in Control of BYOD", Osterman Research White Paper, Black Diamond, WA, USA.

Pahnila, S., Siponen, M. T. and Mahmood, A. 2007b "Which Factors Explain Employees' Adherence to Information Security Policies? An Empirical Study," Proceedings of the Pacific Asia Conference on Information Systems, Paper 73.

Pahnila, S., Siponen, M.T. and Mahmood, A. 2007a. "Employees' Behavior Towards IS Security Policy Compliance," Proceedings of the 40th Hawaii International Conference on System Sciences, pp. 1-10.

Papas, N., O'Keefe, R. M. and Seltsikas, P. 2012. “The action research vs design science debate: reflections from an intervention in eGovernment,” European Journal of Information Systems, Vol. 21, No. 2, pp. 147-159.

Papas, N., O'Keefe, R. M., and Seltsikas, P. 2012. “The action research vs design science debate: reflections from an intervention in eGovernment,“ European Journal of Information Systems, Vol. 21, No. 2, pp. 147-159.

Pavlou, P.A., Liang, H. and Xue, Y. 2007. “Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective,” MIS Quarterly, Vol. 31, No. 1, pp. 105-136.

Peffers, K., Tuunanen, T., Rothenberger, M. A. and Chatterjee, S. 2007. “A design science research methodology for information systems research.” Journal of Management Information Systems, Vol. 24, No. 3, pp. 45-77.

Peterson, R. R. 2004. „Integration Strategies and Tactics for Information Technology Governance,“ in: *Strategies for Information Technology Governance*, W. Van Grembergen (eds.), Hershey: Idea Group Publishing, pp. 37-80.

Petter, S., Straub, D., and Rai, A. 2007. “Specifying formative constructs in information systems research,” MIS Quarterly, Vol. 31 No. 4, pp. 623-656.

Podsakoff, P. M., Bommer, W. H., Podsakoff, N. P., and MacKenzie, S. B. 2006. “Relationships between leader reward and punishment behavior and subordinate attitudes, perceptions, and behaviors: A meta-analytic review of existing and new research,” Organizational Behavior and Human Decision Processes (99:2), pp. 113-142.

Podsakoff, P. M., MacKenzie, S. B., Moorman, R. H., & Fetter, R. 1990. “Transformational leader behaviors and their effects on followers’ trust in leader, satisfaction, organizational citizenship behaviors,” The Leadership Quarterly, Vol. 1, No. 2, pp 107-142.

Podsakoff, P. M., MacKenzie, S. B., Paine, J. B., & Bachrach, D. G. 2000. “Organizational citizenship behaviors: a critical review of the theoretical and empirical literature and suggestions for future research,” Journal of Management, Vol. 26, No. 3, pp. 513-563.

Podsakoff, P.M. and Organ, D. 1986. “Self-reports in organizational research: problems and bprospects”, Journal of Management, Vol. 12, No. 4, pp. 531-544.

Punch, K. F. 2005. *Introduction to Social Research*, London: SAGE Publications.

Putri, F., and Hovav, A. 2014. “Employees’ Compliance with BYOD Security Policy: Insights from Reactance, Organizational Justice, and Protection Motivation Theory,” Proceedings of the European Conference on Information Systems, Paper 10.

Rafferty, A. E., and Griffin, M. A. 2004. “Dimensions of transformational leadership: Conceptual and empirical extensions,” The Leadership Quarterly, Vol. 15, No. 3, pp. 329-354.

Rafferty, A. E., and Griffin, M. A. 2004. “Dimensions of transformational leadership: Conceptual and empirical extensions,” The Leadership Quarterly, Vol. 15, No. 3, pp. 329-354.

Rapoport, R. N. 1970. “Three dilemmas in action research with special reference to the Tavistock experience”, Human Relations, Vol. 23, No. 6, pp. 499-513.

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

Rogers, R. W. 1975. “A protection motivation theory of fear appeals and attitude change,” Journal of Psychology (91:1), pp. 93-114.

Rogers, R. W. 1983. “Cognitive and physiological processes in fear appeals and attitude change: A Revised theory of protection motivation,” in Social Psychophysiology, J. Cacioppo and R. Petty (eds.), New York: Guilford Press.

Rosemann, M. and Vessey, I. 2008. “Toward improving the relevance of information systems research to practice: the role of applicability checks”. MIS Quarterly, Vol. 32 No. 1, pp. 1-22.

Rowe, G. and Wright, G. 1999. “The Delphi technique as a forecasting tool: issues and analysis,” International Journal of Forecasting, Vol. 15, No. 4, pp. 353-375.

Rowley, J. and Slack, F. 2004. Conducting a literature review. Management Research News, Vol. 27, No. 6, pp. 31-39.

Roy, S., Tarafdar, M., Ragu-Nathan, T. S. and Marsillac, E. 2012. ”The Effect of Misspecification of Reflective and Formative Constructs in Operations and Manufacturing Management Research,” The Electronic Journal of Business Research Methods, Vol. 10, No. 1, pp. 34-52.

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

Sadeghi, A., and Lope Pihie Z. A. 2012. “Transformational Leadership and Its Predictive Effects on Leadership Effectiveness,” International Journal of Business and Social Science, Vol. 3, No. 7, pp. 168-197.

Sadeghi, A., and Lope Pihie Z. A. 2012. “Transformational Leadership and Its Predictive Effects on Leadership Effectiveness,” International Journal of Business and Social Science, Vol. 3, No. 7, pp. 168-197.

Sambamurthy, V., and Zmud, R. W. 1999. „Arrangements for Information Technology Governance: A Theory of Multiple Contingencies,“ MIS Quarterly, Vol. 23, No. 2, pp. 261-290.

Scheepers, H. and Scheepers, R 2004. “The Implementation of Mobile Technology in Organizations: Expanding Individual Use Contexts”, Proceedings of the 2International Conference on Information Systems.

Schrader, U. and Hennig-Thurau, T. 2009. “VHB-JOURQUAL2: Method, Results, and Implications of the German Academic Association for Business Research's Journal Ranking,“ BuR - Business Research, Vol. 2, No. 2, pp. 180-204.

Sedlmeier, P. and Renkewitz, F. 2013. *Forschungsmethoden und Statistik: Ein Lehrbuch für Psychologen und Sozialwissenschaftler*, 2nd Edition. München: Person,.

Sein, M.K., Henfridsson, O., Purao, S., Rossi, M. and Lindgren, R. 2011. “Action Design Research”, MIS Quarterly, Vol. 35, No. 1, pp.37-56.

Silvergate, S.H. and Salner, D 2011. “Smartphones and the Fair Labor Standards Act”, For the Defense – Legal Magazine, pp. 41-44.

Silvergate, S.H. and Salner, D 2011. “Smartphones and the Fair Labor Standards Act,” For the Defense – Legal Magazine, pp. 41-44.

Siponen, M. T., 2000. “A Conceptual Foundation for Organizational Information Security Awareness,” Information Management & Computer Security (8:1), pp.31-41.

Siponen, M. T., and Kajava, J. 1998. “Ontology of Organizational IT Security Awareness - From Theoretical Foundations to Practical Framework,” Seventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises Proceedings, Stanford, CA, USA, pp. 327 331.

Siponen, M. T., and Vance, A. 2010. “Neutralization: New Insight into the Problem of Employee Information Systems Security Policy Violations,“ MIS Quarterly, Vol. 34, no. 3, pp. 487-502.

Siponen, M., and Vance, A. 2014. “Guidelines for improving the contextual relevance of field surveys: the case of information security policy violations,” European Journal of Information Systems, Vol. 23, No. 3, pp. 289-305.

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

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

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

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

Stewart, D. W. 1981. ”The Application and Misapplication of Factor Analysis in Marketing Research,” Journal of Marketing Research, Vol. XVIII, pp. 51-62.

Stewart, G. and Thelander, N. 2005. “Can IT Security be Improved with Better IT Leadership in the 21st Century University?,“ Proceedings of the Amaricas Conference on Information Systems (AMCIS), Paper 461.

Stewart, J. 2006. “Transformational Leadership: An Evolving Concept Examined through the Works of Burns, Bass, Avolio, and Leithwood,” Canadian Journal of Educational Administration and Policy, Vol. 54, No. 1, pp. 1-29.

Straub, D. and Ang, S. 2011. “Editor’s comments: rigor and relevance in is research: redefining the debate and a call for future research”. MIS Quarterly, Vol. 35, No.1, pp iii-xi.

Taylor, S. and Todd, P.A. 1995. “Understanding Information Technology Use: A Test of Competing Models,” Information Systems Research, Vol. 6, No. 2, pp. 144-176.

Teddlie, C., and Tashakkori, A. 2011 “Mixed Method Research – Contemporary Issues in an emerging Field”, in: Denzin, N. K., and Lincoln, Y. S., *The SAGE Handbook of Qualitative Research*, SAGE, London, 2011, pp. 285-299.

Tu, Z. and Yuan, Y 2012. “Understanding User’s Behaviors in Coping with Security Threat of Mobile Devices Loss and Theft”, Proceedings of the Hawaii International Conference on System Sciences.

Tu, Z. and Yuan, Y 2012. “Understanding User’s Behaviors in Coping with Security Threat of Mobile Devices Loss and Theft,” Proceedings of the Hawaii International Conference on System Sciences.

Uffen, J., Guhr, N., & Breitner, M. H. 2012. “Personality Traits and Information Security Management: An Empirical Study of Information Security Executives,“ Proceedings of the International Conference on Information Systems (ICIS).

Urbach, N., Buchwald, A., and Ahlemann, F. 2013. „Understanding IT Governance Success And Its Impact: Results From An Interview Study,“ in Proceedings of the 21st European Conference on Information Systems, 5–8 June, Utrecht, Netherlands.

van der Heijden, H. 2003. “Factors influencing the usage of websites: the case of a generic portal in The Netherlands,” Information & Management, Vol. 40, No. 6, pp. 541-549.

Van Grembergen, W., and De Haes, S. 2005. „Measuring and Improving IT Governance through the Balanced Scorecard,“ Information Systems Control Journal, Vol. 2, No. 1, pp. 35-42.

Van Grembergen, W., De Haes, S., & Guldentops, E. 2004. „Structures, Processes and Relational Mechanisms for IT Governance,” in: *Strategies for Information Technology Governance*, W. Van Grembergen (eds.), Hershey, PA: Idea Group Publishing, pp. 1-36.

Van Osch, W., and Coursaris, C. K., 2013. “Organizational Social Media: A Comprehensive Framework and Research Agenda,“ Proceedings of the 46th Hawaii International Conference on System Sciences.

Van Osch, W., and Coursaris, C. K., 2013. “Organizational Social Media: A Comprehensive Framework and Research Agenda,“ Proceedings of the Hawaii International Conference on System Sciences.

Varshney, U. 2003. “Mobile and wireless information systems: Applications, networks, and research problems,” Communications of the Association for Information Systems, Vol. 12, No. 1, pp. 155-166.

Venkatesh, V. and Davis, F.D. 1996. “A Model of the Antecedents of Perceived Ease of Use: Development and Test,” Decision Sciences, Vol. 27, No. 3, pp. 451-481.

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

Venkatesh, V., Morris, M.G., Davis, G.B., Davis, F.D. 2003. “User acceptance of information technology: toward a unified view”, MIS Quarterly, Vol. 27, No. 3, pp. 425-478.

Verizon 2014. “2014 Data Breach Investigation Report,“ http://www.verizonenterprise.com/de/DBIR/2014/.

Vom Brocke, J. 2003. *Referenzmodellierung: Gestaltung und Verteilung von Konstruktionsprozessen*, Berlin: Logos Verlag.

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

Vom Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R. and Cleven, A. 2009. “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.

Vroom, C., von Solms, R. 2004. “Towards Information Security Behavioral Compliance,” Computer & Security (23:3), pp. 191-198.

Walsham, G. 1995. “Interpretive case studies in IS research: nature and method,” European Journal of Information Systems, Vol. 4, No. 2, pp. 74-81.

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

Walumbwa, F. O., Avolio, B. J., and Zhu, W. 2008. “How transformational leadership weaves its influence on individual job performance: The role of identification and efficacy beliefs,” Personnel Psychology, Vol. 61, No. 4, pp. 793-825.

Warkentin, M., Johnston, A.C. and Shropshire, J. 2011. “The influence of the informal social learning environment on information privacy policy compliance efficacy and intention”, European Journal on Information Systems, Vol. 20, No. 3, pp. 267-284.

Webb, P., Pollard, C., and Ridley, G. 2006. “Attempting to Define IT Governance: Wisdom or Folly?,“ Proceedings of the 39th Annual Hawaii International Conference on System Sciences, HI, USA, p. 194b.

Webb, T.L. and Sheeran, P. 2009. “Does Changing Behavioral Intentions Engender Behavior Change? A Meta-Analysis of the Experimental Evidence”, Psychological Bulletin, Vol. 132, No. 2, pp. 249-268.

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

Weeger, A., and Heiko, G. 2014. “Factors influencing future employees’decision-making to participate in a byod program: does risk matter?”, Proceedings of the European Conference on Information Systems, Paper 2.

Weill, P. & Ross, and J. W. 2004a. „IT Governance on One Page,“ CISR Working Paper No. 349.

Weill, P. 2004. „Don’t just lead, govern: How best performing organizations govern IT,“ MIS Quarterly Executive. Vol. 3, No. 1, pp. 1-17.

Weill, P. and Ross, and J. W. 2004b. *IT governance: How top performers manage IT decision rights for superior performance*, Boston: Harvard Business Press.

Wilde, T. and Hess, T. 2006. “Methodenspektrum der Wirtschaftsinformatik: Überblick und Portfoliobildung”, in: Arbeitsbericht des Instituts für Wirtschaftsinformatik und Neue Medien, LMU München, No. 2/06.

Wilde, T. and Hess, T. 2007. “Forschungsmethoden der Wirtschaftsinformatik. Eine empirische Untersuchung”, Wirtschaftsinformatik, Vol. 49, No. 4, pp. 280–287.

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

Williams, B., Brown, T. and Onsman, A. 2010. ”Exploratory factor analysis: A five-step guide for novices,” Australasian Journal of Paramedicine, Vol. 8, No. 3.

Williams, K. R. and Hawkins, R. 1986. “Perceptual Research on General Deterrence: A Critical Review”, Law & Society Review, Vol. 20, No. 4, pp. 545-572.

WKWI 2008. Wissenschaftliche Kommission Wirtschaftsinformatik im Verband der Hochschullehrer für Betriebswirtschaft e.V., WI-Mitteilung der WKWI und des GI-FB-WI. WI Orientierungslisten. Wirtschaftsinformatik Vol. 50, No. 2, pp. 155-163.

Workman, M., Bommer, W.H. and Straub, D. “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.

Workman, M., Bommer, W.H. and Straub, D. 2008. “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.

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

Yukl, G. 2006. *Leadership in organizations*. Upper Saddle River: Pearson Education, Inc.

Zaplata, S., Kunze, C.P. and Lamersdorf, W. 2009 “Context-based Cooperation in Mobile Business Environments – Managing the Distributed Execution of Mobile Processes,” Business & Information Systems Engineering, pp. 301-314.

Zarvic, N., Stolze, C., Boehm, M., and Thomas, O. 2012. „Dependency-based IT Governance practices in inter-organizational collaborations: A graph-driven elaboration,“ International Journal of Information Management Vol. 32, No. 6, pp. 541–549.

Zhu, Y. 2013. “Individual Behavior: In-role and Extra-role,” International Journal of Business Administration, Vol. 4, No. 1, pp. 23-27.

Appendices

Appendix, 1 (A1)

Rechts- und ethikkonforme Identifikation von unternehmensschädlichen Handlungen durch semiautomatisierte Prozesse

Benedikt Lebek, Stefan Hoyer, Halyna Zakhariya, Michael H. Breitner

In: Tagungsband Multikonferenz Wirtschaftsinformatik (MKWI), Braunschweig, Deutschland, 2012, pp. 971 – 982.

Link:

http://digisrv-1.biblio.etc.tu-bs.de:8080/docportal/receive/DocPortal_document_00047576

Abstract

Heutzutage werden in einem Unternehmen eine Vielzahl sensibler Informationen und Daten verarbeitet, die auch vor Attacken aus dem Inneren des Unternehmens geschützt werden müssen. Ein Umdenken im (IT-) Risikomanagement hin zu einer präventiven Identifikation von potenziell unternehmensschädlichen Handlungen wird bereits in der Literatur diskutiert und setzt u. a. starke Mitarbeiterüberwachungen voraus. Dies stößt auf datenschutzrechtliche Grenzen und wirft ethische sowie moralische Bedenken auf. Mit Fokus auf Compliance des (IT-) Risikomanagement wird in diesem Aufsatz gezeigt, wie ein Modell zur automatisierten Identifikation und Prävention unternehmensschädlicher Handlungen aussehen kann, insbesondere wenn deutsches Datenschutzrecht und Mitbestimmungsrechte der Arbeitnehmer beachtet sowie ethische und moralische Bedenken berücksichtigt werden.

Appendix, 2 (A2)
Employees' Information Security Awareness and Behavior: A Literature Review

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

In: Proceedings of the Hawaii International Conference on System Sciences (HICSS), Maui, HI, USA, 2013, pp. 2978 – 2987.

Link:

http://ieeexplore.ieee.org/search/searchresult.jsp?newsearch=true&queryText=lebek

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 a organization's security awareness.

Appendix 3 (A3)

Investigating the Influence of Security, Privacy, and Legal Concerns on Employees' Intention to Use BYOD Mobile Devices

Benedikt Lebek, Kenan Degirmenci, Michael H. Breitner

In: Proceedings of the Americas Conference on Information Systems (AMCIS), 2013, Chicago, IL, USA, Paper 8, pp. 1 – 8.

Link: http://aisel.aisnet.org/amcis2013/ISSecurity/GeneralPresentations/8/

Abstract

The concept of Bring-Your-Own-Device (BYOD) describes the trend of employees using their private mobile devices to manage corporate data from anywhere at any time. BYOD can increase employees' productivity and be cost-cutting for organizations. To implement BYOD, organizations are dependent on employees' acceptance of BYOD, because employees' participation usually is voluntary. As employees' acceptance is affected by uncertainty, we investigate the influence of security, privacy, and legal concerns on the intention to use BYOD mobile devices. A research model is developed based on the theory of reasoned action (TRA) and the technology acceptance model (TAM), which is tested by means of structural equation modeling (SEM) with data collected from, 151 employees. Our results indicate a significant impact of the concerns on employees' acceptance. Moreover, our study reveals employees' indecision towards their intention to use their private mobile devices for working purposes. Several implications for future research and practitioners are given.

Appendix 4 (A4)

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

Benedikt Lebek, Jörg Uffen, Markus Neumann, Bernd Hohler

In: Proceedings of the European Conference on Information Systems (ECIS), 2013, Utrecht, Netherlands, Paper 110, pp. 1 – 12.

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 5 (A5)

Vor- und Nachteile von Bring Your Own Device (BYOD) aus Mitarbeitersicht: Eine qualitative Analyse von Interviews

Benedikt Lebek, Vanessa Vogel, Michael H. Breitner

In: Tagungsband Multikonferenz Wirtschaftsinformatik (MKWI), 2014, Paderborn, Deutschland, Paper 178, pp. 1234 – 1246.

Link: http://digital.ub.uni-paderborn.de/hs/content/pageview/1623769?query=lebek

Abstract

Das Bring-Your-Own-Device (BYOD) Konzept beschreibt die Nutzung privater mobiler Endgeräte von Mitarbeitern für berufliche Zwecke. Aus Unternehmenssicht werden Vorteile wie eine Erhö-hung der Mitarbeiterproduktivität oder Kostenreduktionen mit diesem Konzept in Verbindung ge-bracht. Zur erfolgreichen Implementierung einer BYOD-Strategie sind Unternehmen jedoch auf die Akzeptanz ihrer Mitarbeiter angewiesen, da eine Teilnahme in der Regel freiwillig ist. Diese qualitative Studie zeigt jedoch, dass einige in der Literatur diskutierte Vorteile von BYOD von Mitarbeitern nicht als solche wahrgenommen werden. Zudem führen vor allem Bedenken bezüglich der Wahrung der Privatsphäre sowie der Verwässerung der Grenze zwischen Beruf und Freizeit zu einer negativen Einstellung gegenüber dem BYOD-Konzept. Die Ergebnisse der Studie legen nahe, dass Unternehmen durch Schaffung klarer Richtlinien sowie gezielter Information die Mitarbeiterakzeptanz positiv beeinflussen können.

Appendix 6 (A6)

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

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

In: Management Research Review, Vol. 37, No. 12, 2014, pp.1049 – 1092.

Link: http://www.emeraldinsight.com/doi/full/10.1108/MRR-04-2013-0085

Abstract

This paper aims to provide an overview of theories used in the field of employees' IS security behavior over the past decade. Research gaps and implications for future research are worked out by analyzing and synthesizing existing literature. Within this paper we present the results of a literature review comprising 113 publications. The literature review was designed to identify applied theories and to understand the cognitive determinants in the research field. A meta-model that explains employees' IS security behavior is introduced by assembling the core constructs of the used theories. We identified a total of 54 used theories, but four behavioral theories were primarily used: TPB, GDT, PMT and TAM. By synthesizing results of empirically tested research models, a survey of factors proven to have a significant influence on employees' security behavior is presented. Some relevant publications might be missing within this literature review due to the selection of search terms and/or databases. However, by conduction a forward and a backward search, we have limited this error source to a minimum. This study presents an overview of determinants that have been proven to influence employees' behavioral intention. Based thereon, concrete training and awareness measures can be developed. This is valuable for practitioners in the process of designing Security, Education, Training and Awareness (SETA) programs. This paper presents a comprehensive up-to-date overview of existing academic literature in the field employees' security awareness and behavior research. Based on a developed meta-model, research gaps are identified and implications for future research are worked out.

Appendix 7 (A7)

Big Data, Social, Mobile, and Cloud Computing: A Reference Model for IS Governance and the Nexus of Forces

Benedikt Lebek, Tim A. Rickenberg, Michael H. Breitner

Submitted

Abstract

The Nexus of Forces describes the convergence and mutual reinforcement of the four interdependent trends big data, social, mobile, and cloud computing. Organizations aim to maximize the benefits resulting from the forces while mitigating the associated risks. It is assumed that the interconnectivity of the four individual forces provide unique challenges for IS governance. Although recent studies begin to investigate single forces with regard to IS governance, none of these combine the forces within a comprehensive and integrated reference model. To address this gap, we conduct a Delphi study with, 18 business and IT/IS managers from companies across different industries. Based on qualitative data analysis, we present an initial reference model that helps understanding the impact of the Nexus of Forces on organizational IS governance structures. The model allows organizational decision-makers to develop an effective IS governance implementation. Drawing from the model, implications and areas for future IS research are derived.

Big Data, Social, Mobile, and Cloud Computing: Towards a Reference Model for IS Governance and the Nexus of Forces

1. Introduction

The rapid development of technical innovations and their adoption and diffusion is shaping our current decade. New technologies enable groundbreaking opportunities that impose far-reaching changes to business, economies, and societies. Based on recent advances in processor speed, network bandwidth, and storage, the trends of social, mobile, and cloud computing, as well as big data analytics are on the rise (Goes, 2013). These four forces are predicted to have a lasting impact on the information systems (IS) domain and provide implications and opportunities that go beyond mere technical aspects. In a recent study, the IT research and advisory company Gartner defined these trends as the "Nexus of Forces", referring to the convergence and mutual reinforcement of the four interdependent trends.

Both individually and combined, the Nexus of Forces empowers individuals in their interaction with each other and with associated information through well-designed ubiquitous technology (Gartner, 2013): Information provides the context within the Nexus of Forces for rich social and mobile user experiences. Mobile devices offer a platform for pervasive social networking and new ways of working. Social media and social content allow people to connect with each other and their work in new and innovative ways. Cloud deployment enables ubiquitous and easy access to information and functions for users and IS. Although these forces are innovative and disruptive on their own, together they have the power to revolutionize business and society, breaking down old business models and creating new leaders. Gartner (2013) defines the Nexus of Forces as the basis of the technology platform of the future.

The Nexus of Forces is becoming real as enterprises turn digital and reinvent traditional IT and IS. There is a shift in power towards and emancipation of the users that will also influence traditional management and control mechanisms such as IS governance. Organizations face the problem of how to take advantage of the opportunities that evolve from the Nexus of Forces and maximize the resulting benefits while mitigating the associated risks. A demand for a robust framework to govern these technologies arises. In this context, IS governance is of high relevance, as it focuses on aligning business and IT (De Haes and van Grembergen, 2004; van Grembergen et al., 2004; Dahlberg and Kivijärvi, 2006). By creating flexible IT and IS structures and processes, IS governance addresses the design and implementation of effective organizations (Patel, 2002) and directly influences the benefits generated by organizational IT investments (Webb et al., 2006). A positive correlation between IS governance and organizational performance has been confirmed by several studies (Looso, 2010). For example, Weill and Ross (2004b) state that companies with above average governance earn more than 20 percent higher return on assets (ROA) than organizations with weaker governance. To meet these goals, practitioners have developed several frameworks and tools for IS governance, including COBIT, ITIL, CMMI, and ISO/IEC 17799.

IS governance is an important topic, not only for practitioners, but also for researchers (Webb et al., 2006; Dahlberg and Kivijärvi, 2006). Several recent studies addressed IS governance in the context of one of the trends social, mobile, and cloud computing or big data analytics (e.g., van Osch and Coursaris, 2013; Heier et al., 2012; Malik, 2013). However, the interconnections among the four individual forces provide novel challenges for IS governance and academic research is currently not taking phenomenon into account. In order to address this gap, the purpose of our research is to set up recommendations and to use Delphi methodology to create a reference model that addresses the new requirements and challenges presented by the Nexus of Forces. We pursue the following research question:

RQ: How do the new challenges of big data, social, mobile, and cloud computing influence IS governance?

Existing research in the area of IS governance typically focuses on IT organization, allocation of decision rights for main IT decisions, aligning business and IT, and the consequences of alternative governance and alignment arrangements (Dahlberg and Kivijärvi, 2006). Due to the importance of the emerging trends of social, mobile and cloud computing and big data analytics and their independencies, scientific research that addresses the interaction of the forces and their impact on corporate IT is needed. Following Goes' (2013) proposal that IS research has the task to "recognize emerging areas and phenomena brought about by innovations", (p. v) also aim to uncover potential research areas and provide guidance for future research.

This paper is structured as follows: After the introduction, the theoretical background provides an overview of the related literature explaining IS governance and the Nexus of Forces. On this basis, a conceptual model is formulated to provide the baseline for our research. The next section depicts the underlying research design, including a description of the processes for collecting and analyzing data. Afterwards, a reference model for IS governance and the Nexus of Force is introduced and explained. A discussion with implications for further research follows and provides key areas for future research. Finally, the paper ends with identified limitations and a short conclusion with outlook.

2. Theoretical Background

IS governance is commonly referred to as an integral part of corporate governance (Webb et al., 2006; Burtscher et al., 2009). It draws from corporate governance principles and focuses on the management and use of IT in order to achieve corporate performance goals (Weill and Ross, 2004b). IS governance is closely related to the subjects of IT management, information governance, strategic information systems planning (SISP) and related practitioners' frameworks such as COBIT, ITIL, CMMI, VAL IT, and ISO/IEC 17799 (Burtscher et al., 2009). IS governance forms refer to the placement of decision-making structures within organizations. Literature typically distinguishes between two basic governance designs: centralized and decentralized IS governance (Peterson, 2004; Brown and Grant, 2005). IS governance and its outcomes are impacted by multiple contingencies (Sambamurthy and Zmud, 1999; van Grembergen et al., 2004; Brown et al., 2005; Dahlberg, 2006), which can be divided into internal and external influence factors. With regard to the time dimension and the business orientation, IS governance has a strategic character and must be distinguished from operative IT management.

IS research is starting to address IS governance in the context of one of the forces. Governance of information refers to the structures and processes required to turn data into strategic information assets (Malik, 2013). When dealing with the challenges of data volume, velocity, and variety (Buhl, 2013; Kaisler, 2013), the primary task of governance concerning this regard is the efficient generation of information value while mitigating related risks (Malik, 2013; Tallon, 2013). Due to the increased use of the internet, mobile devices, and social media, new sources for data analysis occur (Chen et al., 2013) and are impacting information governance (Malik, 2013; Tallon, 2013). Cloud governance draws from service oriented architecture (SOA) governance (Guo, 2010; Fortis et al., 2012) and "aims at providing optimum service quality, consistency, predictability and performance" (Guo, 2010, p. 1). Research in this area is needed, as it is expected that cloud computing presents challenges to the IT organization to stay involved and in control (Heier et al., 2012). The transfer of organizational data to cloud providers and the possibility of information crossing national borders leads to unclear data ownership and difficulties concerning privacy laws and other regulations (Janssen, 2011; Kshetri, 2013; Heier et al., 2012). Organizational use of social media has the potential to change processes, collaboration, and communication. However, van Osch and Coursaris (2013) state that there is a lack of studies analyzing the influence of social media on corporate governance in organizations. Increasing convenience, efficiency, and productivity of mobile working drive organizations to implement

mobile devices into the IT infrastructure to take advantage of the flexibility these devices offer (Scheepers and Scheepers, 2004). The concepts of consumerization and bring-your-own-device (BYOD) are strongly related to the topic of mobile device usage in organizations. BYOD creates a "unique set of challenges for IT professionals" (Johnson and Joshi, 2012) as it "redefines the relationship between employees...and the IT organization" (Niehaves et al., 2012, p. 1). In this context, the compliance to legal, privacy, and security regulations becomes important (Lebek et al., 2013).

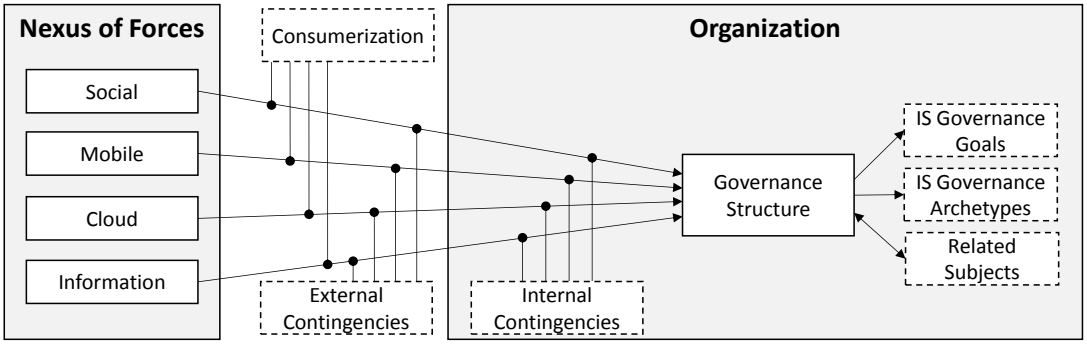


Figure 1. Conceptual Model

Based on existing governance literature and the findings by Gartner (2013), we formulated a conceptual model that provides the baseline for our research (Figure 1). We investigate the influence of the Nexus of Forces on organizations in general and the organizational governance structure in particular. For this purpose, we regard each of the four forces (social, mobile, cloud, and information) and their impact on governance structure. The effect of the forces is moderated by the consumerization pressure, as well as by external and internal contingencies. The governance structure comprises the corporate governance and IS governance including their goals and archetypes as well as related subjects.

3. Research Design and Data Collection

The purpose of this study is to construct a reference model based on our conceptual model and empirical material obtained from qualitative expert interviews. For this purpose, we chose the Delphi method as the underlying research design of this paper. The Delphi method is a “systematic interactive research method that relies on a panel of independent experts" (Olbrich et al., 2011, p. 7). This flexible method for structuring a group communication process (Linstone and Turoff, 1975) is especially suitable to explore new issues with subjective and complex judgments of experts within a series of questionnaires until consensus is reached (Kendall, 1977). Four core elements characterize a Delphi procedure (Rowe and Wright, 1999): anonymity, iteration, controlled feedback, and the statistical aggregation of group response. Anonymity is ensured by questionnaires and one-on-one interviews which allow participants to express opinions and judgments privately without social pressures. The iterative process allows them to change and advance personal judgments and revise earlier answers in light of replies of the other panel members (Olbrich et al., 2011). Controlled feedback between the rounds informs the participants of the opinions of the anonymized panel. The group judgments is created by aggregating and averaging the responses of the iteration. The procedure stops when a stop-criterion is reached or consensus is achieved. Figure 2 shows the research design applied here which includes five phases.

A reference model is a recommendation that is useful for the development of specific models (Goeken, 2003). It provides general solutions for an abstract class of problems and supports the solution of specific tasks. A reference model constitutes a starting point and serves as a pattern for a general class of modeling issues. The content of reference models is intended for the re-

use in the design and construction of further specific models. Recommendations contained in a reference model must fulfill the requirements of general validity and applicability. Consequently, a reference model is an interlinked set of defined concepts providing an abstract framework or domain-specific ontology, which can be created by an expert or body of experts and aims to encourage clear communication (Fettke and Loos, 2007; Falconer, 2014).

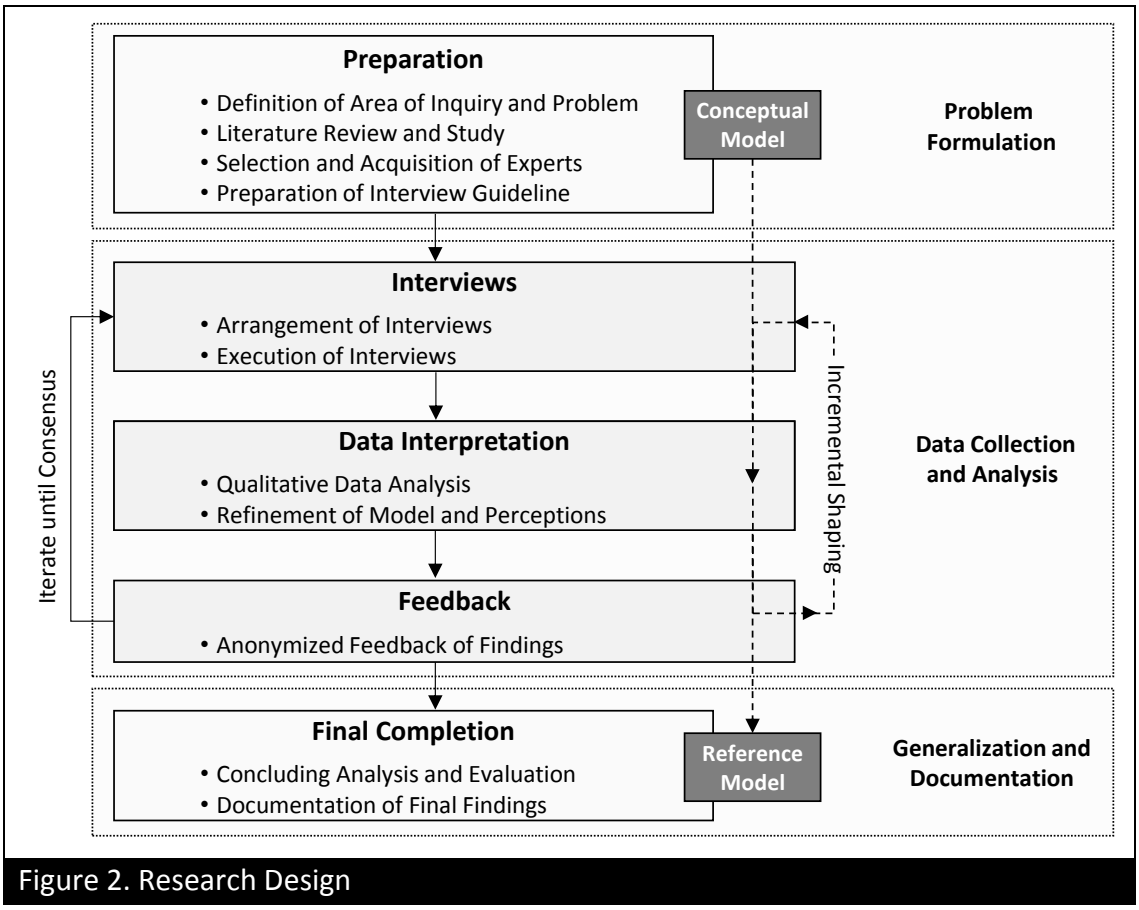


Figure 2. Research Design

Within the preparation phase, initial investigation and problem formulation as well as the creation of theoretical grounding were the focal point. To ensure rigor, a comprehensive literature review was conducted. We used established guidelines for reviewing literature (see Webster and Watson, 2002; Levy and Ellis, 2006; Vom Brocke et al., 2009). A list of search terms was used, including "IT/IS governance", "Nexus of Forces", and search strings referring to the individual forces. We primarily searched within databases (AISeL, IEEExplore, ScienceDirect, etc.) but also directly in IS research journals and conferences. Based on the hit lists, the papers were screened and relevant ones were selected. In addition to scientific literature, we included non-scientific literature such as practical literature and websites as clinical perspective to reduce the gap between the scholars' and practitioners' point of view (Grahlmann et al., 2011). To analyze relevant literature, we used coding techniques (Glaser and Strauss, 1967; Strauss and Corbin, 1998) to generate initial assumptions about possible effects of the Nexus of Forces on organizational governance structures. We created the conceptual model as a basis for the iterative refinement. A Delphi approach was chosen since there were little sources of factual data but a basis for an opinion existed (Grey and Hovav, 2008). To ensure valid and robust results, experts with significant experience in the fields of IS governance and the Nexus of Forces were selected. We were able to acquire 18 participants from different branches for our study; see Table 1 below. The final step of the preparation phase was the creation of an interview guideline and a questionnaire.

Table 1: Participants of the Delphi Study			
#	Role	Focus	Branch
1	Senior IT manager	Enterprise architecture and is strategy	IT services
2	Chief information officer (CIO)	General management of IS	IT services
3	Senior IT manager	Demand and service management	IT services
4	Manager in strategic marketing	Strategy development, market research	Automation Technology
5	Senior business manager	Business process management	Automation technology
6	Senior IT manager	Application development	IT services
7	IT consultant	Security and governance consulting	IT services
8	Software developer	Development of ECM portal solutions	Software development
9	Sales process manager	Management of IT applications sales	Automation technology
10	Chief information officer (CIO)	General management of IS	Automation technology
11	Chief information officer (CIO)	General management of IS	Steel industry
12	Director IS and services	General management of IS	Mechanical Engineering
13	Senior IT manager	Management of IT applications sales	Automation technology
14	Executive director	General business management	Automation technology
15	Senior IT manager	Department manager new technologies	Manufacturing
16	Chief information officer (CIO)	General management of IS	Mechanical engineering
17	Business manager	Business development and restructuring	Finance
18	Senior IS researcher	Enterprise modeling and architecture	IS research

An iterative procedure of data collection and analysis followed. The first explorative round of interviews was conducted within a period of four month within, 2013. This round of interviews was used to explore the opinion of the experts and to evaluate our initial assumptions and model. Half of the interviews were performed in person and the other half with an online collaboration and conference tool. Each of the interviews lasted between 60 to 90 minutes, and each was recorded and transcribed. After (1.) an introduction, the experts were asked to (2.) draw initial sketches linking an exemplary organizational governance model with the Nexus of Forces graphically and to illustrate the impacts. Then (3.) the evaluation of initial assumptions

and (4.) a detailed discussion were performed before (5.) a wrap-up concluded the interviews. Qualitative data analysis (Punch, 2005) and coding techniques were used to analyze and interpret the transcribed responses and sketches. We performed open coding to identify concepts and attached initial labels to the data. Within selective coding, higher level categories were generated from the descriptive open codes. Based on the coding, an aggregated group response was generated and the conceptual model was refined. The participants were informed of the anonymized group response and the refined model by controlled feedback. Consistent with the iterative character of the Delphi methodology, the participating experts from the first round were invited to a second survey round to advance the judgments and opinions. The effective response rate of the second round was 78 percent (14/18). To enable discussion between the experts and test the refined conceptual model, specific participants (7) were invited to a focus group (Krueger and Casey, 2009), which lasted 90 min, and which was also recorded and transcribed. The other participants were again surveyed using interviews (2) or written questionnaires (5). To interpret the additional data, we used the same analysis methods as in the previous round. While the model was essentially confirmed, it was significantly extended and advanced based on the profound statements from the participants.

“One of the more difficult aspects of the Delphi process is the appropriate method of measuring consensus" (Hallowell and Gambatese, 2010, p. 103). The characteristics of the data and empirical material that we gathered pose a further challenge: Due to the qualitative character of our study and the participants’ responses, no quantitative consensus methods were applicable. Instead, we critically reviewed the individual answers and used interpretive reasoning to assess and measure the variance. During the second round of data collection and analysis, and especially during the focus group, a high consensus degree was reached and a consistent model was created. Consequently, the interviews and incremental shaping of the model were finished. Within a phase of final completion, the reference model was finalized and the findings were documented.

4. Results

4.1 An IS Governance Reference Model for the Nexus ofForces

For assessing our RQ whether the Nexus of Forces has an influence on organizations in general and IS Governance in particular, we create and introduce an initial reference model (Figure 3) based on our empirical insights and findings which were gathered within the Delphi study. As proposed by Gartner (2013), the model basically comprises the four forces, information, mobile, social, and cloud computing, as well as consumerization. The four individual forces are closely interrelated, which leads to a mutual reinforcement. The use of mobile devices enables access to corporate information resources, independent from restrictions regarding time and location. Moreover, mobile devices provide a platform to communicate via public and enterprise social networks and thus create a great amount of information. In this context, the cloud represents a necessary transmission medium for delivering information. The consumerization of IT leads to a "blurring of business and personal boundaries" (Niehaves, 2012, p. 2) because this term describes the use of consumer IT in the organizational context. Consumerization leads to an adoption pressure that forces organizations to react and to adjust governance structures including corporate governance, IS governance, and the operative IS management. The reference model and findings are explained in detail in the following sub sections.

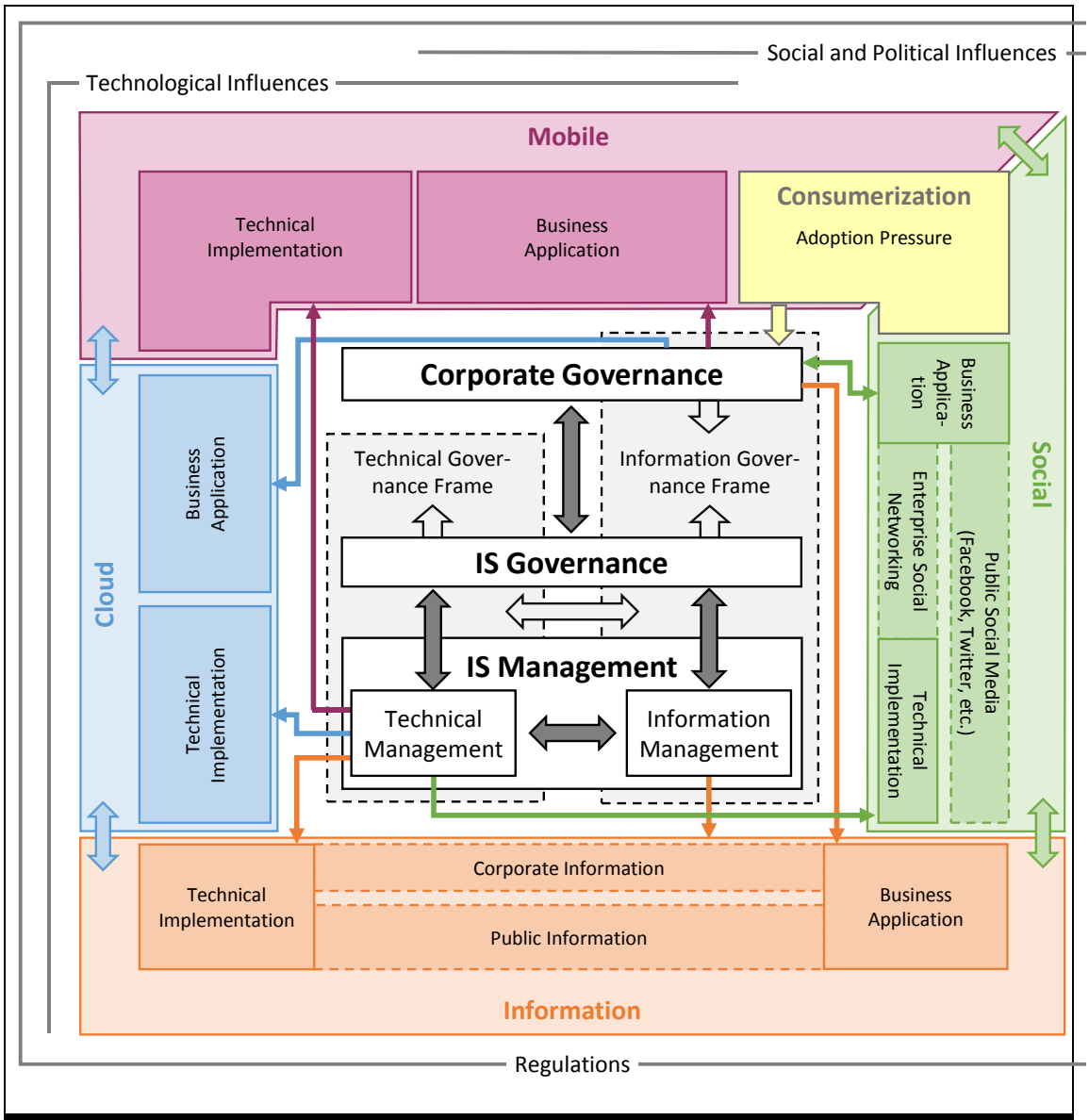


Figure 3. IS Governance Reference Model for the Nexus of Forces

4.1.1 External Contingencies

Organizations operate within an environment that is strongly determined by the geographical, political and cultural region, as well as the industry or branch. Consequently, organizations are exposed to the influence of various external contingencies (Burtscher et al., 2009). The potential effects created by the Nexus of Forces are significantly influenced by regulations, technical influences, and social and political influences. Regulations represent an enclosing frame that prescribes legal guidelines for organizations and its members. In this context, especially statutory requirements relating to data protection and information security are particularly of importance. For example, specifications for collecting, processing, and storing data and information significantly affect the use of cloud services or the possibilities of analyzing user data from social networks.

Within the regulatory frame, social and political influences affect organizations mainly with regard to the areas of mobile, social, and information. The proliferation of mobile computing devices continues to increase as tablets and smartphones became a part of daily life for many users (Moreno et al., 2012). As a result, mobility emerged as a main driving factor of the modern service society (Zaplata et al., 2009) pressuring organizations to find ways to implement mobile

devices into their IT infrastructure in order to take advantage of the flexibility these devices offer (Scheepers and Scheepers, 2004). Organizations operating in branches with a close proximity to consumers must also be present within public social media (Jarvenpaa and Tuunainen, 2012). Moreover, because they are familiar with the advantages of public social media for communicating in private life, employees demand adoption of social media technology within the working context. Last, social and political conditions influence organizational handling of information. This aspect mainly refers to the collection, storage and analysis of personal data from social networks, but also refers to data and information that organizations provide to their environment.

Technological influences refer to (technical) innovations in the areas of mobile devices, cloud computing, and data processing. As a result of improvements in functionality and usability of mobile devices and the development of mobile data network coverage (Tu and Yuan, 2012), tablets and smartphones provide a convenient platform to perform various work processes and tasks. With increasing mobility of the workplace, cloud services emerged as a platform to provide time and location independent access to applications and information. Moreover, recent developments in the area of data analytics (e.g., in-memory computing) allows organizations to gain information from data that was previously merely used and thus is able to create business insights and advantages.

4.1.2 Governance and Decision-Making Structure

The inner part of the reference model describes core elements and interrelationships of the organizational governance structure. According to Weill and Ross (2004a), IS governance encompasses five major domains of decision-making in relation to the management and use of IT in organizations: (1) IT principles relate to corporate level statements about the strategic role of IT in the organization, (2) IT architecture refers to technical choices to satisfy business needs, (3) IT infrastructure are centrally coordinated IT services that provide the foundation for organization-wide IT capabilities (e.g., network services, security, help desks, etc.), (4) business application addresses the opportunities provided by new technologies and (5) IT investment deals with budgeting for IT, including project approvals, and justification techniques. Within the proposed IS governance reference model, the decision-making hierarchy extends over the three levels of corporate governance, IS governance, and IS management.

IS governance must be driven by corporate governance and not by the IT department (Webb et al., 2006). According to its goals, namely value delivery and risk management, corporate governance defines IT principles based on the strategic direction of the organization and is responsible for the business application of the Nexus of Forces. This need to shift accountability and responsibility for IS decisions towards corporate governance is emphasized by the Nexus of Forces.

> *"The Nexus of Forces is a comprehensive issue that needs to be regulated across the organization, and IT can ultimately be used as a tool. But the definitions and regulations must be established on [corporate governance] level". (#10, CIO)*

Based on cost benefit-analyses, corporate governance sets the degree of adoption of new technologies and trends within the organization, defines necessary adjustments of business processes, and establishes rules for implementing the Nexus of Forces.

While corporate governance defines the mission statement, IS governance ensures that the IT is properly aligned to business strategies and objectives. The IS governance includes two main rights: decision rights, such as architecture and infrastructure, which are the core responsibilities of IS governance (Weill, 2004) and input rights with regard to investments, business application, and IT principles. Input rights provide expert advice on key IT decisions (Dahlberg and Kivijärvi, 2006) that are made on corporate governance level. In the reference model, IS governance includes two core frames that are closely related with strong interdependencies. The technical

governance frame sets specifications for architecture and infrastructure focusing on technical decisions on hardware, software, and systems. The information governance frame sets basic rules and policies for collecting, processing, and storing information assets at an enterprise level without primarily focusing on technical aspects. While technical governance is defined on the IS governance level, information governance is set by an interaction of the corporate and IS governance linking business and IT aspects. Corporate and IS governance set the scope for the actual operative execution, which is the responsibility of IS management. Within practice, the boundaries between these entities are not distinct.

> *"The problem is of course: where is the boundary between IS management and IS governance? IS governance defines the basic structures and established processes, and the principal things. And then, of course, the two quite massively correlate". (#12, Director IS and Services)*

Similar to IS governance, operative IS management is divided into two interacting parts: technical and information management. IS management represents the alignment of the actual operative execution and realization to the IS strategy, which is determined by corporate and IS governance decisions. The scope of technical and information management is defined by the respective governance frame. Both technical and information management provide feedback to the IS governance by means of input rights.

4.1.3 Consumerization Pressure

Consumerization as a socio-cultural construct is the main driver of the Nexus of Forces that creates an impact on an organization. The adoption pressure arising from it results from the private use of mobile and social computing and forces organizations to adopt these new capabilities for working purposes.

> *"The [adoption] pressure arises from the employees; they say: I know it one way [from private use], you can do that way, but why is this so complicated in our organization?"* (#9, Sales Process Manager)

In the first place, the adoption pressure affects organizations on the business level and interacts with the corporate governance. As a result, the adoption pressure mainly impacts the corporate governance, which can require a change of the business and IS strategy.

> *"The pressure is really on the IT organization via the [corporate] governance... But what is becoming more important is business transformation...to realize the goals of an organization, which are defined by the corporate governance – but no matter what you specify in the business strategy, there will be changes to IS".* (#1, Senior IT Manager)

General rules about the use of the arising technologies and resulting business opportunities and risks have to be set on the corporate governance level. In order to maximize the benefits and to mitigate the risks associated with the Nexus of Forces, organizations must adjust and improve their business processes, business applications, and possibly their business model. While these possible business changes on governance level ideally follow a top-down approach, the actual trigger originates from the employees as a bottom-up process. Employees ask to use (new) technical solutions for working purposes that they primary know from private life and therefore trigger request and demand management processes within operative IS management. This adoption pressure eventually accumulates on the IS management level and is handed up hierarchically to the corporate (governance) level so that a fundamental business decision can be made.

> *"The big challenge is to accomplish that requests within the IS management are mapped in direction of the governance: When do we get iPhones? What can we do with it? Why can't we do this and that?"* (#6, Senior IT Manager)

User requests mainly focus on social and mobile computing and not, as initially assumed, on cloud computing. Within the study, the participants largely stated that cloud computing as a transfer medium is a rather technical aspect within the backend systems that enables ubiquitous data access, for example for mobile and social services.

> *"The cloud is to me more like some, I'll say it casually: a technical thing that allows me to be mobile and to have access on information, which is perhaps even driven through social media. But [the cloud] is rather a vehicle for me".* (#9, Sales Process Manager)

This also remains true for information as a force of the Nexus. Large amounts of data are produced within the private context, however, data analytics do not originate from and are not driven by the private sector or consumerization. Therefore, the forces cloud computing and information do not represent core components of consumerization within the reference model.

> *"The area of information and big data, I don't think that this actually originates directly from the private sphere".* (#4, Manager in Strategic Marketing)

4.2 Application and Impact of the Nexus of Forces

4.2.1 Corporate Governance

The impact of the Nexus of Forces on an organization is described along the governance hierarchy. Corporate governance aims to maximize the benefits and mitigate the risks associated with the Nexus of Forces and is therefore responsible for defining the frame for the business application in a specific organizational context. Further organizational processes and structures, and possibly the business model, need to be examined and adjusted for useful business applications in order to take advantage of new opportunities provided by the emerging technologies.

> *"IT is not such a big issue at this level and stage – organizations rather...have to look for useful business applications. And if the usefulness is not given, then it does not matter, what kind of innovations are out there".* (#12, Director IS and Services).

Concerning the mobile force, corporate governance regulates whether mobile devices such as smart phones and tablets can be used within the organization, and for which business cases and in which contexts. It defines for instance, whether BYOD is allowed, general restrictions for mobile data access, mobile app restrictions, and allowed standard devices. Due to extensive private use and experience of mobile devices and the resulting adoption pressure, it is particularly crucial to create an effective business application for mobile systems. This emerges from two reasons: First, not to yield to the adoption pressure prematurely without accurately analyzing opportunities and threats. Second, that users already have rich experience with mobile devices from private life and therefore have certain expectations concerning usability and usefulness within the professional working context.

This also applies to the social force. While employees gain rich experience in public social media networks, the use of social media and networks within organizations is relatively new. The reference model differentiates between public social media (Facebook, Twitter, Xing, etc.) and enterprise social networking (ESN), which is defined as the use of "technologies that emerged on

the public internet within the workplaces of organizations to facilitate work-related communication and collaboration" (Richter and Riemer, 2013, p. 2). Corporate governance defines the use of both aspects via the business application. The relationship of the business use of public social media is twofold. On the one hand, corporate governance regulates the way of communicating with the public and thereby it shapes the perception of the organization within society. On the other hand, public social networks represent new opportunities for organizations such as direct contact with customers and undelayed feedback, which in turn can affect the organizational strategy.

The business application of the information and cloud forces is regulated by the corporate governance as well. For instance, rules about the general use of the cloud, whether private, hybrid, or public, have to be set. The business application further specifies rules for the storage and transmission of data via the cloud with regard to information security and data protection policies. Concerning the force information, the business application stands for the definition of general rules about the use of information.

> *"In the corporate governance it is defined or must be defined how to deal with information and [later] the IT governance must ensure that [certain information] can only be accessed by authorized people".* (#6, Senior IT Manager)

These general rules describe the development and implementation of processes for collecting, storing, and processing data. Corporate governance specifies to what extent internal sources (e.g., ERP, CRM, and ECM systems) and external sources (e.g., public social media, market research) are used to collect data. Further these rules address the classification of data and provide guidelines regarding which types and classes of data can be stored in which repositories (in the cloud or on-premise) and processed to generate business information, especially with regard to big data and content analytics. The reference model differentiates between corporate information that is created and used within the organization and public information that is created and resides outside of the organization, including information that the organization publishes to its environment.

4.2.2 IS Governance and IS Management

Subordinated hierarchically under the corporate governance, IS governance in combination with the operative IS management regulates the technical implementation of the forces. Technical management aims to facilitate and to put the business applications in concrete terms in form of tangible technical solutions. Thus, technical management operates within the frame that is set by the governance entities. This means, for instance, if the use of cloud services is prohibited by corporate governance, the technical management for this aspect becomes irrelevant. Concerning the cloud, technical management defines service level agreements (SLA) with public cloud providers, wide area networks (WAN) connections to the cloud, and so forth. The technical implementation of mobile systems takes aspects such as mobile device management (MDM), the employed technical data encryption, and so on into account. With regard to social, technical implementation mainly deals with the deployment of internal social networks rather than adoption of public social media. It includes the selection and sizing of internal ESN systems and their customization. The use of public social media does not require an internal technical implementation and expertise and is therefore not a primary IS topic. The technical implementation of the force information realizes internal and external data and content management systems and their characteristics, for example technical design of database schemes, selection and customization of ECM systems, and implementation of technologies for data analytics. The operative information management on the other hand includes non-technical aspects such as enterprise-wide metadata, taxonomies, and classification of data and information.

5. Discussion

5.1 Research Contribution

To address our RQ, we iteratively derive a reference model from empirical evidence that we gathered from qualitative interviews within a Delphi study. The reference model facilitates clear communication and provide IS researchers with a basis to develop specific models. Further, the model allows organizational decision-makers to design an effective IS governance implementation. Our main findings suggest that the Nexus of Forces' capability to create an impact on organizations and IS governance structures depends on the organization's environment and external contingencies. Consumerization is the main driver for adapting the Nexus of Forces within organizations and influences organizations particularly on the business level. Therefore it is primarily the responsibility of corporate governance to set structures concerning IT investment, business application, and IT principles. Due to increasing quantity and importance of information, information governance is gaining in significance – without a primary focus on technical solutions. The information governance frame is a set of basic rules and policies for collecting, processing, and storing information assets and is defined by corporate governance in combination with IS governance. The IS governance focuses on technical aspects and defines the technical governance frame by setting guidelines with regard to IT architecture and infrastructure. Similar to the governance level, the executing IS management is divided into technical and information management parts. While the business application of the Nexus of Forces is determined by the corporate governance, the IS and technical management realize the actual technical implementation according to the specifications of the governance entities. The proposed reference model depicts the interrelationships of the Nexus of Forces with organizational governance structures, as well as the decision-making structure and responsibilities.

Based on our empirical findings from the results section above, we discuss the Nexus of Forces in the context of its organizational application and relate it to existing IS research literature. This mainly includes the role of internal contingencies, the Nexus of Forces' impact on governance archetypes, threats and challenges emerging from the Nexus of Forces, and socio-technical aspects.

5.2 Interpretation of Results and Comparison with Prior Work

The internal and external contingencies within an organization and its environment determine the impact and adoption pressure that the Nexus of Forces exerts on that organization. Regarding the internal contingencies, the role and perception of IT and the attitude towards technology within the organization represent a substantial factor. While IT constitutes an important part and plays a significant role in some organizations, the significance of IT and of IT innovations is fairly low. As proposed by Chen et al. (2010) and Leidner et al. (2010), organizations can regard IT and IS as innovators or from a rather conservative point of view (IS conservative). Chen et al. (2010) operationalize IS strategy as the degree to which organizations have a shared perspective to seek innovation through IS. Concerning IS as innovator, IT holds a consultative function and initiates innovations that help the business to stay competitive and seek new opportunities. In stark contrast, IS conservative represents a safe and stable approach in which changes to IT are only carried out if they are really promising or necessary, have been carefully examined, and are proven in practice. Along these lines, the impact that the Nexus of Forces is potentially able to create within an organization depends on the role of IT and partially on the branch of the organization. If the importance of IT in an organization is high, then the potential impact that the Nexus of Forces is able to create high as well. Within the study, participants from organizations that regarded IS as an innovator rated the potential impact of the Nexus of Forces higher than participants with a rather conservative attitude towards IT. For instance, organizations from our study that operate close to the consumer assessed the new opportunities and additional value

coming from the Nexus of Forces as being higher than organizations with a rather static business environment. Especially organizations within rigid and regulated markets that were slow to change have not yet taken advantage of cloud, mobile, and social computing or big data. They barely saw the need to investigate these new trends and did not see much potential in them. In contrast, the organizations that operate on the consumer market have experience with the new technologies and are steadily exploring new opportunities arising from the Nexus of Forces.

With regard to the design of decision-making structures, the experts who participated in this study unanimously stated that the Nexus of Forces impacts the governance archetypes within organizations. According to IS governance literature, governance approaches can vary from centralized to decentralized structures. Weill and Ross (2004b) showed that centralized governance approaches are to be found in organizations that mainly focus on profitability. These organizations aim to reduce business process cost and therefore establish a high degree of standardization for business and IT. This includes centralized processes for architecture compliance and organization-wide IT investment decisions. On the other side, organizations that are focused on innovation aim for local accountability through decentralized decision-making structures. These organizations establish only a few organization-wide standards in favor of creativity, business unit autonomy, and proximity to local customers. However, during the interviews, it became apparent that the Nexus of Forces continues to challenge stringent centralized or decentralized governance designs. On the one hand, specific characteristics of consumerization pressure depend on cultural, social, and regional aspects and force organizations to increase responsiveness to local employee demands. Apparently, centralized governance approaches fail due to inflexibility with regard to requests that result from extensive communication and coordination processes. On the other hand, decentralized approaches can fall short in defining stable and lasting infrastructures due to proliferation of solutions and inherent risks. Therefore, hybrid approaches will gain importance (Andriole, 2012) as these attempt to balance the contrasts of standardization and innovation (Weill and Ross, 2004a).

In addition to the advantages and new opportunities that the Nexus of Forces presents, new risks, threats and challenges emerge. While marketing and advertising, as well as outlets of popular science mainly emphasize the benefits, the participants of our study also expressed their doubts and concerns. Typical critical remarks from participants concerning mobile computing centered on the ubiquitous availability – anywhere and at any time. This can be an advantage, but it can also create stress and can interfere with the private lives of employees; see also Niehaves et al. (2012). A main concern of participants with regard to cloud computing is the perceived security risks (see Ackermann et al., 2012), especially when a public cloud is used for sensitive data and the servers are located in a foreign country. Typical critical concerns towards social networking and computing are additional workload and negative comments that can escalate into so-called shit-storms (Yang and Albers, 2013). Information overload, in particular in combination with social media and content, was mentioned by the participants as being a main challenge and risk of the information force. While important negative issues are raised here, the list is merely illustrative rather than exhaustive. In combination, the forces represent an increased level of complexity to some of the participants. This seem to be a contradiction, since these new technologies such as the cloud aims to hide technical complexity. However, organizations have established IT infrastructures, and new technologies require investigation before they can be adopted and integrated. As a result, organizations have to analyze the opportunities and threats of the Nexus of Forces diligently and must adjust governance structures as a consequence. Thus, organizations are not exposed to the risk of reacting too late to the upcoming adoption pressure, but are able to act early and with foresight. Another risk of disregarding or banning the Nexus of Forces is that shadow IT can emerge. Users know the new technologies from private use and also want to take advantage of them in the working context. Next to the use of private smart phones, called BYOD, another trend is emerging: BYOC – bring-your-own-cloud (Costello and Prohaska, 2013). If organizations fall short in creating useful systems and applications that users know from consumerization, users might try to build their own illegal

solutions in terms of shadow IT. Therefore, prohibiting the new technologies does not represent a satisfactory solution. Certainly organizations do not have to adopt all of the forces and under all circumstances. As part of a cost-benefit analysis, organizations need to decide what is worthwhile and what is not investigating further. Accordingly, IT in particular and the organization in general needs to position itself towards the Nexus of Forces, establish rules and a strategy, and adjust governance structures. A well-implemented governance can help to keep the new technologies and opportunities manageable.

Driven by both technical and social developments, the Nexus of Forces impacts organizations on a socio-technical level. Stemming from the context of labor studies, socio-technical refers to the reciprocal interrelationship of social and technical aspects of an organization or the society as a whole (Ropohl, 1999). As Emery et al. (1964) stated, organizational success strongly depends on the organization's ability to work as a socio-technical system. Accordingly, organizations will fail to succeed if they consider themselves to be a solely technical system with individuals that have to adapt to the system and can be replaced. The importance of social and behavioral aspects in the area of management information systems (MIS) has been recognized by practitioners and research for a long time. Bostrom and Heinen (1977) stated that IS will fail if organizational, social, and behavioral aspects are ignored in the design and operation of information systems. If organizations are not able to understand and consider these aspects, IT investments will not benefit since systems are not accepted by users. This rationale is also reflected in the technology acceptance model (TAM) by Davis et al. (1989). The TAM postulates that users' perceptions of usefulness and ease of use of technologies determine their intention to use technology. The consumerization pressure related to the Nexus of Forces emphasizes the importance of the socio-technical and user acceptance perspective once again. Employees form expectations towards the usefulness and ease of use of technologies, such as smartphones or social networks, based on experience from private usage. Organizations now face the challenge of adopting these technologies without failing to live up to employees' expectations. Reasons for missing expectations are for example, restrictions on functionality due to information security measures. Furthermore, our interviews revealed that employees' expectations vary among generations. Different generations of employees that work together in an organization have different experiences and different ways of thinking. Older employees tend to be more skeptical about new technologies while young employees are more open to new technologies (Koning and Gelderblom, 2006). Organizations are challenged to manage this conflict.

5.3 Implications and Key Areas for Future Research

While this study relates to the Nexus of Forces with organizational governance structures, implications and key areas for future research arise. The reference model proposed here can act as a basis for further refinement that focuses on partial aspects and operationalizes the model. For instance, this includes the investigation and definition of roles and responsibilities within IS management concerning the new technologies of the Nexus of Forces. With regard to the archetypes as proposed by Weill and Ross (2004b), hybrid approaches and federal archetypes require further attention since they are becoming more important within the IS governance research domain. Further, the influence of the Nexus of Forces and of consumerization on methods and processes to achieve the five goals of IS governance requires investigation. This applies in particular to value delivery and risk management as the outcomes of IS governance. For instance, this includes the construction of new IS solutions that apply the forces in order to generate additional business value or evaluate and manage the novel risks of the technologies. Irrespective of the proposed reference model, practical changes within organizations that result from the Nexus of Forces demand empirical investigation. The interviews revealed that the organizations are facing or currently starting a transition process that will create measurable empirical evidence within the next few years. Accordingly, based on this initial study, further analysis of the general impact of the Nexus of Forces on society, organizations, and employees are necessary. This goes in hand with recent findings of Bharadwaj et al. (2013) and Andriole (2012)

that state that in addition to the digital trends (i.e., big, data, cloud, pervasive connectivity, social, etc.), there are also key organizational shifts concerning the role of IT in organizations. Accordingly, we endorse Bharadwaj et al. (2013), who propose a digital business strategy and argue that "the time is right to rethink the role of IT strategy“ (p. 471).

5.4 Limitations

After outlining potential practical and theoretical implications of our research, we would like to point out the limitations of the current study. With regard to the proposed IS governance reference model, this study does not raise the claim to be exhaustive. We provide initial inside to this research topic and to facilitate further investigation. The reference model should be refined and validated by future research and discussions. Concerning the research process, the amount of participants was rather limited compared to other Delphi studies for three reasons. First, the topic of the Nexus of Forces is relatively new as it was mainly triggered by Gartner in, 2012. Since our intention was to provide a contemporary and initial insight into the subject matter in order to facilitate further research, a long enquiry period was not applicable. Second, in the course of the first round of interviews we asserted that the gain of new evidence decreased constantly and finally came to halt so that we stopped recruiting new experts after 18 interviews were completed in accordance with our pre-defined stop criteria. Third, we mainly recruited top management experts on CIO and senior management level who were able to provide rich insights regarding the subject-matter during in-depth qualitative interviews. A limitation arises from the fact that the participants mainly come from the industry branch. When interpreting our results, it has to be considered that the impact of the Nexus of Forces varies between different organizations and branches, as stated in the discussion. It would be interesting for future research to focus on those variances between different branches. Furthermore, participants come mainly from the IT side of the organization. This represents a limitation since one of the profound effects of the Nexus of Forces is the shifting of IT responsibilities to other functional areas, such as marketing.

Another limitation is that we only conducted two rounds within our Delphi approach. Due to the lengthy and comprehensive interviews and focus group discussion, as well as detailed written feedback from the participants in the second round, a consensus was reached rather quickly and further rounds became non-essential. The mix of interview types (single interviews, focus group, and written feedback) is uncommon for Delphi studies. We have chosen to incorporate a focus group in order to use its advantages to gain inspiration for further, more detailed, more profound statements from the participants. Due to time restrictions of the members of our expert panel, we were unable to conduct focus groups with all members. However, the focus group provided evidence that was discussed with the remainder of the expert panel in personal or written interviews.

6. Conclusions and Outlook

Our investigation provides initial insight into the challenges and influences that the interacting forces of big data, social, mobile, and cloud computing provide to organizations and governance structures. The starting point for this study was a conceptual model that we derive from a literature and status quo analysis. Following a research design based on the Delphi method, 18 top management experts of IS (governance) field are interviewed in two rounds. To address the identified research gap, a reference model for IS governance and the Nexus of Forces is proposed based on evidence from these interviews. From the reference model, we conclude that the role of corporate governance concerning IS decisions is increasing due to the Nexus of Forces and the underlying consumerization pressure. In this context, IS governance focuses on technical aspects of IS and provides consulting input into decisions made on the top management level within an organization. This shift of responsibility and accountability is accompanied by the introduction of two interacting governance frames for technical and information governance.

As we assume that the Nexus of Forces demands hybrid governance approaches and federal archetypes, future research and discussions are required to examine changes within the governance archetypes as defined by Weill and Ross (2004a). In this context, Gartner (2013) recently introduced the term "democracy of IS“. Future research must investigate whether existing governance approaches can be extended or modified in order to meet the challenges at all. Moreover, the question arises as to whether methods and processes to achieve the five goals of IS governance are impacted by the Nexus of Forces. Digital trends such as big data, social, mobile, and cloud computing are already impacting organizations and are gaining increasing attention from practitioners and outlets of popular science. To increase the relevance of IS research and to not fall behind popular science, it is necessary to investigate practically relevant topics, such as the Nexus of Forces.

References

Ackermann, T., Widjaja, T., Benlian, A., & Buxmann, P. (2012). Perceived IT Security Risks of Cloud Computing: Conceptualization and Scale Development. Paper presented at the 33rd International Conference on Information Systems, Orlando, FL.

Andriole, S. J. (2012). Seven Indisputable Technology Trends That Will Define 2015. Communications of the Association for Information Systems, 30(1), 61-72.

Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). Digital Business Strategy: Toward a Next Generation of Insights. MIS Quarterly, 37(2), 471-482.

Bostrom, R. P., & Heinen, J. S. (1977). MIS Problems and failures: a sociotechnical perspective part I: the cause. MIS Quarterly, 1(3), 17-32.

Brown, A. E., & Grant, G. G. (2005). Framing the Frameworks: A Review of IT Governance Research. Communications of the Association for Information Systems, 15(1), 696-712.

Buhl, H. U., Röglinger, M., Moser, F., & Heidemann, J. (2013). Big Data - A Fashionable Topic with(out) Sustainable Relevance for Research and Practice? Business & Information Systems Engineering, 5(2), 65-69.

Burtscher, C., Manwani, S., & Remenyi, D. (2009). Towards a conceptual map of IT governance: a Review of current academic and practitioner thinking. Paper presented at the UK Academy for Information Systems Conference 2009, Oxford, UK.

Chen, H., Chaing, R. H. L., & Storey V. C. (2013). Business Intelligence and Analytics: From Big Data to Big Impact. MIS Quarterly, 36(4), 1165-1188.

Costello, T., & Prohaska, B. (2013). 2013 Trends and Strategies. IT Professional, 15(1), 62-64.

Dahlberg, T., & Kivijarvi, H. (2006). An Integrated Framework for IT Governance and the Development and Validation of an Assessment Instrument. Paper presented at the 39th Annual Hawaii International Conference on System Sciences, Kauai, HI.

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Quarterly, 13(3), 319-340.

De Haes, S., & Van Grembergen, W. (2004). IT Governance and Its Mechanisms. Information Systems Control Journal, 1, 27-33.

De Koning, J., & Gelderblom, A. (2006). ICT and Older Workers: No Unwrinkled Relationship. International Journal of Manpower, 27(5), 467-490.

Falconer, P. (2014). Enterprise Architecture: Network Architecure Development Model. Retrieved from: www.handdrawnea.com/Framework/Reference%20Model.html, 30.04.2014.

Fettke, P., & Loos, L. (2007). Reference Modeling for Business Systems Analysis. Hershey, PA: Idea Group Publishing.

Fortis, T. F., Munteanu, V. I., & Negru, V. (2012). Steps towards Cloud Governance. A Survey. Paper Presented at the 34th International Conference on Information Technology Interfaces, Cavtat/Dubrovnik, Croatia.

Gartner (Plummer, D. C. & Sribar, V. T.). (2013). "Examining the Depth of the Nexus of Forces," Gartner Report ID: G00239390.

Glaser, B. G., & Strauss, A. L. (1967). The Discovery of Grounded Theory: Strategies for Qualitative Research. Chicago, IL: Aldine Publishing Company.

Goes, P. (2013). Editor's Comments. MIS Quarterly, 37(1), iii-vii.

Grahlmann, K. R., Helms, R. W., Hilhorst, C., Brinkkemper, S., & van Amerongen, S. (2012). Reviewing Enterprise Content Management: a functional framework. European Journal of Information Systems, 21(3), 268-286.

Gray, P., & Hovav, A. (2008). From Hindsight to Foresight: Applying Futures Research Techniques in Information Systems. Communications of the Association for Information Systems, 22(1), 12.

Guo, Z., Meina, S., & Junde, S. (2010). A Governance Model for Cloud Computing. Paper presented at the 4th International Conference on Management and Service Science, Wuhan, China.

Hallowell, M. R., & Gambatese, J. A. (2009). Qualitative research: Application of the Delphi method to CEM research. Journal of construction engineering and management, 136(1), 99-107.

Heier, H., Borgman, H. P., & Bahli, B. (2012). Cloudrise: Opportunities and Challenges for IT Governance at the Dawn of Cloud Computing. Paper presented at the 45th Hawaii International Conference on System Science, Maui, HI.

Jansen, W. A. (2011). Cloud Hooks: Security and Privacy Issues in Cloud Computing. Paper presented at the 44th Hawaii International Conference on System Sciences, Kauai, HI.

Johnson, N., & Joshi, K. D. (2012). The Pathway to Enterprise Mobile Readiness: Analysis of Perceptions, Pressures, Preparedness, and Progression. Paper presented at the 18th Americas Conference on Information Systems, Seattle, WA.

Kaisler, S., Armour, F., Espinosa, J. A., & Money, W. (2013). Big Data: Issues and Challenges Moving Forward. Paper presented at the 46th Hawaii International Conference on System Sciences, Wailea, HI.

Kendall, J. W. (1977). Variations of Delphi. Technological Forecasting and Social Change, 11(1), 75-85.

Krueger, R. A., & Casey, M. A. (2009). Focus Groups: A Practical Guide for Applied Research. London: SAGE Publications.

Kshetri, N. (2013). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. Telecommunications Policy, 34(4/5), 372-386.

Lebek, B., Degirmenci, K., & Breitner, M. H. (2013). Investigating the Influence of Security, Privacy, and Legal Concerns on Employees' Intention to Use BYOD Mobile Devices. Paper presented at 19th Americas Conference on Information Systems, Chicago, IL.

Leidner, D. E., Lo, J., & Gonzalez, E. (2010). An Empirical Investigation of IS Strategy and IS Contribution to Firm Performance. Paper presented at the 2010 International Conference on Information Systems, St. Louis, MO.

Leidner, D. E., Lo, J., & Preston, D. S. (2011). An Empirical Investigation of the Relationship of IS Strategy with Firm Performance. The Journal of Strategic Information Systems, 20(4), 419-437.

Levy, Y., & Ellis, T. J. (2006). A systems approach to conduct an effective literature review in support of information systems research. Informing Science, 9, 181-212.

Linstone, H. A., & Turoff, M. (1975). The Delphi Method: Techniques and Applications. Boston, MA: Addison Wesley Publishing.

Looso, S., & Goeken, M. (2010). Application of Best-Practice Reference Models of IT Governance. Paper presented at the European Conference on Information Systems, Pretoria, South Africa.

Malik, P. (2013). Governing Big Data: Principles and practices. IBM Journal of Research and Development, 57(3/4), 11 - 113.

Moreno, C., Tizon N., & Preda, M. (2012). Mobile Cloud Convergence in GaaS: A Business Model Proposition. Paper presented at the 45th Hawaii International Conference on System Sciences, Maui, HI.

Niehaves, B., Köffer, S., & Ortbach, K. (2012). IT Consumerization – A Theory and Practice Review. Paper presented at the 18th Americas Conference on Information Systems, Seattle, WA.

Olbrich, S., Poeppelbuss, J., & Niehaves, B. (2011). BI Systems Managers' Perception of Critical Contextual Success Factors: A Delphi Study. Paper presented at the 2011 International Conference on Information Systems, Shanghai, China.

Pate, N. V. (2002). Emergent Forms of IT Governance to Support Global E-Business Models. The Journal of Information Technology Theory and Application, 4(2), 33-48.

Peterson, R. R. (2004). Integration Strategies and Tactics for Information Technology Governance. In W. Van Grembergen (Eds.), Strategies for Information Technology Governance (pp. 37-80). Hershey, PA: Idea Group Publishing.

Punch, K. F. (2005). Introduction to Social Research. London: SAGE Publications.

Richter, A., & Riemer, K. (2013). The Contextual Nature of Enterprise Social Networking: A Multi Case Study Comparison. Paper presented at the 21st European Conference on Information Systems, Utrecht, Netherlands.

Ropohl, G. (1999). Philosophy of Socio-Technical Systems. Society for Philosophy and Technology, 4(3), 55-71.

Rowe, G., & Wright, G. (1999). The Delphi Technique as a Forecasting Tool: Issues and Analysis. International Journal of Forecasting, 15(4), 353-375.

Sambamurthy, V., & Zmud, R. W. (1999). Arrangements for Information Technology Governance: A Theory of Multiple Contingencies. MIS Quarterly, 23(2), 261-290.

Scheepers, H., & Scheepers, R. (2004). The Implementation of Mobile Technology in Organizations: Expanding Individual Use Contexts. Paper presented at the 25th International Conference on Information Systems, Charlottesville, VA.

Strauss, A., & Corbin, J. (1998). Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory, 2nd edition. London: SAGE Publications.

Tallon, P. T. (2013). Corporate Governance of Big Data: Perspectives on Value, Risk, and Cost. Computer, 46(6), 32-38.

Thorsrud, E., Trist, E. L., & Emery, F. E. (1964). Industrielt demokrati. Oslo: Oslo University Press.

Tu, Z., & Yuan, Y. (2012). Understanding User's Behaviors in Coping with Security Threat of Mobile Devices Loss and Theft. Paper presented at the 45th Hawaii International Conference on System Sciences, Maui, HI.

Van Grembergen, W., De Haes, S., & Guldentops, E. (2004). Structures, Processes and Relational Mechanisms for IT Governance. In W. Van Grembergen (Eds.), Strategies for Information Technology Governance (pp. 1-36). Hershey, PA: Idea Group Publishing.

Van Osch, W., & Coursaris, C. K. (2013). Organizational Social Media: A Comprehensive Framework and Research Agenda. Paper presented at the 46th Hawaii International Conference on System Sciences, Wailea, HI.

Vom Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R., & Cleven, A. (2009). Reconstructing the Giant: On the Importance of Rigor in Documenting the Literature Search Process. Paper presented at the 17th European Conference on Information System, Verona, Italy.

Webb, P., Pollard, C., & Ridley, G. (2006). Attempting to Define IT Governance: Wisdom or Folly? Paper presented at the 39th Annual Hawaii International Conference on System Sciences, Kauai, HI.

Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. MIS Quarterly, 26(2), xiii-xxiii.

Weill, P., & Ross, & J. W. (2004a). IT Governance on One Page (CISR WP No. 349 and Sloan WP No. 4516-04). Cambridge, MA: Massachusetts Institute of Technology.

Weill, P., & Ross, J. W. (2004b). IT governance: How top performers manage IT decision rights for superior performance. Boston, MA: Harvard Business School Publishing.

Weill, P. (2004). Don't just lead, govern: How best performing organizations govern IT. MIS Quarterly Executive, 3(1), 1-17.

Yang, S., & Albers, A. (2013). Overcoming Information Overload in Online Reputation Management: A Systematic Literature Review. Paper presented at the 21st European Conference on Information Systems, Utrecht, Netherlands.

Zaplata, S., Kunze, C. P. & Lamersdorf, W. (2009). Context-based Cooperation in Mobile Business Environments – Managing the Distributed Execution of Mobile Processes. Business & Information Systems Engineering, 1(4), 301-314.

Appendix 8 (A8)

Transformational Leadership and Employees' Information Security Performance: The Mediating Role of Motivation and Climate

Benedikt Lebek, Nadine Guhr, Michael H. Breitner

In: Proceedings of the International Conference on Information Systems (ICIS), 2014, Auckland, New Zealand, Paper 21, pp. 1 – 22.

Link: http://aisel.aisnet.org/icis2014/proceedings/ISSecurity/21/

Abstract

The importance of organizational information security is constantly increasing. Next to technical information security measures, research has incorporated multidisciplinary behavioral theories in order to explain employees' information security awareness and behavior. While focusing on employees as the weakest link in the information security chain, the role of leadership has been considered less. To address this gap, the purpose of this study is to investigate how transformational leadership can influence employees' information security performance. A research model is developed that is empirically tested by means of structural equation modeling (SEM) with data collected from, 208 employees across different industries. Our results indicate a significant influence of transformational leadership on employees' information security participation. Moreover, our study reveals that transformational leaders are able to form a positive organizational climate towards information security and thereby (indirectly) enhance employees' motivation. Drawing from our findings, implications for practitioners and future IS research are derived.