Employees' Information Security Awareness and Behavior: A Literature Review

Benedikt Lebek, Jörg Uffen, Michael H. Breitner
Leibniz Universität Hannover
{lebek, uffen, breitner}@iwi.uni-hannover.de

Markus Neumann, Bernd Hohler
bhn Dienstleistungs GmbH Co.& KG
{neumann.markus, hohler.bernd}@bhn-services.com

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.

1. Introduction

Information system (IS) security is an important challenge in today's organizations. More and more organizations are highly dependent on information processing. Consequently, organizations implement technical measures to mitigate threats to information security [5]. However, technical measures are insufficient as long as employees are not aware of potential security risks [8] [26]. To achieve IS security, the literature proposes information security policies [7] [22] and Security Education, Training and Awareness (SETA) programs [1] [11] as non-technical measures for preventing security breaches by employees. Since literature refers to employees as the weakest link in IS security [26] [29] employees' information security awareness and behavior has garnered increasing academic attention over the past decade. In this interdisciplinary research domain, theories from social psychology and criminology were adopted to IS literature [21] in order to explain and predict employees' security-related behavior and awareness.

A literature review was conducted to comprehensively identifying applied theories in the research field of employees' information security awareness and behavior within the past decade. Prior literature analysis was conducted by [29] in 2000. The authors analyzed different approaches for minimizing user-related faults in information security. Although the underlying theories were identified, the focus of the study was approach-related. An up-to-date overview of applied theories is necessary to guide further research, since the previous study was published twelve years ago. Another literature analysis by [A2] in 2011 is focused on factors that influence security behavior (i. e. policies, communication practices, peer influences etc.) than on theories. In addition to the literature reviews mentioned above, several target-oriented literature reviews were conducted. 'Target-oriented' means that the literature review was conducted to provide the theoretical basis for further research within the same article (e. g. model construction) and is not the essential part of the article. For instance, [21] gave a short overview of behavioral theories in IS security literature in order to introduce the theory of anomie to the research field. Another article [5] surveyed behavioral theories to present an information security policy (ISP) behavioral compliance framework.

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

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

A systematic literature review was conducted. Relevant literature from 2000 until today was sought in academic databases and analyzed focused on both,

1530-1605/12 $26.00 © 2012 IEEE
DOI 10.1109/HICSS.2013.192

applied theory and research methodology. In total, 113 publications were identified and analyzed.

A meta-model that explains employees' information security behavior is introduced by assembling the core constructs of four primary applied theories. By synthesizing results of empirically tested research models based on adopted theories, a discussion of factors, that were proven to have a significant influence on employees' security behavior or intentions, is presented. Additional factors used in the research domain are identified as well. Gaps in existing research are uncovered by discussing the results of the literature analysis and recommendations for future studies are given. Those refer to research methodologies as well as to the subject of investigation.

This paper is structured as follows: the next section describes the underlying research methodology. The literature search process as well as the literature analysis process is demonstrated in detail, before the identified theories are briefly introduced and a meta-model is presented. On this basis, an analysis of factors that influence employees' security behavior is conducted in section four. Afterwards, section five provides a discussion of the results, implications for further research as well as the limitations of this paper. Within the last section a short summary of the paper and an outlook for future research is presented.

2. Research Design

With a comprehensive review of literature in the research field of employees' information security awareness and behavior the aim of this paper is to synthesize existing knowledge. The underlying research design consists of two phases: First, as the quality of a literature review depends strongly on the search process [34], relevant literature is identified by conducting a rigorous literature search. Second, the identified literature is analyzed for the purpose of appointing applied theories and methodologies in the contemplated research field.

2.1 Identifying Relevant Literature

In order to present a wide-spread overview of applied theories in the variety of literature, a systematic search process was conducted. We chose the structured approach presented by [37] as the underlying methodology. Guidelines from [34] indicate that, a rigorous literature search must be valid and reliable. Generally the term 'validity' refers to the degree in which a method serves the purpose it is used for [20] [40]. Regarding a literature search, "validity characterizes the degree to which the literature search accurately uncovers the sources that the reviewer is attempting to collect" [34]. In our case, validity is based on the selected databases, publications, covered period, used keywords and the application of a forward and backward search. The term 'reliability' aims for the replicability of the literature search process. Therefore a comprehensive documentation of the search process is needed [34].

To fulfill the requirement of validity, we searched through ten databases: AISeL, ScienceDirect, IEEEXplore, JSTOR, SpringerLink, ACM, Wiley, Emerald, InformsOnline, Palgrave Macmillan. A list of search terms was pre-defined to conduct a literature search including 'security awareness', 'awareness training', 'awareness program', 'awareness campaign', 'security education', 'security motivation', 'security behavior' and 'personnel security'. The databases were searched to determine whether a publication contained at least one of the search terms in the title, abstract or keywords. If the field of search (i. e. title, abstract or keywords) could not be specified in the search query, a full text search was conducted. In total, 3,423 potentially relevant publications were identified.

To select the most relevant publications in the research field of employees' information security awareness and behavior, inclusion and exclusion criteria were defined. We chose to focus not only on high-quality literature as recommended in [34] and [37]. Also conferences and journals of minor relevance were included. This is necessary because there are journals which are specialized in the field of IS security (e. g. 'computers & security' [21], 'Information Management & Computer Security') and therefore contain numerous articles dealing with topics relevant for this literature review, but are not highly rated in international conference or journal rankings (e. g. AIS, [35], [38],). However, non-academic articles (e. g. whitepapers) were excluded. Given that the aim of this literature review is to present an up-to-date overview of theories used in the mentioned research field, publications published before the year 2000 were not considered. Furthermore only articles written in English were taken into account.

Publications that do not primary deal with the topic of employees' information security awareness and behavior were also filtered out. This was done by manually screening articles based on title, abstract and if necessary with a glance through the full text. Following this process a number of 95 articles were determined to be relevant. Subsequently a backward as well as a forward search was carried out [37]. The

backward search was performed manually, whereas the forward search was conducted by using Web of Science (www.webofscience.com). As a result eighteen additional relevant articles were identified. Hence a total of 113 articles were identified to be relevant for this literature review. A complete list of all reviewed literature can be found in the appendix which can be requested via e-mail from the authors. References to reviewed literature are labeled by an 'A' for the remainder of this article.

2.2 Analyzing Identified Literature

In order to limit mistakes and subjective biases, a two-step analysis process was chosen and performed by two researchers. In the first step, each researcher independently determined the applied theory and research methodology for each paper. Secondly, results were categorized to theory and methodology and compared to the results of the other researcher. Divergences were discussed until conformity was reached. As the aim of this article is to present a comprehensive overview of theories recently applied in research field of employees' information security awareness and behavior, the list of theories was developed inductively while reviewing the articles.

Following the broad definition of the term 'theory' used in recent IS literature (e. g. [15]), a total of 54 theories that are applied in the contemplated research field were identified. The majority of the identified theories were used in two or fewer publications. Considering the frequency of use, seven primary theories were identified as stated in Table 1.

Table 1: Most frequently used theories

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

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

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

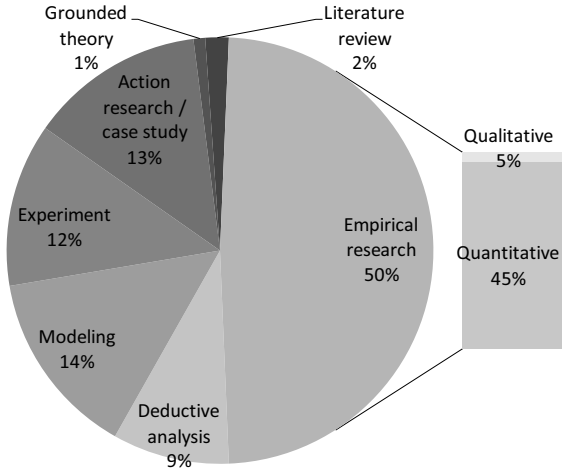


Figure 1: Frequency of applied research methodologies

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

3. Behavioral Science in Information Security Research

In the past decade of employees' information security awareness and behavior research, the predominant focus has been on cognitive behavioral models, as can be inferred from Table 1. Researchers have incorporated multidisciplinary theories, including theories from psychology, sociology, and criminology, into information security success outcome models. The most frequently used theories in the research field are the TRA/TPB, GDT, PMT and TAM. A meta-model composed from those theories is presented in Figure 2.

Theory of Reasoned Action (TRA)/Theory of Planned Behavior (TPB): The TPB, an extension of the TRA, implies that intentions are proximal cognitive antecedents of actions or behavior [13].

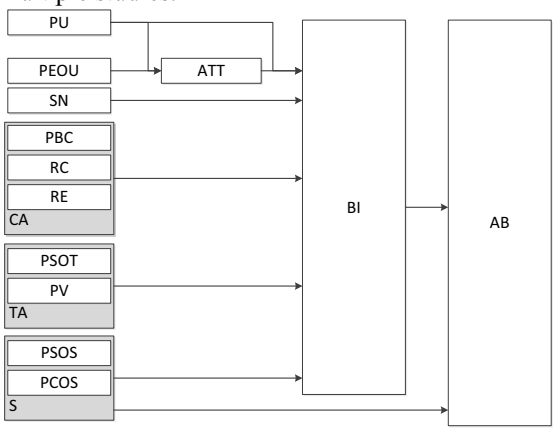
Behavioral intentions (BI) index the motivation to perform a specific action and are determined by three constructs: attitude towards behavior (ATT), subjective norm (SN) and perceived behavioral control (PBC) [2]. In the context of information security behavioral compliance, the employee's intention to perform an information security policy (ISP)-related action is dependent on his/her overall evaluation of and normative beliefs towards compliance-related behavior and the greater the feeling of reflected actual control over those actions, the greater the intention [5] [7]. The PBC construct, also referred to Bandura's (1982) concept of self-efficacy, extends TPB from TRA to account requisite resources necessary for performing a behavior [1].

General Deterrence Theory (GDT): Adapted from criminal justice research, GDT is based on rational decision making. GDT states that perceived severity (PSOS), certainty (PCOS) of sanctions or punishment influence the decision to engage in a crime by balancing the cost and benefits [27]. More specific, studies in information security research have focused on security countermeasures and other preventative strategies that impact the employees' intention to misuse IS [7] [12].

Protection Motivation Theory (PMT): Originated in health psychology, the theory explains the coping process with potential threats by predicting a variety of protective behaviors [24]. Researchers argue that an employee's attitude towards information security is shaped by the evaluation of two cognitive mediated appraisals: threat appraisal (TA) and coping appraisal (CA) [7]. The first consists of two items, perceived severity (PSOT), perceived vulnerability (PV) and comprises the threat perception. The latter is determined by response costs (RC), PBC and response efficacy (RE), which represent an individual's ability to cope with potential threat. An employee who is aware of potential security risks forms attitudes about perceptions of these threats to security and the coping response [4] [14].

Technology Acceptance Model (TAM): The TAM, originally introduced by Davis [10], has been shown as a parsimonious model of representing antecedents of technology acceptance via perceived usefulness (PU) and perceived ease-of-use (PEOU). PU is defined as the employees' subjective probability that using a specific system will increase his/her job performance. PEOU, in contrast, denotes the degree to which an employee expects the target system to be free of effort [28]. In the security awareness context, TAM determines the employees' intention to comply with information security policy (ISP), which is influenced by both, PEOU and PU, afforded through the use of e.g. ISPs [3].

In most cases of theories application, intentions rather than actual behavior is assessed due to the difficulties in observing security behavior [33]. However, each theory specifies theoretical behavioral factors that have been tested and evaluated in multiple studies.



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

Figure 2: Meta-model of primary used theories

One limitation applying these theories is, in most cases, the single level perspective. A single theory focuses on individual behavioral factors, despite evidence from various empirical studies that external-level factors such as organizational or work-related factors are also influential [17]. By disregarding these factors and interdependencies, theories that explain and predict employees' behavior may run the risk of being inefficient. As a result, some researchers added theoretical extensions of additional factors influencing the individual behavior to bridge the gap between individual and external factors and behavioral outcome (e. g. ISP fairness [A15], situational support [A51], visibility [A75]).

4. Results

In general, the contextual analysis showed that numerous authors discussed a variety of factors that are considered to affect employees' information security awareness and behavior. However, when having consolidated the publications, the descriptive analysis showed partly divergent results. Therefore, a qualitative content analysis is worthwhile to determine the relations between the specific constructs within the behavioral theories. These relations will be shortly synthesized in the following.

A detailed compilation of constructs, their relationships and the statistical power can be found in Table 2.

To start with TPB/TRA seven studies applied the complete theory with every core construct. Research has used BI as a predictor of actual behavior (AB) towards compliance with ISP rather than its actual outcome. Due to certain difficulties with observing actual security compliant behavior [33], numerous authors emphasize the use of BI as the dependent variable that indicates AB (e. g. [A46] [A76] [A113]). Assessing BI rather than AB is grounded theoretically and technically. Several authors have demonstrated a strong and consistent relationship between the two constructs [28] [36] in non-information security contexts.

Table 2: Construct relationships

Construct				Author	significance	β	N	Source
Independent Variable	Items	Dependent Variable	Items					
TPB/TRA								
ATT	4	BI	3	A14	**	0.25	464	Empl.
	4		3	A15	***	0.27	464	Empl.
	-		-	A13	**	0.48	464	Empl.
	3		3	A26	*	0.316	332	Stud./ IS Pro.
	3		3	A26	-	0.298	227	Stud./ IS Pro.
	3		3	A41	-	0.073	312	Empl.
	3		3	A43	**	0.29	332	Stud./ IS Pro.
	4		5	A46	***	0.48	124	IS Pro.
	4		2	A66	-	0.079	60	Stud.
	3		4	A76	***	0.537	240	Empl.
	5		4	A113	*	0.18	176	Empl.
BI	2	AB	2	A66	**	0.386	60	Stud.
	3		3	A75	*	0.04	917	Empl.
	4		3	A76	***	0.869	240	Empl.
	3		3	A93	***	0.98	917	Empl.
	3		3	A94	*	0.04	917	Empl.
PBC	3	BI	3	A14	**	0.22	464	Empl.
	2		3	A26	**	0.193	332	Stud./ IS Pro.
	2		3	A26	*	0.197	227	Stud./ IS Pro.
	3		3	A41	*	0.172	464	Empl.
	2		3	A43	**	0.16	332	Stud./ IS Pro.
	7		5	A46	**	0.17	124	IS Pro.
	3		3	A52	**	0.187	215	N.A.
	6		2	A66	**	0.300	60	Stud.
	3		3	A75	*	-	464	Empl.
	3		3	A93	***	0.31	917	Empl.
	3		3	A94	*	0.17	917	Empl.
	8		5	A51	*	0.376	202	Empl.
	4		4	A113	***	0.43	176	Empl.
SN	3	BI	3	A14	**	0.29	464	Empl.
	2		3	A26	-	-	332	Stud./ IS Pro.
	2		3	A26	**	0.324	227	Stud./ IS Pro.
	5		3	A40	***	0.395	312	Empl.
	5		3	A41	***	0.313	464	Empl.
	2		2	A42	**	-0.48	726	Empl.
	3		3	A43	-	-	332	Stud./ IS Pro.
	4		5	A46	**	0.19	124	IS Pro.
	2		3	A52	***	0.298	215	N.A.
	5		2	A66	**	0.210	60	Stud.
	4		3	A75	*	-	917	Empl.
	3		-	A89	-	0.07	1449	Empl.
	4		4	A76	***	0.235	240	Empl.
	4		3	A94	*	0.45	917	Empl.
	4		4	A113	-	0.02	176	Empl.

Empl.: Employees, Stud.: Students, IS Pro.: IS Professionals
*p<0.05, **p<0.01, ***p<0.001

Table 2: Construct relationships (continued)

Construct				Author	significance	β	N	Source
Independent Variable	Items	Dependent Variable	Items					
TAM								
ATT	3	BI	3	A43	**	0.29	332	Stud./ IS Pro.
	3		3	A26	**	0.316	332	Stud./ IS Pro.
	3		3	A26	**	0.298	227	Stud./ IS Pro.
	4		3	A112	*	0.20	118	Empl.
PEOU	3	ATT	3	A43	-	-	332	Stud.
	4		4	A112	**	0.26	118	Empl.
	3		3	A26	-	-	332	Stud./ IS Pro.
	3		3	A26	***		227	Stud./ IS Pro.
PU	2	ATT	3	A26	**	0.5	332	Stud./ IS Pro.
	2		3	A26	**	0.298	227	Stud./ IS Pro.
	3		3	A43	**	0.52	332	Stud./ IS Pro.
	4		4	A112	**	0.50	118	Empl.
	3	BI	3	A43	-	-	332	Stud./ IS Pro.
	4		3	A112	-	0.11	118	Empl.
GDT								
PCOS	2	BI	2	A23	-	-	269	Empl.
	2		3	A40	***	0.260	312	Empl.
	2		3	A41	**	0.155	312	Empl.
	2		2	A42	**	-0.20	726	Empl.
	4		3	A112	-	0.03	118	Empl.
PSOS	2	BI	2	A23	**	-	269	Empl.
	3		3	A40	**	-0.209	312	Empl.
	3		3	A41	**	-0.139	312	Empl.
	2		2	A42	**	-0.14	726	Empl.
S	4	AB	3	A93	***	0.09	917	Empl.
	4		3	A75	*	-	917	Empl.
	6		3	A94	***	0.09	917	Empl.
	2	BI	-	A89	-	0.04	1449	Empl.
	4		4	A76	-	-	240	Empl.
PMT								
PBC	7	BI	5	A46	**	0.17	124	IS Pro.
	3		3	A41	*	0.172	312	Empl.
	6		3	A75	*	-	917	Empl.
	6		3	A93	***	0.31	917	Empl.
	3		3	A94	*	0.17	917	Empl.
CA	3	AB	3	A76	-	-	240	Empl.
RC	5	BI	5	A46	-	-0.12	124	IS Pro.
RE	6	BI	5	A46	**	0.27	124	IS Pro.
	3		3	A52	*	0.213	215	N.A.
	6		3	A75	-	-	917	Empl.
	6		3	A93	*	0.06	917	Empl.
	3		3	A94	-	-0.02	917	Empl.
PSOT	7	BI	5	A46	*	-0.20	124	IS Pro.
PV	7	BI	5	A46	**	0.20	124	IS Pro.
TA	6	BI	3	A75	*	-	917	Empl.
	6		3	A93	***	0.24	917	Empl.
	6		3	A94	*	0.12	917	Empl.
	5	AB	3	A76	***	0.278	240	Empl.

Empl.: Employees, Stud.: Students, IS Pro.: IS Professionals
*p<0.05, **p<0.01, ***p<0.001

Moreover, technically measurement is argued to be difficult due to the sensible context of information security (e.g. [4] [33]), the large and diverse sample sizes [7] [8], and the theoretical background of the applied theory [31]. In a theoretical context, authors e.g. [4] [31] argue that the relationship between BI and AB is grounded in the TPB and TRA by [1] and has been shown to be proven empirically by [4]. A number of studies emphasized the relationship between AB and BI (for example [A66] [A94] [A93]). Contrary to the work of for example [28] or [39], who measured actual behavior via system log files, the studies rely on self-reported data (e.g. [30]).

Further results implicate that the main constructs of TPB are strong predictors of BI. More specifically, 92% of the evaluated relationships between PBC and BI are significant, with at least $p < 0.05$. In general, the determination of the PBC construct is twofold, which allows a detailed examination of internal and external factors. The main influence on the PBC construct comes from Bandura's work on self-efficacy. Self-efficacy is used ten times and reflects the individual's personal beliefs about his or her ability to comply with the information security policy (for example [A14] [A26] [A41] [A46] [A51] [A52] [A75] [A93] [A94] [A106]). In contrast, controllability represents an individual's perception about available resources and opportunities to actually comply with information security policy [A6] [A43]. Some authors used a combination of both constructs to conceptualize PBC [A43] [A113]. The social construct of TPB in the context of security awareness refers to the influence and motivation of an individual's observation about the norm in his or her environment [A46]. The partial influence of SN on BI was shown in six of eight studies. To explore the social influence in the context of security awareness, researchers used different labeled constructs including normative beliefs [A14] [A75] [A76] [A94] or social factors [A66], which represent the SN construct [4]. The third construct that influences BI is ATT. Eight out of ten relationships between ATT and BI are significant, with six strong relationships at $p < 0.01$ level. Attitude is a broad term that has been investigated from different perspectives [A26]. In the context of TPB, ATT reflects the user's positive or negative feelings with regard to complying with the information security policy [A46] [A76] [A113] [A43]. More specifically, in two cases ATT was not significant with BI. Herath et al. [A41] stated that the insignificant effect may be due to context, sample, or other extraneous reasons. The authors combined the PMT and Deterrence Theory based on the core constructs of TPB and used a sample of 312 employees from 78 organizations.

In general, seven studies aggregated the core constructs of TPB as a whole [A14] [A26] [A43] [A41] [A46] [A94] [A113] . Numerous studies combined other theories with the core constructs of TPB [A14] [A40] [A41] [A43]. Based on TRA, TAM predicts the attitude towards the acceptance of objects as factors of adoption and use. Therefore, some authors empirically studied PEOU and PU as predictors of ATT and emphasized the relationship between ATT and BI [A26] [A43] [A112]. Other authors eliminated the attitude construct and emphasized a direct relationship between PEOU and PU [A43] [A112]. These studies imply that both TAM constructs are less related to ATT. It is argued that even if a user may not prefer a specific object, he or she might still use it as long as it increases job performance [A26]. Interestingly, no study suggested a significant relationship between PU and BI [A43] [A112] but together with [A26], the authors showed a positive significant relationship between both constructs.

In the context of security awareness, a widely advocated theory is the GDT [5] [A89]. Especially the core constructs of GDT, PSOS and PCOS were related to BI [A23] [A40] [A41] [A42] [A112]. In the security awareness context and due to the theoretical base of GDT, the theory focuses on a different perspective of the intention construct. BI is measured as a user's perception as to whether a violation of specific portions of information security policy may increase his or her general utility. Some studies incorporated additional constructs to the core constructs of GDT [A75] [A76] [A89] [A93]. For example, the general construct of sanctions (S), according to Siponen et al., is divided into formal sanctions, informal sanctions, and shame [A89]. However, of the six studies that investigated PCOS as a predictor of the BI, three were significant at a minimum $p < 0.01$. PSOS has been shown to be significant in four cases [A23] [A40] [A41] [A42].

The PMT literature is characterized by the application of a plethora of different constructs [A41]. The core constructs were shown to be related to BI. The TA construct was shown to be a predictor of the BI by four research studies [A46] [A75] [A93] [A94] . While [A46] investigated a significant relationship by separation of perceived severity (PSOT) and perceived vulnerability (PV) as TA constructs [A75], [A93], and [A94] considered the whole construct. Response efficacy (RE) and self-efficacy refer to coping appraisal (CA) [A75]. In contrast to TPB, both constructs are viewed from a different perspective as constructs of CA mechanisms [5]. The relationship between RE and BI was shown to be significant in three cases [A46] [A52] [A93].

In order to extend and improve the standard behavioral theories, several further constructs were introduced by academic literature in order to explain employees' IS security related behavior. A detailed list is given in Table A 1 in the Appendix.

With the purpose of explaining employees' BI, fifteen factors beyond the standard theories (i. e. TRA/TPB, TAM, GDT, PMT) were examined. Twelve of them were found to have a significant effect on BI. For example the strength of an employee's identification with and involvement in an organization (organizational commitment) has a highly significant effect on BI [A41]. Herath et al.

[A40] discovered that an employee's perceived effectiveness of behaving securely influences BI. Moreover, the employee's awareness of the ISP [A51] as well as his or her technology awareness [A43] determines the security-related BI. Johnston et al. [A51] show, that employees' awareness of ISP depends on the degree an employee perceives his environment to be favorable for fulfilling a given task (situational support), the degree to which a company provides instructions to fulfill a task (verbal persuasion), and an employee's indirect experience with a task through observation (vicarious experience). With the introduction of the neutralization theory, [A89] showed that the use of neutralization techniques reduces the perceived harm of violating the ISP and therefore influences an employee's BI. According to [A113], an employee's perceived security protection mechanisms do not significantly impact an employee's BI. Consistent to the TAM, where PEOU is only directly linked to ATT, in [A43] no significant direct relationship was found between PEOU and BI.

Eight further constructs were used in literature to explain ATT. General information security awareness (ISA) was found in [A13] [A14] [A15] to have a significant influence on ATT at the minimum $p < 0.01$ level. The perceived fairness of a company's ISP is significant at the $p < 0.001$ level [A15]. Whereas the perceived costs of non-compliance with a organization's ISP affect ATT ([A13] [A14]), the impact of perceived benefits of compliance and perceived costs of compliance are ambiguous. Both factors are significant according to [A14], but not significant according to [A13]. Phanila et al. [A76] show that PBC has a strong significant effect not only on BI but also on ATT.

In contrast to sanctions, which were tested to have a significant influence on AB, rewards do not clearly provide that influence. Of three studies only one found a significant relationship at the $p < 0.05$ level [A75], the other two [A76] [A94] found no significant relationship.

5. Discussion of Results and Implications for Future Research

Fifty-four theories applied in employees' information security awareness and behavior research were identified. Most of them are only used in three or fewer publications. In contrast, TRA/TPB, TAM, GDT and PMT emerged as the four dominantly applied theories which were used 61 times within the reviewed literature. Since all four theories explain employees' behavioral intention by using different factors, the development of a meta-model (Figure 2) was applicable. The core construct relationships from each theory were adopted by most publications that apply the respective theory. A solid confirmation of existing construct relationships in the context employees' security behavior is provided by existing literature, so future studies can focus more on additional constructs than on examining already confirmed core construct relationships.

As mentioned in section 2.2, the literature in information security awareness and behavior research is replete with quantitative research studies. Since factors like employees' intentions, attitudes, motivations or satisfaction are not verifiable by means other than self reporting [23], it is not unexpected that the majority of reviewed literature applying TRA/TPB, TAM, GDT or PMT use quantitative methods to test their 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 [23], and results may be biased. According to [39], self reports are not sufficient predictors of employees' actual behavior, because employees' self-reported perceptions of security behavior are not bound to be in line with their actual security behavior. At first sight, observation seems to be an instrument for gathering more objective data. Due to the sensitive nature of security-related data, organizations are unwilling to reveal information that provides insights into a company's current information security status [16]. In addition, it is impossible to observe all aspects of security behavior (e. g. password strength, encrypting sensitive e-mails, etc.) for a large amount of employees, which means that observations alone are insufficient. If researchers succeed in developing a trustful environment [16], a combination of self-report and observational sampling in triangulation as proposed by [39] is an appropriate means of reducing the lack of qualitative and interpretive studies in this research field. As already stated in [8], case studies including employees from one or more companies would be useful for further research. As an alternative to case studies, experimental studies, as used in e. g. [A52], are also a method of observing employees' actual behavior. However, observations under laboratory conditions change the nature of the subject matter [23], 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 [28] and [39] with the analysis of log-files.

With regard to the difficulties in observing useful empirical data [16], low response rates and the survey of students and IS professionals are emphasized. For instance, within the reviewed literature, only five studies included more than 500 respondents [A42] [A75] [A89] [A93] [A94]. An empirical sample is relevant as long as it is representative and generalizable. For the purpose of measuring employees' security awareness and behavior, samples consisting of students and/or IS professionals do not reflect the population of interest. With reference to internal, external and construct validity, surveying students and IS professionals is seen more critically than having a smaller sample size as long as it represents reality [32]. With regard to globally acting organizations, more studies are required that focus the differences in awareness in an international context such as [A26]. Cultural differences which are fundamental for developing SETA-programs can be assessed in future research.

Regarding the relationships between constructs, only five studies examined the relationship between employees' BI and AB (c. f. Table 2). Although a significant relationship was found between the two constructs, all five studies used self reports to assess employees' actual behavior. The problems with self reported data are already mentioned above. Many other studies postulate a strong and consistent relationship between BI and AB by referring to [28]. Since that study also used self reported data and did not deal with security-related behavior, the assignability of the results has to be challenged. The question arises as to whether employees' behavioral intention is a truly reliable predictor for their actual security-related behavior, or if there are any external or environmental factors mitigating the influence of BI on AB. For example, an employee might intend to behave in compliance with the organization's ISP because of his strong self-efficacy and normative beliefs (c. f. TRA/TPB), but is not able to transform his or her intentions into actual behavior. This might be due to, for example, a heavy workload in combination with complex security measures. The BI – AB gap implicates that individuals hold positive BI but subsequently fail to enact those BI. In addition, changes in BI do not consequently lead to changes in AB [13] [36]. Meta-analytic evidence demonstrates that changes in BI lead to AB in a lower degree [36]. Consequently, the relationship between BI and AB requires further attention by future studies, and factors that affect this relationship must be identified. At this point, the need to combine self-reports to determine employees' BI and observational sampling to determine employees' AB is emphasized again.

Although synthesized literature presents a variety of additional factors beyond the core constructs of TRA/TPB, TAM, GDT or PMT (c. f. Table A 1 in the appendix) little work has been done in developing and testing organizational measures to influence employees' security awareness and behavior. Practitioners face the problem of how the theoretical constructs that were found to be determining employees' behavior can be affected. A gap between theoretically founded explanation of employees' security behavior in academic literature and the need of practitioners to know which interventions to apply has grown [39]. According to [25], academic literature should provide relevance for practitioners in order to prevent research from becoming an end unto it-self. To fulfill this requirement it is necessary to develop and validate concrete measures and process models to influence employees' security awareness and behavior based on already existing theoretical knowledge (c. f. Section 4) of individual factors. This will add value to the research field and will mitigate the gap between theory and practice.

6. Limitations

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

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

The initial aim of this paper was to present a comprehensive overview of theories used in the domain of employees' security awareness and behavior research. Due to the complexity of the subject matter and the diversity of identified theories,

we chose to present an in-depth analysis of the four primarily applied theories.

7. Conclusion and Outlook

This paper presents a theory-based literature review of the extant security awareness in behavioral research. In total, 113 publications were identified and analyzed. Fiftyfour theories applied in employees' information security awareness and behavior research were identified. The four primarily applied theories are the TPB, GDT, PMT and TAM. A meta-model that explains employees' IS security behavior is introduced by assembling the core constructs of the four primarily applied theories. By synthesizing results of empirically tested research models based on TPB, GDT, PMT and/or TAM, a survey of factors proven to have a significant influence on employees' security behavior is presented. Factors outside of the core constructs from the four primarily used theories in the research field were identified. Gaps in existing research are uncovered by discussing the results of the literature analysis

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

8. References

[1] S. Abraham, "Information Security Behavior: Factors and Research Directions", *Proceedings of the American Conference on Information Systems (AMCIS)*, Paper 462, 2011.

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

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

[4] C.L. Anderson, and R. Agarwal, "Practicing Safe Computing: A multimethod empirical examination of home computer user behavioral intentions", *MIS Quarterly*, Vol. 34, No. 3, 2010, pp. 613-643, 2010.

[5] A. Aurigemma, R. Panko, "A Composite Framework for Behavioral Compliance with Information Security Policies", *Proceedings of the 45th Hawaii International Conference on System Sciences (HICSS),* pp. 3248-3257, 2012.

[6] N. Boon Yuen and A. Kankanhalli,. "Processing Information Security Messages: An Elaboration Likelihood Perspective", *Proceedings of the European Conference on Information Systems (ECIS)*, Paper 113, 2008.

[7] B. Bulgurcu, H. Cavusoglu, I. Benbasat, „Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness", *MIS Quarterly*, Vol. 34, pp. 523-548, 2010.

[8] B. Bulgurcu, H. Cavusoglu, I. Benbasat, "Roles of Information Security Awareness and Perceived Fairness in Information Security Policy Compliance", *Proceedings of the American Conference on Information Systems (AMCIS)*, Paper 419, 2009

[9] M. Chan, I. Woon A. Kankanhalli, „Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior", *Journal of Information Privacy Security*, Vol. 1, pp. 18-41, 2005.

[10] 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, 1989.

[11] J. D'Arcy, A. Hovav, "Does One Size Fit All? Examining the Differential Effects of IS Security Countermeasures", *Journal of Business Ethics*, Vol. 89, pp. 59-71, 2009.

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

[13] M. Fishbein, I. Ajzen, "Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research", *MA, Addison-Wesley*, 1975.

[14] T. Herath, H.R. Rao, "Protection motivation and deterrence: a framework for security policy compliance in organizations", *European Journal on Information Systems*, Vol. 18, No. 2, pp. 106-125, 2009

[15] M. Karjalainen, M.T. Siponen, "Toward a New Meta-Theory for Designing Information Systems (IS) Security Training Approaches", *Journal of the*

Association for Information Systems (JAIS), Vol. 12, pp. 518-555, 2011.

[16] A.G. Kotulic, and J.G. Clark, "Why there aren't more information security research studies", *Information & Management*, Vol. 41, 2004, pp. 597-607, 2004.

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

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

[19] T.J. Madden, P.S. Scholder, I. Ajzen, "A Comparison of the Theory of Planned Behavior and the Theory of Reasoned Action", *Personality and Social Psychology Bulletin*, Vol. 18, pp. 3-9, 1992.

[20] W.A. Mehrens, I.J. Lehman, "Using standadized tests in education", Longman Group United Kingdom, 1987.

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

[22] S. Pahnila, M.T. Siponen, A. Mahmood, "Employees' Behavior towards IS Security Policy Compliance", *Proceedings of the 40th Hawaii International Conference on System Sciences (HICSS)*, 2007.

[23] P.M. Podsakoff, D. Organ, "Self-reports in organizational research: Problems and prospects", *Journal of Management*, Vol. 12 No. 4, pp. 531–544, 1986.

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

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

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

[27] D.W. Straub, „Effective IS security: An empirical study", *Information Systems Research*, Vol. 1, No. 3, pp. 255-276, 1990.

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

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

[30] M.T. Siponen, S. Phanila, A.M. Mahmood, "A New Model for Understanding Users' IS Security Compliance", *Proceedings of the Pacific Asia Conference on Information systems (PACIS)*, 2006.

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

[32] S. Sivo, S. Saunders, Q. Chang, and J.J. Jiang, "How low should you go? Low response rates and the validity of inference in IS questionnaire research", *Journal of the Association for Information Systems,* Vol. 7, No. 6, pp. 351-414, 2004.

[33] C. Vroom, and R. von Solms, "Towards information security behavioral compliance", *Computer & Security*, Vol. 23, No. 3, pp. 191-198, 2004.

[34] J. vom Brocke, A. Simons, B. Niehaves, K. Riemer, R. Plattfaut, A. Cleven, „Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process", *Proceedings of the European Conference on Information Systems (ECIS)*, 2009.

[35] K.A. Walstrom, B.V. Hardgrave, "*Forums for Information Systems Scholars: III*", *Infromation & Management*, Vol.39, pp. 117-124, 2001.

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

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

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

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

[40] B.R. Worthen, W.R. Borg, K.R. White, Measurement and evaluation in the school, Longman Group United Kingdom, 1993.