Management Research Review

Information security awareness and behavior: a theory-based literature review

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

Article information:

To cite this document:
Benedikt Lebek, Jörg Uffen, Markus Neumann, Bernd Hohler, Michael H. Breitner, (2014) "Information security awareness and behavior: a theory-based literature review", Management Research Review, Vol. 37 Issue: 12, pp.1049-1092, https://doi.org/10.1108/MRR-04-2013-0085
Permanent link to this document:
https://doi.org/10.1108/MRR-04-2013-0085

Information security awareness and behavior: a theory-based literature review

Benedikt Lebek and Jörg Uffen
Institute for Information Systems Research, Leibniz University of Hannover, Hannover, Germany
Markus Neumann and Bernd Hohler
bhn Dienstleistungs GmbH & Co. KG, Hameln, Germany, and
Michael H. Breitner
Institute for Information Systems Research, Leibniz University of Hannover, Hannover, Germany

Abstract

Purpose – This paper aims to provide an overview of theories used in the field of employees' information systems (IS) security behavior over the past decade. Research gaps and implications for future research are worked out by analyzing and synthesizing existing literature.

Design/methodology/approach – This paper presents 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.

Findings – The paper identified 54 used theories, but four behavioral theories were primarily used: Theory of Planned Behavior (TPB), General Deterrence Theory (GDT), Protection Motivation Theory (PMT) and Technology Acceptance Model (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.

Research limitations/implications – 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, this paper has limited this error source to a minimum.

Practical implications – 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.

Originality/value – This paper presents a comprehensive up-to-date overview of existing academic literature in the field of employees' security awareness and behavior research. Based on a developed meta-model, research gaps are identified and implications for future research are worked out.

Keywords TAM, Behavioral theories, Security awareness, Security behavior, TPB, GDT, PMT

Paper type Literature review

1. Introduction

Today's organizations are highly dependent on information systems (IS). Consequently, they implement technical measures to mitigate threats to information security (Aurigemma

Management Research Review
Vol. 37 No. 12, 2014
pp. 1049-1092

2040-8269
DOI 10.1108/MRR-04-2013-0085

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

Therefore, in this paper, we present the results of a comprehensive literature review that was designed to identify applied theories and understand the cognitive determinants in the research field of employees' ISA and behavior within the past decade. A prior literature analysis was conducted by Siponen (2000a, 2000b). The authors analyzed different approaches to minimizing user-related faults in information security. Although the underlying theories were identified, the focus of the study was approach-related. An up-to-date overview of applied theories is necessary to guide further research, as the previous study was published 12 years ago. Another literature analysis by Abraham (2011) focused on factors that influence security behavior (i.e. policies, communication practices, peer influences, etc.) and not on theories. In addition, several target-oriented literature reviews were conducted. "Target oriented" means that the literature review was conducted to provide the theoretical basis for further research within the same article (e.g. model construction) and is not the essential part of the article. For instance, Mishra and Dhillon (2005) gave a short overview of behavioral theories in IS security literature to introduce the theory of anomie to the research field. Another paper by Aurigemma and Panko (2007) surveyed behavioral theories to present an 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:

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

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

2. Research methodology

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

2.1 Literature search process

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

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

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

Publications that do not primarily deal with the topic of employees' ISA and behavior were also filtered out. This was done by manually screening articles based on title, abstract and, if necessary, by skimming through the full text. Following this process, 95 articles were determined to be relevant. Subsequently, a backward and forward search was carried out (Webster and Watson, 2002). The backward search was performed manually, whereas the forward search was conducted by using Web of Science (www.webofscience.com). As a result, 18 additional relevant articles were identified. In total, 144 articles were identified to be relevant for this literature review (they are marked with a "*" in the references). Table I shows the number of publications for each journal or conference that were identified as relevant.

	Count
Journal	
Computers & Security	12
Information Management & Computer Security	10
European Journal of Information Systems	5
MIS Quarterly	5
Journal of the Association for Information Systems	4
Decision Support Systems	2
Information & Management	2
Information Security South Africa	2
Information Security Technical Report	2
Information Systems Journal	2
Journal of Information Privacy and Security	2
Others*	14
Conference	
Americas Conference on Information Systems	19
Hawaii International Conference on System Sciences	6
International Conference on Information Systems	3
Pacific Asia Conference on Information Systems	3
European Conference on Information Systems	2
International Conference on Information Security and Assurance	2
Others*	16

Note: *Only one relevant publication per journal/conference

Table I. Number of publications for each journal or conference

2.2 Literature analysis

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

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

Theory	Frequency of use
TRA/TPB	27
GDT	17
PMT	10
TAM	7
SCT	3
Constructivism	3
SLT	3

Table II. Most frequently used theories

These theories can be divided into behavioral theories [Theory of Reasoned Action/Theory of Planned Behavior (TRA/TPB), General Deterrence Theory (GDT), Protection Motivation Theory (PMT) and Technology Acceptance Model (TAM)] and learning theories [Constructivism, social cognitive theory (SCT) and social learning theory (SLT)]. Our main focus in the reviewed research domain is on behavioral theories. Due to the complexity of the subject matter and the limited length of this paper, we chose to present an in-depth analysis of the four dominantly applied behavioral theories.

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

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

3. Behavioral science in information security research

Researchers have incorporated multidisciplinary theories, including theories from psychology, sociology and criminology, into behavioral information security success outcome models. The most frequently applied theories in the examined research field are the TRA/TPB, GDT, PMT and TAM.

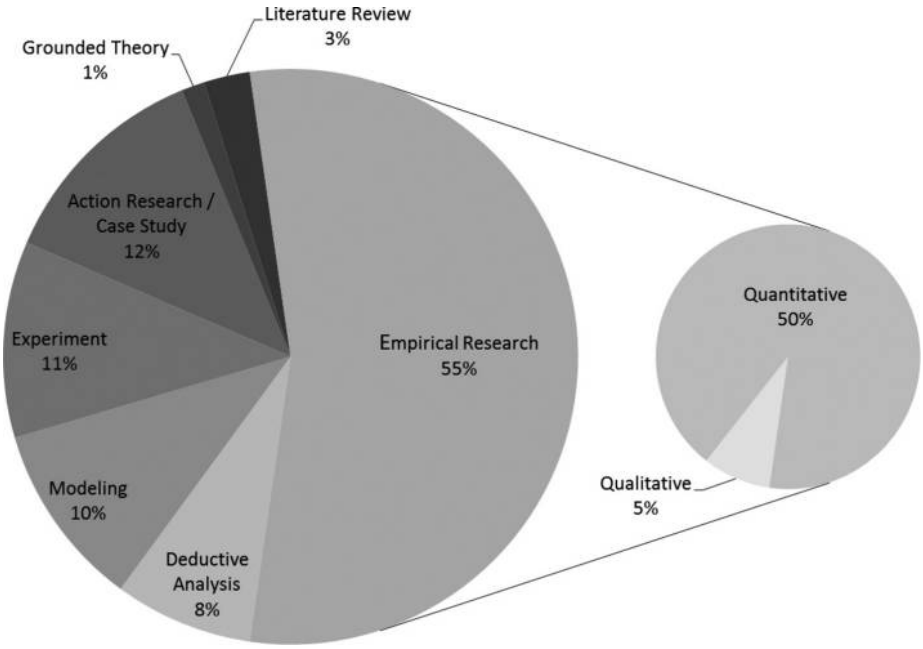

Figure 1.
Frequency of applied research methodologies

Theory of reasoned action/theory of planned behavior: In the context of information security behavioral compliance, the employee's intention to comply with ISPs depends on his/her overall evaluation of and normative beliefs toward compliance-related behavior. The greater the feeling of reflected actual control over those actions, the greater the intention to comply with ISP (Aurigemma and Panko, 2007; Bulgurcu *et al.*, 2010).

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

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

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

All four theories explain employees' behavioral intention (BI) or actual behavior (AB) by adapting different factors. The aforementioned behavioral theories were combined, resulting in a meta-model, as presented in Figure 2. It provides an overview of factors used to explain employees' ISA and behavior. Each behavioral factor has been tested and evaluated in multiple studies.

4. Results

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

Due to certain difficulties with observing actual security-compliant behavior (Vroom and von Solms, 2004), numerous authors emphasize the use of employees' BI as the dependent variable that predicts employees' AB (Ifinedo, 2012; Pahnila *et al.*, 2007, 2007b; Zhang *et al.*, 2009). Assessing BI rather than AB is grounded theoretically and technically. Several researchers demonstrated a strong and consistent relationship between the two constructs (Venkatesh *et al.*, 2003; Webb and Sheeran, 2006) in non-information security context. From a technical point of view, measurement of AB is argued to be difficult due to the sensitive context of information security (Anderson and Agarwal, 2010; Vroom and von Solms, 2004), the large and diverse sample sizes (Bulgurcu *et al.*, 2010; Bulgurcu *et al.*, 2009a, 2009b) and the theoretical background of the applied theory (Siponen and Vance, 2010). In a theoretical context, some authors (Anderson and Agarwal, 2010; Siponen and Vance, 2010) argue that the relationship

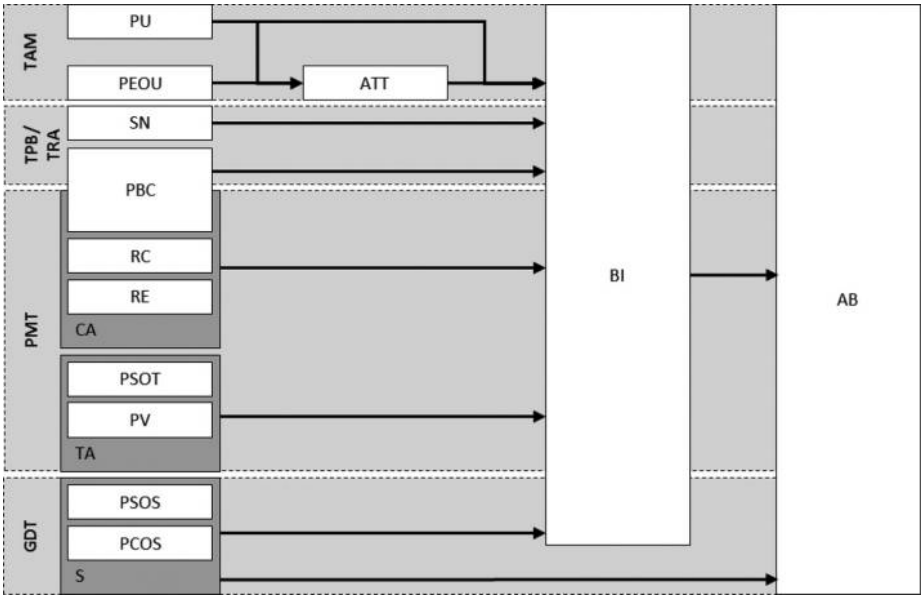

Figure 2.
Meta-model of primary used theories

between BI and AB is grounded in the TPB and TRA by Abraham (2011) and has been shown to be proven empirically by (Anderson and Agarwal, 2010). A number of studies emphasized the relationship between employees' AB and BI (Limayem and Hirt, 2003; Siponen *et al.*, 2010; 2007).

Further results demonstrate that the main constructs of the TPB are strong predictors of BI. More specifically, 92 per cent of the evaluated relationships between perceived behavioral control (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 (Bandura 1982). Self-efficacy is applied in ten research studies. It reflects the individual's personal beliefs about his or her ability to comply with the ISP (Bulgurcu *et al.*, 2010; Dinev *et al.*, 2009; Herath and Rao, 2009a, 2009b; Ifinedo, 2012; Johnston *et al.*, 2010; Johnston and Warkentin, 2010; Pahnila *et al.*, 2007a, 2007b; Siponen *et al.*, 2007; 2010; Warkentin *et al.*, 2011). In contrast, controllability represents an individual's perception about available resources and opportunities to actually comply with ISP (Al-Omari *et al.*, 2012a, 2012b; Hu and Dinev, 2007). Some authors used a combination of the two constructs to conceptualize PBC (Hu and Dinev, 2007; Zhanf *et al.*, 2009). A statistical significant influence of subjective norm (SN) on 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 (Bulgurcu *et al.*, 2010; Pahnila *et al.*, 2007a, 2007b; 2007; Siponen *et al.*, 2010) or general social determinants (Limayem and Hirt, 2003), which represent the SN construct (Albrechtsen and Hovden, 2010). Further, eight out of ten relationships between employees' ATT and their BI are significant, with six strong relationships at $p < 0.01$ level. The attitude construct is a broad term that has been investigated from different perspectives (Dinev *et al.*, 2009). In the context of TPB, employees' attitude (ATT) reflects the users' positive or negative feelings with regard to

Table III.
Construct relationships

Constructs independent variable	Items	Dependent variable	Items	Author(s)	Significance	β	N	Source
TPB/TRA								
ATT	4	BI	3	Bulgurcu *et al.* (2010)	**	0.25	464	Employees
	–		–	Bulgurcu *et al.* (2009a)	***	0.27	464	Employees
	4		3	Bulgurcu *et al.* (2009b)	**	0.48	464	Employees
	3		3	Dinev *et al.* (2009)	*	0.316	332	Students/IS professionals
	3		3	Dinev *et al.* (2009)	–	0.298	227	Students/IS professionals
	3		3	Herath and Rao (2009b)	–	0.073	312	Employees
	3		3	Hu and Dinev (2007)	**	0.29	332	Students/IS professionals
	4		5	Ifinedo (2012)	***	0.48	124	IS professionals
	4		2	Limayem and Hirt (2003)	–	0.079	60	Students
	3		4	Pahnila *et al.* (2007a)	***	0.537	240	Employees
	3		3	Hu *et al.* (2012)	***	0.360	148	Employees
	6		7	Al Omari *et al.* (2012b)	*	0.119	878	Employees
	5		4	Zhang *et al.* (2009)	*	0.18	176	Employees
BI	2	AB	2	Limayem and Hirt (2003)	**	0.386	60	Students
	3		3	Pahnila *et al.* (2007a)	*	0.04	917	Employees
	4		3	Pahnila *et al.* (2007b)	***	0.869	240	Employees
	3		3	Siponen *et al.* (2007)	***	0.98	917	Employees
	3		3	Siponen *et al.* (2010)	*	0.04	917	Employees
PBC	3	BI	3	Bulgurcu *et al.* (2010)	**	0.22	464	Employees
	2		3	Dinev *et al.* (2009)	**	0.193	332	Students/IS professionals
	2		3	Dinev *et al.* (2009)	*	0.197	227	Students/IS professionals
	3		3	Herath and Rao (2009b)	*	0.172	464	Employees
	2		3	Hu and Dinev (2007)	**	0.16	332	Students/IS professionals
	7		5	Ifinedo (2012)	**	0.17	124	IS professionals
	3		3	Johnston *et al.* (2010)	**	0.187	215	NA
	6		2	Limayem and Hirt (2003)	**	0.300	60	Students
	3		3	Pahnila *et al.* (2007a)	*	–	464	Employees
	3		3	Siponen *et al.* (2007)	***	0.31	917	Employees

(*continued*)

Table III.

Constructs independent variable	Items	Dependent variable	Items	Author(s)	Significance	β	N	Source
	3		3	Siponen *et al.* (2010)	*	0.17	917	Employees
	8		5	Johnston *et al.* (2010)	*	0.376	202	Healthcare professionals
	3		3	Hu *et al.* (2012)	***	0.360	148	Employees
	6		7	Al Omari *et al.* (2012b)	*	0.199	878	Employees
	4		4	Zhang *et al.* (2009)	***	0.43	176	Employees
SN	3	BI	3	Bulgurcu *et al.* (2010)	**	0.29	464	Employees
	2		3	Dinev *et al.* (2009)	–	–	332	Students/IS professionals
	2		3	Dinev *et al.* (2009)	**	0.324	227	Students/IS professionals
	5		3	Herath and Rao (2009a)	***	0.395	312	Employees
	5		3	Herath and Rao (2009b)	***	0.313	464	Employees
	2		2	Hovav and D'Arcy (2012)	**	−0.48	726	Employees
	3		3	Hu and Dinev (2007)	–	–	332	Students/IS professionals
	4		5	Ifinedo (2012)	**	0.19	124	IS professionals
	2		3	Johnston *et al.* (2010)	***	0.298	215	NA
	5		2	Limayem and Hirt (2003)	**	0.210	60	Students
	4		3	Pahnila *et al.* (2007a)	*	–	917	Employees
	3		–	Siponen *et al.* (2010)	–	0.07	1,449	Employees
	4		4	Pahnila *et al.* (2007b)	***	0.235	240	Employees
	4		3	Siponen *et al.* (2010)	*	0.45	917	Employees
	3		3	Hu *et al.* (2012)	***	0.366	148	Employees
	5		7	Al Omari *et al.* (2012a, 2012b)	*	0.233	878	Employees
	4		4	Zhang *et al.* (2009)	–	0.02	176	Employees
TAM								
ATT	3	BI	3	Hu and Dinev (2007)	**	0.29	332	Students/IS professionals
	3		3	Dinev *et al.* (2009)	**	0.316	332	Students/IS professionals
	3		3	Dinev *et al.* (2009)	**	0.298	227	Students/IS professionals

(*continued*)

Table III.

Constructs independent variable	Items	Dependent variable	Items	Author(s)	Significance	β	N	Source
	4		4	Herath *et al.* (2012)	***	0.49	174	Students
	4		3	Xue *et al.* (2011)	*	0.20	118	Employees
	4		4	Herath *et al.* (2012)	*	0.20	174	Students
PEOU	3	ATT	3	Hu and Dinev (2007)	–	–	332	Students/IS professionals
	4		4	Xue *et al.* (2011)	**	0.26	118	Employees
	3		3	Dinev *et al.* (2009)	–	–	332	Students/IS professionals
	3		3	Dinev *et al.* (2009)	***		227	Students/IS professionals
PU	4		4	Herath *et al.* (2012)	*	0.27	174	Students
	2		3	Dinev *et al.* (2009)	**	0.5	332	Students/IS professionals
	2		3	Dinev *et al.* (2009)	**	0.298	227	Students/IS professionals
	3		3	Dinev *et al.* (2009)	**	0.52	332	Students/IS professionals
	4		4	Xue *et al.* (2011)	**	0.50	118	Employees
	3	BI	3	Dinev *et al.* (2009)	–	–	332	Students/IS professionals
	4		3	Xue *et al.* (2011)	–	0.11	118	Employees
GDT								
PCOS	2	BI	2	D'Arcy *et al.* (2009)	–	−0.065	269	Employees
	2		3	Herath and Rao (2009a)	***	0.260	312	Employees
	2		3	Herath and Rao (2009b)	**	0.155	312	Employees
	2		2	Hovav and D'Arcy (2012)	–	−0.06	360	Employees
	2		2	Hovav and D'Arcy (2012)	**	−0.20	366	Employees
	4		3	Xue *et al.* (2011)	–	0.03	118	Employees
PSOS	2	BI	2	D'Arcy *et al.* (2009)	**	−0.176	269	Employees
	3		3	Herath and Rao (2009a)	**	−0.209	312	Employees
	3		3	Herath and Rao (2009b)	**	−0.139	312	Employees
	2		2	Hovav and D'Arcy (2012)	**	−0.14	360	Employees
	2		2	Hovav and D'Arcy (2012)	–	−0.04	366	Employees

(*continued*)

Table III.

Constructs independent variable	Items	Dependent variable	Items	Author(s)	Significance	β	N	Source
S	4	AB	3	Siponen *et al.* (2007)	***	0.09	917	Employees
	4		3	Pahnila *et al.* (2007a)	*	–	917	Employees
	6		3	Siponen *et al.* (2010)	***	0.09	917	Employees
	2	BI	–	Siponen *et al.* (2010)	–	0.04	1,449	Employees
	4		4	Pahnila *et al.* (2007b)	–	–	240	Employees
PMT								
PBC	7	BI	5	Ifinedo (2012)	**	0.17	124	IS professionals
	3		3	Herath and Rao (2009b)	*	0.172	312	Employees
	6		3	Pahnila *et al.* (2007a)	*	–	917	Employees
	6		3	Siponen *et al.* (2007)	***	0.31	917	Employees
	8		4	Herath *et al.* (2012)	*	0.17	174	Students
	3		3	Siponen *et al.* (2010)	*	0.17	917	Employees
CA	3	AB	3	Pahnila *et al.* (2007a)	–	–	240	Employees
RC	5	BI	5	Ifinedo (2012)	–	−0.12	124	IS professionals
RE	6	BI	5	Ifinedo (2012)	**	0.27	124	IS professionals
	3		3	Johnston *et al.* (2010)	*	0.213	215	NA
	6		3	Pahnila *et al.* (2007a)	–	–	917	Employees
	6		3	Siponen *et al.* (2007)	*	0.06	917	Employees
	3		3	Siponen *et al.* (2010)	–	−0.02	917	Employees
PSOT	7	BI	5	Ifinedo (2012)	*	−0.20	124	IS professionals
PV	7	BI	5	Ifinedo (2012)	**	0.20	124	IS professionals
TA	4	BI	4	Herath *et al.* (2012)	***	0.30	174	Students
	6		3	Pahnila *et al.* (2007a)	*	–	917	Employees
	6		3	Siponen *et al.* (2007)	***	0.24	917	Employees
	6		3	Siponen *et al.* (2010)	*	0.12	917	Employees
	5	AB	3	Pahnila *et al.* (2007a)	***	0.278	240	Employees

complying with the ISP (Ifinedo, 2012; Pahnila *et al.*, 2007a, 2007b; Zhang *et al.*, 2009; Hu and Dinev, 2007). In two cases, employee attitudes were not significant with BI. Herath and Rao (2009, 2009b) stated that the insignificant effect may be due to context, sample or other extraneous reasons. The authors combined the PMT and GDT based on the core constructs of TPB and used a sample of 312 employees from 78 organizations.

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

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

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

To extend and improve the standard behavioral theories, several other constructs were introduced by academic literature to explain employees' IS-security-related behavior. With the purpose of explaining employees' BI, 15 factors beyond the standard theories (i.e. TRA/TPB, TAM, GDT and PMT) were examined. Twelve of them were found to have a

significant effect on BI. For example, the strength of an employee's identification with and involvement in an organization (organizational commitment) shows a highly significant effect on BI (Herath and Rao, 2009b). Herath *et al.* (2009a) discovered that an employee's perceived effectiveness of behaving securely influences BI. Moreover, the employee's awareness of the ISP (Johnston *et al.*, 2010), as well as his or her technology awareness (Hu and Dinev, 2007), determine the security-related BI. Johnston *et al.* (2010) show that employees' awareness of ISP depends on the degree an employee perceives his environment to be favorable toward fulfilling a given task (situational support), the degree to which a company provides instructions to fulfill a task (verbal persuasion) and an employee's indirect experience with a task through observation (vicarious experience). With the introduction of the neutralization theory, Siponen and Vance (2010) showed that the use of neutralization techniques reduces the perceived harm of violating the ISP and therefore influences an employee's BI.

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

5. Discussion and implications

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

Because factors like employees' intentions, attitudes, motivations or satisfaction are not verifiable by means other than self-reporting (Podsakoff and Organ, 1986), it is not unexpected that the majority of reviewed literature applying TRA/TPB, TAM, GDT or PMT uses quantitative methods to test the hypotheses. However, the use of self-reports to measure security-related behavior might lack validity because self-reports are prone to the problems of common method variance, consistency motif and social desirability (Podsakoff and Organ, 1986), and results may be biased. According to Workmann *et al.* (2008), self-reports are not sufficient predictors of employees' AB because employees' self-reported perceptions of security behavior are not necessarily in line with their AB. At first glance, observation seems to be an instrument for gathering more objective data. Due to the sensitive nature of security-related data, organizations are unwilling to reveal information that provides insights into a company's current information security status (Kotulic and Clark, 2004). In addition, it is impossible to observe all aspects of security behavior (e.g. password strength and encrypting sensitive e-mails) for a large amount of employees, which means that observations alone are also insufficient. If researchers are able to develop a

trustful environment (Kotulic and Clark, 2004), a combination of self-reporting and observational sampling in triangulation, as proposed by Workman *et al.* (2008), is an appropriate means of reducing the lack of qualitative and interpretive studies in this research field. As already stated by Bulgurcu *et al.* (2009b), case studies including employees from one or more companies would be useful for further research. As an alternative to case studies, experimental studies, as used by Johnston and Warkentin (2010), for example, are also a method of observing employees' AB. 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. One method of observing long-time data in actual working environments is proposed by Venkatesh *et al.* (2003) and Workman *et al.* (2008) with the analysis of log-files.

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

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

According to Rosemann and Vessey (2008), academic literature should provide relevance for practitioners to prevent research from becoming an end unto itself. The research topic covered by our work is highly relevant for practice because dependency on information technology (IT) systems has increased rapidly over the past years, and there is a high

demand in security measures that go beyond technical solutions. The key question for practitioners is how to influence employees' behavior to reduce information security risks. Previous research shows a gap between theoretically grounded explanations of employees' security behavior and the need of practitioners to know which interventions to apply (Workman *et al.*, 2008). Our results contribute toward closing this gap by providing an overview of factors that were shown to have a significant influence on employees' BIs and their ABs. Practitioners are, therefore, able to focus on these factors to define effective security measures and ISA programs. Security practitioners should keep in mind the variety of influence factors, resulting in a behavior-specified ISA program. Our findings suggest that effective security awareness programs are dependent on several behavioral influence factors. Based on our results, additional research can support practitioners by developing and validating measures that are able to significantly influence key factors.

6. Limitations

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

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

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

7. Conclusion and outlook

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

Because solid evidence of relationships between the main constructs of TPB, GDT, PMT and TAM is provided by academic literature, future empirical studies have to focus on additional factors that influence employees' ISA 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 BI as a predictor of actual security behavior needs further attention. Regarding the weaknesses of self-reporting as a measure of employees' AB, a stronger consideration of additional research methodologies such as experiments or case studies is required. To prevent an emerging gap between theory and practice, the development of measures and process models to influence employees' security awareness and behavior based on already existing theoretical knowledge is necessary.

References

*Abraham, S. (2011), "Information security behavior: factors and research directions", *Proceedings of the American Conference on Information Systems*, *Detroit*, Paper 462.

*Albrechtsen, E. and Hovden, J. (2010), "Improving information security awareness and behavior through dialogue, participation and collective reflection. An intervention study", *Computers & Security*, Vol. 29 No. 4, pp. 432-445.

*Al-Omari, A., El-Gayar, O. and Deokar, A. (2012a), "Security policy compliance: user acceptance perspective", *Proceedings of the 45th Hawaii International Conference on System Sciences*, *Maui*, pp. 3317-3326.

*Al-Omari, A., El-Gayar, O. and Deokar, A. (2012b), "Information security policy compliance: the role of information security awareness", *Proceedings of the American Conference on Information Systems, Paper 16*.

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.

*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*, *Big Island*, pp. 3248-3257.

Bandura, A. (1982), "Self-efficacy mechanism in human agency", *American Psychologist*, Vol. 37, pp. 122-147.

*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 American 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.

*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., 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.

*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.

Fishbein, M. and Ajzen, I. (1975), *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*, Addison-Wesley, Reading, MA.

Hair, J.F.J., Black, W.C., Babin, B.J., Anderson, R.E. and Tatham, R.L. (2006), "Multivariate data analysis, 6th edition", Pearson Prentice Hall, Upper Saddle River.

*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.

*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.

*Hu, D. and Wang, Y.Y. (2008), "Teaching computer security using Xen in a virtual environment", *Proceedings of the International Conference on Information Security and Assurance*, *Busan*, pp. 389-392.

*Ifinedo, P. (2012), "Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory", *Computers & Security*, Vol. 31 No. 1, pp. 83-95.

*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.

*Johnston, A.C., Wech, B., Jack, E. and Beavers, M. (2010), "Reigning in the remote employee: applying social learning theory to explain information security policy compliance attitudes", *Proceedings of the American Conference on Information Systems*, *Lima*, Paper 493.

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.

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.

Leonard, L.N.K. and Cronan, T.P. (2001), "Illegal, inappropriate, and unethical behavior in an information technology context: a study to explain influences", *Journal of the Association for Information Systems*, Vol. 1 No. 12, pp. 1-31.

*Limayem, M. and Hirt, S.G. (2003), "Force of habit and information systems usage: theory and initial validation", *Journal of Association for Information Systems*, Vol. 4 No. 1, pp. 65-97.

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

*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*, *Big Island*, pp. 1-10.

*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*, *Auckland*, Paper 73.

Podsakoff, P.M. and Organ, D. (1986), "Self-reports in organizational research: problems and prospects", *Journal of Management*, Vol. 12 No. 4, pp. 531-544.

Prasad, J. and Agarwal, R. (1998), "Conceptual and operational definition of personal innovativeness in the domain of information technology", *Information Systems Research*, Vol. 9 No. 2, pp. 204-215.

Rogers, R.W. and Pentice-Dunn, S. (1997), "Protection motivation theory", in Gochman D.S. (Ed), *Handbook of Health Behavior Research I: Personal and Social Determinants*, Plenum Press, New York.

*Siponen, M.T. (2000a), "A conceptual foundation for organizational information security awareness", *Information Management & Computer Security*, Vol. 8 No. 1, pp. 31-41.

*Siponen, M.T. (2000b), "Critical analysis of different approaches to minimizing user-related faults in information systems security: implications for research and practice", *Information Management & Computer Security*, Vol. 8 No. 5, pp. 197-209.

*Siponen, M.T., Pahnila, S. and Mahmood, M.A. (2010), "Compliance with information security policies: an empirical investigation", *Computer*, Vol. 43 No. 2, pp. 64-71.

*Siponen, M.T. and Vance, A.O. (2010), "Neutralization: new insights into the problem of employee systems security policy violations", *MIS Quarterly*, Vol. 34 No. 3, pp. 487-502.

Sivo, S., Saunders, S., Chang, Q. and Jiang, J.J. (2004), "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.

*Spears, J.L. and Barki, H. (2010), "User participation in information systems security risk management", *MIS Quarterly*, Vol. 34 No. 3, pp. 503-522.

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.

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*, *Verona*, pp. 2206-2217.

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

*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 (EJIS)*, Vol. 20 No. 3, pp. 267-284.

Webb, T.L. and Sheeran, P. (2006), "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.

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.

*Zhanf, J., Reithel, B., Brian, J. and Li, H. (2009), "Impact of perceived technical protection on security behaviors", *Information Management & Computer Security*, Vol. 17 No. 4, pp. 330-340.

*Zhang, J., Reithel, B., Brian, J. and Li, H. (2009), "Impact of perceived technical protection on security behaviors", *Information Management & Computer Security*, Vol. 17 No. 4, pp. 330-340.

Further reading

*Abawajy, J.H., Thatcher, K. and Kim, T.-H. (2008), "Investigation of stakeholders commitment to information security awareness programs", *Proceedings of the International Conference on Information Security and Assurance*, *Busan*, pp. 472-476.

Ajzen, I. (1991), "The theory of planned behavior", *Organizational Behavior and Human Decision Processes*, Vol. 50 No. 2, pp. 179-211.

*Al Arifi, A., Tootell, H. and Hyland, P. (2012), "Information security awareness in Saudi Arabia", *CONF-IRM Proceedings*, *Vienna*, Paper 57.

*Albrechtsen, E. (2007), "A qualitative study of users' view on information security", *Computers & Security*, Vol. 26 No. 4, pp. 276-289.

*Alnatheer, M., Chan, T. and Nelson, K. (2012), "Understanding and measuring information security culture", *Proceedings of the Pacific Asia Conference on Information Systems*, *Hochiminh City*, Paper 144.

*Al-Omari, A., El-Gayar, O. and Deokar, O. (2011), "Information security policy compliance: a user acceptance perspective", *Proceedings of the Midwest Association for Information Systems*, *Seattle*, Paper 12.

*Alshare, K.A. and Lane, P.L. (2008), "A conceptual model for explaining violations of the information security policy (ISP): a cross cultural perspective", *Proceedings of the American Conference on Information Systems, Paper 366*, *Toronto*.

*Aytes, K. and Conolly, T. (2003), "A research model for investigating human behavior related to computer security", *Proceedings of the American Conference on Information Systems*, *Tampa*, pp. 2027-2031.

*Banerjee, C. and Pandey, S.K. (2010), "Research on software security awareness: problems and prospects", *ACM SIGSOFT Software Engineering Notes*, Vol. 35 No. 5, pp. 1-5.

*Boon Yuen, N. and Kankanhalli, A. (2008), "Processing information security messages: an elaboration likelihood perspective", *Proceedings of the European Conference on Information Systems*, *Galway*, Paper 113.

*Boss, S.R., Kirsch, L.J., Angermeier, I., Shingler, R.A. and Boss, R.W. (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.

*Boujettif, M. and Wang, Y. (2010), "Constructivist approach to information security awareness in the middle east", *Proceedings of the International Conference on Broadband*, *Wireless Computing, Communication and Applications*, pp. 192-199.

*Brody, R., Brizzee, W. and Cano, I. (2012), "Flying under the radar: social engineering", *International Journal of Accounting and Information Management*, Vol. 20 No. 4, pp. 335-347.

*Burns, M., Durcikova, A. and Jenkins, J. (2012), "On not falling for phish: examining multiple stages of protective behavior of information systems end-users", *Proceedings of the 33rd International Conference on Information Systems*, *Orlando*, Paper 87.

*Burns, M., Durcikova, A. and Jenkins, J. (2013), "What kind of interventions can help users from falling for phishing attempts: a research proposal for examining stage-appropriate interventions", *Proceedings of the 46th Hawaii International Conference on System Sciences*, *Maui*, pp. 4023-4032.

*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.

*Charoen, D., Raman, M. and Olfman, L. (2008), "Improving End User Behaviour in Password Utilization: An Action Research Initiative", *Systemic Practice and Action Research*, Vol. 21 No. 1, pp. 55-72.

Chen, C.C., Medlin, B.D. and Shaw, R.S. (2008), "A cross-cultural investigation of situational information security awareness programs", *Information Management & Computer Security*, Vol. 16 No. 4, pp. 360-376.

*Chia, P.A., Maynard, S.B. and Ruighaver, A.B. (2002), "Exploring organisational security culture: developing a comprehensive research model", *IS ONE World Conference*, *Las Vegas*.

*Clarke, M. and Levy, Y. (2012), "Initial validation and empirical development of the construct of computer security self-efficacy", *Proceedings of the Pre-ICIS Workshop on Information Security and Privacy*, *Orlando*, Paper 4.

*Cone, B.D., Irvine, C.E., Thompson, M.F. and Nguyen, T.D. (2007), "A video game for cyber security training and awareness", *Computers & Security*, Vol. 26 No. 1, pp. 63-72.

*Conklin, A. and Dietrich, G. (2005), "Modeling end user behavior to secure a pc in an unmanaged environment", *Proceedings of the American Conference on Information Systems*, *Omaha*, Paper 449.

*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 Hovav, A. (2004), "The role of individual characteristics on the effectiveness of IS security", *Proceedings of the American Conference on Information Systems*, *New York*, pp. 1395-1402.

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.

*Dodge, R.C., Carver, C. and Ferguson, A.J. (2007), "Phishing for user security awareness", *Computers & Security*, Vol. 26 No. 1, pp. 73-80.

*Dojkovski, S., Lichtenstein, S. and Warren, M.J. (2007), "Fostering information security culture in small and medium size enterprises: an interpretive study in Australia", *European Conference on Information Systems*, *St. Gallen*, pp. 1560-1571.

*Drevin, L., Kruger, H.A. and Steyn, T. (2007). "Value-focused assessment of ICT security awareness in an academic environment", *Computers & Security*, Vol. 26 No. 1, pp. 36-43.

*El-Haddadeh, R., Tsohou, A. and Karyda, M. (2012), "Implementation challenges for information security awareness initiatives in e-government", *Proceedings of the European Conference on Information Systems*, *Barcelona*, Paper 179.

*Eminağaoğlu, M., Uçar, E. and Eren, S. (2009), "The positive outcomes of information security awareness training in companies – a case study", *Information Security Technical Report*, Vol. 14 No. 4, pp. 223-229.

*Fan, J. and Zhang, P. (2011), "Study on e-government information misuse based on general deterrence", *Proceedings of the International Conference on Service Systems and Service Management*, *Tianjin*, pp. 1-6.

*Flores, W. and Ekstedt, M. (2012), "A model for investigating organizational impact on information security behavior", *Proceedings of the Pre-ICIS Workshop on Information Security and Privacy*, *Orlando*, Paper 12.

*Flores, W. and Korman, M. (2012), "Conceptualization of constructs for shaping information security behavior: towards a measurement instrument", *Proceedings of the Pre-ICIS Workshop on Information Security and Privacy*, *Orlando*, Paper 11.

*Furnell, S.M., Gennatou, M. and Dowland, P.S. (2002), "A prototype tool for information security awareness and training", *Logistics Information Management*, Vol. 15 No. 5, pp. 352-357.

*Galvez, S.M. and Guzman, I.R. (2009), "Identifying factors that influence corporate information security behavior", *Proceedings of the American Conference on Information Systems (AMCIS)*, *San Francisco*, Paper 765.

*Gonzalez, J.J. (2012), "Exploring collaborative modeling as teaching method", *Proceedings of the 45th Hawaii International Conference on System Sciences (HICSS)*, *Maui*, pp. 190-196.

*Guimaraes, M., Said, H. and Austin, R. (2012), "Experience with videogames for security", *The Journal of Computing Sciences in Colleges*, Vol. 27 No. 3, pp. 95-104.

*Gundu, T. and Flowerday, S.V. (2012), "The enemy within: a behavioural intention model and an information security awareness process", *Proceedings of the Annual Conference on Information Security South Africa*, *Johannesburg*, pp. 1-8.

*Guo, K.H., Yuan, Y., Archer, N.P. and Connelly, C.E. (2011), "Understanding nonmalicious security violations in the workplace: a composite behavior model", *Journal of Management Information Systems*, Vol. 28 No. 2, pp. 203-236.

*Hadasch, F., Mueller, B. and Maedche, A. (2012), "Exploring antecedent environmental and organizational factors to user caused information leaks: a qualitative study", *Proceedings of the European Conference on Information Systems*, *Barcelona*, Paper 127.

*Hagen, J.M., Albrechtsen, E. and Hovden, J. (2008), "Implementation and effectiveness of organizational information security measures", *Information Management & Computer Security*, Vol. 16 No. 4, pp. 377-397.

*Hagen, J.M. and Albrechtsen, E. (2009), "Effects on employees' information security abilities by e-learning", *Information Management & Computer Security*, Vol. 17 No. 5, pp. 338-407.

*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.

*Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J. and Rao, H.R. (2012), "Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service", *Information Systems Journal*, Vol. 21 No. 1, pp. 61-84.

*Heikka, J. (2008), "A constructive approach to information systems security training: an action research experience", *Proceedings of the American Conference on Information Systems*, *Toronto*, Paper 319.

*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.

*Hu, Q., Dinev, T., Hart, P. and Cooke, D. (2012), "Managing employee compliance with information security policies: the critical role of top management and organizational culture", *Decision Sciences Journal*, Vol. 43 No. 4.

*Ifinedo, P. (2008), "IT security and privacy issues in global financial services institutions: do socio-economic and cultural factors matter?", *Proceedings of the Conference on Privacy, Fredericton, Security and Trust*, *Fredericton*, pp. 75-84.

*Jahner, S. and Krcmar, H. (2005), "Beyond technical aspects of information security: risk culture as a success factor for IT risk management", *Proceedings of the American Conference on Information Systems*, *Omaha*, Paper 462.

*Jenkins, J., Durcikova, A. and Burns, M. (2011), "Get a cue on is security training: explaining the difference between how security cues and security arguments improve secure behavior", *Proceedings of the International Conference on Information Systems*, *Shanghai*.

*Jenkins, J.L., Durcikova, A., Ross, G. and Nunamaker, J.F. (2001), "Encouraging users to behave securely: examining the influence of technical, managerial, and educational controls on users' secure behavior", *Proceedings of the International Conference on Information Systems*, *New Orleans*, Paper 150.

*Jenkins, J.L., Durcikova, A. and Burns, M.B. (2012), "Forget the fluff: examining how media richness influences the impact of information security training on secure behavior", *Proceedings of the 45th Hawaii International Conference on System Sciences*, *Maui*, pp. 3288-3296.

*Kawakami, Yasuda, H. and Sasaki, R. (2010), "Development of an e-learning content-making system for information security (ELSEC) and its application to anti-phishing education", *Proceedings of the International Conference on e-Education*, *Sanya*, pp. 7-11.

*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*, *Montreal*, Paper 103.

*Komatsu, A., Takagi, D. and Takemura, T. (2013), "Human aspects of information security: an empirical study of intentional versus actual behavior", *Information Management & Computer Security*, Vol. 21 No. 1, pp. 5-15.

*Kritzinger, E. and Smith, E. (2008), "Information security management: an information security retrieval and awareness model for industry", *Computers & Security*, Vol. 27 Nos 5/6, pp. 224-231.

*Kruger, H.A., Drevin, L. and Steyn, T. (2010), "A vocabulary test to assess information security awareness", *Information Management & Computer Security*, Vol. 18 No. 5, pp. 316-327.

*Kruger, H.A., Flowerday, S., Drevin, L. and Steyn, T. (2011), "An assessment of the role of cultural factors in information security awareness", *Proceedings of the Annual Conference on Information Security South Africa*, *Johannesburg*, pp. 1-7.

*Kruger, H.A. and Kearney, W.D. (2006), "A prototype for assessing information security awareness", *Computers & Security*, Vol. 25 No. 4, pp. 289-296.

*Kruger, H.A. and Kearney, W.D. (2008), "Consensus ranking – an ICT security awareness case study", *Computers & Security*, Vol. 27 Nos 7/8, pp. 254-259.

*Lee, J. and Lee, Y. (2002), "A holistic model of computer abuse within organizations", *Information Management & Computer Security*, Vol. 10 No. 2, pp. 57-63.

*Lee, S.M., Lee, S.G. and Yoo, S. (2004), "An integrative model of computer abuse based on social control and general deterrence theories", *Information & Management*, Vol. 41 No. 6, pp. 707-718.

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*, *Manchester*, pp. 171-181.

*Liang, H. and Xue, Y. (2010), "Understanding security behaviors in personal computer usage: a threat avoidance perspective", *Journal of the Association for Information Systems*, Vol. 11 No. 7, pp. 394-413.

*Liao, G.-Y. and Wang, C.-M. (2011), "Exploring the influences of implementation intention on information security behaviors", *Proceedings of the American Conference on Information Systems*, *Detroit*, Paper 473.

*Lim, J.S., Ahmad, A., Chang, S. and Maynard, S. (2010), "Embedding information security culture emerging concerns and challenges", *Proceedings of the Pacific Asia Conference on Information Systems*, *Taipei*, Paper 43.

Madden, T.J., Scholder, P.S. and Ajzen, I. (1992), "A comparison of the theory of planned behavior and the theory of reasoned action", *Personality and Social Psychology Bulletin*, Vol. 18 No. 1, pp. 3-9.

*Mahbubur Rahim, M., Cheo, A. and Cheong, K. (2008), "IT security expert's presentation and attitude changes of end-users towards IT security aware behaviour: a pilot study", *Proceedings of the Australasian Conference on Information Systems*, *Christchurch*, pp. 780-790.

*Marett, K. and Ratnamalala, N. (2012), "Examining the coping appraisal process in end user security",. *Proceedings of the Pre-ICIS Workshop on Information Security and Privacy*, *Orlando*, Paper 2.

*Marks, A. and Rezgui, Y. (2009), "A comparative study of information security awareness in higher education based on the concept of design theorizing", *Proceedings of the International Conference on Management and Service Science*, *Beijing*, pp. 1-7.

Mehrens, W.A. and Lehman, I.J. (1987), *Using Standardized Tests in Education*, *Longman Group United Kingdom*.

*Meister, E. and Biermann, E. (2008), "Implementation of a socially engineered worm to increase information security awareness", *Proceedings of the International Conference on Broadband Communications, Information Technology & Biomedical Applications*, pp. 343-350.

*Mejias, R.J. (2012), "An integrative model of information security awareness for assessing information systems", *Proceedings of the 45th Hawaii International Conference on System Sciences, Maui*, pp. 3259-3267.

*Merhi, M. and Midha, V. (2012), "The impact of training and social norms on information security compliance: a pilot study", *Proceedings of the 33rd International Conference on Information Systems, Orlando*, Paper 73.

*Mishra, S., Leone, G., Caputo, D., Galabrisi, R. and Draus, P. (2012), "The role of demographic characteristics in health care strategic security planning", *Proceedings of the 18th Americas Conference on Information Systems, New York*, Paper 16.

*Myyry, L., Siponen, M.T., Pahnila, S., Vartiainen, T. and Vance, A. (2011), "What levels of moral reasoning and values explain adherence to information security rules? An empirical study", *European Journal on Information Systems*, Vol. 18 No. 2, pp. 126-139.

*Ng, B.-Y., Kankanhalli, A. and Xu, Y. (2009), "Studying users' computer security behavior: a health belief perspective", *Decision Support Systems*, Vol. 46 No. 4, pp. 815-825.

*Padayachee, K. (2012), "Taxonomy of compliant information security behavior". *Computers & Security*, Vol. 31 No. 5, pp. 673-680.

*Pattinson, M.R. and Anderson, G. (2007), "How well are information risks being communicated to your computer end-users?", *Information Management & Computer Security*, Vol. 15 No. 5, pp. 362-371.

*Phelps, D. and Gathegi, J. (2006), "Information system security: self-efficacy and implementation effectiveness", *Proceedings of the American Conference on Information Systems, Acapulco*, pp. 3353-3361.

*Puhakainen, P. and Siponen, M.T. (2010), "Improving employees'compliance through information system security training", *MIS Quarterly*, Vol. 24 No 4, pp. 757-778.

*Qing, H., Zhengchuan, X., Dinev, T. and Hong, L. (2011), "Does deterrence work in reducing information security policy abuse by employees?", *Communications of the ACM*, Vol. 54 No. 6.

*Ramachandran, S. (2006), "Influences on espoused and enacted security cultures in organizations", *Proceedings of the American Conference on Information Systems, Acapulco*, Paper 128.

*Ramachandran, S. and Rao, S. (2006), "Security cultures in organizations: a theoretical model", *Proceedings of the American Conference on Information Systems, Acapulco*, Paper 417.

*Reid, R., van Niekerk, J. and von Solms, R. (2011), "Guidelines for the Creation of brain-compatible cyber security educational material in Moodle 2.0", *Proceedings of the Annual Conference on Information Security South Africa, Johannesburg*.

*Rezgui, Y. and Marks, A. (2008), "Information security awareness in higher education: an exploratory study", *Computers & Security*, Vol. 27 Nos 7/8, pp. 241-253.

*Rhee, H., Kim, C. and Ryu, Y. (2009), "Self-efficacy in information security: it's influence on end users' information security practice behavior", *Computers & Security*, Vol. 28 No. 8, pp. 816-826.

Rogers, R.W. (1983), "Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation theory", in Cacioppo, J. and Petty, R. (Eds), *Social Psychophysiology*, Guilford, New York, NY.

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.

*Ryan, J. (2007), "Information security awareness: an evaluation among business students with regard to computer self-efficacy and personal innovation", *Proceedings of the American Conference on Information Systems (AMCIS)*, *Keystone*, Paper 251.

*Shaw, R.S., Chen, C.C., Harris, A.L. and Huang, H.J. (2009), "The impact of information richness on information security awareness training effectiveness", *Computers & Security*, Vol. 52 No. 1, pp. 92-100.

*Shropshire, J., Warkentin, M., Johnston, A. and Schmidt, M. (2006), "Personality and IT security: an application of the five-factor model", *Proceedings of the American Conference on Information Systems (AMCIS)*, *Acapulco*, pp. 3443-3449.

*Silva, I., Menezes, S. and Costa, A. (2012), "A model for evaluating information security with a focus on the user", *Proceedings of the Mediterranean Conference on Information Systems*, *Guimaraes*, Paper 25.

*Silvius, G. and Dols, T. (2012), "Factors influencing non-compliance behavior towards information security policies", *CONF-IRM Proceedings*, *Vienna*, Paper 39.

*Siponen, M.T. (2001), "Five dimensions of information security awareness", *Computers and Society*, Vol. 31 No. 2, pp. 24-29.

*Siponen, M.T., Pahnila, S. and Mahmood, A. (2007), "Employees' adherence to information security policies: an empirical study", *Proceedings of the IFIP SEC*, *Brisbane*, pp. 133-144.

*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*, *Kuala Lumpur*, Paper 48.

*Son, J.-Y. (2011), "Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies", *Information & Management*, Vol. 48 No. 7, pp. 296-302.

*Son, J.-Y. and Rhee, H.-S. (2007), "Out of fear or desire: why do employees follow information systems security policies?", *Proceedings of the American Conference on Information Systems*, *Keystone*, Paper 268.

*Stanton, J., Mastrangelo, P., Stam, K. and Jolton, J. (2004), "Behavioral information security: two end user survey studies of motivation and security practices", *Proceedings of the American Conference on Information Systems (AMCIS)*, *New York*, pp. 1388-1394.

*Stanton, J.M., Stam, K.R., Guzman, I. and Caledra, C. (2003), "Examining the linkage between organizational commitment and information security", *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics*, *Washington*, pp. 2501-2506.

*Stanton, J.M., Stam, K.R., Mastrangelo, P. and Jolton, J. (2005), "An analysis of end user security behaviors", *Computers & Security*, Vol. 24 No. 2, pp. 124-133.

Straub, D.W. (1990), "Effective IS security: an empirical study", *Information Systems Research*, Vol. 1 No. 3, pp. 255-276.

*Talib, S., Clarke, N. and Furnell, S.M. (2010), "An analysis of information security awareness within home and work environments", *Proceedings of the International Conference on Availability*, *Reliability, and Security*, *Krakow*, pp. 196-203.

*Thomson, K. and Niekerk, J. (2012), "Combating information security apathy by encouraging prosocial organizational behavior", *Information Management & Computer Security*, Vol. 20 No. 1, pp. 39-46.

*Tsohou, A. Karyda, M., Kokolakis, S. and Kiountouzis, E. (2012), "Analyzing trajectories on information security awareness", *Information Technology & People*, Vol. 25 No. 3, pp. 327-352.

*Tsohou, A. and Kokolakis, S. (2009), "Aligning security awareness with information systems security management", *Proceedings of the Mediterranean Conference on Information Systems*, *Athens*, Paper 73.

*Tsohou, A., Kokolakis, S., Karyda, M. and Kiountouzis, E. (2008), "Investigating information security awareness: research and practice gaps", *Information Security Journal: A Global Perspective*, Vol. 17 Nos 5/6, pp. 207-227.

Uffen, J. and Breitner, M.H. (2013), "Management of technical security measures: an empirical examination of personality traits and behavioral intentions", *Proceedings of the 46th Hawaii International Conference on System Science*, *Maui*, pp. 4551-4560.

*Vance, A., Siponen, M.T. and Pahnila, S. (2012), "Motivating IS security compliance: insights from habit and protection motivation theory", *Information & Management*, Vol. 49 Nos 3/4, pp. 190-198.

*vom Brocke, J. and Buddendick, C. (2007), "Security awareness management - Konzeption, Methoden und Anwendung", *Proceedings of the Wirtschaftsinformatik Tagung*, *Karlsruhe*, pp. 1227-1246.

*Waly, N., Tassabehji, R. and Kamala, M. (2012a), "Measures for improving information security management in organisations: the impact of training and awareness programs", *Proceedings of the UK Academy for Information Systems Conference*, *Oxford*, Paper 8.

*Waly, N., Tassabehji, R. and Kamala, M. (2012b), "Improving organizational information security management: the impact of training and awareness", *Proceedings of the 14th International Conference on High Performance Computing and Communications*, *Liverpool*, pp. 1270-1275.

*Warkentin, M., Mc Bride, M., Carter, I. and Johnston, A. (2012), "The role of individual characteristics on insider abuse intentions", *Proceedings of the 18th Americas Conference on Information Systems*, *Detroit*, Paper 28.

*Warkentin, M., Malimage, N. and Malimage, K. (2012), "Impact of Protection motivation and deterrence on IS security policy compliance: a multi-cultural view", *Proceedings of the Pre-ICIS Workshop on Information Security and Privacy*, *Orlando*, Paper 20.

*Warner, J. (2006), "Towards understanding user behavioral intentions to use it security: examining the impact of IT security psychological climate and individual beliefs", *Proceedings of the American Conference on Information Systems*, *Acapulco*, pp. 4536-4540.

*Williams, P.A.H. (2008), "In a 'trusting' environment, everyone is responsible for information security", *Information Security Technical Report*, Vol. 13 No. 4, pp. 207-215.

*Willison, R. (2006), "Understanding the perpetration of employee computer crime in the organizational context", *Information and Organization*, Vol. 16 No. 4, pp. 304-324.

*Woodhouse, S. (2007), "Information security: end user behavior and corporate culture", *Proceedings of the IEEE International Conference on Computer and Information Technology*, *Fukushima*, pp. 767-774.

*Workman, M.T. and Gathegi, J. (2007), "Punishment and ethics deterrents: a study of insider security contravention", *Journal of the American Society for Information Science and Technology*, Vol. 58 No. 2, pp. 212-222.

Worthen, B.R., Borg, W.R. and White, K.R. (1993), *Measurement and Evaluation in the School*, Longman Group, White Plains, NY.

Corresponding author
Benedikt Lebek can be contacted at: lebek@iwi.uni-hannover.de

Appendix

Table AI.
List of items

Variable	Author(s)	Item	Scale
ATT	Al-Omari *et al.* (2012b)	Attitude: To me, complying with the requirements of my organization's ISP is:	Not Necessary . . . Necessary
		Attitude: To me, complying with the requirements of my organization's ISP is:	Not Beneficial . . . Beneficial
		Attitude: To me, complying with the requirements of my organization's ISP is:	Not Important . . . Important
		Attitude: To me, complying with the requirements of my organization's ISP is:	Not Useful . . . Useful
		Attitude: To me, complying with the requirements of my organization's ISP is:	Not Exciting . . . Exciting
	Bulgurcu *et al.* (2009a)	*not available*	*not available*
	Bulgurcu *et al.* (2009b)	*not available*	*not available*
	Bulgurcu *et al.* (2010)	To me, complying with the requirements of the ISP is:	Unnecessary . . . Necessary
		To me, complying with the requirements of the ISP is:	Unbeneficial . . . Beneficial
		To me, complying with the requirements of the ISP is:	Unimportant . . . Important
		To me, complying with the requirements of the ISP is:	Useless . . . Useful
	Dinev *et al.* (2009)	Adapted from Hu and Dinev (2007)	*not available*
	Herath and Rao (2009b)	Adopting security technologies and practices is important	Strongly Agree . . . Strongly Disagree
		Adopting security technologies and practices is beneficial	Strongly Agree . . . Strongly Disagree
		Adopting security technologies and practices is helpful	Strongly Agree . . . Strongly Disagree
	Herath *et al.* (2012)	I am likely to continue using eAuth for e-mail screening	*not available*
		I plan to use eAuth for e-mail screening	*not available*
		It is possible that I will continue using eAuth for e-mail screening	*not available*
		I predict that I would use eAuth for e-mail screening	*not available*

(*continued*)

Table AI.

Variable	Author(s)	Item	Scale
	Hu and Dinev (2007)	For me, cleaning spyware from my computer would be:	Very Bad Idea … Very Good Idea
		For me, preventing spyware from self-installing on my computer would be:	Very Bad Idea … Very Good Idea
		For me, protecting my computer from spyware would be:	Very bad idea … Very good idea
	Hu *et al.* (2012)	I believe that it is beneficial for an organization to establish clear ISPs, practices and technologies	Strongly Disagree … Strongly Agree
		I believe that it is useful to for an organization to enforce its ISPs, practices and technologies	Strongly Disagree … Strongly Agree
		I believe that it is a good idea for an organization to establish clear ISPs, practices and technologies	Strongly Disagree … Strongly Agree
	Ifinedo (2012)	Following the organization's ISSP is a good idea	Strongly Agree … Strongly Disagree
		Following the organization's ISSP is a necessity	Strongly Agree … Strongly Disagree
		Following the organization's ISSP is beneficial	Strongly Agree … Strongly Disagree
		Following the organization's ISSP is pleasant	Strongly Agree … Strongly Disagree
	Limayem and Hirt (2003)	The use of WebBoard is smart	Strongly Agree … Strongly Disagree
		The use of WebBoard is enjoyable	Strongly Agree … Strongly Disagree
		The use of WebBoard is boring	Strongly Agree … Strongly Disagree
		The use of WebBoard is pleasant	Strongly Agree … Strongly Disagree

(*continued*)

Table AI.

Variable	Author(s)	Item	Scale
	Pahnila *et al.* (2007a)	*not available*	*not available*
	Zhang *et al.* (2009)	*not available*	*not available*
	Xue *et al.* (2011)	I am _____ with my use of ERP	Extremely Displeased … Extremely Pleased
		I am _____ with my use of ERP	Extremely Frustrated … Extremely Contented
		I am _____ with my use of ERP	Extremely Terrible … Extremely Delighted
		I am _____ with my use of ERP	Extremely Dissatisfied … Extremely Satisfied
BI	Al-Omari *et al.* (2012b)	I intend to comply with the requirements of the ISP of my organization	*not available*
		I intend to protect information resources according to the requirements of the ISP of my organization	*not available*
		I intend to protect technology resources according to the requirements of the ISP of my organization	*not available*
		I intend to carry out my responsibilities prescribed in the ISP of my organization when I use information resources	*not available*
		I intend to carry out my responsibilities prescribed in the ISP of my organization when I use technology resources	*not available*
		I intend to recommend that others comply with ISP	*not available*
		I intend to assist others in complying with ISP	*not available*
	Bulgurcu *et al.* (2009a)	*not available*	*not available*
	Bulgurcu *et al.* (2009b)	*not available*	*not available*

(*continued*)

Table AI.

Variable	Author(s)	Item	Scale
	Bulgurcu *et al.* (2010)	I intend to comply with the requirements of the ISP of my organization in the future	Strongly Agree ... Strongly Disagree
		I intend to protect information and technology resources according to the requirements of the ISP of my organization in the future	Strongly Agree ... Strongly Disagree
		I intend to carry out my responsibilities prescribed in the ISP of my organization when I use information and technology in the future	Strongly Agree ... Strongly Disagree
	D'Arcy *et al.* (2009)	*not available*	*not available*
		Adapted from Leonard and Cronan (2001)	*not available*
	Dinev *et al.* (2009)	Adapted from Hu and Dinev (2007)	*not available*
	Herath and Rao (2009a)	I am likely to follow organizational security policies	Strongly Agree ... Strongly Disagree
		It is possible that I will comply with organizational ISPs to protect the organization's IS	Strongly Agree ... Strongly Disagree
		I am certain that I will follow organizational security policies	Strongly Agree ... Strongly Disagree
	Herath and Rao (2009b)	I am likely to follow organizational security policies	Strongly Agree ... Strongly Disagree
		It is possible that I will comply with organizational ISPs to protect the organization's IS	Strongly Agree ... Strongly Disagree
		I am certain that I will follow organizational security policies	Strongly Agree ... Strongly Disagree
	Hovav and D'Arcy (2012)	If you were Taylor, what is the likelihood that you would have sent the e-mail?	Very Unlikely ... Very Likely
		I could see myself sending the e-mail if I were in Taylor's situation:	Strongly Disagree ... Strongly Agree

(*continued*)

Table AI.

Variable	Author(s)	Item	Scale
	Hu and Dinev (2007)	I intend to periodically use anti-spyware applications to protect my computer from spyware	Strongly Agree ... Strongly Disagree
		In the immediate future, I intend to customize my browser and computer settings to prevent the intrusion of spyware to my computer	Strongly Agree ... Strongly Disagree
		I intend to periodically check my browser and computer settings to prevent the intrusion of spyware to my computer	Strongly Agree ... Strongly Disagree
	Hu *et al.* (2012)	I intend to follow the ISPs and practices at work	Strongly Disagree ... Strongly Agree
		I intend to use the information security technologies at work	Strongly Disagree ... Strongly Agree
		I intend to use common sense on good information security practices at work	Strongly Disagree ... Strongly Agree
	Ifinedo (2012)	It is my intention to continue to comply with the organization's ISSP	Strongly Agree ... Strongly Disagree
		I am certain I will adhere to my organization's ISSP	Strongly Agree ... Strongly Disagree
		It is possible that I will comply with the organization's ISSP to protect the organization's IS	Strongly Agree ... Strongly Disagree
		I am likely to follow the organization's ISSP in the future	Strongly Agree ... Strongly Disagree
		I would follow the organization's security policy whenever possible	Strongly Agree ... Strongly Disagree
	Johnston *et al.* (2010)	*not available*	*not available*

(*continued*)

Table AI.

Variable	Author(s)	Item	Scale
	Limayem and Hirt (2003)	How many times do you intend to access WebBoard during a week for the next month?	Not at All … Several Times Each Day
		How many messages do you intend to post on WebBoard during a week for the next month?	Not at All … Several Times Each Day
	Pahnila *et al.* (2007a)	*not available*	*not available*
	Pahnila *et al.* (2007b)	*not available*	*not available*
	Siponen *et al.* (2007)	Adapted from Prasad and Agarwal (1998)	*not available*
	Siponen *et al.* (2010)	I intend to comply with ISPs	*not available*
		I intend to recommend that others comply with ISPs	*not available*
		I intend to assist others in complying with ISPs	*not available*
		What is the chance that you would do what [the scenario character] did in the described scenario?	*not available*
	Xue *et al.* (2011)	I intend to comply with the ERP operating standard of my company	Strongly Agree … Strongly Disagree
		My intentions are to comply with the ERP operating standard of my company	Strongly Agree … Strongly Disagree
		If I could, I would not like to comply with the ERP operating standard of my company	Strongly Agree … Strongly Disagree
AB	Limayem and Hirt (2003)	How many times have you accessed WebBoard during a week for the last month?	Not at All … Several Times Each Day
		How many messages have you posted on WebBoard during a week for the last month?	Not at All … Several Times Each Day
	Pahnila *et al.* (2007a)	*not available*	*not available*
	Pahnila *et al.* (2007b)	*not available*	*not available*
	Siponen *et al.* (2007)	Adapted from Limayem and Hirt (2003)	*not available*

(*continued*)

Table AI.

Variable	Author(s)	Item	Scale
	Siponen *et al.* (2010)	I comply with ISPs	Strongly Agree ... Strongly Disagree
		I recommend others to comply with ISPs	Strongly Agree ... Strongly Disagree
		I assist others in complying with ISPs	Strongly Agree ... Strongly Disagree
PBC	Al-Omari *et al.* (2012b)	I have the necessary skills to fulfill the requirements of the ISP	*not available*
		I have the necessary knowledge to fulfill the requirements of the ISP	*not available*
		I have the necessary competencies to fulfill the requirements of the ISP	*not available*
		I would feel comfortable following my organization's ISP on my own	*not available*
		If I wanted to, I could easily comply with my organization's ISP on my own	*not available*
		I would be able to follow most of ISP even if there was no one around to help me	*not available*
	Bulgurcu *et al.* (2010)	I have the necessary skills to fulfill the requirements of the ISP	Almost Never ... Almost Always
		I have the necessary knowledge to fulfill the requirements of the ISP	Almost Never ... Almost Always
		I have the necessary competencies to fulfill the requirements of the ISP	Almost Never ... Almost Always
	Dinev *et al.* (2009)	*not available*	*not available*
	Herath and Rao (2009b)	I would feel comfortable following most of the ISPs on my own	Strongly Agree ... Strongly Disagree
		If I wanted to, I could easily follow ISPs on my own	Strongly Agree ... Strongly Disagree
		I would be able to follow most of the ISPs even if there was no one around to help me	Strongly Agree ... Strongly Disagree

(*continued*)

Table AI.

Variable	Author(s)	Item	Scale
	Herath *et al.* (2012)	It is easy for me to verify an e-mail as coming from authentic sender based on "from line" and "subject line"	*not available*
		I feel comfortable in my abilities to identify e-mails that may be forged based on "from line" and "subject line"	*not available*
		I feel confident in my abilities to identify e-mails that are authentic based on "from line" and "subject line"	*not available*
		I feel confident in my abilities to determine whether the identities of e-mails are real based on "from line" and "subject line"	*not available*
		I feel comfortable in my abilities to identify e-mails that may be useful to me based on "from line" and "subject line"	*not available*
		I feel confident in my abilities to identify e-mails that are relevant to me based on "from line" and "subject line"	*not available*
		I feel confident in my abilities to identify malicious e-mails, such as phishing e-mails, based on "from line" and "subject line"	*not available*
		I feel confident in my abilities to identify e-mails that are detrimental based on "from line" and "subject line"	*not available*
	Hu and Dinev (2007)	Please rate the difficulty for you to clean spyware from your computer using anti-spyware applications	Extremely Difficult … Extremely easy
		Please rate the difficulty for you to protect your computer from spyware	Extremely Difficult … Extremely easy
	Hu *et al.* (2012)	I am able to follow the policies and procedures and use the security technologies	Strongly Disagree … Strongly Agree
		I have the resources and knowledge to follow the policies and procedures and use the security technologies	Strongly Disagree … Strongly Agree
		I have adequate training and skills to follow the policies and procedures and use the security technologies	Strongly Disagree … Strongly Agree

(*continued*)

Table AI.

Variable	Author(s)	Item	Scale
	Ifinedo (2012)	I have the necessary skills to protect myself from information security violations	Strongly Agree ... Strongly Disagree
		I have the expertise to implement preventative measures to stop people from getting my confidential information	Strongly Agree ... Strongly Disagree
		I have the skills to implement preventative measures to stop people from damaging my work computer	Strongly Agree ... Strongly Disagree
		I believe that it is within my control to protect myself from information security violations	Strongly Agree ... Strongly Disagree
		I can enable security measures on my work computer but only when I have manuals for reference	Strongly Agree ... Strongly Disagree
		For me, taking information security precautions is:	Hard ... Easy
		My ability to prevent information security violations at my workplace is:	Inadequate ... Adequate
	Johnston *et al.* (2010)	*not available*	*not available*
	Limayem and Hirt (2003)	I have a good understanding of how to use WebBoard	Strongly Agree ... Strongly Disagree
		I have easy access to the Internet	Strongly Agree ... Strongly Disagree
		I have inexpensive access to the Internet	Strongly Agree ... Strongly Disagree
		I have a fast Internet connection	Strongly Agree ... Strongly Disagree
		Assistance provided by WebBoard experts is adequate	Strongly Agree ... Strongly Disagree
		I am too busy to use WebBoard	Strongly Agree ... Strongly Disagree

(*continued*)

Table AI.

Variable	Author(s)	Item	Scale
	Pahnila *et al.* (2007a)	*not available*	*not available*
	Siponen *et al.* (2007)	*not available*	*not available*
	Siponen *et al.* (2010)	I can comply with ISPs by myself	Strongly Agree ... Strongly Disagree
		I can use information security measures if I can call for help if I get stuck	Strongly Agree ... Strongly Disagree
		I can use information security measures if someone tells me what to do as I go along	Strongly Agree ... Strongly Disagree
	Zhang *et al.* (2009)	*not available*	*not available*
SN	Al-Omari *et al.* (2012b)	Upper level management thinks I should comply with the requirements of my organization's ISPs	*not available*
		My boss thinks that I should comply with the requirements of my organization's ISPs	*not available*
		My colleagues think that I should comply with the requirements of my organization's ISPs	*not available*
		The information security/technology department in my organization thinks that I should comply with the requirements of my organization's ISPs	*not available*
		Other computer technical specialists in the organization think that I should comply with the requirements of my organization's ISPs	*not available*
	Dinev *et al.* (2009)	Adapted from Hu and Dinev	*not available*
	Herath and Rao (2009a)	Top management thinks I should follow organizational ISPs	Strongly Agree ... Strongly Disagree
		My boss thinks that I should follow organizational IS security policies	Strongly Agree ... Strongly Disagree

(*continued*)

Table AI.

Variable	Author(s)	Item	Scale
	Herath and Rao (2009a)	My colleagues think that I should follow organizational IS security policies	Strongly Agree ... Strongly Disagree
		The information security department in my organization thinks that I should follow organizational IS security policies	Strongly Agree ... Strongly Disagree
		Computer technical specialists in the organization think that I should follow organizational security policies	Strongly Agree ... Strongly Disagree
	Herath and Rao (2009b)	Top management thinks I should follow organizational IS security policies	Strongly Agree ... Strongly Disagree
		My boss thinks that I should follow organizational IS security policies	Strongly Agree ... Strongly Disagree
		My colleagues think that I should follow organizational IS security policies	Strongly Agree ... Strongly Disagree
		The information security department in my organization thinks that I should follow organizational IS security policies	Strongly Agree ... Strongly Disagree
		Computer technical specialists in the organization think that I should follow organizational security policies	Strongly Agree ... Strongly Disagree
	Hu and Dinev (2007)	Most people who are important to me think it is a good idea to clean spyware from my computers	Strongly Agree ... Strongly Disagree
		Most people who are important to me think it is a good idea to prevent spyware from running on my computer	Strongly Agree ... Strongly Disagree
	Hu *et al.* (2012)	People who are influential to me would think that I should follow the policies and procedures and use the security technologies	Strongly Disagree ... Strongly Agree
		People who are important to me would think that I should follow the policies and procedures and use the security technologies	Strongly Disagree ... Strongly Agree
		People whom I respect would think that I should follow the policies and procedures and use the security technologies	Strongly Disagree ... Strongly Agree

(*continued*)

Table AI.

Variable	Author(s)	Item	Scale
	Ifinedo (2012)	My boss thinks that I should follow the organization's ISSP	Strongly Agree ... Strongly Disagree
		My colleagues think that I should follow the organization's ISSP	Strongly Agree ... Strongly Disagree
		My organization's IT department pressures me to follow the organization's ISSP	Strongly Agree ... Strongly Disagree
		My subordinates think I should follow them organization's ISSP	Strongly Agree ... Strongly Disagree
	Johnston *et al.* (2010)	*not available*	*not available*
	Limayem and Hirt (2003)	The use of WebBoard has become a habit for me	Strongly Agree ... Strongly Disagree
		I am addicted to using WebBoard	Strongly Agree ... Strongly Disagree
		I must use WebBoard	Strongly Agree ... Strongly Disagree
		I don't even think twice before using WebBoard	Strongly Agree ... Strongly Disagree
		Using WebBoard has become natural to me	Strongly Agree ... Strongly Disagree
	Pahnila *et al.* (2007a)	*not available*	*not available*
	Pahnila *et al.* (2007b)	*not available*	*not available*
	Siponen *et al.* (2010)	Top management thinks I should comply with ISPs	Strongly Agree ... Strongly Disagree
		My immediate supervisor thinks I should comply with ISPs	Strongly Agree ... Strongly Disagree

(*continued*)

Table AI.

Variable	Author(s)	Item	Scale
		My peers think I should comply with ISPs	Strongly Agree ... Strongly Disagree
		Information security personnel in the organization think I should comply with ISPs	Strongly Agree ... Strongly Disagree
	Zhang *et al.* (2009)	*not available*	*not available*
PEOU	Herath *et al.* (2012)	My interaction with eAuth tool is clear and understandable	*not available*
		Interacting with eAuth tool does not require a lot of my mental effort	*not available*
		I find eAuth tool easy to use	*not available*
	Hu and Dinev (2007)	The process of configuring my computer to protect from spyware is clear and understandable	Strongly Agree ... Strongly Disagree
		It would be easy for me to prevent spyware from running on my computer	Strongly Agree ... Strongly Disagree
	Hu and Dinev (2007)	It would be easy for me to clean my computer from spyware	Strongly Agree ... Strongly Disagree
	Xue *et al.* (2011)	My interaction with ERP is clear and understandable	Strongly Agree ... Strongly Disagree
		Interacting with ERP does not require a lot of my mental effort	Strongly Agree ... Strongly Disagree
		I find ERP to be easy to use	Strongly Agree ... Strongly Disagree
		I find it easy to get ERP to do what I want it to do	Strongly Agree ... Strongly Disagree
	Dinev *et al.* (2009)	Adapted from Hu and Dinev (2007)	*not available*
PU	Dinev *et al.* (2009)	Adapted from Hu and Dinev (2007)	*not available*
	Herath *et al.* (2012)	Using eAuth service enables me to accomplish the task of e-mail authenticity check more quickly	*not available*

(*continued*)

Variable	Author(s)	Item	Scale
		Using eAuth service helped improve identifying authentic e-mails	*not available*
		Using eAuth service enhances my effectiveness of detecting authentic e-mails	*not available*
		Using eAuth service gives me greater control over e-mail authenticity check	*not available*
	Xue *et al.* (2011)	Using ERP improves my performance in my job	Strongly Agree ... Strongly Disagree
		Using ERP in my job increases my productivity	Strongly Agree ... Strongly Disagree
		Using ERP enhances my effectiveness in my job	Strongly Agree ... Strongly Disagree
		I find ERP to be useful in my job	Strongly Agree ... Strongly Disagree
PCOS	D'Arcy *et al.* (2009)	Taylor would probably be caught, eventually, after sending the e-mail:	Strongly Agree ... Strongly Disagree
		The likelihood the organization would discover that Taylor sent the e-mail is:	Very Low ... Very High
	Herath and Rao (2009a)	Employee computer practices are properly monitored for policy violations	Strongly Agree ... Strongly Disagree
		If I violate organization security policies, I would probably be caught	Strongly Agree ... Strongly Disagree
	Herath and Rao (2009b)	Employee computer practices are properly monitored for policy violations	Strongly Agree ... Strongly Disagree
		If I violate organization security policies, I would probably be caught	Strongly Agree ... Strongly Disagree
	Hovav and D'Arcy (2012)	Jordan would probably be caught, eventually, after installing the software	Strongly Agree ... Strongly Disagree
		The likelihood the organization would discover that Jordan installed the software is:	Very Low ... Very High

(*continued*)

Table AI.

Table AI.

Variable	Author(s)	Item	Scale
	Xue *et al.* (2011)	Employees violating expectations of ERP operations would be disciplined	Strongly Agree … Strongly Disagree
		Employees failing to abide by ERP policies would be disciplined	Strongly Agree … Strongly Disagree
		People not conforming to the ERP operating standard would be disciplined	Strongly Agree … Strongly Disagree
		Even minor violations of ERP operating standard would get an employee disciplined	Strongly Agree … Strongly Disagree
PSOS	D'Arcy *et al.* (2009)	If caught sending the e-mail, Taylor would be severely reprimanded:	Strongly Agree … Strongly Disagree
		If caught sending the e-mail, Taylor's punishment would be:	Not Severe at All … Very Severe
	Herath and Rao (2009a)	The organization disciplines employees who break information security rules	Strongly Agree … Strongly Disagree
		My organization terminates employees who repeatedly break security rules	Strongly Agree … Strongly Disagree
		If I were caught violating organization ISPs, I would be severely punished	Strongly Agree … Strongly Disagree
	Herath and Rao (2009b)	The organization disciplines employees who break information security rules	Strongly Agree … Strongly Disagree
		My organization terminates employees who repeatedly break security rules	Strongly Agree … Strongly Disagree
		If I were caught violating organization ISPs, I would be severely punished	Strongly Agree … Strongly Disagree

(*continued*)

Table AI.

Variable	Author(s)	Item	Scale
	Hovav and D'Arcy (2012)	If caught sending the e-mail, Taylor would be severely reprimanded:	Strongly Agree … Strongly Disagree
		If caught sending the e-mail, Taylor's punishment would be:	Not Severe at All … Very Severe
S	Siponen *et al.* (2007)	Adapted from Hair *et al.* (2006)	*not available*
	Pahnila *et al.* (2007a)	*not available*	*not available*
	Siponen *et al.* (2010)	What is the chance you would receive sanctions if you violated the company ISP?	*not available*
		What is the chance that you would be formally sanctioned if management learned that you had violated company ISP?	*not available*
		What is the chance that you would be formally reprimanded if management learned you had violated company ISP?	*not available*
		How likely is it that you would lose the respect and good opinion of your co-workers for violating the company ISP?	*not available*
		How likely is it that you would jeopardize your promotion prospects if management learned that you had violated company ISP?	*not available*
		How likely is it that you would lose the respect and good opinion of your manager, if management learned that you had violated company IT security policies?	*not available*
CA	Pahnila *et al.* (2007a)	*not available*	*not available*
RC	Ifinedo (2012)	There are too many overhead costs associated with implementing IS security measures in my organization	Strongly Agree … Strongly Disagree
		Enabling IS security measures in my organization is/would be time consuming	Strongly Agree … Strongly Disagree

(*continued*)

Table AI.

Variable	Author(s)	Item	Scale
		The inconvenience of implementing recommended ISP measures is:	Lower than the Benefits … Exceeds the Benefits
		The cost of implementing recommended security policy measures is:	Lower than the Benefits … Exceeds the Benefits
		The impact of the organization's IS security measures on my work is:	Lower than the Benefits … Exceeds the Benefits
RE	Ifinedo (2012)	Enabling the security measures on my work computer is an effective way to deter hacker attacks	Strongly Agree … Strongly Disagree
		Enabling security measures at my workplace will prevent hackers from gaining access to important personal or financial information	Strongly Agree … Strongly Disagree
		At my work, efforts to ensure the safety of my confidential information are:	Ineffective … Effective
		The effectiveness of available measures to protect my organization's information from security violations are:	Ineffective … Effective
		The preventative measures available to me to stop people from gaining access to my organization's information are:	Inadequate … Adequate
		The preventative measures available to me to prevent people from damaging my IS at work are:	Inadequate … Adequate
	Johnston *et al.* (2010)	*not available*	*not available*
	Pahnila *et al.* (2007a)	*not available*	*not available*
	Siponen *et al.* (2010)	The information security personnel in our organization keep information security breaches down	Strongly Agree … Strongly Disagree
		Complying with ISPs in our organization keeps information security breaches down	Strongly Agree … Strongly Disagree
		Having ISPs in our organization keeps information security breaches down	Strongly Agree … Strongly Disagree

(*continued*)

Table AI.

Variable	Author(s)	Item	Scale
PSOT	Ifinedo (2012)	I believe that protecting my organization's information is:	Unimportant ... Important
		Having someone successfully attack and damage my computer at work is:	Harmless ... Harmful
		Threats to the security of my organization's information are:	Harmless ... Harmful
		I view information security attacks on my organization as:	Harmless ... Harmful
		In terms of security risks at work, the vulnerability of my computer and data is:	Very low ... Very high
		At work, having my confidential information accessed by someone without my consent or knowledge is a serious problem for me	Strongly Agree ... Strongly Disagree
		Loss of data resulting from hacking is a serious problem for me	Strongly Agree ... Strongly Disagree
PV	Ifinedo (2012)	I know my organization could be vulnerable to security breaches if I don't adhere to its ISP	Strongly Agree ... Strongly Disagree
		I could fall victim to a malicious attack if I fail to comply with my organization's ISP	Strongly Agree ... Strongly Disagree
		I believe that trying to protect my company's information will reduce illegal access to it	Strongly Agree ... Strongly Disagree
		My organization's data and resources may be compromised if I don't pay adequate attention to guidelines	Strongly Agree ... Strongly Disagree
		The likelihood of an information security violation occurring at my workplace is:	Likely ... Unlikely
		The likelihood of someone damaging my organization's computer systems is:	Likely ... Unlikely
		My organization's information and data is vulnerable to security breaches:	Likely ... Unlikely

(*continued*)

Table AI.

Variable	Author(s)	Item	Scale
TA	Herath *et al.* (2012)	My decision to open e-mails is risky	*not available*
		Opening e-mail will lead to high potential for loss	*not available*
		There is considerable risk involved in potential consequence of opening e-mails	*not available*
		Opening e-mails will lead to considerable risks	*not available*
	Pahnila *et al.* (2007a)	Adapted from Rogers and Prentice-Dunn (1997)	*not available*
	Pahnila *et al.* (2007b)	Adapted from Rogers and Prentice-Dunn (1997)	*not available*
	Siponen *et al.* (2007)	Adapted from Rogers and Prentice-Dunn (1997)	*not available*
	Siponen *et al.* (2010)	An information security breach in my organization would be a serious problem for me	Strongly Agree ... Strongly Disagree
		An information security breach in my organization would be a serious problem for my organization	Strongly Agree ... Strongly Disagree
		Information security breaches are becoming more and more serious	Strongly Agree ... Strongly Disagree
		I could be subjected to a serious information security threat	Strongly Agree ... Strongly Disagree
		My organization could be subjected to a serious information security threat	Strongly Agree ... Strongly Disagree