JOURNAL OF INFORMATION TECHNOLOGY THEORY AND APPLICATION

ISSN: 1532-3416

Factors that Affect the Success of Security Education, Training, and Awareness Programs: A Literature Review

Denitsa Kirova
Chair of Information Management
University of Hagen
denitsa.kirova@fernuni-hagen.de

Ulrike Baumöl
Chair of Information Management
University of Hagen
ulrike.baumoel@fernuni-hagen.de

Abstract:

Preventing IT security incidents poses a great challenge for organizations. Today, senior managers allocate more resources to IT security programs (especially those programs that focus on educating and training employees) in order to reduce human misbehavior—a significant cause of IT security incidents. Building on the results of a literature review, we identify factors that affect the success of security education, training, and awareness (SETA) programs and organize them in a conceptual classification. The classification contains human influencing factors derived from different behavioral, decision making, and criminology theories that lead to IT security compliance and noncompliance. The classification comprehensively summarizes these factors and shows the correlations between them. The classification can help one to design and develop SETA programs and to establish suitable conditions for integrating them into organizations.

Keywords: Organizational Security, Security Compliant Behavior, Security Education, Training and Awareness, SETA.

1 Introduction

With the increasing reports of IT security incidents, practitioners and researchers have shown growing interest in IT security. Different surveys, such as the "Cyber Security Survey" (BSI, 2015), "2014: A Year of Mega Breaches" (Ponemon, 2015), and "The Global State of Information Security Survey" (PwC, 2014, 2015) have examined the influence of IT security incidents on organizations. The surveys show that the incidents have raised senior managers' concerns about IT security issues and involvement in IT security in general, which has led to increased organizational budgets for coping with IT security risks. In particular, organizations have allocated a significant part of these budgets to training and awareness programs (Ponemon, 2015; PwC, 2014, 2015) and to "specialized education for the IT security staff" because human misbehavior (BSI, 2015) and the lack of expertise (Ponemon, 2015) frequently cause IT security incidents. Consequently, organizations have a need for IT security education, training, and awareness (SETA) programs, which focus on educating employees such that they act according to certain IT security principles and goals (Kayworth & Whitten, 2010; Thomson & von Solms, 1998).

Researchers have recognized the need for such programs many years before today (Thomson & von Solms, 1998), and several studies have criticized the technical orientation of many existing and commonly used IT security programs (e.g., Baker & Wallace, 2007; Choobineh, Dhillon, Grimaila, & Rees, 2007; Siponen, 2005). These studies have concluded that we need more research on securing the human factor since human beings represent the "weakest link" in an IT security system (Bowen, Hash, & Wilson, 2006; Sasse, Brostoff, & Weirich, 2001). Consequently, effective IT security management should consider both technological and socio-organizational measures, and SETA programs constitute an important part of the latter (Kayworth & Whitten, 2010). Literature reviews also show that SETA programs constitute a critical success factor of effective IT security management (Alnatheer, 2015; Tu & Yuan, 2014). However, the surveys we mention above indicate that current SETA programs have not achieved the desired success, and other researchers have made similar observations (e.g., Zhang, Reithel, & Li, 2009). These programs can fail due to issues in the programs themselves or because organizations insufficiently integrate them into their overall IT security programs.

In order to identify reasons for why SETA programs fail to succeed, we systematically reviewed the literature on factors that affect their success. In doing so, we concentrated on factors that influence individuals to comply or not comply with organizational IT security. These factors serve as the starting point for designing, developing, and integrating SETA programs since the factors predefine these programs' characteristics and features. Additionally, we focus on theories that explain and classify relevant factors that affect the success of SETA programs. We do so because the lack of theory-grounded approaches to create SETA programs may represent one reason for their ineffectiveness (Puhakainen & Siponen, 2010). Thus, our review extends the literature review that Aurigemma and Panko (2012) conducted on theories on human behavior in the IT security context but that concentrated only on human behavior related to information security policy compliance. Additionally, in our review, we synthesize relevant factors that affect the success of SETA programs in a conceptual classification due to the fact that many isolated factors influence individuals' IT security behavior that individually deliver only a fragmented picture of possible causal effects. Classifying them in a proper way will better explain the correlations between them.

This paper proceeds as follows: in Section 2, we explain the research methodology we used to conduct our review. In Section 3, we present the theories that research has used to explain human behavior in the IT security context and classify relevant factors that affect the success of SETA programs. In Section 4, we summarizing the paper's main contributions, discuss its limitations, and suggest directions for future research.

Contribution:

We conducted a systematic literature review on factors that explain individuals' compliant and noncompliant behavior in the IT security context. As such, we contribute to existing knowledge on the topic with a conceptual classification and discuss future research directions. The conceptual classification comprehensively summarizes relevant factors that affect the success of security education, training, and awareness (SETA) programs that we derived from different theories and found empirical evidence for. Furthermore, the paper discusses the dependencies and the influencing directions between the factors and suggests implications for SETA programs. Researchers and practitioners in the organizational IT security management field should find interest in this paper. Both parties can use our findings in designing, developing, and implementing SETA programs. Additionally, the paper outlines research directions that target researchers who want to advance research on the topic.

2 Methodology

A literature review gathers, analyzes, and synthesizes the existing knowledge on a certain topic (Cooper, 1988). One can conduct such a review to, among other things, show inconsistencies in the existing literature, identify research gaps, derive a research agenda, or develop a conceptual framework or a classification of constructs (Torraco, 2005; Webster & Watson, 2002). In this study, we focus on the latter: on developing a conceptual classification of the factors that influence human behavior in the IT security context. Our literature review builds on vom Brocke et al.'s (2009) framework. The framework comprises five steps: 1) define the review scope, 2) conceptualize the topic, 3) search the literature, 4) analyze and synthesize the literature, and 5) propose research agenda. However, we focus only on the first four steps since, as Torraco (2005) notes, the fifth step simply represents one possible way to synthesize the literature. As we explain in Section 1, we focus on another form of synthesis (i.e., conceptually classifying constructs). Nevertheless, we provide an agenda for future research in Section 4.

2.1 Review Scope

To define the review's scope, we used an established taxonomy from Cooper (1988) that vom Brocke et al. (2009) recommend. In our review, we focused on research outcomes (i.e., identified factors that affect whether SETA programs succeed) and on theories that explain and classify these factors. Additionally, we concentrated on empirical studies because we wanted to include only empirically evaluated factors in our classification since SETA programs also need empirical evidence to succeed (Puhakainen & Siponen, 2010). We conducted the review in order to integrate the outcomes in a conceptual classification. As such, we organize the review conceptually. We take a neutral perspective since we focus on integrating different positions. Further, we consider the coverage of our review as representative of the literature in which researchers investigate human behavior in the context of IT security by using different theories. We used a sound process to identify this literature, which we explain in Section 2.3. The target audience for the review includes general scholars interested in the topic and scholars specialized in IT security management. Table 1 highlights the categories relevant for this review.

Table 1. Positioning of This Review in Cooper's Taxonomy of Literature Reviews (Cooper, 1988)

Characteristic	Categories			
Focus	Research outcomes	Research methods	Theories	Applications
Goal	Integration	Criticism	Central issues	
Organization	Historical	Conceptual	Methodological	
Perspective	Neutral representation		Espousal of position	
Coverage	Exhaustive	Exhaustive with selective citation	Representative	Central or pivotal
Audience	Specialized scholars	General scholars	Practitioners	General public

2.2 Topic Conceptualization

Conceptualizing a review's topic allows one to organize the review in a coherent way since doing so provides "working definitions of the key terms" (vom Brocke et al., 2009, p. 8), information on what is known about the topic, and a conceptual structure (Torraco, 2005). Following these recommendations, we start with explaining the key terms in our review.

SETA programs provide individuals with general IT security knowledge and skills to cope with IT security issues properly and knowledge of an organization's IT security policy (D'Arcy, Hovav, & Galletta, 2009; Wilson & Hash, 2003). As a result, a security policy represents a precondition for an organization's SETA program (Whitman, 2003). Generally, a policy refers to "a communication document from management" that determines what action the organization's stakeholders take (ISACA, 2015, p. 71; von Solms & von Solms, 2004; Whitman & Mattord, 2012, p. 177). An IT security policy defines rules, instructions, roles, and responsibilities for an organization's members to protect its IT and the consequences in case individuals violate the IT security policy (Whitman & Mattord, 2012, p. 177). Organizations define their general IT security policies at the strategic management level, and they need to concretize or expand them into "lower-level" policies that generally handle a specific issue or system in a detailed manner

(Swanson & Guttman, 1996, p. 13 ff.; von Solms, Thomson, & Maninjwa, 2011; Whitman & Mattord, 2012, p. 179 ff.).

Little research has examined the effects and effectiveness of SETA programs. Puhakainen and Siponen (2010) investigated several awareness program approaches for information systems (IS) security policy compliance and found that most lacked a theoretical ground and empirical evidence of practical applicability, which, they argued, may constitute reasons for their ineffectiveness. Based on these findings, they proposed and empirically tested a theory-based program for IS security policy compliance training. The test's results suggest that both content-related characteristics (e.g., how comprehensively the program describes issues, how difficult employees find using the security techniques it mandates) and environmental factors (e.g., whether top management becomes involved in the program and how well the organization integrates the program as a continuation process) influence program success. D'Arcy et al. (2009) created a model for IT security awareness and tested it empirically on about 200 computer users. They found that SETA programs deter users from misusing IT since it helps them to develop awareness about the consequences they may experience if caught doing so. Tarwireyi, Flowerday, and Bayaga (2011) examined the competency of university students regarding password management and found that, even though students were familiar with password-management policies, many did not comply with them. Therefore, the authors suggest that the success of awareness programs depends on two main factors (i.e., human skills/knowledge and human behavior) and that the skills and knowledge are a prerequisite for the behavior. Parsons, McCormac, Butavicius, Pattinson, and Jerram (2014) examined the relationship between knowledge, attitude and behavior in the information security field and concluded that individuals' knowledge about information security policies and procedures positively influences their attitude towards policy and procedures and that both good knowledge and attitudes lead to a more risk-reverse behavior. Knowledge alone turned out to have a weak effect on behavior. Therefore, the authors suggest that SETA programs should contain both knowledge-related components that refer to how an employee should act and attitude-related components that refer to why they should act in the expected way (Parsons et al., 2014, pp. 165, 174). Maqousi, Balikhina, and Mackay (2013) suggest that, in order for a SETA program to be effective, one should individually tailor it to a specific group of people or organization. According to these authors, group- and organization-specific factors lead people to react differently to a program. Therefore, in developing a SETA program, one should follow a certain approach that begins with analyzing the specific human and organizational factors in the organization one develops the program for and that also contains maintenance and measurement processes to keep the program up to date and measure its success.

The above studies show that we can divide the research on SETA programs into two main streams: 1) a stream that investigates human behavior and, in particular, the factors that lead to security compliant or noncompliant behavior and 2) a stream that deals with processes for developing SETA programs. In our paper, we focus on the first stream and, therefore, need a suitable framework to structure relevant factors that affect the success of SETA programs. As we explain above, organizations implement SETA programs to achieve certain human behaviors (e.g., report identified security risks) through influencing two main factors: knowledge (e.g., by explaining what security risks are) and motivation (e.g., by awarding reports on identified security risks). The knowledge, attitude and behavior (KAB) model represents one suitable framework that integrates these factors. Researchers have used the KAB model in different areas but generally to measure educational effects or performance improvement (Schrader & Lawless, 2004). Parsons et al. (2014) also use it as their theoretical base. We use its three constructs—knowledge, attitude, and behavior—as the main dimensions for our classification.

2.3 Literature Search

Following Levy and Ellis' (2006) and vom Brocke et al.'s (2009) recommendations for concentrating on qualitative literature, we restricted our search to peer-reviewed journal and conference papers. For this search, which we conducted in May and June, 2016, we used the databases Web of Science and EBSCOhost because they contain highly ranked IS journals and conference proceedings. However, in addition to papers from the IS research domain, we also included the behavioral and organizational research domains in the search because we considered them relevant for the topic. Specifically, we searched the title, keyword, and abstract fields with the keyword combination "('information security' OR 'information technolog* security' OR 'information system* security') AND human AND (incident* OR accident* OR breach* OR error* OR *behavior)". We limited the search to papers published from 2006 to 2016. From this search, we obtained 96 hits (Web of Science: 53, EBSCOhost: 43). We removed 23 duplicates and irrelevant papers based on reading their title and/or abstract, which left 63 papers

remaining. From these 63 papers, only 16 discussed theory-grounded factors. However, two of those 16 papers did not empirically evaluate the factors, so we dropped them. As a result, 14 papers remained.

Although the databases Web of Science and EBSCOhost index high-quality journal and conference papers, the 14 papers we identified as relevant came from only journals. Therefore, we conducted a second search using the AIS Electronic Library (AISeL) data that, in addition to established IS journal papers, also contains the leading IS conference proceedings (e.g., International Conference on Information Systems (ICIS), European Conference on Information Systems (ECIS), Pacific Asia Conference on Information Systems (PACIS), Hawaii International Conference on System Sciences (HICSS)). We conducted this second search in December, 2017. We limited the search to papers published from 2006 to 2017. We initially obtained 87 hits. After reviewing their titles and abstracts, we dropped 59 papers, which left 28 for further consideration. At this point, we excluded further six papers because they did not fulfill our defined criteria (most only proposed a research model without testing it empirically or did not ground their model with theory). We also conducted a third search to update our first one: we followed the same procedure for the first search as we explain above but expanded the timeframe to the end of 2017. As a result, we obtained six further journal papers. Thus, the second and third searches added 28 papers in total to the initial 14. Altogether, we considered 42 papers (22 conference and 20 journal papers) for the final analysis.

3 Literature Analysis and Synthesis

In Section 3.1, we review the theories that the papers we analyzed used. The Section 3.2, we use the KAB model to classify relevant factors that affect the success of SETA programs.

3.1 Relevant Theories

The studies we reviewed used 27 theories to explain various IT security-related behaviors. The theory of planned behavior (TPB), the most frequently used theory, appeared in 14 papers. Following that, the deterrence theory (DT) and the protection motivation theory (PMT) appeared in nine papers each. Rational chance theory (RChT) and reactance theory (RT) appeared in three papers each. As for the remaining 22 theories, 11 appeared in two papers each, and the other 11 appeared in only one paper each. Table 2 lists the theories, briefly describes them, and notes how many times papers used them.

Table 2. Theories Used to Explain IT Security Behavior in the Literature

Theory	Description	Times used
Theory of planned behavior (TPB)	According to the TPB, intention is the main predecessor of behavior and describes the motivation to behave in a certain manner. TPB assumes that "the stronger the intention to engage in a behavior, the more likely should be its performance" (Ajzen, 1991, p. 181). The constructs attitude towards behavior, subjective norm, and perceived behavioral control explain intention itself. The TPB extends the TRA: it adds perceived behavior control to the explaining factors of intention (Ajzen, 1991).	14
Deterrence theory (DT)	DT, sometimes also referred to as general deterrence theory (GDT), postulates that humans take actions based on rational decisions, which requires them to know the possible consequences of their actions. In its basic form, DT stipulates that punishment (which the theory explains with the three components certainty, severity, and celerity) as a consequence of an illegal action has a negative influence on an individual's motivation to execute an action and, thus, works as deterrence (Akers, 1990). Researchers have continuously refined DT over the years by adding further components to punishment, such as formal and informal sanctions and as rewards, to explain not only illegal but also noncompliant or undesired behavior (Akers, 1990; Paternoster & Simpson, 1996).	9
Protection motivation theory (PMT)	PMT deals with motivating individuals to adopt recommended responses that come from messages that focus on preventing noxious events from occurring. The theory suggests that individuals adopt a recommended response based on the amount of protection motivation. Thus, the perception of threat, which threat severity and occurrence probability describe, and the perception of efficacy of the recommended response influence protection motivation (Rogers, 1975).	9
Rational choice theory (RChT)	RChT suggests that individuals make rational decisions to take illegal or noncompliant action by balancing the perceived costs and benefits of the action in question (Paternoster & Simpson, 1996).	3
Reactance theory (RT)	RT suggests that "people become motivationally aroused by a threat to or elimination of a behavioral freedom" (Brehm, 1989, p. 72). As a result, individuals try to restore their freedom, which can lead to undesired behavior (Brehm, 1989).	3
Theory of reasoned action (TRA)	TRA, a predecessor of the TPB, explains intention just with two factors: attitude and subjective norms (Ajzen, 1991).	2

Table 2. Theories Used to Explain IT Security Behavior in the Literature

General theory of crime (GTC)	The theory posits that individuals with low self-control are more likely to engage in criminal acts than individuals with high self-control (Akers, 1991).	2
Social cognitive (learning) theory (SCT)	In the SCT, three categories of factors (behavioral patterns, environmental influences, and internal personal factors) and the causal, bi-directional relationships between them explain human behavior (Bandura, 2001).	2
Neutralization theory (NT)	NT suggests that people justify (or neutralize) their criminal or deviant behavior by applying different neutralization techniques (also called rationalizations) (Sykes & Matza, 1957).	2
(Organizational) Control theory (CT)	CT explains the main different forms of organizational control and the conditions under which these forms occur (Ouchi & Maguire, 1975).	2
Knowledge, attitude and behavior (KAB) model	The model explains the relationship between its constructs (knowledge, attitude, and behavior) (Schrader & Lawless, 2004).	2
Health belief model (HBM)	"The HBM hypothesizes that health-related action depends upon...three classes of factors: 1) ...Sufficient motivation (or health concern) to make health issues salient or relevant. 2) The belief that one is susceptible (vulnerable) to a serious health problem.... This [belief] is often termed perceived threat. 3) The belief that following a particular health recommendation would be beneficial in reducing the perceived threat, and at a subjectively-acceptable cost. Cost refers to perceived barriers that must be overcome in order to follow the health recommendation" (Rosenstock, Strecher, & Becker, 1988, p. 177).	2
Self-determination theory (SDT) / organismic integration theory (OIT)	The theory suggests that "if external prompts are used by significant others...to encourage people to do an uninteresting activity…, the individuals will tend to internalize the activity's initially external regulation. ...People will tend to take in the regulation and integrate it with their sense of self." (Deci & Ryan, 2002, p. 15).	2
Extended parallel process model (EPPM)	EPPM is a fear appeal theory that explains the relationship between threat and efficacy of the response to the threat. The theory "claims that perceived efficacy determines whether *danger control* accesses or *fear control* processes are initiated, and perceived threat determine the intensity of these responses. ...Danger control processes are primarily cognition processes where individuals evaluate their susceptibility to the threat, the severity of the threat, their ability to perform the recommended response (perceived self-efficacy), and the effectiveness of the recommended response (perceived response efficacy). ...Fear control processes are defined as primarily emotional processes where people respond to and cope with their fear, not to danger." (Witte, 1992, p. 337 f.).	2
Organizational climate (OC)	Organizational climate refers to "the shared meaning organizational members attach to the events, policies, practices, and procedures they experience and the behaviors they see being rewarded, supported, and expected…. It helps [them to] understand important effectiveness outcomes that are conceptually seen to emerge from the climate." (Ehrhart, Schneider, & Macey, 2014, p. 2 f.).	2
Technology acceptance model (TAM)	TAM tries to explain the causes of individuals' accepting or rejecting technology. It uses two determinates for this reason: perceived usefulness (PU) (i.e., "the extent they believe it will help them perform their job better") and perceived ease of use (PEOU) (i.e., "the degree to which a person believes that using a particular system would be free of effort") (Davis, 1989, p. 320).	2
Expectancy-value theory (EVT)	According to EVT, beliefs about the consequences of performing a certain behavior and the evaluation of these consequences form the attitude towards the behavior (Fishbein & Ajzen, 1975, p. 30 f.).	1
Involvement theory (IT)	Researchers have used involvement theories in different domains, which has resulted in different conceptual models for explaining involvement (Andrews, Durvasula, & Akhter, 1990; Astin, 1999; Huang, Chou, & Lin, 2010). The theories suggest that the level of involvement influences an individual's motivation and, thus, the level of engagement in a certain act.	1
Risk compensation/ homeostasis theory (RCT)	In RCT, also called risk homeostasis theory, two variables (target level of risk (i.e., the level of risk individuals consider acceptable or are willing to take) and perceived level of risk) explain individuals' risk-taking behavior. The theory suggests that, if a discrepancy between the two variables exists, individuals will adjust their behavior to eliminate the discrepancy. (Wilde, 1998)	1
Causal reasoning theory (CRT)	CRT explains counterproductive or deviant behavior based on the cognitive processing of workplace events. The cognitive processing comprises two stages: 1) an individual perceives some type of disequilibrium (e.g., injustice or inequity) and 2) the individual makes an attribution for the disequilibrium. If the individual assigns external and stable reasons to the disequilibrium, then the individual is more likely to engage in counterproductive behavior (Martinko, Gundlach, & Douglas, 2002).	1

Table 2. Theories Used to Explain IT Security Behavior in the Literature

Elaboration likelihood model (ELM)	ELM deals with how individuals process messages. According to it, when people have to react to a persuasive message, they can take one of two possible routes: the central or peripheral route. Individuals take the central route when they have the motivation to and can scrutinize a message. Individuals take the peripheral route when they lack the motivation and/or the ability to scrutinize a message. As such, factors that lie in the persuasion context (e.g., number of arguments, attractive source) influence the peripheral route (Petty & Cacioppo, 1986).	1
Preventive adoption model (PAM)	PAM describes the antecedents of individual intentions to engage in preventive information security behaviors. It integrates constructs from preventive health behavior theories (specifically from the PMT and the HBM) and the TPB with constructs from the IS technology acceptance literature (Wynn, Karahanna, Williams, & Madupalli, 2012, p. 5).	1
Structural empowerment model (SEM)	SEM suggests that "power is derived from the structural conditions in an organization". Such structural conditions include "access to opportunity, access to information, and participation in decision-making" (Talib & Dhillon, 2015, p. 5).	1
Transformational leadership (TL)	TL "involves inspiring followers to commit to a shared vision and goals for an organization" (Bass & Riggio, 2006, p. 4).	1
Expectancy valence theory (EVcT)	The theory suggests that motivation explains choices an individual makes among different voluntary responses. Individuals make choices based on valence (i.e., „affective orientations towards particular outcomes") and outcome expectancy (i.e., the probability that the outcomes will result from a particular act) (Vroom, 1964, p. 15-17).	1
Dual-task interference (DTI)	DTI refers to individuals' inability to perform two tasks concurrently. The "tasks [can] interfere with each other quite drastically, even though they are neither intellectually challenging nor physically incompatible" (Pashler, 1994, p. 220).	1
Agency theory (AT)	AT tries to explain the agency relationship in which one party (the principal) delegates work to another (the agent) who performs that work. The theory "is concerned with resolving two problems that can occur in agency relationships. The first is the agency problem that arises when (a) the desires or goals of the principal and agent conflict and (b) it is difficult or expensive for the principal to verify what the agent is actually doing." (Eisenhardt, 1989, p. 58).	1

3.2 Classifying Relevant Factors

As we state in Section 2.2, we use the KAB model as a framework to classify the factors that affect the success of SETA programs. We found that a significant number of papers focused on explaining the two KAB model constructs attitude and behavior. However, the majority concentrated on another factor—intention—to explain human compliance or noncompliance in the context of IT security (see Table A1). Two reasons may explain why so many papers concentrated on intention rather than on behavior or attitude. First, according to the TPB, which researchers have widely used to explain human behavior in general and in the specific context of IT security, intention is the main predecessor of behavior (Ajzen 1991). Second, one cannot easily empirically evaluate actual behavior. While one can test intention using questionnaires with a rather large sample of people, objective evaluating actual behavior requires one to observe people's activities—a difficult task (Bulgurcu, Cavusoglu, & Benbasat, 2010). Questionnaire-based empirical (self-reporting) tests on actual behavior are problematic because individuals naturally avoid reporting deviant behavior (Chu, Chau, & So, 2015; Hu, Xu, Dinev, & Ling, 2011). Intention, however, cannot sufficiently predict actual behavior because having the intention to comply with organizational IT security does not necessarily mean that actual compliant behavior will occur (Komatsu, Takagi, & Takemura, 2013; Merritt & Dhillon, 2016). Due to these reasons, we extend the KAB model by adding intention as a fourth dimension (see Figure 1).

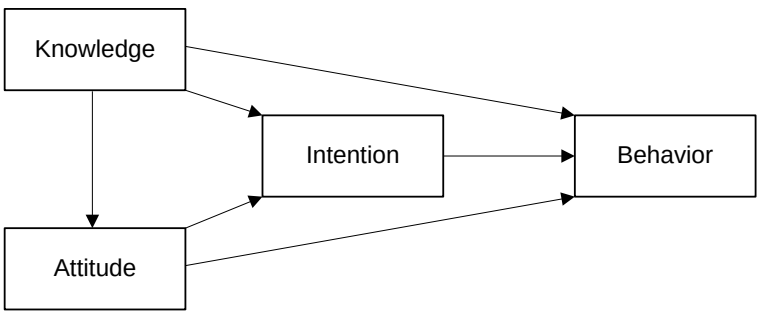

Figure 1. Knowledge, Attitude, Intention, and Behavior Model

In Sections 3.2.1 to 3.2.4, we explain which factors in the literature influence each dimension (i.e., knowledge, attitude, intention, and behavior) in the extended model. In doing so, we also depict the relations and the influencing directions between the different factors. We summarize the analysis in Tables 3 to 6. The tables include factors with both a direct and indirect impact on each dimension. Additionally, we propose several subdimensions that apply only to the factors with a direct impact. With this classification, we provide a comprehensive view of relevant factors that affect the success of SETA programs. Therefore, it contains duplicates (i.e., factors that influence more than one dimension or have both a direct or indirect impact appear more than once).

3.2.1 Factors that Influence Knowledge

As we explain in Section 2, SETA programs provide individuals with general IT security knowledge and skills to cope with IT security issues properly and knowledge about an organization's IT security policy. Previous research in different domains has shown that knowledge alone has a rather weak effect on behavior (Schrader & Lawless, 2004). In the IT security domain in particular, Tarwireyi et al. (2011) and Parsons et al. (2014) have also shown the same weak correlation between knowledge and behavior, which may explain why most of the literature we reviewed concentrated on motivational factors in connection to attitude and intention rather than on knowledge. However, based on the results in the studies we reviewed, we can see that several factors play an important role in increasing learning effects. We can divide these factors into two main groups: 1) factors that focus on SETA programs' content and 2) factors that pertain to creating and distributing knowledge. Responsibility represents an important factor related to SETA programs' content (Alhogail, Mirza, & Bakry, 2015; Johnston, Warkentin, & Siponen, 2015; Siponen & Vance, 2010). Information about responsibilities should describe not only the responsibilities themselves but also how the organization will monitor and control activities related to these responsibilities and how it will sanction and reward compliant and noncompliant behavior (Alhogail et al., 2015). A SETA program should provide this information in a persuasive and comprehensible way, which means that it needs to consider the comprehension level of an organization's members (Alhogail et al., 2015; Komatsu et al., 2013). Furthermore, such a program should use respectful language to deliver the information; otherwise, reactance can occur (Lowry & Moody, 2015). Further, this information should clearly define employees' role vis-à-vis technical measures in order to reduce the negative impact that perceived technical protection has on behavior (Zhang et al., 2009), which we explain more in Section 3.2.3.

Sohrabi Safa, von Solms, & Furnell (2016) identified four factors that, when in an organization, increase its employees' information security awareness and knowledge: knowledge sharing, collaboration, intervention and experience. Knowledge sharing refers to distributing skills, knowledge, and experience. In addition to distributing knowledge, collaboration refers to reviewing and commenting on it to improve its quality. Intervention refers to participation in rather informal meetings and group discussions that focus on sharing knowledge and experience. Unlike approaches (e.g., formal presentations, posters, messages and e-mails), which involve one-way communication, active participation and group processes can improve IT security awareness among employees in the short term and, thus, lead to changes in their security behavior (Albrechtsen & Hovden, 2010). Experience with security incidents and with measures to deal with the incidents provides an important source of knowledge. An organization can increase the experience that employees gain by letting them actively participate in IT security (Sohrabi Safa et al., 2016). Therefore, a SETA program should motivate and provide a suitable platform for an organization's members to enable them to share knowledge, collaborate, intervene in security-related issues, and gain experience. Table 3 summarizes the factors that influence knowledge.

Table 3. Factors that Influence Knowledge

Dimension	Subdimension	Factor with direct influence
Knowledge	Content	Role and responsibilities of individuals Role of technical measures Consequences Persuasiveness Comprehensibility Respectful language
	Creation/distribution	Knowledge sharing Collaboration Intervention Experience

3.2.2 Factors that Influence Attitude

Attitude, a construct of human behavior, refers to the degree to which an individual favorably or unfavorably evaluates a certain behavior (Ajzen, 1991). In the context of IT security compliance, the study of Sohrabi Safa et al. (2016) identified three relevant factors that can influence attitude: involvement in security issues, commitment to organizational policies and plans, and personal norms. Based on the context in which they conducted their study, the authors defined the latter as beliefs in the importance of organizational information assets (Sohrabi Safa et al., 2016).

Bulgurcu et al. (2010) identified two categories of factors that influence attitude towards security compliance. The first category, which has a direct impact on attitude, comprises individual's beliefs about the individual's overall assessment of the consequences of compliance and noncompliance. This category has three underlying factors: perceived benefit of compliance, perceived cost of compliance, and perceived cost of noncompliance. The second category, beliefs about the outcomes of compliance and noncompliance, influence the first category. Intrinsic benefit (e.g., satisfaction, accomplishment, fulfillment), safety (which refers to making information resources safe), and rewards all affect perceived benefit of compliance. Kajtazi and Bulgurcu (2013) also showed that safety has a direct positive effect on compliance attitude. According to Bulgurcu et al. (2010), the factor work impediment affects perceived cost of compliance and refers to the perception that compliance can hinder business functioning. However, Kajtazi and Bulgurcu (2013) found results that partially contradict these findings since they could not find empirical evidence that work impediment has a direct negative impact on employees' compliance attitude. As for perceived costs of noncompliance, relevant influencing factors include punishment, intrinsic cost (which in this case involve guilt, embarrassment, shame), and vulnerability of information resources (Bulgurcu et al., 2010).

Researchers have also found two other factors to be positively associated with individuals' attitude towards information security: 1) organizational information security culture (i.e., the shared beliefs and values among colleagues in the workplace concerning information security) (Rocha Flores & Ekstedt, 2016) and 2) individuals' perceived fairness of security policies' requirements (Bulgurcu, Cavusoglu, & Benbasat, 2009).

The OIT focuses on explaining individuals' motivations in a specific context. It distinguishes between:

> *Extrinsic motivation including external regulation as measured by the construct external [perceived locus of causality (PLOC)]…and identification and integration as measured by internal PLOC…. The more an extrinsic motivation is internalized, the more autonomous an individual will perceive her/his behavior.* (Kranz & Haeussinger, 2014, p. 3)

In the context of information security compliance, an external PLOC means that an individual complies due to external pressure (e.g., sanctions) and an internal PLOC means that an individual complies due to the individual's own values and personal beliefs. Kranz and Haeussinger (2014) found both internal and external PLOC to positively influence individuals' compliance attitude.

Several studies also investigated another important factor; namely, awareness. As we state earlier in the paper, among their goals, SETA programs focus on raising individuals' IT security awareness. Information security awareness (Al-Omari & El-Gayar, 2012; Bauer & Bernroider, 2017; Bulgurcu et al., 2010; Rocha Flores & Ekstedt, 2016) and technology awareness (Al-Omari & El-Gayar, 2012; Dinev & Hu, 2007) are significant predecessors of individuals' attitude towards applying security measures and complying with security policies.

The factors we have identified for this dimension show the correlation between knowledge and attitude: in order to positively influence individuals' attitude toward compliance with organizational IT security, certain knowledge should exist (i.e., knowledge about security policies and knowledge about the importance of information and IT assets to the organization). This knowledge can enable individuals to create an opinion about the possible consequences of their actions and, thus, form an attitude towards compliance or noncompliance. Individuals can achieve knowledge via training, which research has also found to have a positive direct effect on attitude (Jenkins & Durcikova, 2013). An organization needs to adequately and equally inform all individuals because information asymmetry has a negative effect on their security compliance attitude (Kajtazi & Bulgurcu, 2013).

Table 4. Factors that Influence Attitude

Dimension	Subdimension	Factor with direct influence	Factor with indirect influence / explaining factor
Attitude		Knowledge Involvement Commitment Personal norms Awareness (of information security and technology) Training Information asymmetry Organizational information security culture Perceived fairness (of the requirements of security policies) Internal and external perceived locus of causality	
	Beliefs about overall assessment of consequences	Perceived benefit of compliance	Intrinsic benefit Safety (of IT resources) Rewards
		Perceived cost of compliance	Work impediment
		Perceived cost of noncompliance	Intrinsic cost Punishment Vulnerability (of IT resources)
		Safety	

3.2.3 Factors that Influence Intention

As we explain in Section 3.2, the majority of papers we examined studied intention more than any other behavior construct in the context of IT security compliance. Zhang et al. (2009) and Bulgurcu et al. (2010) tested the influence that the TPB constructs attitude, subjective norms (also referred to as normative beliefs (Bulgurcu et al. 2010)), and perceived behavioral control had on the intention to comply with security policies. Subjective norms describe "the perceived social pressure to perform or not to perform [a certain] behavior" and perceived behavior control means "the perceived ease or difficulty of performing the behavior" (Ajzen, 1991, p. 188). Researchers have found that attitude (Al-Omari & El-Gayar, 2012; Bauer & Bernroider, 2017; Bulgurcu et al., 2010; Jenkins & Durcikova, 2013; Kranz & Haeussinger, 2014; Rocha Flores & Ekstedt, 2016), subjective norms (Al-Omari & El-Gayar, 2012; Bauer & Bernroider, 2017; Bulgurcu et al., 2010; Jenkins & Durcikova, 2013; Kim & Kim, 2017; Kranz & Haeussinger, 2014; Rocha Flores & Ekstedt, 2016; Wynn et al., 2012), and perceived behavior control (Bulgurcu et al., 2010; Jenkins & Durcikova, 2013) have a significant influence on the intention to perform preventive security behaviors and comply with security policies. However, another study found that subjective norms and attitude did not significantly influence the intention to misuse IT resources (Chu et al., 2015).

Whereas Zhang et al. (2009) formulate two underlying factors to explain perceived behavior control (perceived availability of resources and self-efficacy), Bulgurcu et al. (2010) argue that self-efficacy can solely replace perceived behavior control because they measure the same construct. The latter define self-efficacy as an individual's judging whether the individual has the necessary skills and knowledge to perform the behavior in question. For our classification, we use both explaining factors that Zhang et al. (2009) suggest because we consider that, in addition to knowledge and skills, the availability of resources such as time and technical support can positively influence the intention to comply with organizational IT security. Additionally, many studies have confirmed that self-efficacy influences intention (Al-Omari & El-Gayar, 2012; Johnston et al., 2015; Johnston, Wech, Jack, & Beavers, 2010; Kranz & Haeussinger, 2014; Nguyen & Kim, 2017; Rocha Flores & Ekstedt, 2016; Warkentin, Johnston, Walden, & Straub, 2016). However, some studies have not found support for it (Pahnila, Karjalainen, & Siponen, 2013; Putri & Hovav, 2014; Wynn et al., 2012).

Similar to the factor perceived availability of resources and perceived costs of compliance (which we discuss in connection with attitude), perceived response costs influence the intention such that, when an

individual perceives the costs to perform a secure behavior as low, the individual will be more likely to perform the behavior (Warkentin, Mcbride, Carter, & Johnston, 2012). The perception of response efficacy is also a significant predecessor of intention in that, if an individual perceives that the individual can effectively implement security measures or comply with security policies, then a positive intention towards these behaviors will arise (Johnston et al., 2015; Komatsu et al., 2013; Pahnila et al., 2013; Putri & Hovav, 2014; Warkentin et al., 2016; Wynn et al., 2012).

Perceived psychological empowerment derived from SEM also represents another factor that positively influences the intention to comply with security policies (Talib & Dhillon, 2015). Empowerment refers to "increased intrinsic task motivation" (Thomas & Velthouse, 1990, p. 666). In the context of security compliance, individuals can achieve psychological empowerment via SETA programs, access to information regarding security strategies and goals, and participate in security decision making.

Johnston et al. (2015) argue that the perception of threat should include both threat to IT/information assets and threat to the individual in order for the PMT to apply in the IT security context because noncompliance to IT security poses a threat first to the IT/information assets and the PMT deals with threats to an individual. Therefore, the term perceived threat refers to the threat to IT/information assets, whereas sanctions describe the threat to the individual.

Johnston et al. (2015) and Pahnila et al. (2013) found that perceived threat severity had a strong effect on the intention to implement security policies and perform security measure, whereas Warkentin et al. (2016) and Wynn et al. (2012) could not find evidence for a strong influence. Some studies have also found perceived threat susceptibility (also referred to as perceived threat vulnerability) to have a significant effect on the policy violation intention (Johnston, Warkentin, McBride, & Carter, 2016; Warkentin et al., 2016), and while others found that it had no significant impact (Warkentin et al., 2012).

Concerning the perception of one's own actions, Wynn et al. (2012) show that the perceived compatibility of a security behavior with an individual's work practices and the perceived ease of use of security behaviors positively influence the intention to perform secure behavior. These results partially contradict what Dinev and Hu (2007) found: that both TAM constructs, perceived usefulness and perceived ease of use, had no significant influence on the intention to use protective technologies. Reflective autonomy, which positively influences security policy compliance intention, represents another relevant factor in this context. The reflective autonomy construct comes from SDT/OIT and "refers to an individual's belief that his/her actions are self-guided through considerate thought and reflection" (Wall & Palvia, 2013, p. 1).

Zhang et al. (2009) identified another relevant factor that they call perceived technical security protection. They argue that one should not examine human behavior independently of technical security measures and, based on the RCT, hypothesize that perceived technical security protection has a negative impact on human security compliance intention because the perception of more protection leads to one to behave less cautiously. If, for instance, an organization introduced additional technical security measures to a system that individuals already considered secure, it would make individuals behave less carefully (Stewart, 2004). In their empirical analysis, Zhang et al. (2009) found both that perceived technical protection had both a positive (indirect via influencing perceive behavioral control) and negative (direct) effect on intention.

Researchers identified perceived benefit of noncompliance, a complex factor, to significantly influence intention in the context of IT security compliance. The benefit can be either intrinsic or extrinsic, though perceived intrinsic benefit has a greater effect on intention than extrinsic (Hu et al., 2011). Moral beliefs and self-control influence perceived benefit of noncompliance (Hu et al., 2011). Moral belief, another construct of the RChT (e.g., in the model of Paternoster and Simpson (1996)), formulates intention independently of individuals' belief about the outcomes (costs and benefits) of certain behavior. Moral beliefs describe an individual's evaluation or judgment about whether a certain behavior is right or wrong (Paternoster & Simpson, 1996). Hu et al. (2011) found that moral beliefs negatively influenced the perceived intrinsic benefit of noncompliance and, thus, had a positive influence on the intention to comply. Similar to moral beliefs, the factor internal PLOC (which we discuss already in Section 3.2.2 in connection to attitude) had a positive effect on the intention to comply with security policies (Kranz & Haeussinger, 2014). Gottfredson and Hirschi's (1995) GTC uses self-control as a main construct to explain criminal behavior. As Table 2 describes, the theory posits that individuals with low self-control are more likely to engage in criminal acts than individuals with high self-control (Akers, 1991). Low self-control refers to "the inability to consider the long-term consequences of one's act" (Gottfredson & Hirschi, 1995, p. 32) and

positively influences the perceived benefit of noncompliance and, thus, has a negative effect on the intention to comply (Hu et al., 2011).

The DT focuses on the next relevant factor we identified for this domain: deterrence. Siponen and Vance (2010) examined the influence that formal sanctions (e.g., punishment, codes of ethics), informal sanctions (e.g., disapproval of peers), and shame had on employees' intention to violate organizational security policies and concluded that only informal sanctions had a significant influence. In addition, D'Arcy et al. (2009) identified perceived certainty and perceived severity of sanctions as relevant factors that influence employees' intention to misuse information systems but that perceived severity had a greater influence than perceived certainty. These results concur with both Johnston et al.'s (2015) and Hu et al.'s (2011) results: the former found that informal sanction severity and certainty had a significant influence on intention, and the latter found that formal sanction (specifically punishment) severity, formal sanction certainty, and shame had no significant impact on intention. Additionally, without distinguishing between formal and informal sanctions, Ifinedo (2016), Johnston et al. (2016), and Warkentin et al. (2012) found that sanction severity had a positive influence on the compliance intention and a negative effect on the policy violation intention. Further, Johnston et al. (2016) confirmed that high sanction certainty had a negative effect on the policy violation intention.

User awareness of security policies, SETA programs, and computer monitoring represent further deterrence techniques that significantly influence the perception of sanctions and, thus, the intention to misuse IS (D'Arcy et al., 2009). Furthermore, information security awareness (Johnston et al., 2010) and technology awareness (Dinev & Hu, 2007) have positive effects on compliance intention and the intention to use protective technologies, respectively. In the context of security awareness and knowledge, Kim and Kim (2017) tested the influence that compliance knowledge had on compliance intention. They defined this factor as "an employee's judgment of personal skills and knowledge about fulfilling the requirements of the laws and regulations" (p. 990) and found that it had a positive effect on the intention.

However, interpersonal and organizational factors can strongly affect the impact that deterrence and especially sanctions have on intention (Siponen & Vance, 2010). NT provides one group of such factors. Siponen and Vance (2010) identified six relevant neutralization techniques in the security violation context: denial of responsibility, denial of injury, defense of necessity, condemnation of the condemners (i.e., neutralizing actions by blaming the target of the actions, such as violating information security policies because they are unreasonable), appeal to higher loyalties (e.g., violating policy in order to get work done), and the metaphor of the ledger (i.e., compensating bad acts with good acts, such as compensating occasional violation of security policies with general adherence to them). With the presence of these techniques, sanctions lose their significant influence on the violation intention, which means that neutralization has a significant impact on the intention to violate security policies (Siponen & Vance, 2010) or on noncompliant intention (Bauer & Bernroider, 2017).

Researchers derived three further factors from the CT: organizational formal control, mandatoriness, and reactance (Lowry & Moody, 2015). Organizational formal control includes all formal structures and measures in an organization that serve to monitor, evaluate, and correct behavior in a desired direction (Lowry & Moody, 2015; Ouchi, 1979). Generally, an organizational IT security policy should define organizational formal control with regard to IT security. Mandatoriness refers to the degree to which individuals perceive (in this case IT security) policies and procedures as being compulsory (Boss, Kirsch, Angermeier, Shingler, & Boss, 2009). Reactance, which the RT explains, refers to a behavior or emotional state. Factors that can invoke reactance to a security policy include a threat to freedom that results from the policy and reactance proneness. Organizational formal control and mandatoriness can positively influence the intention to comply with security policies. However, noncompliance can arise from reactance if individuals experience security policies as a threat to freedom and if they are prone to reactance (Lowry & Moody, 2015; Putri & Hovav, 2014; Wall & Palvia, 2013).

By combing and extending PMT and HBM, Hwang, Kim, Kim, and Kim (2017) identified three further factors that had a negative effect on the intention to comply with security policies: work impediment, security system anxiety (which refers to the fear to use IS when an organization adopts excessively strict policies), and peer noncompliance. However, as Lebek, Guhr, and Breitner (2014) note, the following "positive" factors can confront these "negative" factors: transformational leadership, security motivation, and perceived organizational security climate. These authors found that these factors had a significant positive influence on employees' intentions to comply with security policies and participate in security activities. Transformational leadership means to inspire people to commit to an organization's vision and goals (see Table 2). Information security climate refers to "employees' perceptions of management and

organizational approaches to information security, which helps employees to make sense of the priority accorded to information security within the organization" (Lebek et al., 2014, p. 7). Ifinedo (2016) confirmed that organizational climate and, especially, top management support and beliefs related to security issues had a positive influence on compliance intention.

Table 5. Factors that Influence Intention

Dimension	Subdimension	Factor with direct influence	Factor with indirect influence / explaining factor
Intention		Attitude	
		Subjective/social norms	
		Perceived behavioral control	Perceived availability of resources
			Perceived self-efficacy
			Perceived technical security protection
		Perceived response efficacy	
		Perceived compatibility	
		Perceived ease of use	
		Perceived technical security protection	
		Perceived benefit of noncompliance	Intrinsic and extrinsic benefits
			Moral beliefs
			Self-control
		Internal PLOC	
		Perceived response costs	
		Perceived threat severity	
		Perceived threat susceptibility/ vulnerability	
		Perceived psychological empowerment	SETA programs
			Access to security strategies' information
			Participation in security decision making
		Reflective autonomy	
		Work impediment	
		Security system anxiety	
		Noncompliance of peers	
		Transformational leadership	
		Motivation	
		Perceived organizational security climate	Top management support and beliefs
		Trust in sender	IT skills
	Organizational control / deterrence	Organizational formal control	
		Mandatoriness (of IT security policies and procedures)	
		Reactance	Threat to freedom
			Reactance proneness
		Informal sanctions	Perceived certainty
			Perceived severity
		Awareness of security policies	
		SETA programs	
	Neutralization / rationalization	Denial of responsibility	
		Denial of injury	
		Defense of necessity	
		Condemnation of the condemners	
		Appeal to higher loyalties	
		The metaphor of the ledger	

Trust in sender represents the last factor we identified to have a strong impact on the intention to comply with IT security (Komatsu et al., 2013). Researchers derived the factor from the ELM, and it affects individuals with low IT skills. When individuals do not have the knowledge and skills necessary to evaluate a certain message (e.g., to implement a certain security measure), the trust they have in the sender of the message will positively influence their intention to fulfill what the message requests.

To sum up, intention represents a complex construct that SETA programs can only partially address because some influencing factors, such as self-control, are interpersonal aspects that develop at an early age and remain rather stable over the years (Gottfredson & Hirschi, 1995). Further, an individual's environment causes or affects other factors, such as moral beliefs, which means that such a program needs to implement different measures not connected to the IT security domain to change their influence in a desired direction. Nevertheless, we can derive several implications from analyzing the literature with regard to SETA programs. First, knowledge represents an important predecessor of intention, especially when a program provides employees with information and skills to implement certain measures, to understand the role of information and IT assets and how they can damage these assets, to understand the role of technical security protection, and to understand their individual responsibility. Control mechanisms, such as computer monitoring and sanctions, can also influence the intention. However, a program needs to clearly define these mechanisms' goals and roles and properly communicate them throughout the organization so that they will not motivate (e.g., through reactance) noncompliant behavior. Organizational conditions such as climate, top management support, peers' behavior represent crucial factors for whether a SETA programs will succeed because they significantly impact the intention to fulfill security requirements and goals.

3.2.4 Factors that Influence Behavior

Many theories across nearly all domains investigate behavior. The papers we reviewed applied 11 different theories (apart from the KAB model) to identify factors that directly affect behavior towards compliance or noncompliance with IT security. We can divide the relevant factors into three categories. The first category, which we call environmental factors, concerns an organization's environment and an individual's own private environment. The second category, which we call cognitive and interpersonal processes, concerns an individual's cognitive and interpersonal processes. Researchers derived these two categories from the SCT (Alhogail et al., 2015). However, other factors that affect behavior towards compliance and noncompliance with IT security and involve aspects related to both an individual's environmental context and cognitive processes exist as well. Since one cannot assign these factors to either the environmental or the cognitive category, we define a third category for these factors that we call perception of environmental influences.

Relevant environmental factors with a positive influence on behavior include culture (national and organizational), standards and regulations (in the security domain, which includes relevant government laws), practices (e.g., management support and involvement in information security issues), security policy (existence and comprehensiveness), and communication (Alhogail et al., 2015). Furthermore, formal organizational control (e.g., monitoring individuals' computer activities) has a positive influence on behavior because it can prevent deviant behavior (Ifinedo & Idemudia, 2017). Security systems, security education, and security visibility in an organization also have a positive effect on behavior through preventing noncompliant behavior (Hwang et al., 2017).

Other influencing factors include punishment and ethics training. Punishment certainty and severity have a negative influence on employees' participation in nonmalicious but deviant information security behavior (Ifinedo & Idemudia, 2017). Additionally, Workman and Gathegi (2007) examined how attitude towards the law, social norms (also called social influences), and self-control (instead of perceived behavioral control) influenced the effects that punishment and ethics training (i.e., approaches to deterrence) had on employees' participation in deviant information security behavior. They found that punishment effectively influenced individuals who followed rules to avoid negative consequences (i.e., their attitude toward the law) and had low self-control, whereas ethics training effectively influenced individuals who followed rules out of social conformity (i.e., their attitude toward the law and social norms) and had high self-control (Workman & Gathegi, 2007). As for whether perceived behavioral control has a direct impact on secure behavior, Merhi and Ahluwalia (2015) found that it did, but Jenkins and Durcikova (2013) did not.

Preparedness and responsibility represent two relevant factors of the cognitive and interpersonal processes category. Preparedness combines both aspects of knowledge and awareness in itself (Alhogail et al., 2015). Organizations can achieve it by using just-in-time reminders to overcome the effects of dual-

task interference (Jenkins & Durcikova, 2013) and by providing their employees with information with a good quality (Pahnila et al., 2013), which represent other environmental factors that influence secure behavior. We depict responsibility's importance in connection with knowledge and attitude in Section 3.2.1 and Section 3.2.2, respectively. In addition, Alhogail et al. (2015) found that individuals will not necessarily perform their responsibilities just because they know about them. In order for a desired behavior to occur, individuals should also accept their responsibilities, which means they should be willing to behave in accordance with their organization's information security policies and requirements. Furthermore, monitoring and control, affect responsibility, so an organization should properly implement them in order to not negatively impact behavior. An organization should also reward individuals who take responsibility and sanction those who deny it to motivate compliant behavior (Alhogail et al., 2015).

Risk propensity represents another relevant interpersonal factor. It refers to "an individual['s] current tendency to take risk" (p. 4950) and influences secure behavior negatively (Nguyen & Kim, 2017).

By combining the PMT and ELM, Komatsu et al. (2013) identified several factors that influence behavior, some of which we introduce earlier in the paper in connection with the other dimensions of our framework. They divide the factors into positive factors: negative factors and factors for collective coping behavior. Positive factors refer to factors that motivate an individual to cope with threats and involve perceived response efficacy and perceived self-efficacy. Chen (2017), Huang, Parolia, and Cheng (2016), Ng and Xu (2007) and Nguyen and Kim (2017) have also examined and established self-efficacy's positive effect on behavior. Negative factors refer to factors that invoke a perception of threat and involve perceived threat severity, perceived probability of occurrence/perceived susceptibility, and perceived cost (i.e., costs that can arise as a consequence of the threat to the organization, such as lost data) (Komatsu et al., 2013). From their empirical test, Komatsu et al. (2013) found that perceived threat severity and perceived costs promoted secure behavior. These results partially contradict to the results that Ng and Xu (2007) found: that perceived threat susceptibility but not perceived threat severity have a positive effect on secure behavior. Perceived threat severity and susceptibility generally trigger fear in individuals. High fear of the consequences of security threats impacts secure behavior negatively because it leads to inaction and avoidance of secure behavior (Chen, 2017). Additionally, Ng and Xu (2007) investigated individuals' perceived benefit of practicing computer security (which one can also refer to as perceived benefit of compliance) on secure behavior and found that it had a significant positive effect.

The third category (i.e., factors for collective coping behavior) assumes individuals collectively, not individually, cope with security issues in an organization and includes the responsibility and social norms that we present earlier and the perceived ratio of others implementing IT security measures (Komatsu et al., 2013). Merhi and Ahluwalia (2015) also confirmed that social norms have a positive effect on compliance behavior.

Further factors that influence actual behavior in the context of implementing IT security measures include persuasiveness of message and level of comprehension. Persuasiveness of message, an environmental factor, concerns the content of a message (e.g., a security policy) that comes from the organization. Level of comprehension, which concerns an individual's cognitive processes, depends on the IT skills and degree of an individual's involvement in security incidents. However, Komatsu et al. (2013) found that these factors influenced actual behavior only if intention was present, which suggests that intention influences actual behavior indirectly.

Perceived lack of attributed trust represents another factor in this dimension (Posey, Bennett, & Roberts, 2011). Attributed trust refers to "the degree with which an employee believes he or she is trusted by his or her organization" (Posey et al., 2011, p. 487). In the context of IT security, Posey et al. (2011) suggest that increased information security measures lead to employees' perceived lack of attributed trust and that perceived lack of attributed trust leads to deviant behavior, such as information or computer abuse. Environmental and interpersonal factors form perceived lack of trust. Relevant environmental factors include mechanistic organizational structure and perceived uncertainty of management style. Mechanistic organizational structure features high bureaucracy and less flexibility. Perceived uncertainty of management style pertains to an employee's beliefs "that management's future actions will be unpredictable, surprising, and filled with uncertainty" (Posey et al., 2011, p. 488). Relevant interpersonal factors include negative affectivity (i.e., which concerns constantly concentrate on the negative aspects of daily life) and external assignment tendency (i.e., individuals' tendency to assign negative events to others rather than themselves).

The factors we discuss in this section until now are mostly based on an individual's rational decision making process. However, an unintentional emotional act that occurs as a consequence of a desire to misuse can also cause noncompliant behavior. The desire to misuse, an interpersonal factor that attitude and perceived behavioral control impact, influences the behavior to misuse indirectly (through intention) and directly (Chu et al., 2015).

Table 6. Factors that Influence Behavior

Dimension	Subdimension	Factor with direct influence	Factor with indirect influence / explaining factor
Behavior	Environment	Culture	
		Standards and regulations	
		Practices	
		Security policy	
		Security systems	
		Security education	
		Security visibility	
		Communication	
		Punishment	Attitude towards law
			Self-control
			Attitude towards law and social norms
		Ethics training	
		Formal organizational control	
		Just-in-time reminders	
		Information quality	
		Persuasiveness of message	Intention
	Cognitive/interpersonal processes	Knowledge/preparedness	
		Perceived self-efficacy	
		Level of comprehension	Intention
			IT skills
			Involvement
		Responsibility	Acceptance of responsibility
			Monitoring and control
			Reward and sanctions
			Intention
		Fear	
		Desire	Attitude
			Perceived behavioral control
		Perceived benefit of compliance	
		Risk propensity	
		Intention	Desire
	Perception of environmental influences	Perceived lack of attributed trust	Perceived uncertainty of management style
			Mechanistic organizational structure
			Negative affectivity
			External assignment tendency
		Perceived social norms	Intention
		Perceived ratio of others	
		Perceived response efficacy	
		Perceived threat severity	
		Perceived cost	
		Perceived threat susceptibility	

Finally, three studies focused on the direct impact of intention on secure behavior with controversial results: Pahnila et al. (2013) and Bauer and Bernroider (2017) found a direct impact, whereas Jenkins and Durcikova (2013) found no empirical evidence for a direct impact.

From analyzing the literature for factors that directly affect security behavior, we can see that SETA programs provide a crucial means to change behavior. Organizations can achieve a positive and desirable change in their employees' behavior via SETA programs if they take into consideration the factors we discuss in this section and summarize in Table 6 when they design, develop, and implement such programs.

4 Conclusion and Research Agenda

While researchers have long recognized the importance of the human factor in the IT security context and the relevance of SETA programs for managing it, different studies and current events question how much one can control the human factor and SETA programs' effectiveness at doing so. In order for SETA programs to be effective, they should consider the factors that influence individuals to comply or not comply with IT security guidelines. In reviewing the literature, we found a significant number of such factors that researchers have derived from different behavioral, decision making, and criminology theories. However, we previously lacked work that has comprehensively reviewed and structured these factors. In order to fill this gap, we systematically reviewed the literature and synthesized the results to conceptually classify relevant factors that affect the success of SETA programs. The classification highlights the importance of knowledge, awareness, and responsibility, which SETA programs can and should address. However, it also contains environmental factors, such as management support and involvement, and interpersonal factors, such as desire and rationalization, which SETA programs can only partially address and, therefore, require additional measures. One can use our classification to derive fields of action and, thus, develop modules for SETA programs that one can subsequently adjust and integrate depending on the specific organizational context.

Our approach has several limitations. First, we concentrated on three databases when searching the literature. We found only journal papers in two of the databases (Web of Science and EBSCOhost), so we searched for papers from leading IS conferences in the third database. We did not consider conferences that have a special focus on IT security or are from the organizational or psychological research domains. Second, we only retained papers that contained theory-grounded and empirically evaluated factors and, thus, excluded papers that could have delivered further explanatory factors (e.g., Farahmand & Spafford, 2013; Willison & Warkentin, 2013).

Based on the findings of our review, we suggest two main directions for future research in the IT security compliance and SETA program domain.

4.1 Knowledge Creation and Distribution

Organizational information systems continue to become more complex for individuals and organizations need to provide IT security-related information that matches employees' comprehension level. Therefore, researchers should provide organizations with suitable approaches to measure their IT security comprehension. These approaches should measure general IT comprehension as a pre-stage to IT security comprehension. Thus, one needs to first operationalize the construct "comprehension" in the IT security context.

Proposition 1: How can one operationalize comprehension in the IT security context?

Proposition 2: How can one measure the level of IT security comprehension in an organization's employees?

Furthermore, as different levels of IT security comprehension require different approaches to create and distribute knowledge, we need research to investigate how suitably different knowledge creation and distribution approaches address different levels of comprehension. To successfully impart knowledge, one needs to balance information's difficulty for the recipient: in order to be intrinsically motivated, individuals need to feel empowered (Talib & Dhillon, 2015) through knowledge and not overstrained.

Proposition 3: What methods allow one to create and distribute IT security knowledge to individuals with low, medium, and high IT security understanding?

Another important research direction concerns the distribution of IT security knowledge internally and externally. Rashid, Zakaria, and Zulhemay (2013), for example, discuss the integration of information security and knowledge management and argue its importance for the effectiveness of information security. As such, one can regard the knowledge management field as a source for knowledge-creation and -distribution approaches, and research should further investigate its applicability to the IT security context. Considering that organizations can be unwilling to exchange IT security knowledge, we need to examine the reasons that prevent organizations and individuals from sharing their knowledge and develop methods to address them. Agrawal and Snekkenes (2017), for example, provide some promising findings in this direction.

Proposition 4a: How can an organization organize the way in which it distributes knowledge?

Proposition 4b: How can organizations stimulate and organize interfirm knowledge sharing?

4.2 Organizational Integration of SETA Programs

The second research direction we believe researchers need to follow involves how organizations integrate SETA programs. Generally, IT users consider IT security issues as the IT department's concern and responsibility. Thus, IT users can perceive participating in an organization's IT security program as additional work that costs much time an effort (Warkentin et al., 2012) or as a task that keeps them from doing their work (e.g., Bulgurcu et al., 2010). Thus, organizations need integration approaches that will lower the perceived negative influence of participating in SETA programs, which research in the literature often discusses as perceived costs of compliance.

Proposition 5: How can an organization integrate SETA programs into its employees' daily work so that they do not perceive such programs as burdensome?

A SETA program forms part of an organization's overall security program. As such, an organization should clearly define the SETA program's role in and connections to the remaining parts of the overall program and make such information transparent for the organization's members. As the literature we analyzed shows, organizations especially need to depict the interdependences between SETA programs and their security goals, strategies, procedures, policies, and technical security protection. A proper approach to achieve this goal could involve developing conceptual models.

Proposition 6: What interdependences exist between a SETA program and the remaining components of an overall organizational security program? How can one model these interdependences?

As many studies show, organizational climate and culture (which includes factors such as management style, support and attitude towards IT security, peers' involvement and attitudes, and organizational structure) have an important influence on security-related behavior. Therefore, research should also concentrate on how to create a proper climate, culture, and structures that support security-compliant behavior.

Proposition 7a: How can organizations achieve a security culture?

Proposition 7b: What does a security-promoting climate entail, and how can an organization achieve it?

Proposition 7c: What are security-promoting organizational structures, and how can organizations build them?

We plan to conduct future research in two directions. First, we plan to determine which factors we identified that SETA programs can address and to propose a suitable approach for designing, developing, and implementing SETA programs. Second, we plan to examine what additional measures organizations should take and how they should implement them to make SETA programs successful. To do so, we believe that we will require innovative and unconventional approaches (Ruighaver, Maynard, & Chang, 2007) because organizational information systems continue to become more complex and incomprehensible for individuals, which makes it difficult for organizations to keep their IT and IT security competency current through conventional educational and awareness programs.

References

Agrawal, V., & Snekkenes, E. A. (2017). An investigation of knowledge sharing behaviors of students on an online community of practice. In *Proceedings of the 5th International Conference on Information and Education Technology* (pp. 106-111).

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179-211.

Akers, R. L. (1990). Rational choice, deterrence, and social learning theory in criminology: The path not taken. *Journal of Criminal Law and Criminology*, *81*(3), 653-676.

Akers, R. L. (1991). Self-control as a general theory of crime. *Journal of Quantitative Criminology*, *7*(2), 201-211.

Al-Omari, A., & El-Gayar, O. (2012). Information security policy compliance: The role of information security awareness. In *Proceedings of the 18th Americas Conference on Information Systems* (pp. 1-10).

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers and Security*, *29*(4), 432-445.

Alhogail, A., Mirza, A., & Bakry, S. H. (2015). A comprehensive human factor framework for information security in organizations. *Journal of Theoretical and Applied Information Technology*, *78*(2), 201-211.

Alnatheer, M. A. (2015). Information security culture critical success factors. In *Proceedings of the 12th International Conference on Information Technology* (pp. 731-735).

Andrews, J. C., Durvasula, S., & Akhter, S. H. (1990). A framework for conceptualizing and measuring the involvement construct in advertising research. *Journal of Advertising*, *19*(4), 27-40.

Astin, A. W. (1999). Student involvement: A developmental theory for higher education. *Journal of College Student Development*, *40*(5), 518-529.

Aurigemma, S., & Panko, R. (2012). A composite framework for behavioral compliance with information security policies. In *Proceedings of the Annual Hawaii International Conference on System Sciences* (pp. 3248-3257).

Baker, W. H., & Wallace, L. (2007). Is information security under control? Investigating quality in information security management. *IEEE Security & Privacy*, *5*(1), 36-44.

Bandura, A. (2001). Social cognitive theory: An agentic perspective. *Annual Review of Psychology*, *52*(1), 1-26.

Bass, B. M., & Riggio, R. E. (2006). *Transformational leadership* (2nd ed.). Mahwah, NJ: Lawrence Erlbaum Associates.

Bauer, S., & Bernroider, E. W. N. (2017). From information security awareness to reasoned compliant action: Analyzing information security policy compliance in a large banking organization. *The DATA BASE for Advances in Information Systems*, *48*(3), 44-68.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & 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*, *18*(2), 151-164.

Bowen, P., Hash, J., & Wilson, M. (2006). Information security handbook: A guide for managers. Gaithersburg: National Institute of Standards and Technology.

Brehm, J. W. (1989). Psychological reactance: Theory and applications. *Advances in Consumer Research*, *16*(1), 72-75.

BSI. (2015). *Cyber-Sicherheits-Umfrage 2015: Ergebnisse*. Bonn: Allianz für Cyber-Sicherheit.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2009). Roles of information security awareness and perceived fairness in information security policy compliance. In *Proceedings of the 15th Americas Conference on Information Systems.*

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523-548.

Chen, Y. (2017). Examining Internet users' adaptive and maladaptive security behaviors using the extended parallel process model. In *Proceedings of the 38th International Conference on Information Systems*.

Choobineh, J., Dhillon, G., Grimaila, M. R., & Rees, J. (2007). Management of information security: Challenges and research directions. *Communications of the Assocation for Information Systems*, *20*, 958-971.

Chu, A. M. Y., Chau, P. Y. K., & So, M. K. P. (2015). Explaining the misuse of information systems resources in the workplace: A dual-process approach. *Journal of Business Ethics*, *131*(1), 209-225.

Cooper, H. M. (1988). Organizing knowledge synthesis: A taxonomy of literature reviews. *Knowledge in Society*, *1*, 104-126.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79-98.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319-340.

Deci, E. L., & Ryan, R. M. (Eds.). (2002). *Handbook of self-determination research*. Rochester, NY: The University of Rochester Press.

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems*, *8*(7), 386-408.

Ehrhart, M. G., Schneider, B., & Macey, W. H. (2014). *Organizational climate and culture: An introduction to theory, research, and practice*. New York, NY: Routledge, Taylor and Francis Group.

Eisenhardt, K. M. (1989). Agency theory: An assessment and review. *Academy of Management Review*, *14*(1), 57-74.

Farahmand, F., & Spafford, E. H. (2013). Understanding insiders: An analysis of risk-taking behavior. *Information Systems Frontiers*, *15*(1), 5-15.

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

Gottfredson, M. R., & Hirschi, T. (1995). National crime control policies. *Society*, *32*(2), 30-36.

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM*, *54*(6), 54-60.

Huang, C.-Y., Chou, C.-J., & Lin, P.-C. (2010). Involvement theory in constructing bloggers' intention to purchase travel products. *Tourism Management*, *31*(4), 513-526.

Huang, H.-W., Parolia, N., & Cheng, K.-T. (2016). Willingness and ability to perform information security compliance behavior: Psychological ownership and self-efficacy perspective. In *Proceedings of the Pacific Asia Conference on Information Systems*.

Hwang, I., Kim, D., Kim, T., & Kim, S. (2017). Why not comply with information security? An empirical approach for the causes of non-compliance. *Online Information Review*, *41*(1), 2-18.

Ifinedo, P. (2016). Critical times for organizations: What should be done to curb workers' noncompliance with IS security policy guidelines? *Information Systems Management*, *33*(1), 30-41.

Ifinedo, P., & Idemudia, E. C. (2017). Factors influencing employees' participation in non-malicious, information systems security deviant behavior: Focus on formal control mechanisms and sanctions. In *Proceedings of the 23rd Americas Conference on Information Systems*.

ISACA. (2015). *Glossary*. Retrieved from https://www.isaca.org/Pages/Glossary.aspx?tid=1506&char=I

Jenkins, J. L., & Durcikova, A. (2013). What, I shouldn't have done that? The influence of training and just-in-time reminders on secure behavior. In *Proceedings of the 34th International Conference on Information Systems.*

Johnston, A. C., Warkentin, M., McBride, M., & Carter, L. (2016). Dispositional and situational factors: Influences on information security policy violations. *European Journal of Information Systems*, *25*(3), 231-251.

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly*, *39*(1), 113-134.

Johnston, A. C., Wech, B., Jack, E., & Beavers, M. (2010). Reigning in the remote employee: Applying social learning theory to explain information security policy compliance attitudes. In *Proceedings of the 16th Americas Conference on Information Systems.*

Kajtazi, M., & Bulgurcu, B. (2013). Information security policy compliance: An empirical study on escalation of commitment. In *Proceedings of the 19th Americas Conference on Information Systems*.

Kayworth, T., & Whitten, D. (2010). Effective information security requires a balance of social and technology factors. *MIS Quarterly Executive*, *9*(4), 163-175.

Kim, S. S., & Kim, Y. J. (2017). The effect of compliance knowledge and compliance support systems on information security compliance behavior. *Journal of Knowledge Management*, *21*(4), 986-1010.

Komatsu, A., Takagi, D., & Takemura, T. (2013). Human aspects of information security: An empirical study of intentional versus actual behavior. *Information Management & Computer Security*, *21*(1), 5-15.

Kranz, J. J., & Haeussinger, F. J. (2014). Why deterrence is not enough: The role of endogenous motivations on employees' information security behavior. In *Proceedings of the 35th International Conference on Information Systems.*

Lebek, B., Guhr, N., & Breitner, M. H. (2014). Transformational leadership and employees' information security performance: The mediating role of motivation and climate. In *Proceedings of the 35th International Conference on Information Systems*.

Levy, Y., & Ellis, T. J. (2006). A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research. *Informing Science*, *9*, 181-212.

Lowry, P. B., & Moody, G. D. (2015). Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. *Information Systems Journal*, *25*(5), 433-463.

Maqousi, A., Balikhina, T., & Mackay, M. (2013). An effective method for information security awareness raising initiatives. *International Journal of Computer Science & Information Technology*, *5*(2), 63-72.

Martinko, M. J., Gundlach, M. J., & Douglas, S. C. (2002). Toward an integrative theory of counterproductive workplace behavior: A causal reasoning perspective. *International Journal of Selection and Assessment*, *10*(1/2), 36-50.

Merhi, M. I., & Ahluwalia, P. (2015). Top management can lower resistance toward information security compliance. In *Proceedings of the 36th International Conference on Information Systems.*

Merritt, C. D., & Dhillon, G. S. (2016). What interrupts intention to comply with IS-security policy? In Proceedings of the *22nd Americas Conference on Information Systems*.

Ng, B.-Y., & Xu, Y. (2007). Studying users' computer security behavior using the health belief model. In *Proceedings of the Pacific Asia Conference on Information Systems* (pp. 423-437).

Nguyen, Q. N., & Kim, D. J. (2017). Enforcing information security protection: Risk propensity and self-efficacy perspectives. In *Proceedings of the 50th Hawaii International Conference on System Sciences* (pp. 4947-4956).

Ouchi, W. G. (1979). A conceptual framework for the design of organizational control mechanisms. *Management Science*, *25*(9), 833-848.

Ouchi, W. G., & Maguire, M. A. (1975). Organizational control: Two functions. *Administrative Science Quarterly*, *20*(4), 559-569.

Pahnila, S., Karjalainen, M., & Siponen, M. (2013). Information security behavior: Towards mulit-stage models. In *Proceedings of the Pacific Asia Conference on Information Systems*.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers and Security*, *42*, 165-176.

Pashler, H. (1994). Dual-task interference in simple tasks: Data and theory. *Psychological Bulletin*, *116*(2), 220-244.

Paternoster, R., & Simpson, S. (1996). Sanction threats and appeals to morality: Testing a rational choice model of corporate crime. *Law & Society Review*, *30*(3), 549-583.

Petty, R. E., & Cacioppo, J. T. (1986). The elaboration likelihood model of persuasion. *Advances in Experimental Social Psychology*, *19*, 123-205.

Ponemon. (2015). *2014: A year of mega breaches*. Retrieved from https://www.ponemon.org/local/upload/file/2014%20The%20Year%20of%20the%20Mega%20Breach%20FINAL_3.pdf

Posey, C., Bennett, R. J., & Roberts, T. L. (2011). Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes. *Computers and Security*, *30*(6-7), 486-497.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quaterly*, *34*(4), 757-778.

Putri, F., & Hovav, A. (2014). Employees' compliance with BYOD security policy: Insights from reactance, organizational justice, and protection motivation theory. In *Proceedings of the European Conference on Information Systems.*

PwC. (2014). *Managing cyber risks in an interconnected world: Key findings from The Global State of Information Security Survey 2015*. Retrieved from https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf

PwC. (2015). *Turnaround and transformation in cybersecurity: Key findings from The Global State of Information Security Survey 2016*. Retrieved from https://www.pwc.com/sg/en/publications/assets/pwc-global-state-of-information-security-survey-2016.pdf

Rashid, R. M., Zakaria, O., & Zulhemay, M. N. (2013). The relationship of information security knowledge (ISK) and human factors: Challenges and solution. *Journal of Theoretical and Applied Information Technology*, *57*(1), 67-75.

Rocha Flores, W., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers and Security*, *59*, 26-44.

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

Rosenstock, I. M., Strecher, V. J., & Becker, M. H. (1988). Social learning theory and the health belief model. *Health Education Quarterly*, *15*(2), 175-183.

Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers and Security*, *26*(1), 56-62.

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the "weakest link"—a human/computer interaction approach to usable and effective security. *BT Technology Journal*, *19*(3), 122-131.

Schrader, P. G., & Lawless, K. A. (2004). The knowledge, attitudes, & behaviors approach: How to evaluate performance and learning in complex environments. *Performance Improvement*, *43*(9), 8-15.

Siponen, M. T. (2005). An analysis of the traditional IS security approaches: Implications for research and practice. *European Journal of Information Systems*, *14*(3), 303-315.

Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee systems security policy violations. *MIS Quarterly*, *34*(3), 487-502.

Sohrabi Safa, N., von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers and Security*, *56*, 1-13.

Stewart, A. (2004). On risk: perception and direction. *Computers and Security*, *23*, 362-370.

Swanson, M., & Guttman, B. (1996). *NIST special publication 800-14: Generally accepted principles and practices for securing information technology systems.* Gaithersburg: National Institute of Standards and Technology. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review*, *22*(6), 664-670.

Talib, Y. Y. A., & Dhillon, G. (2015). Employee ISP compliance intentions: An empirical test of empowerment. In *Proceedings of the 36th International Conference of Information Systems.*

Tarwireyi, P., Flowerday, S., & Bayaga, A. (2011). Information security competence test with regards to password management. In H. S. Venter, M. Loock, & M. Coetzee (Eds.), *Information security for South Africa*. Johannesburg, South Africa: IEEE.

Thomas, K. W., & Velthouse, B. A. (1990). Cognitive elements of empowerment: An "interpretive" model of intrinsic task motivation. *The Academy of Management Review*, *15*(4), 666-681.

Thomson, M. E., & von Solms, R. (1998). Information security awareness: Educating your users effectively. *Information Management & Computer Security*, *6*(4), 167-173.

Torraco, R. J. (2005). Writing integrative literature reviews: Guidelines and examples. *Human Resource Development Review*, *4*(3), 356-367.

Tu, Z., & Yuan, Y. (2014). Critical success factors analysis on effective information security management: A literature review. In *Proceedings of the 20th Americas Conference on Information Systems*.

vom Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R., & Cleven, A. (2009). Reconstructing the giant: On the importance of rigour in documenting the literature search process. In *Proceedings of the 17th European Conference on Information Systems.*

von Solms, R., Thomson, K.-L., & Maninjwa, P. M. (2011). Information security governance control through comprehensive policy architectures. In H. S. Venter, M. Loock, & M. Coetzee (Eds.), *Information security for South Africa*. Johannesburg, South Africa: IEEE.

von Solms, R., & von Solms, B. (2004). From policies to culture. *Computers and Security*, *23*(4), 275-279.

Vroom, V. H. (1964). *Work and motivation*. New York, NY: John Wiley & Sons.

Wall, J. D., & Palvia, P. (2013). Control-related motivations and information security policy compliance: The effect of reflective and reactive autonomy. In *Proceedings of the 19th Americas Conference on Information Systems*.

Warkentin, M., Johnston, A. C., Walden, E. A., & Straub, D. W. (2016). Neural correlates of protection motivation for secure IT behaviors: An fMRI exploration. *Journal of the Association for Information Systems*, *17*(3), 194-215.

Warkentin, M., Mcbride, M., Carter, L., & Johnston, A. C. (2012). The role of individual characteristics on insider abuse intentions. In *Proceedings of the 18th Americas Conference on Information Systems*.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *Management Information Systems Quarterly*, *26*(2), xiii--xxiii.

Whitman, M. E. (2003). Enemy at the gate: Threats to information security. *Communications of the ACM*, *46*(8), 91-95.

Whitman, M. E., & Mattord, H. J. (2012). *Principles of information security* (4th ed.). Boston, MA: Cengage.

Wilde, G. J. S. (1998). Risk homeostasis theory: An overview. *Journal of the International Society for Child and Adolescent Injury Prevention*, *4*(2), 89-91.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly*, *37*(1), 1-20.

Wilson, M., & Hash, J. (2003). *NIST special publication 800-50: Building an information technology security awareness and training program.* Gaithersburg: National Institute of Standards and Technology.

Witte, K. (1992). Putting the fear back into fear appeals: The extendend parallel process model. *Communication Monographs*, *59*, 329-349.

Workman, M., & Gathegi, J. (2007). Punishment and ethics deterrents: A study of insider security contravention. *Journal of the American Society for Information Science and Technology*, *58*(2), 212-222.

Wynn, D., Karahanna, E., Williams, C. K., & Madupalli, R. (2012). Preventive adoption of information security behaviors. In *Proceedings of the 33rd International Conference on Information Systems.*

Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management & Computer Security*, *17*(4), 330-340.

Appendix A: Summary of Search Results

Table S1. Central Issues in the Reviewed Literature

Central issue	References	Applied theories
Examining factors that influence employees' **attitude** towards compliance with security policies or towards protective technologies (10)	Al-Omari & El-Gayar (2012)	TPB
	Bauer &Bernroider (2017)	KAB
	Bulgurcu et al. (2009)	TPB, perceived fairness
	Bulgurcu et al. (2010)	EVT, RChT
	Dinev & Hu (2007)	TPB, TAM
	Kajtazi & Bulgurcu (2013)	TPB, AT
	Kranz & Haeussinger (2014)	SDT/OIT
	Parsons et al. (2014)	KAB
	Rocha Flores & Ekstedt (2016)	TPB (ISA, culture)
	Sohrabi Safa et al. (2016)	SBT, IT
Examining factors that affect behavioral **intention** towards compliance/noncompliance with security policies and procedures (24)	Al-Omari & El-Gayar (2012)	TPB
	Bauer & Bernroider (2017)	TRA, NT
	Bulgurcu et al. (2010)	TPB
	D'Arcy et al. (2009)	DT
	Hu et al. (2011)	RChT, DT, TPB, GTC
	Hwang et al. (2017)	HBM, PMT
	Ifinedo (2016)	DT, RChT, OC
	Jenkins & Durcikova (2013)	TPB
	Johnston et al. (2010)	SCT
	Johnston et al. (2015)	PMT, DT
	Johnston et al. (2016)	PMT, DT
	Kim & Kim (2017)	TPB
	Kranz & Haeussinger (2014)	TPB, SDT/OIT
	Lebek et al. (2014)	TL, OC, EVcT
	Lowry & Moody (2015)	CT, RT
	Pahnila et al. (2013)	PMT
	Putri & Hovav (2014)	PMT, RT, OJ
	Siponen & Vance (2010)	DT, NT
	Sohrabi Safa et al. (2016)	Attitude (TPB)
	Talib & Dhillon (2015)	SEM
	Warkentin et al. (2012)	PMT, DT
	Wall & Palvia (2013)	RT, SDT/OIT
	Zhang et al. (2009)	TPB, RCT
Examining factors that influence employees' **intention** towards protective technologies/to implement security measures/ to perform preventive security behaviors (5)	Dinev & Hu (2007)	TPB, TAM
	Komatsu et al. (2013)	PMT, ELM
	Nguyen & Kim (2017)	TPB, TRA, self-efficacy (SCT)
	Warkentin et al. (2016)	EPPM
	Wynn et al. (2013)	PAM, PEOU (TAM)
Examining factors that influence employees' **intention** to resist social engineering (1)	Rocha Flores & Ekstedt (2016)	TPB

Table S1. Central Issues in the Reviewed Literature

Identifying factors that influence actual **behavior** towards information security/implementing security measures/policy (non-)compliance (14)	Alhogail et al. (2015)	SCT
	Bauer & Bernroider (2017)	TRA
	Chen (2017)	EPPM
	Chu et al. (2015)	TPB
	Huang et al. (2016)	Self-efficacy (SCT)
	Ifinedo & Idemudia (2017)	OT, DT
	Jenkins & Durcikova (2013)	TPB, DTI
	Komatsu et al. (2013)	PMT, ELM
	Merhi & Ahluwalia (2015)	TPB
	Ng & Xu (2007)	HBM, PMT
	Nguyen & Kim (2017)	TPB, TRA, self-efficacy (SCT)
	Pahnila et al. (2013)	PMT
	Parsons et al. (2014)	KAB
	Workman & Gathegi (2007)	DT, TPB
Identifying factors that influence insiders' perceived attributes trust; examine the impact of attributed trust on computer abuse (1)	Posey et al. (2011)	CRT
Examining factors that influence deterrence techniques (1)	Workman & Gathegi (2007)	DT, TPB, GTC

About the Authors

Denitsa Kirova is a research assistant at the Chair of Information Management, University of Hagen, Germany. She received her Master of Science degree from the University of Rostock, Germany. Her research focuses on behavioral and managerial aspects of organizational IT security and specifically on educational and motivational approaches to raise the awareness and expertise of IT users.

Ulrike Baumöl holds the Chair of Information Management at the University of Hagen, Germany. She received her PhD from the University of Dortmund, Germany, and her postdoctoral lecture qualification in the field of Management Information Systems from the University of St. Gallen, Switzerland. Her current research focuses on digital innovation and business transformation of organizations and institutions.

JITTA

JOURNAL OF INFORMATION TECHNOLOGY THEORY AND APPLICATION

JITTA is a Publication of the Association for Information Systems
ISSN: 1532-3416