Computers & Security 93 (2020) 101782

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Toward a stage theory of the development of employees' information security behavior

Mari Karjalainen[a], Mikko Siponen[b,*], Suprateek Sarker[c]

[a] M3S Research Unit, Faculty of Information Technology and Electrical Engineering, University of Oulu, Oulu, FI 90014, Finland
[b] Faculty of Information Technology, University of Jyvaskyla, P.O. Box 35, FI 40014, Finland
[c] McIntire School of Commerce, University of Virginia, USA

ARTICLE INFO

Article history:
Received 1 May 2019
Revised 30 January 2020
Accepted 26 February 2020
Available online 4 March 2020

Keywords:
Information security
Information security behavior
Compliance with information security policies
Stage theory
Learning

ABSTRACT

Existing behavioral information security research proposes continuum or non-stage models that focus on finding static determinants for information security behavior (ISB) that remains unchanged. Such models cannot explain a case where the reasons for ISB change. However, the underlying reasons and motives for users' ISB are not static but may change over time. To understand the change in reasoning between different antecedents, we examine stage theorizing in other fields and develop the requirements for an emergent theory of the development of employees' ISB: (1) the content of stages based on the stage elements and their stage-specific attributes; (2) the stage-independent element explaining the instability of ISB; and (3) the temporal order of stages based on developmental progression. To illustrate the stage theory requirements in an information security context, we suggest four stages: intuitive thinking, declarative thinking, agency-related thinking, and routine-related thinking. We propose that learning is a key driver of change between the stages. According to our theorizing, employees start with intuitive beliefs and later develop routine-related thinking. Furthermore, using interview data collected from employees in a multinational company, we illustrate the differences in the stages. For future information security research, we conceptualize ISB change in terms of stages and contribute a theoretical framework that can be empirically validated. In relation to practice, understanding the differences between the stages offers a foundation for identifying the stage-specific challenges that lead to non-compliance and the corresponding information security training aimed at tackling these challenges. Given that users' ISB follows stages, although not in a specific order, identifying such stages can improve the effectiveness of information security training interventions within organizations.

1. Introduction

The central role of information and information technology has made information security a key concern for organizations. One of the issues identified in the so-called behavioral information security literature concerns why employees comply with or violate their organization's information security procedures (ISPs). This literature examines cases where employees can bypass some information security procedures, such as leaving their computers unlocked, sending confidential e-mails without encryption, or opening links to infected websites (Vroom and von Solms, 2004; Karjalainen et al., 2019). From a practical perspective, understanding such behaviors is important; if users do not comply with ISPs, information security solutions, however technically sophisticated, lose their effectiveness (Kruger and Kearney, 2006; Furnell and Moore, 2014). Indeed, employees' adoption of insecure behaviors continues to be a key explanation for information security breaches that creates significant financial losses for organizations (Safa and Maple, 2016; Ponemon Institute, 2014a, 2014b; SafeNet, 2014).

A dominant approach to understanding employees' information security behavior (ISB) (or intentions behind them) has been to test non-stage—also known as continuum—theories in order to take static "snapshots" of behavior and its antecedent (see Weinstein et al., 1998; Schwarzer, 2008). In these non-stage models, the explanations or predictors are static and timeless. For example, deterrence theory is among the most commonly applied theories in behavioral information security research (Sommestad et al., 2014). It explains ISB violations (or intentions) through static and

* Corresponding author.
E-mail address: mikko.t.siponen@jyu.fi (M. Siponen).

https://doi.org/10.1016/j.cose.2020.101782

timeless reasons, such as severity, certainty, and celerity of sanctions. We argue that different reasons may have differing importance based on, for example, employees' work experience. Previous research, in assuming static (non-stage) explanations, cannot explain a situation in which the role of different reasons—such as fear appeals or the severity and certainty of sanctions—changes. An alternative approach is to understand the development through stages (Velicer and Prochaska, 2008), a common approach in social psychology, moral psychology, and criminology (e.g., Prochacka and DiClemente, 1983; Weinstein et al., 1998; Thornberry, 1987). In this paper, we seek to answer the following research question: How can we explain a change in employees' reasons for their ISBs over time and across different situations? As an answer to this research question, we propose the requirements for a stage model approach in the context of ISB research. We also illustrate the stages with interview data collected from interviews with organizational employees.

Such a stage model approach has the potential to create a new understanding for information security research and practice. If the reasons for ISB differ or are changing over time for an individual, research and practice should benefit from research aimed at capturing such ISB dynamics into qualitatively distinct stages. For example, as a managerial control mechanism, the severity of sanctions can be useful for initiating a motivation for compliant ISB, but it may be less effective for maintaining compliant ISB over time, which may require experiencing more intrinsic benefits from ISB. Research and practice can also capture ISB dynamics in the sense that, regardless of the tendency to comply with ISPs, ISB can periodically differ from this pattern due to certain situation-specific demands, such as changes in the work environment or time pressure. From these perspectives, the dynamics of ISB have largely remained unstudied.

For information security research, we offer a dynamic conceptual framework, which may increase our understanding of how information security–related reasoning may change over time and in different situations. As an implication for practice, the stages offer a tool for identifying differences in users' reasons for ISB (or compliance/non-compliance).

The remainder of this paper is organized as follows. The second section explains the principles of stage theories. The third section shows that existing research on employees' ISB has not studied the topic from the stage theory perspective, as outlined in our study. The fourth section presents a discussion on our theorizing and the related empirical data collection and analysis process. The fifth section presents the requirements and empirical illustrations of the emergent stage theory. The sixth section outlines the contributions and implications for practice and research. Finally, the seventh section summarizes the key findings.

2. On stage theories

2.1. Some stage theory principles

Classical behavioral change theories have been proposed in the fields of developmental psychology, health psychology, and moral psychology. Examples of these include stage theories for moral development (Kohlberg, 1981), addictive behaviors (Prochaska et al., 1992), and grieving (Kübler-Ross and Kessler, 2006). While a few stage theories also exist in information systems (IS) (Venkatesh et al., 2011), change theorizing in IS is often associated with process theories, distinct from the variance theories proposed by Mohr (1982; Burton-Jones et al., 2015; Sabherwal and Robey, 1995). In turn, the change theories in psychology are often called *stage theories*, while theories without stages are referred to as *non-stage theories* (Velicer and Prochaska, 2008) or *continuum theories* (Weinstein et al., 1998). Mohr (1982) only recognized event-based change theories, which he called process theories. However, a number of process and stage theories in, e.g., psychology are not fundamentally event-based (Weinstein et al., 1998). Therefore, the key distinction between stage/process and continuum/non-stage theories is not necessarily the existence of events. Moreover, variance models can have events that may even induce change. For example, protection motivation theory is used as a classical example of a non-stage theory in health psychology (Weinstein et al., 1998). According to this theory, fear contributes to threat recognition and the adoption of protective behaviors (Rogers, 1975). As fear is raised by some event, protection motivation theory has an event (implicitly). However, why protection motivation theory is viewed as a non-stage theory in health psychology (Weinstein et al., 1998) has nothing to do with events: It is because the reasons for change (e.g., fear) do not change; they always remain the same. In other words, for non-stage theories, the independent variables are expected to remain unchanged during the life cycle of the phenomenon. In turn, stage or process theories are needed when the factors are believed to change during the entire life cycle of the phenomenon. Stage theories suggest that a development is linked to stages. Therefore, a stage theory endeavors to explain the development path of a specific phenomenon by dividing the development into distinct stages (Weinstein et al., 1998).

2.2. On the development of stage theories

Reichenbach (1938) separated "theory discovery" from "theory justification". For theory discovery, there are multiple possible processes describing how stage theories are developed. Common to the discovery of many stage theories is that they are originally based on speculation or imagination) or/and scholars' empirical observations. As stage theory has been proposed in many cases, later a significant number of studies have tested the original assumptions over the years (theory justification). Feyerabend (1975) conducted a review of scientific breakthroughs and noted that theory discovery must have significantly less evidence than theory justification, otherwise new theory discovery and breakthroughs will be seriously hindered. The development of requirements for our stage theory of ISB represents a theory discovery approach. Our stage theory is largely based on theorizing on concepts from previous stage theories.

2.3. An empirical versus a theoretical concept

Schwarzer (2008) claimed that in health psychology, stages have nothing to do with discovering scientific truth. Instead, "the question is not whether stages truly exist, but whether stage is a useful construct" (p. 85). Instead of trying to capture all possible stages, stage theories try to capture typical stages with instrumental value, either theoretically or empirically (Schwarzer, 2008). Somewhat similarly, Weinstein et al., 1998, p. 291) reported that a "stage is a theoretical construct. We can define a prototype for each stage, but few people will match this ideal perfectly." For example, given that humans are intentional and that they may change their behavior even several times a day, development and change can be individual and situational. A stage theory that seeks to capture all changes would result in a considerable number of stages and a highly complicated model. This is a key reason to view stages as theoretical constructs, which do not exist in reality as such, but present ideal types for certain purposes (Schwarzer, 2008; Weinstein et al., 1998).

Stage theories have more than two ordered stages, which comprise different elements that explain individuals' behavior and movement between the stages (Weinstein et al., 1998). Yet, even in ideal cases, not all people necessarily go through all (theoretical)

stages (Kohlberg, 1981), and people may remain in one stage forever (Weinstein et al., 1998). Often, the precise duration in which people reside in a stage cannot be known, and neither is this important (Weinstein et al., 1998).

Our resulting stage theory reflects the above ideas of the theoretical nature of stage theory concepts. We outline the content of stage theory by combining our observations from employee interviews with the existing literature on stage theories, different types of knowledge, and stages of behavior. However, our approach is somewhat Kohlbergian in the sense that the stages are theoretically defined and put in order (following Kohlberg, 1981), and only their content is illustrated with empirical data. We now look at previous research and the focus on non-stage models rather than stage theories.

3. Previous empirical work on employees' ISB

The existing research on ISB comprises three closely related research areas. First, influenced by Straub (1990), computer abuse/misuse studies examine different unethical or illegal actions, such as sending racist emails and using illegal software within organizations (e.g., Lee et al., 2004; D'Arcy et al., 2008; Siponen, 2001). These studies have mainly applied theories from criminology (e.g., deterrence theory in D'Arcy et al., 2008). Another related research area focuses on investigating employees' intentions to comply with or violate organizations' ISPs (Herath and Rao, 2009a; Siponen and Vance, 2010), their actual behavior (Ng et al., 2009), or both (Myyry et al., 2009). Third, several studies have investigated users' insecure behaviors without connecting them to computer abuse/misuse or policy violations. Such studies include the use of protective technologies (Dinev et al., 2009), good password practices (Stanton et al., 2003), and security conscious behavior (Rhee et al., 2009). Appendix A summarizes the previous research in greater detail.

Our literature review shows that three above-mentioned perspectives offer non-stage models (see theory type in Appendix A). Most previous studies have explained ISB or intention thereof. Moreover, previous research has also examined changes in ISB or intentions behind it (see instances of the dynamic nature of ISB in Appendix A). For example, in experimental studies, fear appeals (Johnston and Warkentin, 2010; Boss et al., 2015), group activities (Albrectsen and Hovden, 2010), or feedback and gamification (Furnell et al., 2019) have been linked to changes in ISB or intentions. However, even if these studies explain ISB change (or intended change), they do not examine changes in reasoning for ISB.

Finally, previous ISB studies also include moderator variables (see Appendix A). The moderators in these studies concern the influence of sanctions (Chen et al., 2013), cultural dimensions (Dinev et al., 2009), personal values (Li et al., 2010; Borena and Bélanger, 2013), or personality traits (Shropshire et al., 2015). Instead of explaining ISB change across situations, these studies focus on explaining the influence of relatively stable individual or cultural characteristics on ISB. They do not explain the change of moderators.

To summarize, in terms of independent variables (IVs) and dependent variables (DVs), previous research has proposed models in which the IVs or moderators remain unchanging. Moreover, there are experimental studies explaining changes in the level of DVs, not in terms of IVs. In other words, previous studies do not examine changes in users' information security cognitions over time or across situations. More precisely, existing studies do not examine: 1) how different factors might be relevant for users in different stages of development (i.e., stage-specific information security cognitions and change enhancers in our model); 2) how a user's compliant ISB can periodically change from this usual pattern due to certain situation-specific demands (i.e., overriding cognitions in our model); and 3) overall, how a user's ISB may become routinized over time as an outcome of a learning process. This study endeavors to take the first step by providing a novel view that may explains ISB in terms of stages.

4. Role of empirical data in our study

We started our research by collecting interview data on employees' reasons for their ISB. Interview data were collected in multiple locations of a global company operating in the marine industry and energy market. The data were collected through semi-structured interviews conducted by the two authors. Appendix B presents the number of interviews, the different organizational positions, and the countries. Interviewees in different countries and organizational positions were randomly selected to decrease possible bias in our findings on the basis of the characteristics of a certain profession or organizational culture. The interviews were of a strong conversational nature, and rather than the elicitation of facts, they involved active listening and an activation of interviewees' construction of meaning (Schulze and Avital, 2011). However, broad interview themes and open-ended questions were planned beforehand (see interview outline in Appendix B). Altogether, 72 face-to-face interviews were recorded and transcribed, with an average interview lasting 47 min.

Our data collection and analysis fall under qualitative content analysis, defined as "subjective interpretation of the content of text data through the systematic classification process of coding and identifying themes or patterns" (Hsieh and Shannon, 2005, 1278). The first author conducted an initial data analysis, with the analysis proceeding collaboratively among all authors' engagement in discussions, sorting of ideas, and conceptualizations. To describe the phenomenon under study, we first collected some viewpoints explaining information security attitudes and ISB and created the initial data-driven categories without connecting our interview questions with a specific behavioral theory (Hsieh and Shannon, 2005). After several iterations, 88 initial categories of reasons for employees' ISB emerged from the data. Next, in the absence of longitudinal research settings, we utilized our theoretical sensitivity to understand behavioral change. We developed the requirements of a stage theory, based on social and organizational research, so as to support the emergence of our information security–specific theory (see Section 5.1). Based on the requirements, we interpretably defined three high-level categories (i.e., information security cognitions, change enhancers, and overriding cognitions) and categorized the initial open codes (i.e., reasons for ISB) under these categories. Further, we established the order of the stages as relying on four progressive stages of behavior (Geller, 2002; Howell, 1982). Thus, even though empirical observations served as our starting point and pointed to the content of the stages (see related empirical factors in Table 1), the literature on different types of knowledge and the stages of behavior, in the spirit of theoretical sensitivity (Patton, 1990), guided the precise formulation of the stages and the development of the emerging stage theory. Therefore, the stages were theoretically defined and placed in order, and only their content is illustrated with empirical data. The requirements and resulting stage theory are introduced below.

5. Findings

We first introduce the requirements of a stage theory and their meaning in an information security context. In what follows, we present the four stages of the development of employees' ISB.

Table 1
Development stages of employees' ISB: Elements, attributes, and factors.

Elements of a stage theory	Attributes in Stage 1: Intuitive thinking	Attributes in Stage 2: Declarative thinking	Attributes in Stage 3: Agency-related thinking	Attributes in Stage 4: Routine-related thinking
Stage-specific information security cognitions explaining ISB, i.e., compliance (C) and/or non-compliance (N) with ISPs	Intuitive cognitions (N) – Related empirical factors: – Segregation – Competence overestimation/ information security requirement underestimation – Information security contentment	Declarative cognitions (C/N) – Related empirical factors: – Information security conflict–related (N); value conflict; inconvenience – Heteronomous (C/N); dependency on authority; dependency on role model; social conformity	Agency cognitions (C) – Related empirical factors: – Evaluation of risks – Value congruence – Trust in ISPs	Routine-related cognitions (C) – Related empirical factors: – Agency cognitions explaining ISB with low cognitive effort
Stage-specific change enhancers promoting behavioral change	Between 1–2: Motivation enhancers – Related empirical factors: – Internal; personal interest and activity – External; direct and indirect information security accidents, media visibility – Organizational control–related; mandatory ISPs, monitoring, rewards, and sanctions	Between 2–3: Reflection enhancers – Related empirical factors: – Experiential learning content – Collaborative learning methods	Between 3–4: Frequency enhancers – Related empirical factors: – Increasing susceptibility of information security risks – Enhancing value connectivity – Reconciling behavioral efficiency	
Stage-independent overriding conditions: Conditions for instability of ISB that are common to stages 2–4	Overriding cognitions (N) – Related empirical factors: – Working Environment – Shortcuts – Social Pressure – Opportunism			

5.1. Requirements of a stage theory in the context of employees' ISB

Stage theories are underpinned by different meta-characteristics (e.g., Weinstein et al., 1998; Kohlberg, 1981). Meta-characteristics define the requirements for a stage theory in the information security context (in our case), a viewpoint that is currently missing from the existing information security literature. We define the content and order of stages by combining our empirical observations of information security cognitions and ISB with concepts from the previous literature on human thinking and behavior.

First, *the content of the stages* can be defined in terms of certain elements that define the stages, and each element has specific attributes (Nolan, 1973). To define the elements and their stage-specific attributes in the information security context, we adopted the basic assumptions of the organizational routine change literature that a behavioral change is closely related to knowledge (Bresman, 2013). Further, we establish and support the meaning of the knowledge-related elements with concepts from the previous literature on human thinking and behavior (as presented in Section 5.2). Accordingly, we select the nature of employees' knowledge of their organization's ISPs as the element for identifying the stages, calling them *information security cognitions* (Hedström and Swedberg, 1998). We also recognize another element, i.e., *change enhancers*, which promotes the development of information security cognitions (Prochaska and Diclemente, 1983; 1992). Further, we submit that these elements have different stage-specific attributes: Stage 1 has typical cognitions i and enhancers A, while Stage 2 has typical cognitions ii and enhancers B. Further, our stage theory presents different factors for each stage-specific attribute derived from the empirical data (see Table 1).

Second, our stage theory recognizes that human behavior is prone to exceptions (Johns, 2006) and that developmental changes are not necessarily permanent (Green, 1989). Thus, our stage theory includes a stage-independent element: *the cognitions explaining the instability of ISB*. These *overriding cognitions* are related to the experienced situational constraints or circumstances that change employees' prevalent ISB from compliant to non-compliant (Kaiser and Fuhrer, 2003; Hare, 1963). Based on this understanding, scholars and practitioners can understand the conditions under which employees relapse from compliance to non-compliance with ISPs and their need for support to maintain their compliance. Our stage theory presents different factors of this stage-independent overriding cognition, derived from the empirical data (see Table 1).

Third, we define *the relations between different elements and related attributes in terms of their developmental trajectory* (van de Ven, 1992; Weinstein et al., 1998; Nolan, 1973). In defining this temporal characteristic, we view the development of behavior as progressive, which means that behavior/reasoning becomes more advanced at later stages (Green, 1989). Moreover, the organizational routine change literature often assumes that behavioral change proceeds as a learning process (Bresman, 2013). Accordingly, we argue that the development of information security cognitions is a progressive learning process based on increasing context-specific information security understanding, for example, regarding information security risks and responsibilities. Thus, we submit that compliance with ISPs in later stages requires more knowledge of the ISPs and more cognitively advanced reasoning in terms of increasing motivation, reflection, and routinization. We define the order of information security cognitions and change enhancers guided by the four progressive stages of behavior (Geller, 2002), also called levels of competence (Howell, 1982): unconsciously incompetent, consciously incompetent, consciously competent, and unconsciously competent (see Section 5.2). Along with pro-environment behavior (Geller, 2002), the stages of behavior have been used in other contexts, e.g., for understanding the development of an individual's consciousness and competence in relation to intercultural literacy (Heyward, 2002), cross-cultural communication (Gudykunst, 1994), organizational success (May and Kruger, 1988; Thompson, 1996), and institutional change (Carnes et al., 2012).

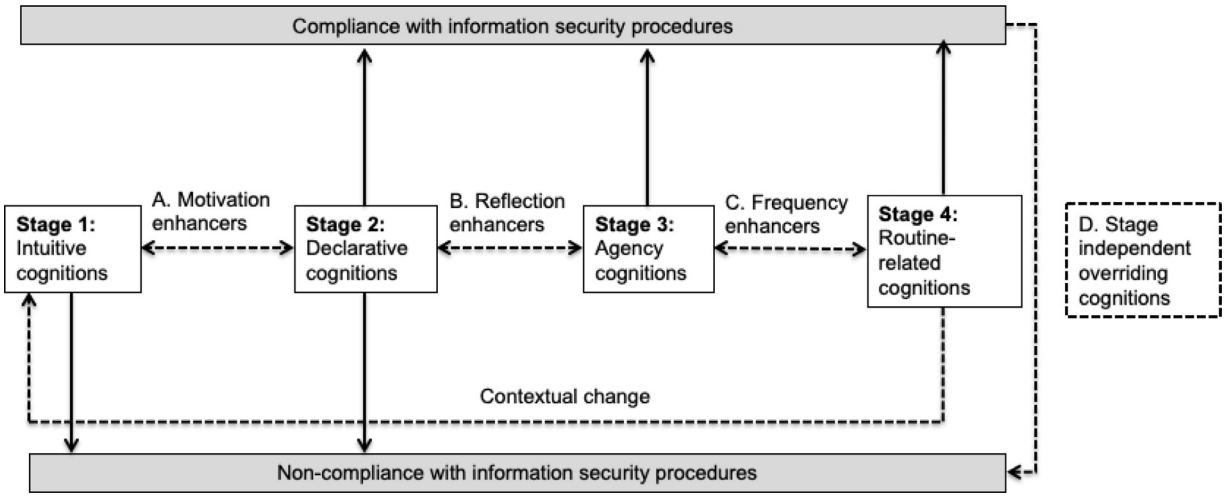

Fig. 1. The stage theory of the development of employees' ISB.

In sum, the requirements of our stage theory include (1) the content of stages based on the stage elements and their stage-specific attributes (i.e., information security cognitions and change enhancers); (2) the stage-independent element that explain ISB instability (i.e., overriding cognitions); and (3) the temporal order of stages based on developmental progression (i.e., progressive stages of behavior). The characteristics are used interpretively as high-level principles guiding our data analysis and theory development. The purpose of our data analysis is to empirically illustrate the meaning of information security cognitions, change enhancers, and overriding cognitions in the context of employees' ISB (see factors in Table 1), while the characteristic regarding the temporal order is purely theoretical in nature.

5.2. Illustrating the requirements of a stage theory of the development of employees' ISB

As presented above, stage theory includes the developmental trajectory of elements that can be specified by a set of attributes (Nolan, 1973). Fig. 1 presents the overall idea of this pattern in the context of employees' ISB.

In this context, elements include stage-specific information security cognitions (white solid squares 1–4 in Fig. 1), stage-independent overriding cognitions (the dashed white square D with the dashed arrow in Fig. 1), and change enhancers, which promote behavioral change between the stages (dashed arrows A–C in Fig. 1). By information security cognitions, we refer to the reasons explaining ISB as individual beliefs and desires that generate a specific action (Hedström and Swedberg, 1998). A set of attributes that specify the cognition element includes intuitive, declarative, agency, and routine-related cognitions as well as stage-independent overriding cognitions. In turn, by change enhancers, we refer to activities and experiences that lead to change in intentions, attitudes, or behavior—issues that promote movement from one stage to the next (Prochaska and Diclemente, 1983; 1992). A set of attributes that specifies enhancers of change includes motivation, reflection, and frequency enhancers. Fig. 1 also presents how each stage is related to compliance and non-compliance with ISPs (gray squares and related solid arrows). Finally, Fig. 1 presents the development of ISB as a cyclical process because when a work situation or circumstances change (e.g., employees' work tasks or an organization's information security policies), a new development process is needed to direct the prevailing intuitive thinking toward new routine-related thinking so as to correspond to the requirements of contextual change (see dashed arrow between stages 4 and 1 in Fig. 1). Table 1 provides a summary of the elements, attributes, and factors associated with each stage as well as their relation to compliance (C) and/or non-compliance (N) with ISPs.

The four stages in the development of employees' ISB will now be elaborated on the basis of the interview narratives and supporting literature. In addition, factors related to the stage attributes (i.e., information security cognitions, change enhancers, and overriding cognitions) will be illustrated with interview quotations in Appendix C and italicized in the text.

5.2.1. Stage 1: intuitive thinking stage

5.2.1.1. Stage description. Our results indicate that employees have certain intuitive information security–related beliefs, which as "a most fundamental category of cognition" (Sperber, 1997, 67), are obtained through upbringing, education, or previous experiences. We found that such beliefs are sometimes in contrast with organizations' ISPs. Therefore, compliant ISB—such as avoiding email for sending critical information or using strong passwords—often does not intuitively make sense to employees. Consequently, employees do not recognize their information security–related weakness and/or the instrumental value of new ISB, such as the benefits of choosing a strong password. Thus, employees in this stage are unconsciously incompetent (Geller, 2002), i.e., their ISB is unconsciously incompatible with their organization's ISPs. Next, we introduce some typical intuitive cognitions related to this pre-intentional stage, which were derived from our data.

Segregation means that an interviewee intuitively relates responsibility for ensuring information security to other parties, such as information technology (IT) employees or technologies, or has a false trust in IT. For example, employees may expect that information security is being taken care of by IT staff and, hence, may not be aware of their information security–related responsibilities. An example of false trust in IT is that employees may not understand that their passwords are overly simple and, hence, easy to break. Further, because employees in the intuitive thinking stage are unfamiliar with the organization's formal ISPs and contextual need, they can overestimate their own information security knowledge and abilities, underestimate the significance of ISPs, or may not see the need for improvement. These inabilities—*competence overestimation, information security requirement underestimation, and information security contentment*—act as typical cognitions in the

intuitive thinking stage and hinder employees from seeing the need to alter their behavior. We thus introduce motivation enhancers, which are effective for creating information security–related intentions.

Change enhancers from Stage 1 to Stage 2: Motivation enhancers

For employees in the intuitive thinking stage, one of the challenges is to initiate motivation for behavioral change. For this purpose, social science has identified a plethora of environmental conditions and cognitive structures that trigger the conscious cognitive processing of intuitive beliefs (see Louis and Sutton, 1991). In the information security context, we found experiences and conditions that can trigger employees to question their intuitive non-compliant ISB, which we termed *internal, external, and organizational control–related motivation enhancers*. Our results show that the initiation of information security cognitions and behavior change rarely occurs spontaneously on account of internal motivation enhancers, i.e., *personal interest and activity* geared toward learning new ISPs. Instead, sometimes, ISPs are both in contrast with employees' intuitive thinking (Stage 1) and not intrinsically motivating (i.e., inherently satisfactory activity, see Deci and Ryan, 1987). Consequently, the initiation of learning typically requires external events or acts of organizational control. Motivation enhancers can change employees' information security cognitions from intuitive to declarative. This means that they enable employees to realize a discrepancy between their current ISB and ISP and, in some cases, motivate them toward compliance. External and control-related motivation enhancers in the information security context are illustrated next.

The interviews frequently showed that various external events propelled the employees' toward becoming aware of the ISPs. These motivation enhancers included confronting information security–related events, e.g., in news or social media (*media visibility*) and experiencing an *information security accident directly* through personal experience *or indirectly* through the experience of others. In addition, organizational control–related motivation enhancers (i.e., management's acts of control) included experiencing an ISP as *mandatory* through management's orders, *monitoring, rewards*, and *sanctions*. We found that both external and control-related enhancers can motivate employees toward both changing their cognitions (from intuitive to declarative, see Sub-Section 5.2.2) and actual behavioral change.

However, we found that even if motivation enhancers are available, employees can fail to change their intuitive cognitions and ISB. This is so if change enhancers (e.g., information security accidents) are not sufficient for eliciting causal reasoning between employees' ISB and its consequences (see Sub-Section 5.2.2). Without effective motivation enhancers, employees continue to think and behave according to their existing intuitive cognitions instead of developing new ones. Thus, a recurrent motivation enhancer is needed for promoting behavioral change. Successful motivation enhancers move employees to the declarative thinking stage, which is introduced next.

5.2.2. Stage 2: declarative thinking stage

5.2.2.1. Stage description. *Declarative cognitions* emerge as a consequence of successful knowledge acquisition and communications involving motivation enhancers. This means that employees have the ability to evaluate the correctness of their ISB based on a fact-based understanding of the ISPs and their related consequences (Kaiser and Fuhrer, 2003). However, employees in this stage typically knowingly violate ISPs; thus, they are consciously incompetent (Geller, 2002). We found that this is because factually grounded information alone is often not a sufficient basis for compliant ISB, as it does not offer an understanding of the importance of ISPs in the specific organizational context and personal situation. Therefore, our study reveals *information security conflict–related cognitions* that explain non-compliance if positive consequences of non-compliance (e.g., more efficiently meeting other competing work priorities) are considered more important, immediate, or certain—with compliance being inconvenient or inefficient (see Geller, 2002). However, compliance with ISPs is still possible if employees have developed *heteronomous cognitions*, determined by external forces, without the need for personal work situation-specific information security justifications. We now look at the typical declarative cognitions derived from our data.

As mentioned above, in this stage, information security cognitions can be either heteronomous (explaining both compliance and non-compliance) or information security conflict–related (explaining non-compliance) (see Table 1). Our interviews showed that the presence of heteronomous declarative cognitions means that compliance is dependent on issues extrinsic to information security: whether employees experience an obligation to do so by an authority figure (*dependency on authority*), whether they feel that it is important to follow management as a role model (*dependency on role model*), or whether they adjust their behavior according to how they think or perceive the behavior of others (*social conformity*). However, as mentioned earlier, people in this stage often knowingly violate ISPs because motivation enhancers alone are not always sufficient for ensuring compliant ISB. Information security conflict–related declarative cognitions mean that employees do not comply with ISPs because of other experiences that override their existing motivation for information security compliance: value conflict and inconvenience. These cognitions illustrate that employees are unwilling to undergo additional learning and effort, for the sake of information security, without a profound understanding of the importance of information security requirements in a specific work context and without having externally motivated heteronomous cognitions.

Value conflict means that even if employees are cognizant of the information security requirements, how to comply with them, and why compliance is necessary (i.e., information security values), a person may not see how compliance fits in with their own work. Instead, this person may prefer other work values, which could lead to non-compliance. For example, sales employees may experience a contradiction between information security requirements and productivity requirements that explain non-compliance. Moreover, employees often consider the extent of the *inconvenience* associated with ISPs, which sometimes leads to non-compliance with ISPs, instead of expending additional effort into seeking and learning suitable technical information and skills or circumventing insecure procedures. For example, the interviewees stated that email encryption or password practices are too restrictive, time-consuming, or difficult.

In sum, while intuitive cognitions are related only to non-compliance (Stage 1), declarative cognitions (heteronomous and information security conflict–related in Stage 2) explain both non-compliance and compliance with ISPs. Further, besides declarative cognitions, non-compliance in this stage can be explained through *overriding cognitions*, which can stimulate compliant employees to violate ISPs (common in stages 2–4; see Section 5.2.5). Indeed, we found that without contextual information security understanding, and due to competing motivations, employees may be insufficiently motivated to maintain compliant ISB. We also found evidence of how the absence of heteronomous cognitions (e.g., management's orders and role model) can propel employees to abandon their compliant behavior. A greater persistence of compliant behavior needs to be supported through reflection enhancers, addressed below.

Change enhancers from Stage 2 to Stage 3: Reflection enhancers

One of the essential challenges in the declarative thinking stage is to make employees reflect on their fact-based knowledge in order to generate personally meaningful and active ISB.

Reflection refers to the active and deliberative cognitive processing of the knowledge needed to reach solutions to practical problems (Hatton and Smith, 1995), such as non-compliance with ISPs. In this regard, our interviews revealed several *reflection enhancers*, i.e., experiential learning content and collaborative learning methods (see Karjalainen and Siponen, 2011). We found that reflection enhancers can improve the understanding and relevance of information security–related communications, correct employees' false conceptions, and offer procedures to decrease an experienced inconvenience with ISPs. Reflection enhancers can support employees' transition between the second and third stages, i.e., formation of *agency-related cognitions* (see Section 5.2.3) and compliance with ISPs.

Experiential learning content, which was revealed in our interviews, refers to the possibility of reflecting on the meaning of ISPs in terms of the perceptions of the information security threats and values that characterize a personal situation. For example, while a function of information security accidents in the first stage was to create awareness and motivation toward compliance, a function of information security accidents, as part of experiential learning, is to understand and reflect on their meaning in personal situations. While interviewers often considered the value of ISPs from the viewpoint of confidentiality, other information security values (e.g., integrity, availability) were rarely recognized and, thus, need to be clarified. Moreover, their concrete meaning needs to be understood from the viewpoint of different professional values. In addition, we found that *collaborative learning methods* (instead of one-way delivery of information security knowledge) are enhancers that can encourage employees to learn and commit themselves to information security. Examples include employees' active participation in information security implementation (e.g., information security policy development) and personal involvement during information security training through knowledge sharing.

Without reflection enhancers, employees continue to behave according to their existing cognitions instead of developing new ones. Therefore, ISB continues to be highly dependent on heteronomous declarative cognitions (i.e., dependency on authority, role models, social conformity), strongly influenced by information security conflict–related declarative cognitions (i.e., value conflict, inconvenience), and vulnerable to the overriding cognitions that lead them toward non-compliance in certain circumstances (see Section 5.2.5). Successful reflection enhancers move employees to the agency-related thinking stage, which is introduced next.

5.2.3. Stage 3: agency-related thinking stage

5.2.3.1. Stage description. Reflection enhancers enable the formation of *agency-related cognitions*, indicating that employees are consciously competent (Geller, 2002) in complying with ISPs. We submit that, in this stage, information security cognitions and behavior transform from externally directed to self-directed (Geller, 2002) based on knowledge on the effectiveness (Kaiser and Fuhrer, 2003) and internalization (O'Reilly and Chatman, 1986; Ryan et al., 2008) of values. This means that compliant ISB is based on information security-conscious reasoning related to employees' subjective estimations between personal effort and information security benefits as well as personal values and goals. Consequently, we found that employee compliance is explained by agency cognitions that are situation-specific—namely, consideration of the advantages of procedural compliance linked with the external environment (*evaluation of risks*), professional values (*value congruence*), and the effectiveness of ISPs (*trust in ISPs*). Agency cognitions mean that employees comply with ISPs because they are "experienced as action for which one is responsible" (Deci and Ryan, 1987, 1025) and not as a conflict between the ISPs and cognitions regarding the evaluation of risks, value congruence, and/or trust in ISPs.

The first agency cognition, the *evaluation of risks*, means balancing information security threats with the value of the information in a specific work context. Besides being aware of the value to protect (work-related or personal) information, employees' ISB is strongly attached to their conceptions of information security threats in their work environment. Employees' decisions to engage in compliant ISB are consistently based on the observation that threats could be realized. Thus, compliance is based on the conscious situation-specific decision determined by the increased risk-propensity level of an employee. Compliance also emerges due to *trust in ISPs*. This means that when the interviewees believe that there is a significant (positive) consequence of using certain ISPs, they tend to trust their efficiency and, consequently, comply with them. In addition, a sense of *value congruence* explains ISB in this stage. This means that employees' compliance with ISPs depends on their understanding of how information security–related values help them implement important professional values. For example, the information security value of confidentiality in terms of protecting personnel and salary information is strongly connected to human resources (HR) employees' professional values. Interestingly, we found value congruence to be typically expressed not only as individual-level cognition but also at the group, departmental, or even organizational level.

Even if employees in this stage comply with ISPs, as in the previous stages, *overriding cognitions* (see Section 5.2.5) can stimulate compliant employees toward violating ISPs. Thus, a greater persistence regarding compliant ISB needs to be supported through frequency enhancers, the subject of the next section.

Change enhancers from Stage 3 to Stage 4: Frequency enhancers

At the agency-related thinking stage, the goal is to make compliant ISB part and parcel of employees' work routines, without additional cognitive effort (i.e., situation-specific conscious decisions). For this purpose, employees need frequency enhancers that reinforce agency-related cognitions through autonomy-supportive feedback associated with the increasing persistence of behavioral change (Deci and Ryan, 1987) and increasing automaticity of behavior (Geller, 2002). Frequency enhancers strengthen the connection between compliant ISB and the expected influence of meeting behavioral goals (Ouellette and Wood, 1998). Without this affirmation of the correctness and effectiveness of their behavioral choices, employee cognitions are not necessarily strong enough to maintain compliant behavior, and instead of becoming habitual, compliance can decrease over time (Geller, 2002). This means that due to the intangible nature of information security threats and the consequences of compliant ISB (Karjalainen and Siponen, 2011), employees may be unable to recognize the positive consequences of ISP compliance without receiving autonomy-supportive feedback (Geller, 2002; Deci and Ryan, 1987) on compliant ISB.

We argue that autonomy-supportive feedback, which confirms employees' compliance with ISPs, should increase the susceptibility of information security risks, reconcile behavioral efficiency, and enhance value connectivity. As a result of the experienced *increase in the susceptibility of information security risks,* employees' decision to comply with ISPs is not based on their situation-specific estimation of the likelihood of information security risks; instead, it is based on an emphasis of the potential information security risks arising from the neglect of ISPs. Through experienced *reconciliation with behavioral efficiency*, compliant ISB is still considered valuable in mitigating information security risks, even if it is not expected to offer definite protection for all occasions and that information security breaches can occur in a climate of compliance. The experience of *enhancing value connectivity* can be achieved by supporting employees' awareness of their professional

and information security values and the connections between them.

Without frequency enhancers, compliance with ISPs is achievable through conscious and situation-specific decision-making, but it is also vulnerable to overriding cognitions (see Section 5.2.5). Information security communication that continuously utilizes these frequency enhancers moves employees to the final routine-related thinking stage, which is introduced below.

5.2.4. Stage 4: routine-related thinking

5.2.4.1. Stage description. In the final stage of the development process, employees comply with ISPs on relatively stable ground. The *routine-related information security cognitions* characterizing this stage suggest that as a result of frequency enhancers, employees comply with ISPs with low cognitive effort, i.e., they become unconsciously competent in complying with ISPs (Geller, 2002). Routine-related cognitions, as an outcome of a development process, indicate that ISPs have become taken-for-granted in certain social contexts (Tost, 2011) that are more proactive and independent of environmental feedback and reinforcement. In addition, employees' behavior in this stage is not as strongly dependent on overriding cognitions as in the earlier stages. At first glance, the first and final stages of the stage theory may seem almost identical. However, in order to reach the routine-related cognitions stage, a learning process is always needed to form compliant ISB. During the process of adopting new ISPs, employees' form new thinking and ISB that are valid in specific work situations or circumstances. Nevertheless, it is possible that employees' compliant ISB is learned in a different context and can meet the ISPs of the current organizational context. Further, for some people, awareness of the ISP is enough to make them compliant (depending on their information security cognitions), which can become routinized over time.

5.2.5. Stage-independent overriding cognitions

As noted earlier, compliant behavior can turn into non-compliance with ISPs due to stage-independent overriding cognitions. Overriding cognitions refer to experienced contextual and situational influences or constraints that may decrease the influence of the stage-specific cognitions that explain compliance with ISPs (Kaiser and Fuhrer, 2003; Hare, 1963). Recognizing these cognitions is important, regardless of an employee's stage in the development process. With respect to the stage theory characteristics, the overriding cognitions explaining the instability of ISB point to the circumstances regarding the possibility of abandoning certain behavioral patterns.

First, the *working environment* as an overriding cognition means that employees recognize potential threats but do not seem to realize their possibility because they have high trust in the company's technical information security solutions or other people in the working environment. For example, while some employees usually lock computers, they may not do so in their own office, as this might be deemed unnecessary in this environment.

The second overriding cognition is the need to *take a shortcut*, which refers to situations in which one is being lazy, hurried, or stressed. For example, a computer is usually locked, but not in situations when it is left attended for a short period of time or of sudden interruptions.

According to the interviewees, ISPs are usually complied with, except in situations where a person feels *social pressure*, which can be internal (e.g., avoiding negative feelings) or external (e.g., experiencing fear). An example of internal social pressure is that employees may reveal sensitive information because they want to help others or maintain good working relationships; they might not ask to see employee badges or might not lock their computers because they feel embarrassed to act in this way. An example of external social pressure is an employee revealing sensitive information, either personally or through email, because they feel threatened.

Finally, *opportunism* means that ISPs are complied with, except if a person has a motivation for intentional abuse in the sense of gaining personal benefit (e.g., monetary benefit, fulfilled curiosity) or causing harm to the company.

Even if the overriding cognitions can potentially influence employees' compliant ISB in stages 2–4, it is assumed that in the last stage of the process, employees' ISB is not as strongly dependent on these overriding cognitions as in other stages. This is so because in the last stage, ISB requires less conscious effort, and thus, the cognitive load required for ISB is lower. As an exception, this trend is not valid in cases where an employee makes a conscious decision to cause harm to the company by violating ISPs and overriding the effects of social pressure or opportunism.

6. Discussion

6.1. Contributions

Our study aimed at finding out how to explain a change of employees' reasons for their ISB over time and across different situations. Our results contribute to information security research by introducing a new theoretical perspective that indicates that employees' compliance with ISPs can be studied as a sequence of ideal and theoretical stages that lead to routinization over time. This is different from much of the existing behavioral information security research, which examines the phenomenon through non-stage models. To give an example, previous information security studies suggest that habit, as an unconscious or automatic behavior, explains information security policy compliance (Pahnila et al., 2007; Vance et al., 2012). These studies, however, do not explain how the habit develops. We try to capture the change through stages. Specifically, our study proposes four stages that differ in terms of cognitions in explaining ISB. The first stage is characterized by intuitive cognitions, which result in non-compliance with ISPs. The second stage is characterized by declarative cognitions, including heteronomous and information security conflict–related cognitions that result in both non-compliance and compliance. The third stage is characterized by agency-related cognitions, while the fourth stage is characterized by routine-related information security cognitions, both resulting in compliance with ISPs. The majority of the individual cognitions identified in our study can be related to the variables identified in previous studies (see Appendix E). For example, the variables in the theory of planned behavior (e.g., subjective norms and control beliefs) are conceptually related to declarative cognitions in Stage 2. However, no existing study has qualitatively separated the different stages for the purpose of explaining the development of employees' ISB-related cognitions. To further clarify this difference, let us look closer at Myyry et al. (2009), who found that only lower levels of moral reasoning (avoiding punishment and gaining personal benefit) explain compliance with the ISP. Further, they conclude that other personal interests are prioritized over ISP compliance. Interestingly, a positive relationship was not found between higher-level moral principles (e.g., social and professional roles) and ISP compliance. Although conceptualized through stages, our study's perspective is not focused on moral development; it focuses on theories of types of knowledge and behavior. However, their findings are similar to ours in terms of heteronomous cognitions determined by external forces, without the need for personal work situation–specific information security justifications (e.g., dependency on authority), and information security conflict–related cognitions that prioritize positive consequences of non-compliance (e.g., more efficiently

meeting other competing work priorities). Thus, from the perspective of our study, the respondents in the study of Myyry et al. (2009) represent declarative thinking that is typical of Stage 2. The main emphasis in our study is to argue that employees' ISB develops in different stages through a developmental trajectory, where different variables or factors are important. This is a new finding in terms of employees' ISB, regardless of the stage-based viewpoint in the field of information security.

Further, our results also suggest that each stage differs in terms of ideal stage-specific change enhancers, which explain how employees' information security cognitions and behavior may change as they proceed from the first stage toward the last stage. Change enhancers may be useful for overcoming information security cognitions that explain non-compliance and thus may promote movement from one stage to the next. These stage-specific change enhancers include motivation, reflection, and frequency enhancers, which are important goals for information security interventions (see also Geller, 2002). This is a novel finding in the information security literature. Our study offers new insights about reflection enhancers and how to motivate employees to change their information security cognitions and ISB from the declarative thinking stage, characterized by a dependency on authority and value conflicts, to agency cognitions.

Our study also found some explanations as to why compliant behavior can turn into non-compliance, particularly in the second and third stages of the process. The overriding cognitions explaining the instability of ISB include the work environment, taking a shortcut, social pressure, and opportunism. Any information security communication needs to recognize these cognitions. Previous studies have recognized different moderation variables related to stable individual or cultural characteristics (see Appendix A, Table 2: Instances of the dynamic nature of the ISB – Moderators). However, instead of explaining ISB change across situations, these studies focus of explaining the influence of relatively stable individual or cultural characteristics on ISB. Our study complements the understanding of the moderators by providing overriding cognitions that shed light on the contextual nature of ISB.

6.2. Implications for research

Our stage theory presents a foundation for the stage theorizing and development of information security interventions in the field of behavioral information security. First, while non-stage theories dominate the information security field, our study offers a perspective for theorizing behavioral change in the information security context. In particular, we propose that the requirements outlined in our study can be applied (generalizable) beyond the specific phenomenon of compliance and non-compliance with ISPs. Further, the stage theory perspective outlined in this study can be complemented with theoretical principles highlighted in other process meta-theories, such as life-cycle, dialectical, or evolutionary perspectives (e.g., van de Ven, 1992). Moreover, future studies can use different empirical methods, such as longitudinal research design or narrative analysis, to study behavioral change and development in order to validate our stage theory.

Second, given our theoretical assumptions that employees are at different stages and that, in each stage, there are (a) different reasons (i.e., stage-specific cognitions), (b) similar reasons (i.e., stage-independent overriding cognitions) that influence their decision to comply and/or not to comply, and (c) enhancers that influence why behavior (or cognitions behind it) changes, future research should develop a practical survey instrument for identifying an individual's stage. Stages can be operationalized through identifying employees' level of competence (Geller, 2002; Howell, 1982), for example, whether they are unconsciously incompetent, consciously incompetent, consciously competent, or unconsciously competent in practicing certain ISPs. This would be helpful, since information about employees' actual stage would help organizations design customized information security training programs aimed at overcoming stage-specific information security cognitions that explain non-compliance while creating motivation for compliance, reflecting on information security requirements in personal situations, and increasing the frequency of compliant behavior. Further, future research can seek to control one's stage in order to test the existence of qualitatively different stages, for example, different information security cognitions (i.e., factors) that explain employees' ISB in different stages.

Third, future research should examine whether the enhancers of change in each stage can be influential, such that employees can progress from one stage to the next. Different interventions (e.g., training or campaigning), along with different research methods (e.g., experiments, case studies, and action research), can be used. Research in moral psychology aimed at increasing individuals' moral maturity in light of the stages of moral development (Kohlberg, 1981), or stage-specific health interventions (Weinstein et al., 1998), can be used as examples for designing such intervention research.

6.3. Implications for practice

International security standards, such as ISO 17799, require that employees receive information security training. To this end, previous research has pointed to the effectiveness of the same generic motivations for all employees, such as sanctions drawn from criminological theories or fear appeals taken from heath science theories (Theohariduo et al., 2005; D'Arcy and Herath, 2011; Boss et al., 2015), sometimes with contradictory results. Our results suggest that such generic explanatory factors may not be static and invariant, thus offering a framework for recognizing possible differences in the reasons for compliance/non-compliance between individuals. Therefore, we suggest the need for a new approach to information security training, where the aim is to understand the effectiveness of different information security motivations in terms of stages. If users' ISB follows stages, even if not in a specific order, the recognition of such stages will provide a means to revolutionize information security training approaches, which are currently based on non-stage theories.

For information security practitioners, our model advises that for developing effective information security interventions it is essential to understand employees existing information security cognitions (i.e., stage of thinking) and ISB (i.e., if they are compliant or non-compliant). Recognizing the flow of our stages on the development of employees ISB (different information security cognitions and barriers of change) supports organizations to develop instruments to measure the current information security cognitions (e.g., online surveys) and further, to match their information security training goals with the specific needs of their employees. In practice, based on the stage model, organizations can customize the content and order of their continuous training materials including face-to-face training sessions, information security instructions, or online information security training systems. The purpose of such tailored information security intervention materials is to get employees motivated for compliant ISB, reflect on information security requirements in personal situations, and increase the frequency of compliant ISB, respectively. For example, if noncompliant employees' ISB is strongly influenced by intuitive cognitions (such as segregation, competence overestimation/information security requirement underestimation, or information security contentment), information security training programs focused on developing agency cognitions (such as

evaluation of risks, value congruence, or trust in ISPs) may fall short of the purpose, since employees do not have the necessary contextual and information security–related understanding required for learning. In the case of employees with intuitive cognitions, the purpose of information security intervention is mainly to inform them about the information security procedures and their responsibilities, while in the case of employees with agency cognitions it is more essential to focus on strengthening the current thinking and compliant ISB.

As an overall goal, it is also important that practitioners focus their effort on creating routine-related information security cognitions, which suggests that instead of being merely compliant, people are more autonomous, complying with ISPs rather automatically, with little cognitive effort and with fewer exceptions. Routinized compliance is an important goal not only for individual employees (i.e., ISPs become more frequent with less effort) but also for organizations, because the internalization of ISPs represents congruence between individual and organizational information security goals and values, which reduces the costs associated with information security breaches and the building of information security control mechanisms (see O'Reilly and Chatman, 1986).

Our findings also indicate that information security cognitions often do not develop naturally, irrespective of the organizational context. Instead, concrete acts of learning or problem-solving are needed for informing employees of the information security requirements and roles (Stage 1), solving the tensions between information security requirements and employees' information security cognitions (Stage 2), and offering changes for internalization and maintenance of compliant ISB (Stage 3). ISB also often requires collective interpretation of the information security requirements and must be rooted in current work practices. Such social construction can include action planning in terms of specifying requirements for ISB and coping planning in terms of anticipating procedures to overcome expected problem situations (Schwarzer, 2008).

6.3. Limitations of the study

Stage theories present ideal types that simplify complex phenomena (Weinstein et al., 1998; van de Ven, 1992). This means that people may reside between the ideal stages and that the stage theory may not capture all the possible developmental trajectories (Weinstein et al., 1998). For example, our process theory does not capture all the possible differences between the different information security policies, although specific ISB may vary based on the degree of difficulty in overcoming barriers and situational influences (see Kaiser and Fuhrer, 2003). In addition, not all information security policies are necessarily reasonable in the particular context, and reaching the final routine-related thinking stage may not always be desirable for all types of information security policies. Further, an examination of the conditions for explaining the differences in employees' cognitions in specific stages is out of the scope of this study. For example, previous studies have suggested that ISB is influenced by personality traits (Alohali et al., 2018) and social or cultural biases (Tsohou et al., 2015). However, our interviews showed that these conditions may include differences in personality characteristics and national and organizational cultures.

We also acknowledge that our concepts (factors summarized in Table 1) are illustrative and that additional factors could be identified in studies of other contexts. However, we submit that the emergence of other factors would not reduce the contribution of our stage theory, given that it offers a new way to examine and understand ISB.

In addition, one can ask whether interviews can provide honest reports with respect to compliance with ISPs, especially if employees feel that their employer may be able to trace their responses back to them. To address this concern, we communicate to the interviewees that we would not reveal the individual results to their employer and that we were interested in the general patterns stemming from the data. They were also provided with the option of having us write down their interview responses as field notes rather than digitally recording them. Our interviewees mentioned a number of concrete examples of their insecure ISB, such as using extremely simple passwords, not locking their computers, or sending confidential information without encryption.

7. Summary

Our study complements the perspective offered by previous non-stage models of ISB by providing the stage theorizing view: how information security cognitions and behavior develop in a sequential trajectory, under which conditions individuals can move from one stage to another, and under which conditions relapses occur. Our stage theory suggests that employee information security–related thinking and behavior develop through a sequence of stages and that each stage is associated with stage-specific reasons for compliance and/or non-compliance with ISPs as well as with change enhancers that promote employees' progression from one stage to the next. For future research, we propose the need to further test our stage theory, control the employees' stage, further examine stage-specific attributes, and examine the effects of stage-specific interventions aimed at improving ISB. For information security practice, our results imply that one size may not fit to all. Instead, our study offers a framework for recognizing possible differences in the reasons for compliance/non-compliance between individuals. Specifically, guided by our stage theory, practitioners could identify the specific enhancers that promote employees' transitions to subsequent stages toward the development of routinized ISB.

Note: references in Appendix A included.

Declaration of Competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendix A: previous studies

Table 2 summarizes the previous empirical studies in employees' ISB through presenting the theory type (variance approach, factor approach, dynamic variance approach, or process approach). Variance approach (i.e., non-stage/continuum) refers to studies that are aimed at measuring the variance explained in behavioral intention or actual behavior. Factor approach refers to certain factors, mainly obtained through qualitative studies, that explain ISB. Dynamic variance approach refers to studies that examine influence of moderators or an experiment on employees' ISB. Table 1 also presents instances of dynamic nature of the ISB (moderators, experiment, or stage theory characteristics), and the related theories and concepts. In sum, even if experiments and moderator are applied in some studies, Table 2 shows that measuring behavioral change and development of information security cognitions in terms of stage theory characteristics are missing from the current literature.

Table 2
Previous studies in employees' ISB.

Authors	Theory type	Instances of the dynamic nature of the ISB	Theories and concepts
1. Models on computer abuse /misuse			
Harrington (1996)	Dynamic variance approach	Moderators: Responsibility denial moderates the relationship between codes of ethics and computer abuse intentions	Ethical decision making, deterrence theory
Lee et al. (2004)	Variance approach	–	Social control theory, deterrence theory, theory of planned behavior, and theory of reasoned action
D'Arcy et al. (2008)	Variance approach	–	Deterrence theory
D'Arcy & Hovav (2007)	Variance approach	–	–
Hovav & D'Arcy (2012)	Variance approach	–	Deterrence model, Hofstede's cultural dimensions, and research on confucianism and face-saving within East-Asian society
Posey et al. (2011)	Dynamic variance approach	Moderators: External locus of causality and stable causal assignment (partial) moderate the relationship between lack of attributed trust and computer abuse	Causal reasoning theory
2. Studies on compliance with information security procedures			
Siponen et al. (2006)	Variance approach	–	Protection motivation theory
Siponen et al. (2007)	Variance approach	–	Protection motivation theory, general deterrence theory, and theory of reasoned action
Herath & Rao (2009a)	Variance approach	–	Protection motivation theory, deterrence theory, organizational commitment, theory of planned behavior, and decomposed theory of planned behavior
Johnston & Warkentin (2010)	Dynamic variance approach	An experiment: Fear appeals influence ISB intentions: perceived threat severity influence the statements of efficacy that, along with social influence, explain intention to comply	Protection motivation theory
Ng et al. (2009)	Dynamic variance approach	Moderators: Perceived severity of security incident moderates the effects of benefits, general security orientation, cues to action, and self-efficacy	Health belief model
Herath & Rao (2009b)	Variance approach	–	Literature in agency theory
Li et al. (2009)	Variance approach	Moderators: Personal norms moderate the influence of formal sanctions	Rational choice theory, cost-benefit calculus, personal norms, organizational and contextual factors
Li et al. (2010)	Dynamic variance approach	Moderators: Personal norms moderate the influence of formal sanctions	Rational choice theory, cost-benefit analysis, personal norms, organizational context factors
Myyry et al. (2009)	Variance approach	–	Theory of cognitive moral development, and the theory of motivational types of values
Bulgurcu et al. (2010a)	Variance approach	–	Theory of planned behavior
Bulgurcu et al. (2010b)	Variance approach	–	The group engagement model, literature linking quality and behavioral intention
Chan et al. (2005)	Variance approach	–	Safety climate literature, the social information processing approach
Siponen & Vance (2010)	Variance approach	–	Neutralization theory and deterrence theory
Pahnila et al. (2007)	Variance approach	–	General deterrence theory, Protection motivation theory, the Theory of reasoned action, Information systems success, Triandi's behavioral framework and rewards
Boss et al. (2009)	Variance approach	–	Organizational control literature
Son (2011)	Variance approach	–	The extrinsic motivation model and the intrinsic motivation model.
Vance et al. (2012)	Variance approach	–	Habit and the protection motivation theory
Kolkowska & Dhillon (2013)	Factor approach	–	Dimensions of power
Hu et al. (2012)	Variance approach	–	The theory of planned behavior, the competing value framework, and literature on top management
Cox (2012)	Variance approach	–	The theory of planned behavior, the threat control model, and organizational narcissism
Chen et al. (2013)	Dynamic variance approach	Moderators: Certainty of control and rewards moderate the effect of punishments on compliance intention	The compliance theory and the general deterrence theory
Hedström et al. (2011)	Factor approach	–	Theory of organizational learning, Social action theory, Concept of security rationale, The value based compliance model
Guo et al. (2011)	Variance approach	–	The composite behavior model
Johnston et al. (2015)	Dynamic variance approach	An experiment: sanctioning rhetoric improves the effectiveness of a fear appeal on compliance intentions	Fear appeals and related behavioral modeling theories
D'Arcy & Greene (2014)	Dynamic variance approach	Moderators: employee position, industry, and tenure with the organization moderate the influence of security culture, job satisfaction, and perceived organizational support	Literature in security culture (top management commitment to security, security communication and computer monitoring) and organizational behavior (employment relationship: job satisfaction and perceived organizational support)
Ifinedo (2014)	Dynamic variance approach	–	Theory of planned behavior, social cognitive theory, social bond theory
Ifinedo (2012)	Variance approach	–	The theory of planned behavior and the protection motivation theory
Foth (2016)	Dynamic variance approach	–	Theory of planned behavior and general deterrence theory

(*continued on next page*)

Table 2 (*continued*)

Authors	Theory type	Instances of the dynamic nature of the ISB	Theories and concepts
Lowry & Moody (2015)	Dynamic variance approach		Organisational control theory and reactance theory
Shropshire et al. (2015)	Dynamic variance approach	Moderators: Personality constructs moderate the relationship between intention and ISB	Theory of reasoned action, technology acceptance model, personality constructs of conscientiousness and agreeableness
Siponen et al. (2014)	Variance approach	–	Protection motivation theory, theory of reasoned action, and cognitive evaluation theory
Warkentin et al. (2011)	Variance approach	–	Social learning theory
Borena & Bélanger (2013)	Dynamic variance approach	Moderators: Religiosity moderates the relationship between conservative-value and ISB	Motivational value theory: values of religiosity and conservation
Safa et al. (2016)	Variance approach	–	Social bond theory, involvement theory
Safa et al. (2019)	Variance approach	–	General deterrence theory, situational crime prevention theory, theory of planned behavior
3. Studies on appropriate ISB			
Dinev et al. (2009)	Dynamic variance approach	Moderators: Relationship between subjective norm and behavioral intention is moderated by cultural dimensions (priority of group norms, power distance, uncertainty avoidance, and masculinity); relationship between technology awareness and attitude toward behavior and behavioral intention is moderated by cultural dimensions (collectivism and masculinity)	Theory of planned behavior, awareness, integrated model of user acceptance of e-commerce, and cultural dimensions and indices
Dinev & Hu (2007)	Variance approach	–	Theory of planned behavior, awareness
Stanton et al. (2005)	Factor approach	–	–
Adams & Sasse (1999)	Factor approach	–	–
Albrechtsen (2007)	Factor approach	–	–
Albrechtsen & Hovden (2010)	Dynamic variance approach	An experiment: Employee participation, collective reflection, and group processes influence ISB	–
Sasse et al. (2001)	Factor approach	–	Research on human / computer interaction design approach
Karjalainen et al. (2013)	Factor approach	–	Paradigms of learning
D'Arcy & Greene (2009)	Variance approach	–	Social exchange theory
Stanton et al. (2003)	Variance approach	–	–
Rhee et al. (2009)	Variance approach	–	Social cognitive theory
Boss et al. (2015)	Dynamic variance approach	An experiment: Fear appeals generate higher fear and stronger intentions and actual ISB	Protection motivation theory
Safa et al. (2018)	Variance approach	–	Social bond theory, Situational crime prevention
Alohali et al. (2018)	Factor approach	–	Big five inventory, demographics, IT proficiency, IT usage

Appendix B. interviewees and interview outline

At the time of the interview in 2009, the company had over 18,000 employees in 70 countries. The selected data collection locations were Switzerland, UAE, and China. While the offices formally belong to the same organization, they can be seen as different organizations, because they had independent economic responsibilities, were previously owned by other companies, and were bought by the multinational company they now formally belong to. Table 3 presents a number of interviews in different positions and countries.

Our data collection and analysis were guided by the notion of theoretical saturation. In other words, data collection and analysis continued until we felt that additional data would not result in a new or different understanding of the reasons for employees' ISB for the time being. Further, a key point in our *interpretive* methodological approach is that interpretation is not necessarily obtained by aggregating similar views of respondents, and we acknowledge that the same phenomenon can have different meanings for different interpreters (Lee, 1991; Klein and Myers, 1999). Therefore, our interpretation of data is not dependent on quantitative measures, such as sample size or frequency of utterance that would be more consistent with what is referred to as positivist approach in the discipline.

We informed interviewees about the research, emphasized our purpose of understanding their own viewpoint regarding information security in their daily work, and carefully explained that the interview was confidential. Given the sensitivity of our research

Table 3
Interviewees and Interview Outline.

Position	UAE	China	Switzerland	Total
Manager	10	7	6	23
Officer	15	13	9	37
Engineer	2	3	5	10
Unclear	2	0	0	2
Total	29	23	20	72

Interviewees' titles:
Officers: Marketing coordinator (1), HR officer/assistant (8), Business controller (2), Spare parts coordinator (1), Sales coordinator/Service sales (5), SP merchant (3), Order processor (4), Accountant (1), Purchase officer/Material specialist (3), Credit controller (1), Service coordinator (2), Cost analyst (1), Assistant (5)
Managers: Engineering manager (1), IM manager (4), Reconditioning manager (1), Environment, health, safety and security manager (1), Sales account manager (2), Facility manager (1), Contract manager (1), Quality Control/Assurance manager (2), Account manager (2), HR manager (1), Regional support manager (1),Business development manager (2), Sales support manager (1), Manager (1), Service sales manager (1), Design & development manager (1)
Engineers: R&D/Engine performance (1), Sales support engineer (3), Design engineer (1), Project engineer (1), R&D/Automation & Control (2), R&D/ Fuel injection (2)

Table 4
Interview Quotes.

Stage-specific factors at the four stages	Illustrative quote
Stage 1: Intuitive thinking	
Segregation	*I don't think that [email encryption] would be very much required here. Because I think, those side, the technical side being already covered by the company. (UAED5, officer)*
Information security contentment	*Do you think that you have enough information to protect information? It's enough or not, but I think I have not seen any urgency for improvement for information security. Because now I have not faced any experience that the information is disclosed to the wrong person. And also maybe because very negative consequence from that disclosure. I have not found kind of cases so that's why I don't see any emergency for that (ChinaC8, manager)*
Competence overestimation/ information security requirement underestimation	*Do you think that people have enough informational skills to protect information? Yeah. Everybody? Of course there are hundreds of people and everybody here are well qualified…I had some experience in a previous company and the company before that also. I have been working in this industry for the past nine or ten years, so of course I have enough [security compliance-related] skills (UAED1, manager).*
Between stages 1–2: Motivation enhancers	
Internal: IT interest and activity	*I keep myself updated by things. I read a lot…On the internet. And basically I get more information about information systems from my brother-in-law. He is a IT guy…most of the time I keep on discussing these things, like…he keeps on, informing me new technologies and new things and new techniques and things…You really need to have…willingness to learn about it or know about it. Or else nobody cares about it. (UAED5, officer)*
External: Media visibility	*Since I'm studying and surfing the Internet, reading a lot of stuff and some kind of computer addict, so I think you learn it by yourself, if, just if you think about that. And also, I think also when it started with Internet banking; you're really starting to be aware. (SwitzerlandB2, engineer)*
External: Information security accidents	Direct: *We did the mistake, now how can we improve by not doing it in future? Because we are working for a very critical department, so we are focusing on this kind of improvements very strongly. So we are calling a meeting. This information which went wrong to the customer, we did this, he did in this way, you are the other person in dptt. You make sure you do not repeat the same. (UAEC6, engineer)* Indirect: *The best way (to learn) is … listening to the people actually whoever had some bad experience. Say now whenever we hear something about bad experience from somebody then we definitely think about that if it happens to me, then what steps we will be taking. (UAEC7, unclear)*
Organizational control–related: Mandatory nature of information security procedures	*papers, regulations, nobody reads them [laughs], unfortunately. This is always the thing, you can bring some regulations, but if people work against it or with it, this is always the question. Because if you're not force the regulation through, it's not in. (SwitherlandA2, engineer)*
Organizational control–related: Monitoring	*we don't encourage employees to do personal things in the company laptop otherwise they will be seen by the headquarters…warning that people know it and they are actually being watched it is a good thing in order to control the employees using things which are not supposed to be done during working hours (UAEC15, officer)*
Rewards or sanctions	*When you manage people in China, you must set out a test. And the test, the result is related to his salary or bonus or some [laughs] gifts. Then we can make the information exactly in his mind, otherwise he's only "oh, listen," then out of the class, nothing new was in his mind. (…) we must have the award and penalty. (ChinaA14, manager)*
Stage 2: Declarative thinking	
Heteronomous: Dependency on authority	*I do not do it (lock the computer) here, because managers don't ask me to do that…The manager should ask their subordinates to follow every type of company rule (ChinaC11, manager)*
Heteronomous: Dependency of management's role model	*…when your manager is not complying to things the subordinates below you would take it, so likely that's okay; he is not too keen about that, why should we?* (UAE5, officer)
Heteronomous: Social conformity	*Humans are not only individuals. They are living in a group. And if the majority of the group is doing certain things, then the others will follow* (SwitzerlandD4, officer).
Information security conflict–related: Value conflict	*he says, "It's okay, if virus attacks my computer it's your business, your responsibility to remove those viruses, not me....I believe most of the people know the policy, know the guideline. Yes, but the problem is they don't think it's their responsibility, that's a major problem. (ChinaC5, manager)*
Information security conflict–related: Inconvenience	*Even after, even after the training that you mentioned, I don't think many people will use the complicated one [password]… It's inconvenient. Every time you change it, you have to remember it; it's hard.* (ChinaA13, officer)
Between stages 2–3: Reflection enhancers	
Experiential content of learning	*So if you are looking both to even the same picture we can both have different interpretations…If you have certain thing in mind, it is really difficult by reading, or by lecture or by words to change that… we need of course some pictures and we need to have the same interpretation of things…If you have a real case, then you cannot say this is, let's say, theoretical. That is the problem of many theoretical stuff, people don' t buy it because they say that you make it up…So if you find now mistakes…If you give these examples, that's very good of course, if you lecture that for people and say look we found, you think this it is okey, but you see what is the hazard or what is the danger of that. (UAED3, manager)*
Collaborative learning methods	Personal involvement during learning*: It can also be discussed with the employees themselves, so that they are involved in the discussion. So that there's a better understanding and a better way. And so that they follow better later on… Because they are involved in the process and finally, then, in the result. So that they feel that they are just involved and that they can bring in their opinion. It's always better if you are involved in the discussion and [are] part of the decision.* (SwitzerlandD4, officer) Participation in information security*: Would you like to participate in the development of these instructions? Of course. If it will develop my knowledge, so why not, because it's better if you know all the, what is really happening and what are the measures and all these things (UAEA1b, officer)*
Stage 3: Agency-related thinking	
Evaluation of risks	*Sometimes my feeling is other persons can have access to my emails. This is always in my mind and according this you have to adjust your behavior. What you write. What you sending out and what is coming in. (ChinaA16, engineer)*

(*continued on next page*)

Table 4 (*continued*)

Stage-specific factors at the four stages	Illustrative quote
Trust in information security procedures	*When I leave, for example I go outside, I need only press one button, I go. For me, what is the problem. I press some button and go. I hold my information, I will not lose my information. (DA3b)*
Value congruence	*I think in Human Resources you deal with so much sensitive information that it's clear that you have to be very careful of what you are telling to other people and so on. And if you, I don't know, have another profession..... [this may not be the case]..... If you are a carpenter, then that is no issue at all (SwitzerlandA5, officer)*
Between stages 3–4: Frequency enhancers	
Increasing susceptibility of information security risks	*Do you lock your PC when you leave it? Always…I don't want that somebody can do something with my PC, because if someone changed something within the source code of my program, I would have the hell to find what he has changed. How likely you think it could be? What do you think? Very rare, but even then. (SwitzerlandA2, officer)*
Reconciling behavioral efficiency	*regarding the Internet, yes there are some possible information security leaks. I think if you just at least act the same way as you I do it at home, and everyone should do. Don't download anything from the Internet, just from some sources you don't know and so on and so forth. Then these threats are more or less closed. (SwitzerlandC5, manager)*
Enhancing value connectivity	*It's always there with us that we work in HR and information picture is highly confidential. It's not a threat like but it's always [there]… I feel it's not a threat. A part of our basic routine which we do. We are aware so it, it just comes into us. It's not conscious effort that OK this we should, - we know this is highly confidential we will keep, we won't keep it on our desk. Just keep it close. If there are highly sensitive things to be discussed, we will close the doors and have a discussion so it's automatically there. (UAED9, officer)*
Stage 4: Routine-related thinking	
Agency cognitions explaining ISB with low cognitive effort	Has to be a reason. *No, that's sometimes because it's a habit.* Habit? *Yeah, just, lock and go, that's all…It just, also if I leave my computer open, in one minute it go by itself to lock down. I really don't know why I'm locking that. (UAEDA5b, manager)*
All stages: Overriding cognitions	
Work environment	*We feel like a family here. I've never had any problem with any colleague, and I've never heard of any problem happening between others"* (UAEDA5a, manager).
Taking a shortcut	*Maybe there's an emergency call…Or maybe his boss called to come to my office and he just ran. (ChinaC1, officer)*
Social pressure	Internal: *Before was one hundred percent. Now it is 90 percent, because of the environment, I think… its atmosphere. If every person was doing it, then nobody would disobey. If every person was not doing that, you would feel that [you were] idiot to do [it].* (ChinaC11, manager) External: *Maybe if someone puts enough pressure on it and says you really need now urgently that they give the access because they feel pressured, that they may be a bit scared and then they give the access although they should not.* (SwitzerlandC1, officer)
Opportunism	*they might try to behave unsafely so that they can get some information by doing this, you give me this I give you this…I think that I can imagine only this reason [for non-compliance] because I cannot imagine anything else.(UAED9, officer)*

topic, we specifically emphasized that anonymity of the company and interviewees is maintained in all circumstances and individual's opinions and experiences are not revealed even for the employer and can't be recognized based on our research outcomes. We also offered to write notes instead of recording our interviews, but all participants did not oppose recording. Furthermore, to avoid representing our own opinions of the research topic, it was emphasized that there were no right or wrong responses, but instead, understanding interviewees' personal views is in an essence in our study. The interview outline included the broad substantive information security themes including several open-ended questions based on interviewees' initial responses. Examples of the themes and related question are provided below:

1. **Background information**
2. **Awareness of the information security**
   - How do you understand information security? What information is the most valuable in your work? Do you experience any information security threats towards that information in your work surroundings?
3. **Information security competence: knowledge, skills and attitudes relating to protection activities**
   - Do you conduct any activities aimed at protecting valuable information (identified earlier)? Who has the responsibility over information security in your surroundings? Can you tell me more about this?
4. **Communications of information security issues**
   - Do you recognize any communications about information security in your surroundings? Please elaborate.
5. **Information security training and learning preferences**
   - How do you prefer learning things in general? What would be the best way to learn information security issues?
6. **Information security policies and compliance with the policies**
   - How do you understand the meaning of information security policies and instructions? What do you think about the current instructions and their applicability to the organization and own work? Do you think that the work community influences to the compliance of information security instructions? Why you/people in general comply/violate information security policies? What explains differences between people? Can you tell me more about that?
7. **Management's role, commitment and support in information security issues**
   - According to your experience, what is management's role in information security? How do you recognize if management is committed in information security? Do you expect more support from the management in information security issues?
8. **Existence and influence of monitoring, punishments and rewards**
   - Do you think information security activities should be monitored/punished/rewarded. Please elaborate.
9. **Change and improvement suggestions and questions**
   - Do you have any improvement ideas about information security issues in your organization?

Appendix C: interview quotes for stage-specific factors representing information security cognitions and enhancers of change, and stage-independent overriding cognitions

Appendix D: connection of the stage theory concepts with the previous is security behavior literature

Examples of the theory-based variables/factors of the previous information security literature with similar results for each individual component of the stage theory of employee compliance with information security procedures – information security cognitions, enhancers of change, and overriding cognitions - are listed in Table 5.

Table 5
Previous studies' theory-based concepts compared with stage theory factors.

Information security cognitions and enhancers of change at each stage	Existing research that supports information security cognitions and enhancers of change at each stage
Stage 1. intuitive thinking	
a. Intuitive cognitions	
Segregation	–
Competence overestimation and information security requirement underestimation	–
Information security contentment	–
b. Enhancers of change between stages 1–2: Motivation enhancers	–
Internal: Personal interest and activity	– Technology awareness (Dinev et al. 2009; Dinev and Hu 2007) – Computer and internet experience (Rhee et al., 2009) – Computer self-efficacy and apathy (Boss et al., 2009)
External: Media visibility	–
External: Direct and indirect information security accidents	– Security breach incidents lower self-efficacy (Rhee et al., 2009)
Organizational control–related: Mandatory nature of information security procedures	– Mandatoriness (Boss et al., 2009)
Organizational control–related: Monitoring	– Computer monitoring (D'Arcy et al. 2008) – Detection certainty (Herath and Rao 2009a; Herath and Rao 2009b) – Detection probability (Li et al., 2010) – Certainty of control (Chen et al., 2013) – Behavioral control (Cox, 2012; Hu et al., 2012) – Evaluation of compliance (Boss et al., 2009)
Organizational control–related: Sanctions	– Sanctions as a cost of non-compliance (Bulgurcu et al., 2010a) – Perceived severity of sanctions (D'Arcy et al. 2008) – The effect of sanction severity is conditioned on personal norms (Li et al., 2010) – Fear of punishments (preconventional moral reasoning) (Myyry et al., 2009) – Punishments (Chen et al., 2013) – Sanction certainty, sanction severity (Safa et al., 2019)
Organizational control–related: Rewards	– Rewards as a benefit of compliance (Bulgurcu et al., 2010a) – Rewards (Chen et al., 2013)
Stage 2. declarative thinking	
a. Declarative cognitions:	
Heteronomous: Dependency on authority	–
Heteronomous: Dependency on role model	– Management participation (Hu et al., 2012)
Heteronomous: Social conformity	– Normative beliefs (Bulgurcu et al., 2010a; Herath and Rao 2009b; Pahnila et al., 2007: Siponen et al., 2006) – Co-worker socialization (Chan et al., 2005) – Subjective norm (Dinev et al., 2009; Herath and Rao 2009a; Cox, 2012; Hu et al., 2012; Safa et al., 2019) – Descriptive norm (Herath and Rao 2009a) – Peer behavior (Herath and Rao 2009b) – Social influence (Johnston and Warkentin 2010) – Workgroup norm (Guo et al., 2011)
Information security conflict–related: Value conflict	– Denial of responsibility (Harrington 1996) – Value conflicts between IS security values and health care values (Hedström et al., 2011)
Information security conflict–related: Inconvenience	– Work impediment as a cost of compliance (Bulgurcu et al., 2010a) – Self-efficacy (Chan et al., 2005; Bulgurcu et al., 2010a; Herath and Rao 2009a; Johnston and Warkentin 2010; Ng et al., 2009; Siponen et al., 2007; Siponen et al., 2006; Cox, 2012; Vance et al., 2012; Rhee et al., 2009) – Perceived usefulness and ease of use, Controllability, Perceived behavioral control (Dinev and Hu 2007) – Response costs (Herath and Rao 2009a; Vance et al., 2012) – Usability issues (Sasse et al., 2001)
b. Enhancers of change between stages 2–3: Reflection enhancers:	
Experiential learning content	–
Collaborative learning methods	– Organizational involvement (Lee et al., 2004) – Involvement: energy, time and effort (Safa et al., 2018) – Involvement: knowledge sharing, collaboration, intervention and experience (Safa et al., 2016)
STAGE 3. AGENCY-RELATED THINKING	
a. Agency cognitions:	
Trust in information security procedures	– Safety of resources as a benefit of compliance (Bulgurcu 2010a) – Response efficacy (Herath and Rao 2009a; Johnston and Warkentin 2010; Siponen et al., 2007; Siponen et al., 2006; Vance et al., 2012) – Perceived effectiveness (Herath and Rao 2009b) – Perceived benefits (Ng et al., 2009) – General controllability of IS security threats (Rhee et al., 2009)
Evaluation of risks	– Vulnerability of resources as a cost of non-compliance (Bulgurcu et al., 2010a) – Security breach concern level (Herath and Rao 2009a) – Perceived threat severity (Johnston and Warkentin 2010) – Perceived security risks (Li et al., 2010; Guo et al., 2011) – Perceived susceptibility and severity of security incidents (Ng et al., 2009) – Threat appraisal (Pahnila et al., 2007; Siponen et al., 2007; Siponen et al., 2006; Vance et al., 2012) – Perceived vulnerability (Cox, 2012)

(*continued on next page*)

Table 5 (*continued*)

Information security cognitions and enhancers of change at each stage	Existing research that supports information security cognitions and enhancers of change at each stage
Value congruence	– Intrinsic benefits as a benefit of compliance (Bulgurcu et al., 2010a) – Organizational commitment (Herath and Rao 2009) – Relative advantage for job performance (Guo et al., 2011) – Perceived identity match (Guo et al., 2011) – Perceived value congruence (Son 2011) – Commitment (Safa et al., 2016; 2018) – Personal norms (Safa et al., 2016; 2018)
b. Enhancers of change between stages 3–4: Frequency enhancers	
Increasing susceptibility of information security risks	–
Reconciling behavioral efficiency	–
Enhancing value connectivity	–
STAGE 4. ROUTINE-RELATED THINKING	
a. Routine-related cognitions	
Agency cognitions explaining ISB with low cognitive effort	– Habits (Pahnila et al., 2007; Vance et al., 2012)
Common cognitions for Stages 1–4: Overriding Cognitions	
Opportunism	– Attitude in terms of work ethics (Dinev and Hu 2007) – Norms related with law compliance (Lee et al., 2004) – Perceived benefits, personal norms (Li et al., 2010) – Lack of attributed trust explain computer abuse (Posey et al., 2011) – Perceived legitimacy of ISPs (Son 2011) – Positive attitude towards IS security behavior (Bulgurcy et al., 2010a; Cox, 2012; Hu et al., 2012; Pahnila et al., 2007) – Situational crime prevention (Safa et al., 2018 ; Safa et al., 2019)
Social Pressure	– Intrinsic costs as a cost of noncompliance (Burgurcu et al. 2010a)
Working Environment	–
Shortcuts	–

CRediT authorship contribution statement

Mari Karjalainen: Conceptualization, Methodology, Investigation, Resources, Data curation, Writing - original draft, Writing - review & editing, Project administration, Funding acquisition. **Mikko Siponen:** Methodology, Investigation, Resources, Data curation, Writing - original draft, Writing - review & editing, Visualization, Supervision, Project administration, Funding acquisition. **Suprateek Sarker:** Methodology, Resources, Writing - original draft, Writing - review & editing, Visualization, Supervision, Project administration, Funding acquisition.

References

Adams, A., Sasse, M.A., 1999. Users are not the enemy. Commun. ACM 42 (12), 40–46.

Albrechtsen, E., 2007. A qualitative study of user's view on information security. Comp. Secur. 26 (4), 276–289.

Albrechtsen, E., Hovden, J., 2010. Improving information security awareness and behavior through dialogue, participation and collective reflection. Inter. Study. Comp. Secur. 29, 432–445.

Alohali, M., Clarke, N., Li, F., Furnell, S., 2018. Identifying and predicting the factors affecting end-users' risk-taking behavior. Inf. Comp. Secur. 26 (3), 306–326.

Borena, B. & Bélanger, F. (2013) Religiosity and information security policy compliance. Proceedings of the Nineteenth Americas Conference on Information Systems, Chicago, Illinois, August 15-17, 1–8.

Boss, S.R., Galletta, D.F., Lowry, P.B., Moody, G., Polak, P., 2015. What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. MIS Q. 39 (4), 837–864.

Boss, S.R., Kirsch, L.J., Angermeier, I., Shingler, R.A., Boss, W., 2009. If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. Eur. J. Inf. Syst. 18, 151–164.

Bresman, H., 2013. Changing routines: a process model of vicarious group learning in pharmaceutical R&D. Acad. Manag. J. 56 (1), 35–61.

Bulgurcu, B., Cavusoglu, H., Benbasat, I., 2010a. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Q. 34 (3), 523–548.

Bulgurcy, B., Cavusoglu, H. & Benbasat, I. (2010b) Quality and fairness of an information security policy as antecedents of employees' security engagement in the workplace: an empirical investigation. Proceedings of the 43rd Hawaii International Conference on System Sciences.

Burton-Jones, A., McLean, E.R., Monod, E., 2015. Theoretical perspectives in IS research: from variance and process to conceptual latitude and conceptual fit. Eur. J. Inf. Syst. 24 (6), 664–679.

Carnes, M., Devine, P.G., Isaac, C., Manwell, L.B., Ford, C.E., Byars-Winston, A., Fine, E., Sherida, J.T., 2012. Promoting institutional change through bias literacy. J Divers High Educ 5 (2), 63–77.

Chan, M., Woon, I., Kankanhalli, A., 2005. Perceptions of information security in the workplace: linking information security climate to compliant behavior. J. Inf. Privacy. Secur. 1 (3), 18–41.

Chen, Y., Ramamurthy, K.R., Wen, K.-W., 2013. Organizations' information security policy compliance: stick or carrot approach. J. Manag. Inf. Syst. 29 (3), 157–188.

Cox, J., 2012. Information systems user security: a structured model of the knowing-doing gap. Comput. Hum. Behav. 28, 1849–1858.

D'Arcy, J., Greene, G., 2014. Security culture and the employment relationship as drivers of employees' security compliance. Inf. Manag. Comp. Secur. 22 (5), 474–489 232.

D'Arcy, J. & Greene, G. (2009) The multifaceted nature of security culture and its influence on end user behavior. IFIP TC 8 International Workshop On Information Systems Security Research, Cape Town South Africa, May 29–30.

D'Arcy, J., Herath, T., 2011. A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. Eur. J. Inf. Syst. 20 (6), 643–658.

D'Arcy, J., Hovav, A., 2007. Deterring internal information systems misuse. Commun. ACM 50 (10), 113–117.

D'Arcy, J., Hovav, A., Galletta, D.F., 2008. User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. Inf. Syst. Res. 20 (1), 79–98.

Deci, E.L., Ryan, R.M., 1987. The support of autonomy and the control of behavior. J. Pers. Soc. Psychol. 53 (6), 1024–1037.

Dinev, T., Goo, J., Hu, Q., Nam, K., 2009. User behaviour towards protective information technologies: the role of national cultural differences. Inf. Syst. J. 19, 391–412.

Dinev, T., Hu, Q., 2007. The centrality of awareness in the formation of user behavioral intention toward protective information technologies. J. Assoc. Inf. Syst. 8 (7), 386–408.

Feyerabend, P., 1975. Against method. Outline of an Anarchistic Theory of Knowledge. New Left Books, London.

Foth, M., 2016. Factors influencing the intention to comply with data protection regulations in hospitals: based on gender differences in behaviour and deterrence. Eur. J. Inf. Syst. 25, 91–109.

Furnell, S.M., Alotaibi, F., & Esmael, R. (2019) Aligning security practice with policy: guiding and nudging towards better behavior. Proceedings of the 52nd Hawaii International Conference on System Sciences (HICSS), 5618–5627.

Furnell, S., Moore, L., 2014. Security literacy: the missing link in today's online society? Comp. Fraud. Secur. 5, 12–18.

Gudykunst, W.B., 1994. Bridging differences. Effective Intergroup Communication. Sage, London.

Guo, K.H., Yuan, Y., Archer, N.P., Connelly, C.E., 2011. Understanding non-malicious security violations in the workplace: a composite behavior model. J. Manag. Inf. Syst. 28 (2), 203–236.

Geller, E.S., 2002. The challenge of increasing pro-environment behavior. In: Bechtel, R.B., Churchman, A. (Eds.), Handbook of Environmental Psychology. Wiley, New York, pp. 525–540.

Green, M., 1989.

Hare, R.M., 1963. Freedom and Reason. Oxford University Press, Oxford, UK.

Harrington, S.J., 1996. The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. MIS Q. 20 (3), 257–278.
Hatton, N., Smith, D., 1995. Reflection in teacher education: towards definition and implementation. Teach. Teach. Educ. 11 (1), 33–49.
Hedström, K., Kolkowska, E., Karlsson, F., Allen, J.P., 2011. Value conflicts for information security management. J. Strateg. Inf. Syst. 20, 373–384.
Hedström, P., Swedberg, R., 1998. Social mechanisms: an introductory essay. In: Hedström, P., Swedberg, R. (Eds.), Social mechanisms. An analytical Approach to Social Theory. Cambridge University Press, New York, Cambridge UK.
Herath, T., Rao, H.R., 2009a. Protection motivation and deterrence: a framework for security policy compliance in organizations. Eur. J. Inf. Syst. 18 (2), 106–125.
Herath, T., Rao, H.R., 2009b. Encouraging information security behaviors in organizations: role of penalties, pressures, and perceived effectiveness. Decis. Support Syst. 47, 154–165.
Heyward, M., 2002. From international to intercultural. Redefining the international school for a globalized world. J. Res. Int. Educ. 1 (1), 9–32.
Hovav, A., D'Arcy, J., 2012. Applying an extended model of deterrence across cultures: an investigation of information systems misuse in the U.S. and South Korea. Inf. Manag. 49, 99–101.
Howell, W.S., 1982. The Empathic Communicator. Wadsworth Publishing Company, University of Minnesota.
Hsieh, H.-F., Shannon, S.E., 2005. Three approaches to qualitative content analysis. Qual. Health Res. 15 (9), 1277–1288.
Hu, Q., Dinev, T., Hart, P., Cooke, D., 2012. Managing employee compliance with information security policies: the critical role of top management and organizational culture. Dec. Sci. 43 (4), 615–659.
Ifinedo, P., 2014. Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition. Inf. Manag. 51, 69–79.
Ifinedo, P., 2012. Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. Comp. Secur. 31 (1), 83–95.
Johns, G., 2006. The essential impact of context on organizational behavior. Acad. Manag. Rev. 31 (2), 386–408.
Johnston, A.C., Warkentin, M., 2010. Fear appeals and information security behaviors: an empirical study. MIS Q. 34 (3), 549–566.
Johnston, A.C., Warkentin, M., Siponen, M., 2015. An enhanced fear appeal rhetorical framework: leveraging threats to the human asset through sanctioning rhetoric. MIS Q. 39 (1), 113–134.
Kaiser, F.G., Fuhrer, U., 2003. Ecological behavior's dependency on different forms of knowledge. Appl. Psychol. 52 (4), 598–613.
Karjalainen, M., Siponen, M., Puhakainen, P., Sarker, S., 2013. One Size Does Not Fit All: Different Cultures Require Different Information Systems Security Interventions. Pasific Asia Conference of Information Systems, Jeju Island, Korea.
Karjalainen, M., Siponen, M., 2011. Toward a new meta-theory for designing information systems (IS) security training approaches. J. Assoc. Inf. Syst. 12 (8), 518–555.
Karjalainen, Mari, Siponen, Mikko, Sarker , Suprateek, et al., 2019. Towards a Theory of Information Systems security Behaviors of Organizational Employees: A dialectical Perspective. Inf. Syst. Res. 30 (2), 687–704.
Klein, H.K., Myers, M.D., 1999. A set of principles for conducting and evaluating interpretive field studies in information systems. MIS Q. 23 (1), 67–93.
Kohlberg, L., 1981. Essays on moral development. Vol. I: The Philosophy of Moral Development. Harper & Row, San Francisco, CA.
Kolkowska, E., Dhillon, G., 2013. Organizational power and information security rule compliance. Comp. Secur. Spec. Issue 33, 3–11.
Kruger, H.A., Kearney, W.D., 2006. A prototype for assessing information security awareness. Comp. Secur. 25 (4), 289–296.
Kübler-Ross, E., Kessler, D., 2006. On Grief and grieving: Finding the Meaning of Grief Through the Five Stages of Loss. Scribner, New York.
Lee, A.S., 1991. Integrating positivist and interpretive approaches to organizational research. Organ. Sci. 2 (4), 342–365.
Lee, S.M., Lee, S.G., Yoo, S., 2004. An integrative model of computer abuse based on social control and general deterrence theories. Inf. Manag. 41 (6), 707–718.
Li, H., Zhang, J., Sarathy, R., 2010. Understanding compliance with internet use policy from the perspective of rational choice theory. Decis. Support Syst. 48, 635–645.
Li, H. Zhang, J. & Sarathy, R. (2009) Understanding the compliance with the internet use policy from a criminology perspective. Proceedings of the Fifteenth Americas Conference on Information Systems, San Francisco, California August 6th-9th. Paper 418, 1–8.
Louis, M.R., Sutton, R.I., 1991. Switching cognitive gears: from habits of mind to active thinking. Hum. Relat. 44 (1), 55–76.
Lowry, P.B., Moody, G., 2015. Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. Inf. Syst. J. 25, 433–463.
May, G.D., Kruger, M.J., 1988. The manager within. Person. J. 67 (2), 56–65.
Mohr, L.B., 1982. Explaining Organizational Behavior. Jossey-Bass, San Francisco.
Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., Vance, A., 2009. What levels of moral reasoning and values explain adherence to information security rules? An empirical study. Eur. J. Inf. Syst. 18, 126–139.
Ng, B., Kankanhalli, A., Xu, Y., 2009. Studying users' computer security behavior: a health belief perspective. Decis. Support Syst. 46, 815–825.
Nolan, R., 1973. Managing the computer resource: a stage hypothesis. Commun. ACM 16 (4), 399–405.
O'Reilly, C., Chatman, J., 1986. Organizational commitment and psychological attachment: the effects of compliance, identification, and internalization on prosocial behavior. J. Appl. Psychol. 71 (3), 492–499.
Ouellette, J.A., Wood, W., 1998. Habit and intention in everyday life: the multiple processes by which past behavior predicts future behavior. Psychol. Bull. 124 (1), 54–74.
Pahnila, S., Siponen, M. & Mahmood, A. (2007) Employees' behavior towards IS security policy compliance. Proceedings of the 40th Annual Hawaii International Conference On System Sciences (HICSS'07), 156b-156b.
Patton, M.Q. (1990) Qualitative evaluation and research methods. Sage: Newbury Park CA.
Ponemon Institute (2014a) 2014: a year of megabreaches. Sponsored by Identity Finder. Available: http://www.identityfinder.com/us/Files/2014TheYearOfTheMegaBreach.pdf.
Ponemon Institute (2014b) 2014 Cost of data breach study: global analysis. Benchmark research sponsored by IBM. Available: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&appname=GTSE_SE_SE_USEN&htmlfid=SEL03027USEN&attachment=SEL03027USEN.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. Comp. Secur. 30, 486–497.
Prochaska, J.O., DiClemente, C.C., 1983. Stages and processes of self-change of smoking: toward an integrative model of change. J. Consult. Clin. Psychol. 51 (3), 390–395.
Prochaska, J.O., DiClemente, C.C., Norcross, J.C., 1992. In search of how people change. Applications to addictive behaviors. Am. Psychol. 47 (9), 1102–1114.
Reichenbach, H. (1938) Experience and prediction: an analysis of the foundations and the structure of knowledge. University of Chicago Press.
Rhee, H.S., Kim, C., Ryu, Y.U., 2009. Self-efficacy in information security: its influence on end users' information security practice behavior. Comp. Secur. 28, 816–826.
Rogers, R.W., 1975. A protection motivation theory of fear appeals and attitude change. J. Psychol. 91 (1), 93–114.
Ryan, R.M., Patrick, H., Deci, E.L., Williams, G.C., 2008. Facilitating health behavior change and its maintenance: interventions based on self-determination theory. Eur. Health Psychol. 10, 2–5.
Sabherwal, R., Robey, D., 1995. Reconciling variance and process strategies for studying information system development. Inf. Syst. Res. 6 (4), 303–327.
Safa, N.S., Maple, C., Furnell, S., Azad, M.A., Perera, C., Dabbagh, M., Sookhak, M., 2019. Deterrence and prevention-based model to mitigate information security insider threats in organisations. Fut. Gener, Comp. Syst, 97, 587–597.
Safa, N.S., Maple, C., Watson, T., Von Solms, R., 2018. Motivation and opportunity based model to reduce information security insider threats in organisations. J. Inf. Secur. Appl. 40, 247–257.
Safa, N.S., Maple, C., 2016. Human errors in the information security realm – and how to fix them. Comp. Fraud. Secur. 9, 17–20.
Safa, N.S., Von Solms, R., Furnell, S., 2016. Information security policy compliance model in organizations. Comp. Secur. 56, 70–82.
SafeNet (2014). Customer sentiment survey. Available: http://www.safenet-inc.com/news/2014/data-breaches-impact-on-customer-loyalty-survey/#sthash.VfTVqGI5.dpuf.
Sasse, A., Brostoff, S., Weirich, D., 2001. Transforming the 'weakest link. human / computer interaction approach to usable and effective security. BT Technol. J. 19 (3), 122–131.
Schulze, U., Avital, A., 2011. Designing interviews to generate rich data for information systems research. Inf. Organ. 21, 1–16.
Schwarzer, R., 2008. Some burning issues in research on health behavior change. Appl. Psycho. 57 (1), 84–93.
Shropshire, J., Warkentin, M., Sharma, S., 2015. Personality, attitudes, and intentions: predicting initial adoption of information security behavior. Comp. Secur. 49, 177–191.
Siponen, Mikko, 2001. On the Role of Human Morality in Information System Security: From the Problems of Descriptivism to Non-Descriptive Foundations. Inf. Resour. Manag. J. 14 (4), 15–23.
Siponen, M., Mahmood, M.A., Pahnila, S., 2014. Employees' adherence to information security policies: an exploratory field study. Inf. Manag. 51, 217–224.
Siponen, M.T., Pahnila, S. & Mahmood, A. (2007) Employees' adherence to information security policies: an empirical study. In: New Approaches For security, Privacy and Trust in Complex Environments, Venter, H., Eloff, M., Labuschagne, L., Eloff, J. & von Solms, R. (eds.), 133–144. Proceedings of the IFIP TC-11 22nd International Information Security Conference (SEC 2007), 14–16 May 2007, Sandton, South Africa, 232/2007.
Siponen, M., Pahnila, S. & Mahmood, A. (2006) Factors influencing protection motivation and is security policy compliance. Innovations in Information Technology, 1–5.
Siponen, M., Vance, A., 2010. Neutralization: new insights into the problem of employee information systems security policy violations. MIS Q. 34 (3), 487–502.
Sommestad, T., Hallberg, J., Lundholm, K., Bengtsson, J., 2014. Variables influencing information security policy compliance. A systematic review of quantitative studies. Inf. Manag. Comput. Secur. 22 (1), 42–75.
Son, J.Y., 2011. Out of fear or desire? Toward a better understanding of employees' motivation to follow is security policies. Inf. Manag. 48, 296–302.
Sperber, D., 1997. Intuitive and reflective beliefs. Mind Language 12 (1), 67–83.
Stanton, J.M., Stam, K.R., Guzman, I. & Caldera, C. (2003) Examining the linkage between organizational commitment and information security. In IEEE Systems, Man, and Cybernetics Conference. Washington DC, USA.
Stanton, J.M., Stam, K.R., Mastrangelo, P., Jolton, J., 2005. Analysis of end user security behaviours. Computers and Security 24 (2), 124–133.

Straub, D.W., 1990. Effective is security: an empirical study. Inf. Syst. Res. 1 (3), 255–276.
Theoharidou, M., Kokolakis, S., Karyda, M., Kiountouzis, E., 2005. The insider threat to information systems and the effectiveness of ISO17799. Comput. Secur. 24, 472–484.
Thompson, J.L., 1996. Strategic effectiveness and success: the learning challenge. Manag. Dec. 34 (7), 14–22.
Thornberry, T.P., 1987. Toward an interactional theory of delinquency. Criminology 25 (4), 863–891.
Tost, L.P., 2011. An integrative model of legitimacy judgments. Acad. Manage. Rev. 36 (4), 686–710.
Tsohou, A., Karyda, M., Kokolakis, S., 2015. Analyzing the role of cognitive and cultural biases in the internalization of information security policies: recommendations for information security awareness programs. Comput. Secur. 52, 128–141.
Van de Ven, A.H., 1992. Suggestions for studying strategy process: a research note. Strateg. Manag. J. 13, 169–191.
Vance, A., Siponen, M., Pahnila, S., 2012. Motivating IS security compliance: insights from habit and protection motivation theory. Inf. Manag. 49, 190–198.
Warkentin, M., Johnston, A.C., Shropshire, J., 2011. The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. Eur. J. Inf. Syst. 20 (3), 267–284.
Velicer, W.F., Prochaska, J.O., 2008. Stage and non-stage theories of behavior and behavior change: a comment on schwarzer. Appl. Psychol. An Int. Rev. 57, 75–83.
Venkatesh, V., Thong, J.Y.L., Chan, F.K.Y., Hu, P.J-H., Brown, S.A., 2011. Extending the two-stage information systems continuance model: incorporating UTAUT predictors and the role of context. Inf. Syst. J. 21, 527–555.
Weinstein, N.D., Rothman, A.J., Sutton, S.R., 1998. Stage theories of health behavior: conceptual and methodological issues. Health Psychol. 17 (3), 290–299.
Vroom, C., von Solms, R., 2004. Towards information security behavioral compliance. Comput. Secur. 23 (3), 191–198.

Mari Karjalainen is postdoctoral researcher in the University of Oulu. She has a Master's degree in Education and holds a Ph.D. in Information Processing Science. Her research interests include IS security behavior, training, and decision-making processes. She has published papers in journals such as *Journal of the Association for Information Systems*.

Mikko Siponen is a professor of Information Systems at the University of Jyväskylä. He holds a Ph.D. in philosophy from the University of Joensuu, Finland, and a Ph.D. in Information Systems from the University of Oulu, Finland. His-research interests include IS security, IS development, computer ethics, and philosophical aspects of IS. Mikko has published more than 70 articles in journals such as *MIS Quarterly, Journal of the Association for Information Systems, Information & Management, European Journal of Information Systems, Information & Organization, Communications of the ACM, IEEE Computer, IEEE IT Professional*, and others. He has received over 10 million EUR of research funding from corporations and numerous funding bodies. He has been a track chair for the International Conference on Information Systems and the European Conference on Information Systems three times. His-other editorial board experiences include positions with *Journal of the Association for Information Systems, European Journal of Information Systems, Information & Management*, and *Communications of the Association for Information Systems*.

Suprateek Sarker Suprateek Sarker is Rolls-Royce Commonwealth Commerce Professor at the McIntire School of Commerce, University of Virginia. His-past work has been published in many leading journals. He is a Senior Editor of ISR, on the Board of Editors of JMIS, the out-going EIC of JAIS, and former Senior Editor of MISQ and Decision Sciences.