Toward Process Theories on Employees' Compliance with IS Security Procedures: An Empirical Study

Mari Karjalainen, Mikko Siponen and Suprateek Sarker

Abstract

Employees' compliance with IS security policies has become an important area in IS security research. Existing research has applied variance or factor model settings aimed explaining or predicting IS security behavior. We submit that IS security behavior compliance is not static in nature, as implicitly characterized in existing variance studies relying on a "snapshot view" of the phenomenon, but dynamic where the importance lies in understanding how the behavior develops. The lack of such a development perspective in current research means that the previous research offers an incomplete view of employees' IS security policy compliance, and may result non-effective treatments aimed at improving employees' behavior.

In this study, we take the first step toward closing this gap in the research through the development of a process theory, which outlines the different stages toward IS security policy compliance behavior.

For IS security research, our study suggests the need to investigate IS security behavior from new paradigm, which is built upon understanding the development trajectory, stages of the IS security behavior, and stage-specific cognitions, barriers, and impetus factors. For IS security practice, our results suggest that understanding the process is necessary for designing optimal interventions for improving employees' IS security behavior.

Keywords: IS security, IS security policy compliance, Process theory

1. Introduction

The increasingly central role of information and IT at organizations has made information security a key concern for organizations. Not surprisingly, Information systems (IS) scholars have devoted increasing attention to questions of information security as evinced by special issues of *MIS Quarterly* (Mahmood et al. 2010) and the *European Journal of Information Systems* (Warkentin & Willison 2009). One of the key issues identified in the IS security literature pertains to how employees view information security. This research stream is based on the practical problem that although organizations have published policies in place on information security that prescribe required behavior, employees barely comply with these policies (Siponen & Vance, 2010). This is a problem, because if users do not comply with IS security policies, security solutions, however technically sophisticated, lose their effectiveness (Kruger & Kearney, 2006).

To understand why employees comply (or do not comply) with information security policies, IS security scholars have, in the past, formulated variance or factor models, by drawing upon theories from social psychology (e.g., Protection Motivation Theory), and criminology (e.g., Deterrence Theory) (Straub, 1990; Siponen & Vance, 2010). An alternative to variance models is the view offered by process models, which are increasingly being used in social psychology, moral psychology, and criminology (e.g., Prochaska et al., 1992; Prochacka & DiClemente, 1983, 1988). In these fields, such process or stage theories are seen to be necessary, because human behavior is seen as complex behavior, which is hard to capture using variance perspectives that do not model change or development. Indeed, research shows that human behavior in the areas of health decisions (Prochaska et al., 1992; Prochacka & DiClemente, 1983; Weinstein et al., 1998; Briedle, Riemsma, Pattenden, Sowden et al., 2005), moral psychology (Kohlberg, 1981), and criminology (Thornberry, 1987) unfolds and is best captured as a series of stages. Our premise underlying this work is that employees' IS security compliance behavior also develops dynamically over time, and the static, factor-based conceptualizations (Siponen & Vance, 2010; Warkentin & Johnston, 2010; Puhakainen & Siponen, 2010), while valuable, are necessarily incomplete.

In this study, we take the first step toward closing this gap in the research. More specifically, this study develops a process model aimed at providing an understanding of how and why employees' IS security behavior may change over time, highlighting the sequence of stages into which all employees could be classified, and the barriers of change that produce or impede movement from one stage to another.

Such research is worthwhile for both research and practice. For IS security research, the results suggest the need to understand IS security behavior development through the concepts of development stages, stage-specific cognitions, barriers, and impetus factors. For practice, such a process theory is needed to match interventions with people by identifying the stage they have

reached in changing behavior and helping them overcome the specific barriers that impede transition to the next stages (cf., Briedle, Riemsma, Pattenden, Sowden et al., 2005).

The rest of this paper is organized as follows. The second section discusses the difference between process theories and variance (factor) models/theories and concludes with a review of the previous literature on employees' compliance with IS security behavior by stating that existing research has not studied the topic from the viewpoint of process theories. Meta-theories of process theories and corresponding criterion for process theories are introduced in section three.

The data collection and inductive analysis procedures are described in section four. A process theory of employees' adoption of IS security procedures based on a set of interviews is described and theorized in the fifth section. The sixth section outlines the implications for practice and research and, finally, the seventh section summarizes the key findings of the paper.

2. Process Theories and Requirements for Process Theories

In section 2.1, we briefly highlight process theories in IS and point out the need to synthesize requirements for Process theories. Section 2.2 presents these requirements for process theories.

2.1. Variance models and the need for process theories/models

The origins of process models can be traced back to Heraclitus, who believed as early as 500 BC that a river is not a stable object but an ever-changing flow. Later, process theories were introduced in various disciplines ranging from management science and human development to IS. In IS, especially qualitative process models are influenced by Mohr's (1982) conception of the process model, including those by Markus and Robey (1988), Montealegre and Keil (2000), McLeod and Doolin (2012), Thummadi et al. (2011), Newman and Robey (1992), Robey and Newman (1996), Lyytinen et al. (2009), Sarker and Sahay (2003), and more recently by Chakraborty et al. (2010). The common assumption among these process theories is that no

phenomenon is static but develops through stages or events. This results in process models not only viewing the time order of events or stages as important but also expecting that the time order may change over time (Burton-Jones et al., 2013). Following Mohr (1982), in the IS and organizational literature, process models are often contrasted with variance models (Mohr, 1982; Newman & Robey, 1992; Burton-Jones et al., 2013). In variance models, the aim is to find variables or factors (independent variables) that predict the phenomenon in question, such as employees' compliance with IS security procedures (dependent variable) (Burton-Jones et al., 2013). Moreover, variance models view employees' compliance with IS security procedures as unidirectional causal structures that represent employees' compliance with security policies in a static rather than dynamic fashion, without examining developmental progressions (see Thornberry, 1987; Weinstein et al., 1998). This is the case, since in variance models, time ordering among independent variables (properties) is irrelevant and variables do not change over time (only the scale-item measurement value may change from one context or sample to another) (Burton-Jones et al., 2013). Indeed, variance models seem to have difficulty capturing a phenomenon in which these assumptions (e.g., the phenomenon develops and changes over time; the time order of things is important; there are different stages with different independent variables) hold. Given that variance models are subjected to these potential boundary conditions, critical concerns have been expressed about variance models:

> "*Is it reasonable to assume that behavior change can be described by a single prediction equation? Many natural phenomena pass through qualitatively different stages. Water, for example, changes from solid to liquid to gas. Insects of the order Lepidoptera develop from egg to caterpillar to chrysalis to butterfly.*" (Weinstein *et al*., 1998)

Although this rhetoric regarding variance models looks appealing, it does not sufficiently define what exactly **a process theory** is. Although the definitions in IS, based on the "variance model, [which is] based on static independent variables that do not change over time," are enough to capture some models without mediators, there are variance models in which this view does not hold (e.g., Johnston & Warkentin, 2010; Burton-Jones et al., 2013). Further, variance studies with longitudinal data and analysis have been featured in the literature, albeit infrequently (e.g.,

Kim, 2009). Interestingly, while researchers acknowledge the existence of (and relevance of) processes in the IS domain, such acknowledgement is not followed up by theorizing about the processes. Before we can build a process theory, we need to understand what makes a theory a process theory. This issue is briefly outlined in the following sub-section.

2.2 Requirements for IS security behavioral process theories

This sub-section synthesizes the requirements for process theories of IS security behavior based on two meta-characteristics of process theories (Weinstein et al., 1998; Rutter & Quine, 2002) and four paradigms of process theories (van de Ven, 1992); see Table 1. Van de Ven (1998) provides generic requirements for process theories, while Weinstein et al. (1998) provide important viewpoints related to behavior change, which is essential in the context of IS security behavior (Karjalainen & Siponen, 2011; Siponen, 2000; Johnston & Warkentin, 2010). Table 1 provides a summary of the requirements. These nine criteria for process theories, based on van de Ven (1992) and Weinstein et al. (1998), are elaborated upon in Appendix 1.

Requirements for process theories	**Source**
(1) Process theories must have stages, which are ordered and define the development trajectory.	Weinstein et al. (1998)
(2) Process theories must take a stand regarding whether the stages are predefined or not	van de Ven (1992), Rutter and Quine (2002)
(3) Process theories must include similar attributes (barriers of change)	Weinstein et al. (1998)
(4) Process theories must include different attributes (barriers at different stages)	Weinstein et al. (1998)
(5) Process theories must define whether the progression from one stage to another is linear or not (yes; mainly yes; or no)	van de Ven (1992)
(6) Process theories must define whether the progression is unitary or multiple	van de Ven (1992)
(7) Process theories must define whether the progression is cumulative	van de Ven (1992)
(8) Process theories must define whether the possibility of relapse exists	van de Ven (1992)
(9) Process theories must define whether the goal of development progression is known and predetermined	van de Ven (1992)

Table 1. Requirements for process theories.

3. Previous Empirical Work in IS Security

This section provides a review of extant research and highlights the gap in the body of knowledge. Specifically, we show that previous research has not examined the issue of employee compliance with IS security policies from a process perspective. Although the previous literature does have a few instances wherein the dynamic nature of the phenomenon in acknowledged and modeled using a variance perspective, these works do not represent process theories and thus do come close to satisfying the requirements summarized in Table 1.

Authors	Theory type	Theoretical background	Main results
1. Models on computer abuse/misuse			
Harrington (1996)	Variance approach with a moderator	Ethical decision making, deterrence theory	- Ethical statements (IV) influence computer abuse judgments and intentions (DV) - Responsibility denial (M) is related to computer abuse judgments and intentions
Lee et al. (2004)	Variance approach with antecedent variables	Social control theory, deterrence theory, theory of planned behavior, and theory of reasoned action	- Involvement and norms (AV) affect employees' intention to control others' computer abuse (IV), which decreases insiders' computer abuse (DV)
D'Arcy et al. (2008)	Variance approach with antecedent variables	Deterrence theory	- IS security policy awareness, training, and monitoring (AV) deter IS misuse (DV) - Severity of sanctions (IV) is more effective than certainty of sanctions (IV)
D'Arcy & Hovav (2007)	Variance approach		- Security awareness programs, awareness of IS security procedures, and preventive security software (IV), respectively, reduce IS misuse intentions (DV) - Awareness of computer monitoring does not reduce IS misuse intentions
2. Models on compliance with IS security procedures			
Siponen et al. (2006)	Variance approach with antecedent variables	Protection motivation theory	- Visibility and normative beliefs (AV1) influence threat appraisal and coping appraisal (AV2) - Threat appraisal (AV2) influences the intention to comply (IV) - Intention to comply (IV) influences actual compliance (DV)
Herath & Rao (2009a)	Variance approach with antecedent variables	Protection motivation theory, deterrence theory, organizational commitment, theory of planned behavior, and decomposed theory of planned behavior	- IS security policy attitudes (IV) are influenced by high security breach concerns, response efficacy, self-efficacy, and response cost perceptions (AV1) - Intention to comply (DV) is influenced by subjective and descriptive norms, certainty of detection, severity of penalty, and self-efficacy, and is not influenced by attitudes toward IS security policies (IV) - Security breach concerns are influenced by severity (AV2), but not probability - Availability of recourse (AV1) increases self-efficacy (IV)

Authors	Theory type	Theoretical background	Main results
			- Organizational commitment (AV2) increases response efficacy (AV3)
Johnston & Warkentin (2010)	Variance approach with experiment and antecedent variables	Protection motivation theory	- Fear appeals influence intentions to comply with recommended computing practices: perceived threat severity (AV) influence the statements of efficacy (IV) that, along with social influence, explain intention to comply (DV)
Ng et al. (2009)	Variance approach with a moderator	Health belief model	- Susceptibility, benefits, and self-efficacy (IV) are determinants of email-related security behavior (DV) - Severity (M) moderates the effects of benefits, general security orientation, cues to action, and self-efficacy
Herath & Rao (2009b)	Variance approach	Literature in agency theory	- Intention (DV) is influenced by subjective norms and peer behaviors, effectiveness, and certainty of detection (IV), and not influenced by severity of punishment
Li et al. (2010)	Variance approach with a moderator	Rational choice theory	- Intention to comply with Internet procedures (DV) is influenced by benefits, detection probability, personal norms, and security risks (IV) - The influence of sanction severity (IV) is moderated by personal norms (M) - Organizational norms and organizational identification influence personal norms
Myyry et al. (2009)	Variance approach	Theory of cognitive moral development, and the theory of motivational types of values	- Preconventional moral reasoning (IV) influences users' compliance (DV) - Openness to change (IV) influences compliance (DV) - Hypothetical and actual behavioral compliance are related to each other (at least in the case of giving one's password to others)
Bulgurcy et al. (2010a)	Variance approach with antecedent variables	Theory of planned behavior	- Compliance intention (DV) is influenced by attitude, normative beliefs, and self-efficacy (IV) - Intrinsic benefit, safety, reward, work impediment, intrinsic cost, vulnerability, and sanctions (AV2) affect beliefs about overall assessment of consequences (AV1) - Overall assessment of consequences (AV1) affects attitudes (IV) - IS awareness (AV3) affects attitude (IV) and outcome beliefs (AV2)
Chan et al. (2005)	Variance approach with antecedent variables	Safety climate literature, the social information processing approach	- Management, supervisory practices, and co-workers' socialization (AV) influence perceptions of the information security climate (IV) - Perceptions of security climate and self-efficacy (IV) affect compliant behavior (DV)

Authors	Theory type	Theoretical background	Main results
Siponen & Vance (2010)	Variance approach	Neutralization theory and deterrence theory	- Employee non-compliance (DV) is better explained by neutralization techniques (IV) than by sanctions (IV)
3. Studies on appropriate IS security behavior			
Dinev et al. (2009)	Variance approach with a moderator and antecedent variables	Theory of planned behavior, integrated model of user acceptance of e-commerce, and cultural dimensions and indices	- Relationship between subjective norm (IV) and behavioral intention (DV) is stronger in Korea than in the US, which is explained through the high priority of group norms, high power distance, strong uncertainty avoidance, and weak masculinity (M) - Relationship between technology awareness (AV) and attitude toward behavior (IV) and behavioral intention (DV) is weaker in Korea than in the US, which is explained by high collectivism and low masculinity (M)
Dinev & Hu (2007)	Variance approach with antecedent variables	Theory of planned behavior	- Threat awareness (IV) influences intention to use protective technologies (DV) - Subjective norm (IV) influences behavioral intention DV) more in cases of advanced technology users - Ease of use and computer self-efficacy do not influence behavioral intentions
Stanton et al. (2005)	Factor approach		- Training, monitoring, and rewards improve users' password behavior
Adams & Sasse (1999)	Factor approach		- Factors influencing effective password usage are multiple passwords, password content, compatibility with work practices, users' perceptions of organizational security, and information sensitivity
Albrechtsen (2007)	Factor approach		- Users are motivated for IS, but do not perform many IS actions - High IS workload creates a conflict of interest between functionality and IS - IS procedures and awareness campaigns alone have little effect on behavior and awareness - A user-involving approach is more effective

Table 2. Previous studies. M in the table means that a study includes moderators (M), and (AV) indicates that a study includes antecedent variables for the independent variables (IV) explaining IS security behavior (DV). AV1 precedes independent variables, and AV2 precedes AV1. Variance refers to studies that are aimed at measuring the variance explained in behavioral intention (being the dependent variable of the model) or actual behavior (being the dependent variable). Factor means certain factors, mainly obtained through qualitative studies, explain IS security behavior. For factor models, the aim is not to measure variance.

Influenced by Straub (1990), the research area computer abuse/misuse examines different computer misuses, such as racist emails and the use of illegal software within organizations (e.g., Lee et al., 2004; D'Arcy et al., 2008; D'Arcy & Hovav, 2007). Computer abuse/misuse studies have mainly applied theories from criminology, such as deterrence theory or social control theory (Harrington, 1996; Lee et al., 2004; D'Arcy et al., 2008; D'Arcy & Hovav, 2007). These studies have especially contributed to our understanding of the role of deterrence in minimizing computer abuse. Although computer misuse studies look at illegal or ethically questionable computing, studies on employee compliance with IS security policies investigate employees' intentions to comply with organizations' IS security procedures (Bulgurcy et al., 2010a; Johnston & Warkentin, 2010; Herath & Rao, 2009a, 2009b; Siponen & Vance, 2010), their actual behavior (Chan et al., 2005; Ng et al., 2008), or both (Siponen et al., 2006; Myyry et al., 2009). Computer abuse and employee compliance apply the variance model research paradigm (see Burton-Jones et al., 2012).

Several studies have investigated employees' appropriate IS security behavior from various perspectives. To explain the use of protective technologies, Dinev and Hu (2009) and Dinev et al. (2009) used a quantitative and theory-testing approach. In turn, Adams and Sasse (1999) and Stanton et al. (2005) investigated password behavior, and Albrechtsen (2007) studied experiences of information security inductively without a theory-testing research setting. Instead of building statistical models, these studies present different qualitative factors influencing different information security behaviors.

In light of the nine requirements for the process theories, existing research has examined employees' compliance with IS security policies by building variance models and by conducting qualitative studies to build factor-like compliance or IS security behavior models. The experimental research designs (Johnston & Warkentin, 2010), measuring the moderating effect (Harrington, 1996; Ng et al., 2009; Li et al., 2010; Dinev et al., 2009), and the influence on the

antecedent variables that precede the independent variables predicting the compliant behavior (or intention) (Lee et al., 2004; D'Arcy et al., 2008; Siponen et al., 2006; Herath & Rao, 2009a; Johston & Warkentin, 2010; Bulgurcy et al., 2010b; Chan et al., 2005; Dinev et al., 2009; Dinev & Hu, 2007) can be seen to touch the dynamic nature of the phenomenon by time ordering things and stages (Johnston & Warkentin, 2010). The time ordering takes place in preceding factors (e.g., Bulgurcy et al., 2010a), and an intervention within an experiment involves two stages (Johnston & Warkentin 2010). However, the previous work was not designed to meet the nine requirements for process theories. First, no previous study meets the first criterion for process theories (Table 1), which is the basis for a process theory in this area. This criterion suggests the need to *define the development trajectory in terms of stages with stage-specific attributes,* namely, the development path of an individual toward IS security behavior (Weinsten et al., 1998). Yet each individual should reside in one stage at time. This means that previous studies do not recognize the different stages of employees' IS security behavior in the sense of a developmental trajectory with stage-specific reasons for compliance, and development of behavior from one stage to the next. To give an example, although the impact of an experiment (Johnston & Warkentin, 2010) moves an individual from a stage to another, no IS security study has modeled the entire development path of an individual in terms of all possible stages and respective stage-specific attributes.

Because the previous studies do not meet the first criterion, they cannot offer any means of distinguishing at which stage an individual resides. This is an important shortcoming, given that the stage where one resides defines which actions are optimal or right to change the individual's behavior (Briedle, Riemsma, Pattenden, Sowden et al., 2005). This study endeavors to take the first step in closing this gap in research.

4. Methodology

4.1 Data collection

Data collection was executed in multiple locations of a global company (Globalcomp Company, a pseudonym) that operates in the field of the marine industry and energy market. 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 operate independently and have independent economic responsibilities. Also, they were all previously owned by other companies and were bought by the multinational company they now formally belong to.

Data was collected through semi-structured interviews. To avoid a situation in which only certain groups of employees within an organization were interviewed, resulting in interviews that do not represent the views of the whole organization, interviewees in different organizational positions were randomly selected. In all, 72 face-to-face interviews were conducted. The average interview lasted 47 minutes.

It is important that theoretical perceptions and perspectives do not drive the interview questions (Stinger, 1999; Myers & Newman, 2007), and that the interviewees and interviewers understand each other. For the development of the interview questions, we followed Spradley (1979), who suggests that the researcher first ask questions that are general and neutral in order to enable participants to describe their situations in their own terms. The use of interviewees' own words and phrases in the formulation of interview questions—a mirroring technique—was also used to enable interviewees to explain their experiences in their own words (Meyers & Newman, 2007). The interviews had a strongly conversational nature involving active listening and activation of interviewees' construction of meaning rather than the elicitation of facts (Schulze & Avital, 2011).

4.2 Data analysis

The purpose of the inductive data analysis was to develop a theoretical framework that explains the collected data (Charmaz, 2000). First, the interviews were examined at the sentence or paragraph level using an initial or open-coding process (Charmaz, 2000; Glaser, 1978). In other words, all presented viewpoints about IS security attitudes and behavior were collected, and open codes were created through the process of constant comparison. After several iterations, 88 open codes emerged from the data.

Next, the identified open codes were organized into a coherent framework, thus offering a more abstract and comprehensive conceptual framework of the data (Glaser, 1978; Charmaz, 2000). Accordingly, the 88 open codes were further condensed into 5 high-level categories and 22 low-level categories. Finally, the process theory was established through organizing the categories guided by the 9 criteria for process theories that were derived from the meta-theories of Weinstein et al. (1998) and van de Ven (1992) (see Table 1 and Table 2). A connection between the meta-theories and the high- and low-level categories is presented in Appendix 2.

5. Results: A Process Theory for Employees Compliance with IS Security Procedures

This section describes the explanatory type of process theory (Gregor, 2006), explaining the reasons (i.e., cognitions) and barriers of change for employees' IS security behavior (section 5.1). In section 5.2, we show how the process theory meets the nine criteria of process theories based on the meta-theories (see section 4.2 and Table 3).

5.1 Introducing the Theory of Employee Compliance with IS Security Procedures

Figure 1 presents the theory of compliance with IS security procedures, including the five stages (1-5) with their different natures (i), cognitions explaining compliance and non-compliance with IS security procedures (ii), and barriers of change (A-D).

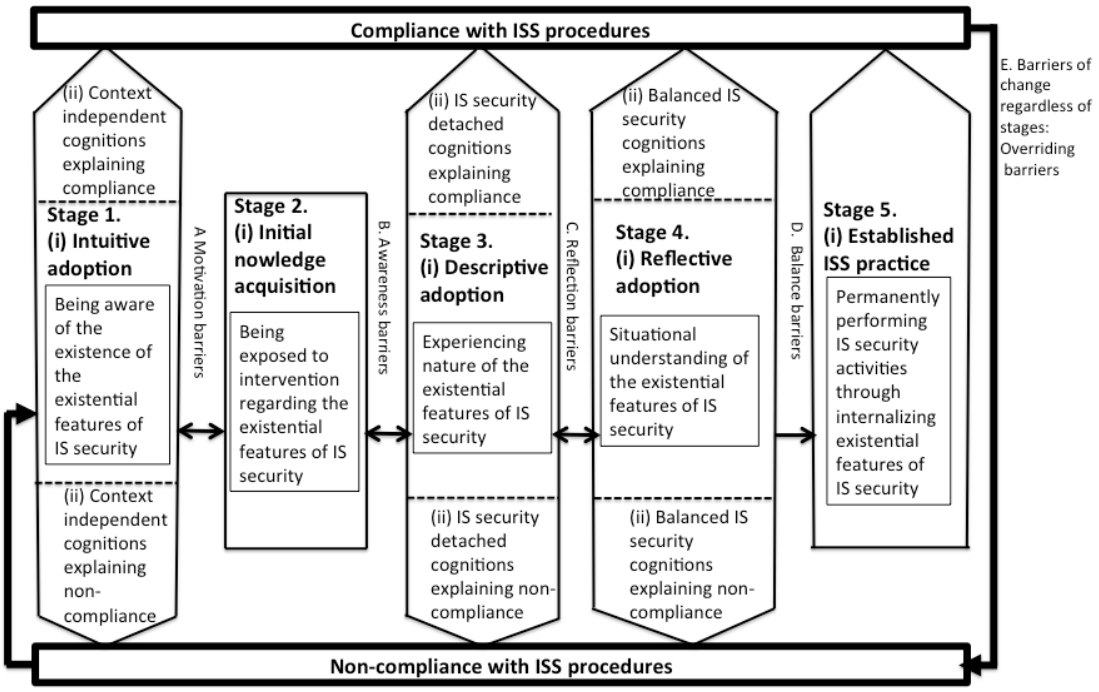

Figure 1: The Theory of Employee Compliance with IS Security Procedures

While our theory is predominantly inductive, consistent with recommendations of methodologists, we did utilize our theoretical sensitivity on the focal phenomenon and broader social theory. Some of the key concepts used in the proposed process theory are explained upfront in Table 3, to make the process theory more understandable to the reader. The contents of the five stages are summarized in Table 4.

Concepts of the process theory	**Source**	**Description**
Intuitive thinking	Intuitive beliefs (Sperber, 1997)	Employees' security behavior is based on intuitive thinking, which is based on previous experience without awareness of organizational policies.
Descriptive thinking	Declarative thinking (ten Berge & van Hezewijk, 1999)	The knowledge of IS security behavior at this stage is declarative, without the ability to apply this descriptive knowledge to the procedural requirements of how and why IS security procedures should be performed in a specific organizational context (ten Berge & van Hezewijk, 1999).
Reflective thinking	Reflective beliefs (Sperber, 1997)	Thinking based on the analysis of a situation in the view of conscious and

		deliberate reasoning (Sperber, 1997; Hatton & Smith, 1995).
Tacit IS security practice	Tacit knowledge (Polanyi, 1957)	Compliance with IS security procedures are internalized and they are part and parcel with employees' work actions without additional cognitive effort (Nonaka et al., 2003).
Cognitions	Cognitions (Hedsröm & Swedberg, 1998)	Reasons explaining employees' compliance with IS security as individual beliefs and desires that generate a specific action (Hedström & Swedberg, 1998).
Barriers of change	Processes of change (Prochaska & Diclemente, 1983)	Activities and experiences by which change in intentions, attitudes, or behavior that promote movement from stage to stage are accomplished (Prochaska & Diclemente, 1983, 1992).
Overriding barriers	Overriding (Hare, 1963)	Stimulate employees to move from compliance to non-compliance.

Table 3. Concepts underlying the proposed process theory

The following table (Table 4) provides a summary of the patterns associated with each stage.

Table 4. Stages of the Process Theory

	Stage 1	**Stage 2**	**Stage 3**	**Stage 4**	**Stage 5**
Nature of stage	**Intuitive thinking** IS security behavior is based on intuitive knowledge	**Initial knowledge acquisition** IS security behavior is still based on intuitive knowledge	**Descriptive thinking** IS security behavior is based on descriptive knowledge	**Reflective thinking** IS security behavior is based on reflective knowledge	**Tacit IS security practice** IS security behavior is based on tacit knowledge
Goal of stage	Being aware of IS security requirements, but not knowing the details	Being exposed to intervention regarding the IS security requirements	Experiencing the nature of the IS security requirements	Situational understanding of the IS security requirements	Permanently performing IS security activities through internalizing IS security requirements
Cognitions explaining IS security behavior	**Context-independent cognitions:** - Habits - Social conformity - Unclear IS security role	**Evolving cognitions:** -New cognitions begin to evolve	**IS security detached cognitions:** - Authority - Obedience - Role model	**Balanced IS security cognitions:** - Trust of IS security procedures - Evaluation of risks - Professionalism	**Internalized cognitions:** - Balanced IS security cognitions exclusively
Stage-specific barriers of change	**Between 1–2: Motivation barriers:** - Interest - Activity - Mandatory nature of procedures - IS security accidents	**Between 2–3: Awareness barriers:** - Effective delivery of IS security information - Failure to become aware of the organization's IS security procedures	**Between 3–4: Reflection barriers:** - Relating one's own experiences - Participation/ involvement - Discussion - Non-suitability - Inconvenience	**Between 4-5: Balance barriers:** - Balance between IS security procedures and all IS security cognitions	-
Common barriers of change for stages 1–4	**Overriding barriers** - Opportunism, Regression, Social Pressure, Working Environment, Taking a Shortcut				

The five stages of the process theory of employees' compliance with IS security procedures are discussed next.

5.1.1 Stage 1: Intuitive thinking stage

Stage description

At this stage, an employee is aware of the existence of organizational IS security requirements, but has not received any company-specific IS security instruction, and is not aware of the requirements' specific contents. Instead, an employees' IS security behavior is based on intuitive thinking that is formed, for example, by previous work experience, upbringing, national or organizational culture, personality qualities, or religion. Intuitive IS security compliance is explained by context-independent cognitions, which means that they are not necessarily compatible with the security procedures of the current organization.

The first context-independent cognitions (i.e., common sense thinking) lead to either compliance or non-compliance with IS security procedures, depending on whether they are compatible or inconsistent with the organization's IS security procedures. Because employees at stage 1 are unfamiliar with the organization's formal IS security procedures, an employee typically overestimates his/her own IS security knowledge and abilities, or underestimates the significance of IS security procedures.

Context-independent cognition at the second stage is social conformity, meaning that without knowledge of company-specific IS security procedures, people easily behave according to how they think or perceive others to behave, which can lead to both compliance and non-compliance with IS security procedures: "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).

An unclear role of IS security is the third context-independent cognition typical of the intuitive thinking stage, which means that a person denies her/his personal responsibility (e.g., through "outsourcing" responsibility for IS security to other parties such as IT employees or technologies, or to have a false trust in IT). For example, employees may expect that IS security is being taken care of by IT staff, and hence that it is not their responsibility. An example of false trust in IT is that employees may not understand that their passwords are simple and hence easy to break.

Barriers of change from stage 1 to stage 2

Employees' IS security behavior changes towards the next stage of the process, through motivation barriers of change including intrinsic or extrinsic motivation (marked with arrow A in Figure 1), to acquire new knowledge about an organization's IS security requirements. Intrinsic motivation refers to the personal interest towards IS security. Employees' decisions are based on extrinsic motivation if the action is mandatory (e.g., if an employee participates in the IS security training only because she/he is required to do so), or if they are experiencing an IS security accident.

5.1.2 Stage 2: Initial knowledge acquisition stage

Stage description

At this stage, an employee's context-independent cognitions change through organizational communications, such as IS security training. At this stage, an employee has the ability to evaluate the correctness of his/her IS security behavior against information he/she receives from the organization. Here, one-way communication of the organization's IS security procedures, such as by presentations, email, or delivering policies, is sufficient.

Barriers of change from stage 2 to stage 3

If IS security communication fails during this stage, an employee fails to become aware of IS security procedures, which leads to a relapse of the intuitive thinking stage in the sense of responsibility denial, following previous habits, or social conformity. An example of ineffective written IS security communications is presented below:

> …normally people tend to just scan it [information security policies] and don' t really read it as point to point… if it is really too long and too much text, if there are no bulleted points, then people just tend to see and scan and not really understand what it is all about. (UAED2, officer)

Besides overriding barriers (see section 5.1.6), the awareness barrier to change demonstrates how the process is cyclical by nature, and how relapses to the previous stages are possible if communication fails in creating awareness of IS security procedures.

5.1.3 Stage 3: Descriptive thinking stage

Stage description

After the successful initial knowledge acquisition stage, an employee has internalized what kind of IS security procedures are expected in the organization, how these are supposed to be executed in practice, and why these IS security practices are important. However, at the descriptive thinking stage, the importance of IS security practices is not connected to the specific work context; thus, cognitions explaining IS security behavior are IS security detached (i.e., not based on work context-specific IS security justifications). The IS security detached cognitions at the descriptive thinking stage are not based on security-conscious decisions, but on other motivations such as obedience, authority, and role modeling.

Having IS security detached cognitions means that an employee can comply with security procedures due to policy obedience for its own sake, or if they are ordered to do so by an authority, or if they must either comply with or violate IS security procedures due to following

management's role model. In these cases, it is not necessary to understand the rationale of IS security procedures in their personal work environment. Compliance with IS security procedures in this stage can also turn into non-compliance with IS security procedures due to the overriding barriers (see section 5.1.6). Policy obedience can occur without necessarily understanding the IS security rationale behind it, as illustrated below:

> …when I am an employee of a company, then it's my responsibility to follow all the policies or procedures, whatever they have laid down. Definitely I can put my objections, [but] finally it has to be as per policies laid down which we need to follow. (UAE7, officer)

Another example of IS security detached cognitions, in this case of management's role model leading to non-compliance, is demonstrated below:

> …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)

Barriers of change from stage 3 to stage 4

Reflecting security threats and security-sensitive organizational assets specific to the work environment and personal work tasks plays a significant role in the transition between the third and fourth stages. At this stage, employees' active involvement is necessary in order for them to learn and commit themselves to IS security. A personal involvement during IS security communication can be seen as a way to improve the understanding and relevance of IS security-related communications; it also corrects employees' false conceptions, and provides concrete means for situations in which they may feel pressured to behave against IS security procedures. Effective IS security intervention makes an employee process her/his own experiences in relation to the presented IS security requirements. The influence of personal involvement on learning is demonstrated below:

> 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)

Besides failure to reflect IS security knowledge, it is also possible that employees don't comply with IS security procedures because they are experiencing other reflection barriers of change: non-suitability and inconvenience. Non-suitability means that IS security procedures may seem to be contradictory with the current work environment. For example, if an employee learns that employees are not allowed to send any sensitive information through email without encryption, and feels that they are not provided with any technical means for encryption, it is likely that this IS security procedure will be violated.

Employees also often consider the extent of the inconvenience associated with IS security procedures, and this sometimes leads to non-compliance with IS security procedures. For example, interviewees stated that IS security procedures relating to the secure use of the Internet (e.g., email encryption, remote connection, using PDF formats, and link creation) or password practices are too restrictive, time-consuming, or difficult. The inconvenience related to strong password selection is illustrated below:

> Even after, even after the training that you mentioned, I don't think many people will use the complicated one… It's inconvenient. Every time you change it, you have to remember it; it's hard. (ChinaA13, officer)

Without responding to the reflection barriers of change, employees continue to behave according to their existing cognitions instead of developing new ones. Again, such as in the

previous stage, this shows that the process is cyclical by its nature, and relapses to previous stages are possible.

5.1.4 Stage 4: Reflective thinking stage

Stage description

A successful descriptive thinking stage leads to a reflective thinking stage, which is when an employee has enough knowledge to make an informed decision about why they should comply with or violate IS security procedures. At this stage, employee compliance is explained by balanced IS security cognitions—namely, consideration of the advantages and disadvantages of policy compliance/non-compliance. Balanced IS security cognitions means that IS security procedures are complied with if there is no contradiction between the IS security procedure and the employee's IS security cognitions regarding the evaluation of risks, trust in IS security procedures, and professionalism. Accordingly, the purpose of communication at this stage is to ensure this balance between IS security procedures and all IS security cognitions. Again, such as in the previous stages 2 and 3, this shows that the process is cyclical by its nature, and relapses to previous stages may be needed to bring about progression to the next stages.

The first IS security cognition, the evaluation of risks, means balancing threats with the value of the information in a specific work context. Besides being aware of the value of information, the employees' IS security behavior is strongly attached to their conceptions of IS security threats in their work environment. Consistently, employees' decisions to engage in risky IS security behavior depends on the likelihood that potential threats could come to be realized.

At this stage, non-compliance also emerges due to a lack of employee trust in IS security procedures. This means that when interviewees saw that there was no significant (positive) consequence of using (or not using) certain IS security procedures, they tended to not comply with them, as the following quotation illustrates:

> If somebody wants to really get something from your computer and if he's competent, he always gets it. It doesn't matter if you protect it with this long password or that long password. (UAEA5b, manager)

Finally, a sense of professionalism (meaning that IS security is seen as an aspect of work responsibility or work duty) is developed at this stage. In particular, protecting information of a confidential nature (e.g., personnel and salary information) is strongly connected to ones' professional competence.

Barriers of change from stage 4 to stage 5

In order to move to the phase of tacit IS security practice, an employee needs to strike a balance between the organization's IS security procedures and all three IS security cognitions—evaluation of risks, professionalism, and trust in IS security procedures (marked with Arrow D in Figure 1). This means that if a person recognizes the potential risk of losing sensitive information due to neglecting IS security procedures, views IS security as his/her work responsibility, and believes that the IS security procedure is effective, then IS security becomes a natural part of one's work.

5.1.5 Stage 5: Tacit IS security practice

Stage description

During the last stage in the process, an employee performs IS security procedures on a relatively stable ground with internalized IS security cognitions. This means that as a result of balancing IS security procedures with all IS security cognitions, IS security procedures become a natural part of one's work in a specific environment without extra effort. Usually, reaching this stage requires moving back and forth along the stages for as long as the employees need to sufficiently acquire knowledge for overcoming the barriers of change at each stage of the process. In addition, employees' behavior at the tacit IS security practice stage is not as strongly dependent on overriding barriers (see section 5.1.6) as it was in the earlier stages. Reaching this stage means

that a person has internalized the current IS security requirements of a specific work environment.

5.1.6 Overriding barriers: Barriers of change regardless of stage

Regardless of whether a person complies with IS security procedures in the first (or second, third, fourth, or fifth) stage, compliant behavior can turn into non-compliance with IS security procedures due to a phenomenon called overriding barriers (marked as E in Figure 1; see also Table 3). Hence, recognizing these barriers of change is important regardless of the employee's stage in the process.

First, working environment as an overriding barrier means that employees recognize potential threats, but do not seem to realize their possibility because they have high trust towards the company's technical security solutions or towards other people in the working environment. For example, an employee might usually lock her/his computer except in his/her own office, because locking it is not considered necessary in this environment. This may be because "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).

Regression as a second overriding barrier means that, without any reminders, compliance decreases over time, as demonstrated below:

> [If] you do things quite a long time, it will become… common sense for you… for the security. But before that, you have got to be reminded occasionally, so [you have to work] for a long time… to get this feeling. (ChinaC4, officer)

The third overriding effect is taking a shortcut, which refers to situations when one is being lazy, hurried, or stressed. For example, a computer is usually locked, but not in situations when the computer is left attended for a short period of time, or due to sudden interruptions or hurry.

According to the interviewees, IS security procedures are usually complied with, except in situations where a person feels pressured, which can be intrinsic (e.g., avoiding negative feelings) or extrinsic (e.g., experiencing fear). As an example of intrinsic pressure, employees may reveal sensitive information because they want to help others or maintain good work relationships; they might not ask to see employee badges, or they might not lock their computers because they feel embarrassed to act in this way, as illustrated below:

> 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)

As an example of extrinsic pressure, employees may reveal sensitive information personally or through email because they feel threatened, as illustrated below:

> 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)

Finally, opportunism means that IS security procedures 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 effect can potentially have an influence on employees' IS security behavior at any stage, it is assumed that in the last stage of the process, an employee's IS security behavior is not as strongly dependent on this overriding effect as compared to other stages. This is so because at the stage of tacit IS security procedures, compliance with IS security procedures

requires less conscious effort, and thus the cognitive load required for compliance with IS security procedures 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 through violating IS security procedures by overriding either the effects of social pressure or opportunism.

6. Discussion

6.1. Contributions

Our results indicate that employees' compliance with IS security procedures include a sequence of five stages, and employees are at different stages. This is different from mainstream IS security behavioral research, which examines the phenomenon through variance or factor approaches without such stages; none of the existing studies separate qualitatively different stages for the purpose of explaining employees' IS security behavior. However, while this is a new finding in terms of employees' compliance with IS security behavior, IS research in other areas reports the existence of such stages (e.g., Madsen et al., 2006; McLeod & Doolin, 2012; Newman & Robey, 1992).

The new contribution of our study is that each stage differs in terms of different cognitions that explain IS security behavior. The first stage is characterized by intuitive thinking, which results in context-independent cognitions. The second stage means that cognition evolves through initial knowledge acquisition. The third stage is characterized by descriptive thinking in terms of IS security detached cognitions. The fourth stage is characterized by reflective thinking in terms of balanced IS security cognitions. And the fifth stage is characterized by establishing IS security practices with internalized IS security cognitions. Although most of these IS security cognitions are recognized in the previous literature, none of the existing studies qualitatively separate the different stages for the purpose of explaining employees' IS security behavior. Without this stage-specific interventions to improve the employees' IS security behavior is not possible.

As a second contribution our results suggest that each stage also differs in terms of stage-specific barriers of change; these barriers explain how and why employees' IS security behavior may change or remain the same as employees proceed from the first stage towards the last stage. The barriers of change may produce or impede movement from one stage to the next. These stage-specific barriers of change include motivation, learning, reflection, and balance barriers of change. This is a new finding in IS security, and necessary information in order to arrange customized IS security interventions that overcomes these barriers.

Third contribution are stage-specific reasons that explain changes in IS security behavior, and also that there are barriers that can turn compliant behavior into non-compliance at any stage of the process. Such overriding barriers of change (regardless of the stage) include work environment, regression, taking a shortcut, social pressure, and opportunism. Any IS security communication needs to recognize these barriers. This is a new finding in IS security.

6.2 Implications for research and practice

Based on our empirical results, we suggest four implications for future research.

First, our results suggest that, besides looking at variance models, behavioral IS research should also examine the different issues of IS security behavior through process models, formulated in accordance with guidelines highlighted in process meta-theories. In addition to employees' compliance with IS security procedures, other areas that could benefit from the process theories include computer abuse, computer crime, and cyber-loafing.

Second, future research needs to pay attention to the possibility that employees have stage-specific reasons for compliance and non-compliance. As a result, future research needs to control the stage.

Third, given that employees are at different stages, and that at each stage there are different and similar (a) reasons and (b) barriers that influence their decision to comply or not to comply,

future research should develop a practical instrument for testing an individual's stage. This would be helpful, since information about the stage where employees are would help organizations to design customized interventions at each stage.

Fourth, future research should study how the barriers of change at each stage can be overcome so 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.

Based on our empirical results, we suggest two implications for practice. First, our study offers a framework for recognizing possible differences in reasons for compliance/non-compliance between individuals. Accordingly, our results suggest that practitioners should first test to determine at which stage their employees are with respect to employee compliance. Such testing is necessary to find the underlying reasons as to why their employees do not comply with IS security procedures.

Second, our results suggests that after the stage of each employee is found, practitioners should customize their IS security interventions in a way that each employee receives an intervention that matches with their stage. Through such a matching of interventions to the stage that employees have reached in terms of changing behavior, practitioners could better overcome the specific barriers that impede employees' transitions to the next stages.

6.3 Limitations of the Study

First, it is not claimed that the rationale found for employees' compliance with IS security procedures is exhaustive; further research, especially within different organizations, might find alternative cognitions and different barriers of change, and might be able to present them in a different sequential order. Although interviews were conducted in three organizations that

formally form one company, it was seen by the managers of the company and the authors that due to the independent nature of the three separate locations (UAE, Switzerland, and China), the results do not necessarily reflect the experiences of one coherent organization with common management, business areas, and organizational culture.

In addition, it can be questioned whether interviews can provide honest reports in respect to such matters as employee compliance with IS security procedures—especially if those employees fear that their employer may be able to trace the responses to the respondents who provided the answers. To address this concern, it was clearly communicated to the employees (interviewees) that we would not show the individual results to their employer, and that we are interested in the general patterns stemming from the data—not in what any individual respondent says. They were also provided the option of having us write down their interview as field notes rather than recording them digitally.

7. Conclusions

The key goal of IS security behavioral studies is to understand information security behavior so that it can be improved. The existing research has increased this understanding by offering numerous variance or factor models that explain or predict employees' compliance with IS security procedures. We argue that these models are inadequate for capturing the complexity of IS security behavior, including how the behavior develops gradually, the exact development trajectory, under which conditions there are relapses, under which conditions individuals can move from one stage to another, and which conditions hinder individuals' development from one stage to another. Previous work has shown no interest in these matters, which are necessary for better understanding of employees' IS security behavior.

As the first step in overcoming this gap in the research, we inductively developed a process theory aimed at addressing these issues by interviewing (N=72) employees.

Our process theory suggests that employee compliance with IS security policies develops through a sequence of stages, and that each stage is associated with stage-specific reasons for compliance and non-compliance with IS security procedures and with barriers of change that produce and impede employees' progression from one stage to the next. New implications for research and practice were outlined based on our results. For research, there is a need to control the employees' stage, to further examine stage-specific attributes, and to examine the effect of stage-specific interventions aimed at improving IS security behavior. For IS security practice, our results suggest that one size does not fit all. Instead, to design optimal interventions to improve employees' IS security behavior, there is a need to understand employees' development stage, stage-specific cognitions, barriers, and impetus factors.

References

Adams A & Sasse MA (1999) Users Are Not the Enemy. Communications of the ACM 42(12): 40–46.

Albrechtsen E (2007) A qualitative study of user's view on information security. Computers & Security 26(4): 276–289.

ten Berge, T. & van Hezewijk, R. (1999). Procedural and Declarative Knowledge. An Evolutionary Perspective. Theory & Psychology, 9(5), pp. 605 – 624.

Bridle, C., Riemsma, R. P., Pattenden, J., Sowden, A. J., Mather, L., Watt, I. S., et al. (2005). Systematic review of the effectiveness of health behavior interventions based on the transtheoretical model. Psychol. Health 20(3): 283-301.

Bulgurcy B, Cavusoglu H & Benbasat I (2010a) Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Quarterly 34(3): 523–548.

.

Burton-Jones, A., McLean, E.R., & Monod, M. (2011). On Approaches to Building Theories: Process, Variance, and Systems. Working Paper, Sauder School of Business.

Chan M, Woon I & Kankanhalli A (2005) Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior. Journal of Information Privacy & Security 1(3): 18–41.

Charmaz K (2000) Grounded Theory: Objectivist and Constructivist Methods. In: Denzin NK & Lincoln YS (eds) Handbook of Qualitative Research (2nd Edition). London, Sage: 509–536.

Chakraborty S, Sarker S & S (2010) An Exploration into the Process of Requirements Elicitation: A Grounded Approach. Journal of the Association for Information Systems 11(4).

D'Arcy J & Hovav A (2007) Deterring Internal Information Systems Misuse, Communications of the ACM 50(10): 113–117.

D'Arcy J, Hovav A & Galletta DF (2008) User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. Information Systems Research 20(1): 79–98.

Dinev T, Goo J, Hu Q & Nam K (2009) User Behaviour towards Protective Information Technologies: The Role of National Cultural Differences. Information Systems Journal 19: 391–412.

Dinev T & Hu Q (2007) The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies. Journal of the Association for Information Systems 8(7): 386–408.

Glaser BG (1978) Theoretical Sensitivity: Advances in the Methodology of Grounded Theory. Mill Valley CA, The Sociology Press.

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

Harrington SJ (1996) The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions. MIS Quarterly 20(3): 257–278.

Hatton, N. and Smith, D. (1995). Reflection in Teacher Education: Towards Definition and Implementation. Teaching and Teacher Education, 11(1), pp. 33 - 49.

Hedström, P. & Swedberg, R. (1998). Social Mechanisms: An Introductory Essay. In: Hedström P & Swedberg R (eds) Social Mechanisms. An Analytical Approach to Social Theory. New York, Cambridge UK, Cambridge University Press.

Herath T & Rao HR (2009a) Protection Motivation and Deterrence: a Framework for Security Policy Compliance in Organizations. European Journal of Information Systems 18(2): 106–125.

Herath T & Rao HR (2009b) Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures, and Perceived Effectiveness. Decision Support Systems 47: 154–165.

Johnston AC & Warkentin M (2010) Fear Appeals and Information Security Behaviors: An Empirical Study. MIS Quarterly 34(3): 549–566.

Kim SS (2009) The Integrative Framework of Technology Use: An Extension and Test. MIS Quarterly 33(3), pp. 513-537.

Kohlberg, L. (1981). Essays on Moral Development, Vol. I: The Philosophy of Moral Development. San Francisco, CA: Harper & Row.

Kruger HA & Kearney WD (2006) A Prototype for Assessing Information Security Awareness. Computers and Security 25(4): 289–296.

Lee SM, Lee SG & Yoo S (2004) An Integrative Model of Computer Abuse Based on Social Control and General Deterrence Theories. Information Management 41(6): 707–718.

Li H, Zhang & Sarathy R (2010) Understanding Compliance with Internet Use Policy from the Perspective of Rational Choice Theory. Decision Support Systems 48: 635–645.

Lyytinen, K., Newman, M. and Al- Muharifi, A.R.A. (2009) Institutionalizing enterprise resource planning in Saudi steel industry: a punctuated socio-technical analysis. Journal of Information Technology. 24(4) pp.286-304.

Madsen, S., Kautz, K., and Vidgen, R., (2006). A framework for understanding how a unique and local development method emerges in practice. European Journal of Information Systems, (15): 225-238.

Markus & Robey (1988). Information technology and Organizational Change: Causal Structure in theory and Research. Management Science 34(5), 583 – 598).

McLeod, L. & Doolin, B. (2012). Information systems development as situated socio-technical change: a process approach**.** European Journal of Information Systems, 21(2) 25, pp. 176-191.

Mohr, L. B. (1982). Explaining Organizational Behavior. Jossey-Bass, San Francisco.

Montealegre, R., Keil, M. (2000). De-escalating information technology projects: lessons from the Denver International Airport. *MIS Quarterly*, 24(3), pp. 417-47.

Myers M & Newman M (2007) The Qualitative Interview in IS Research: Examining the Craft. Information and Organization 17(1): 2–26.

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. European Journal of Information Systems 18: 126–139.

Newman, M. and D. Robey (1992), A Social Process Model of User-Analyst Relationships. *MIS Quarterly*, 16(2), pp. 249-266.

Ng B, Kankanhalli A & Xu Y (2009) Studying Users' Computer Security Behavior: A Health Belief Perspective. Decision Support Systems 46: 815–825.

Nonaka, I., Toyama, R., & Byosière, P. (2003). A Theory of Organizational Knowledge Creation: Understanding the Dynamic Process of Creating Knowledge. In Dierkes, M., Antal, A.B., Child, J. & Nonaka, I. (eds.) Handbook of Organizational Learning and Knowledge. Oxford: Oxford University press., pp. 491 – 517.

Parker DB (1976) Crime by Computer. New York, Scribner.

Poole, M.S., Van de Ven, A.H., Dooley, K. & Holmes, M.E. (2000). Organizational Change and Innovation Processes. Theory and Methods for Research. Oxford University Press

Prochaska & DiClemente (1983). Stages and Processes of Self-Change of Smoking: Toward an Integrative Model of Change. Journal of Consulting and Clinical Psychology 51(3), 390 – 395.

Prochaska, DiClemente, & Norcross (1992). In Search of How People Change. Applications to Addictive Behaviors. American Psychologist 47(9), 1102 – 1114.

Puhakainen, P. & Siponen, M. (2010). Improving Employee's Compliance through IS Security Training: An Action Research Study. MIS Quarterly, 34(4). pp. 1 – 23.

Robey & Newman (1996). Sequential Patterns in Information Systems Development: An Application of a Social Process theory. ACM Transactions on Information Systems 14(1), 30 – 63).

Sarker, S., and Sahay, S. "Information Systems Development by US-Norwegian Virtual Teams: Implication of Time and Space", *Proceedings of the Thirty-Fifty Annual Hawaii International Conference on System Science,* Big Island, Hawaii, January 7-10th, 2002.

Schulze U & Avital A (2011) Designing Interviews to Generate Rich Data for Information Systems Research. Information & Organization 21: 1–16.

Seale, C. (1999). Quality in qualitative research. *Qualitative Inquiry, 5*(4), 465-478.

Siponen, M., & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. MIS Quarterly, 34(1), pp. 1 – 15.

Sperber, D. (1997). Intuitive and Reflective beliefs. Mind Language, 12(1), pp. 67 – 83.

Spradley (1979) The ethnographic interview. Holt, Rinehart and Winston, New York.

Stanton JM, Stam KR, Mastrangelo P & Jolton J (2005) Analysis of End User Security Behaviours. Computers and Security 24(2): 124–133.

Stinger ET (1999) Action Research. Second edition, Thousand Oaks CA, Sage Publications.

Straub, D.W. (1990). Effective IS Security: An Empirical Study. Information Systems Research, 1(3), pp. 255-276.

Thornberry, T.P. (1987). Toward an Interactional Theory of Delinquency. Criminology 25 (4), 863 – 891.

Thummadi, B.V., Shiv, O., Lyytinen, K., and Berente, N. 2011. "Enacted Software Development Routines Based on Watefall and Agile Methods: A Socio-Technical Event Sequence Study," in: *DESRIST*.

Weinstein, Rothman, & Sutton (1998). Stage Theories of Health Behavior: Conceptual and Methodological Issues. Health Psychology 17(3), 290 – 299.

Wheeler, B.C. (2002). NEBIC: A Dynamic Capabilities Theory for Assessing Net-Enablement. Information Systems Research, 13(2), pp. 125 – 146.

Van de Ven, A.H. (1992). Suggestions for Studying Strategy Process: A Research Note. Strategic Management Journal, 13, 169 – 191.

Appendix 1: Nine Requirements for Process Theories and the Pluralistic Deontological Process Theory of Employees' Adoption of IS Security Procedures

This section describes to what extent our process theory meets the requirements derived from Weinstein et al. (1998) and van de Ven (1992). Requirements and their explanation are summarized in Table 5.

Table 5. Explanation of How Our Study Meets Each Requirement

Requirements for process theories	**Explanation of how our study meets each criterion**
(1) Process theories must have a concept of stage and must define whether the stages are predefined or not.	The process theory includes stages of the employees' compliance with IS security procedures.
(2) Process theories must take a stand as to whether the stages are predefined or not.	The process theory lists typical stages.
(3) The stages of process theories must include similar barriers of change.	Common barriers of change for stages 1–4 are overriding barriers. Barriers of change produce or impede movement between the

	stages.
(4) Process theories must include different barriers at different stages.	Barriers of change are different between the stages. Barriers of change at each stage specify different issues for how and why employees' IS security cognitions and behavior may change over time when an employee proceeds from the intuitive adoption stage towards tacit IS security practice.
(5) Process theories must define whether the progression from one stage to another is linear or not (yes; mainly yes; or no).	The process theory contains the most typical step-by-step sequence of the stages. The five stages of the process theory are presented in the most typical sequential order that is expected to be followed by most of people, although it's not the only possible existing sequence.
(6) Process theories must define if the progression of the stages is unitary or multiple.	In the process theory, progression of the stages is multiple. Multiple progression means that employees may follow more than a single path from the first stage toward the fifth stage due to alternative barriers of change explaining the progression between the stages. In addition to these several paths leading to the change, employees have two additional paths toward either compliance or non-compliance with IS security procedures within the stages.
(7) Process theories must define if the progression of the stages is cumulative.	Cumulative progression means that the main goals of the earlier stages need to be accomplished at the later stages as well. For example, in order to be able to permanently perform IS security activities at work in the fifth stage, an employee needs to first be aware of the existence of the IS security requirements (the first stage), be exposed to communication regarding them (second stage), experience their nature (third stage), and attain situational understanding of them and reach balanced IS security cognitions (fourth stage).
(8) Process theories must define whether the possibility of relapse exists (yes; no).	There exits the possibility of relapses between the stages. If an employee fails to meet and maintain the main goals of the stages, a relapse to an earlier stage is possible before the last stage of the adoption process can be reached. Relapses to the earlier stages are possible before reaching the tacit IS security practice stage (i.e., the goal of the behavioral change). Relapses occur if an employee fails to meet and maintain the main goal of each stage. For example, in the third stage, non-suitability of IS security procedures with work practices, or inconvenience, may cause an

	employee to relapse to the previous stage.
(9) Process theories must define whether the goal of development progression is known and predetermined.	The process theory has the known and predetermined goal of behavioral change. The ultimate goal of an adoption process is to reach the last stage—namely, tacit IS security practice.

R1: Process theories must have stages, which are ordered and define the development trajectory. Stages are a theoretical construct that helps define the development path of an individual toward certain behavior. Each individual is at a different stage (Weinstein et al., 1998), and each stage has certain different attributes, defined by the process theory in question (see R3 and R4 for more details). Stages with different attributes are important; otherwise, there is no need for a stage theory. For Weinstein et al. (1998) and van de Ven (1998), stage is an ideal prototype. The key is to distinguish at which stage an individual resides, because that defines which actions are optimal or right to change the individual's behavior (Briedle, Riemsma, Pattenden, Sowden et al., 2005).

R2: Process theories must take a stand regarding whether the stages are predefined or not. R2 holds that process theories need to know whether all the stages are known before (e.g., there is always a fixed number of stages), or alternatively, the exact number of stages is unknown for the process theory. This is an important requirement: Since the idea of stage theory is to model the development trajectory, there is a need to know if the stages that form the trajectory are the only ones, or there are other possible stages.

R3: Process theories must include similar attributes (barriers to change). R1 suggested the need to connect attributes with stages. For behavior change theories, one type of attribute is barriers to change, which define the factors that hinder people's progress from one stage to another (Weinstein et al., 1998). R3 holds that Employees A and B face similar barriers (or attributes) in the same stage (e.g., in stage 3). This idea contradicts relativism (Hare, 1981). If the barriers (or any types of attributes) are not similar, but are unique for each person, then helping people overcome these barriers is difficult. In fact, if each individual has unique "barriers" with no

similarities, then any learning is impossible, including helping these individuals overcome these barriers (see Hare, 1981).

R4: Process theories must include different attributes (barriers) at different stages. An employee faces different barriers at different stages (e.g., stage 1 has barrier A, while stage 2 has barrier B). The idea that each stage has some stage-specific attributes is crucial for a process theory. Otherwise, there is no need to have a stage that has no stage-specific attributes.

R5: Process theories must define whether the progression from one stage to another is linear or not (yes; mainly yes; or no). The theory needs to state if people move from one stage to another in a linear, step-by-step manner (from 1 to 2, from 2 to 3), or if they can bypass certain stages (e.g., move from stage 1 to 3 without visiting stage 2). In the case of IS security, this is important so that interventions to improve the behavior can consider the possibility that bypassing a certain stage is possible.

R6: Process theories must define whether the progression is unitary or multiple. Whether there is one path (unitary) or more than one path (multiple) to reach a goal must be defined. This has implications for IS security interventions: Is there only one way to achieve the goals, or multiple ways?

R7: Process theories must define whether the progression is cumulative. Whether the progression is cumulative (e.g., information obtained from stage 1 is necessary in later stages) or not must be defined. This has implications for the IS security interventions by indicating to what extent an intervention at stage 3 needs to focus on issues that are important at the previous stages.

R8: Process theories must define whether the possibility of relapse exists. Can employees progress backward (e.g., from stage 4 to stage 3)? This is important so that scholars and practitioners can understand under what conditions employees can relapse. Such conditions cannot be avoided if we do not know that they are.

R9: Process theories must define whether the goal of development progression is known and predetermined. Does the theory hold that the goal of the progression can be either predetermined (there is one predefined goal such as people die at some point in time whether

they want to or not), or alternatively, can people have different goals and the freedom to decide their goals?

Appendix 2. A connection between the nine criteria of the process theories, and high- and low-level categories identified in the data analysis.

According to the nine criteria, the process theory (1) has a concept of predetermined stages;(2) (2) has the exact number of predetermined stages; (3) includes barriers of change that are similar for people in the same stage, and (4) different for people in different stages; (5) defines linear progression from one stage to another; (6) includes the multiple and (7) cumulative type of progression; (8) includes the possibility of relapses; and (9) defines the known and predetermined goal of development progression. A connection between the nine criteria of the process theories, and high- and low-level categories identified in the data analysis are shown in Table 6.

Table 6. A connection between the meta-theories and the high- and low-level categories.

	Meta-characteristics of process theories (Weinstein et al. 1998)	**Meta-characteristics of process theories (from van de Ven 1992)**	**Five high-level categories in the data analysis**	**22 low-level categories in the data analysis**
Stages of change	a. A classification system to define the stages (1. criterion)	e. Predetermined and most typical stages (1. criterion)	1. Stages in the process	1a. Intuitive thinking 1b. Initial knowledge acquisition 1c. Descriptive thinking 1d. Reflective thinking 1e. Tacit IS security practice
		f. Known and predetermined goal of the behavioral	2. Reasons for compliance and non-compliance with IS security	2a. Context-independent cognitions

		change (7. criterion)	procedures	2b. IS security detached cognitions 2d. Balanced IS security cognitions
Ordering of the stages of change	b. An ordering of the stages (4. criterion)	g. Most typical step-by-step sequence of the stages (4. criterion) h. Not unitary but multiple and cumulative progression of the stages (5. criterion) i. The possibility of relapses among the stages (6. criterion)	-	-
Barriers of change	c. Similar barriers of change facing people in the same stage (2. criterion) d. Different barriers of change facing people in different stages (3. criterion)	-	3. Stage-specific barriers of change 4. Barriers of change regardless of stages: Overriding barriers	3a. Motivation barriers of change 3b. Awareness barriers of change 3c. Reflection barriers of change 3d. Balance barriers of change 3e. Negative barriers of change 4a. Opportunism 4b. Regression 4c. Social pressure 4d. Working environment 4e. Taking a shortcut