Journal of the Association for Information Systems
JAIS

Research Article

Toward a New Meta-Theory for Designing Information Systems (IS) Security Training Approaches*

Mari Karjalainen
University of Oulu
mari.karjalainen@tol.oulu.fi

Mikko Siponen
University of Oulu
mikko.siponen@oulu.fi

Abstract

Employees' non-compliance with IS security procedures is a key concern for organizations. To tackle this problem, there exist several training approaches aimed at changing employees' behavior. However, the extant literature does not examine the elementary characteristics of IS security training, such as the ways in which IS security training differs from other forms of training. We argue that IS security training needs a theory that both lays down these elementary characteristics and explains how these characteristics shape IS security training principles in practice. We advance a theory that suggests that IS security training has certain elementary characteristics that separate it from other forms of training, and we set a fundamental direction for IS security training practices. Second, the theory defines four pedagogical requirements for designing and evaluating IS security training approaches. We point out that no existing IS security training approach meets all of these requirements and demonstrate how to design an IS security training approach that does meet these requirements. Implications for research and practice are discussed.

***Keywords**: IS Security, Meta-Theory, Learning Paradigms, IS Security Training.*

* Ananth Srinivasan was the accepting senior editor. This article was submitted on 31th March 2010 and went through two revisions.

Volume 12, Issue 8, pp. 518-555, August 2011

Toward a New Meta-Theory for Designing Information Systems (IS) Security Training Approaches

1. Introduction

No modern organization can survive without IS security. While the media have called attention to hacking and computer viruses as visible hazards to computer security, the majority of serious IS security problems result from employees failing to comply with basic security procedures related to their work (CSI Survey, 2007; Siponen & Vance, 2010). If users do not comply with IS security policies, security solutions lose their usefulness (Kruger & Kearney, 2006; Thomson, von Solms & Louw, 2006). To ensure that employees follow their companies' key IS security procedures, alternative approaches have been advanced in the literature, such as the use of sanctions and deterrence (Straub, 1990; Siponen, Pahnila & Mahmood, 2007), marketing campaigns (McLean, 1992), and training (Puhakainen & Siponen, 2010). Of these approaches, IS security training is the most common approach to improving employees' IS security behavior (Puhakainen & Siponen, 2010). Although scholars and practitioners generally agree on the need for organizations to implement IS security training, the existing literature does not offer an understanding of the elementary characteristics of IS security training, such as how IS security training differs from other forms of training. We argue that, in order for IS security training research and practice to develop further, there is a need not only to examine the fundamentals of IS security training (how IS security training differs from other types of training) but also to provide theory-based advice on how scholars and practitioners can design, select, and evaluate the pedagogical merit of different IS security training principles. To address these goals, we argue that IS security training needs a theory that (i) lays down these elementary characteristics of IS security training, (ii) explains how these elementary characteristics shape IS security training principles in practice, and (iii) provides models for how IS security training practices can be evaluated pedagogically.

As a step toward remedying this situation, we advance a meta-theory for IS security training that addresses these issues. First, this theory suggests that IS security training has certain elementary characteristics that separate it from other forms of training. Second, this theory defines four pedagogical requirements for designing and evaluating IS security training approaches. We review extant IS security training approaches and conclude that no previous approach meets all of these requirements. Finally, we illustrate how an IS security training approach can meet these requirements and present a research agenda for future research.

The results of this study will be welcomed by scholars and practitioners engaging in IS security training. For scholars, this paper will offer a new theoretical contribution, a meta-theory for IS security training approaches, which not only provides new understanding of the fundamental characteristics of IS security training and how it differs from other forms of training but also suggests new principles for designing IS security training approaches. The paper also offers an agenda for future research. For practitioners, this study will illustrate how to put our meta-theory to practical use by offering important insights into how to improve IS security training in practice through the theoretical framework.

The rest of the paper is organized as follows: the second section discusses extant IS security training approaches and points out the need for a meta-theory of IS security training. We advance this meta-theory at the beginning of the third section, including four pedagogical requirements for IS security training approaches. We review extant IS security training approaches in section 3.2.1 in light of these requirements, finding that no existing IS security training approach meets these requirements. At the end of this section, we demonstrate how an IS security training approach can meet these requirements. The fourth section outlines implications for practice and research, and finally, the fifth section concludes with the paper's findings.

2. Previous IS Security Training Approaches

Thirty-two IS security training approaches for increasing employees' compliance with IS security procedures exist in the literature, which can be thematically divided into seven categories (Figure 1).

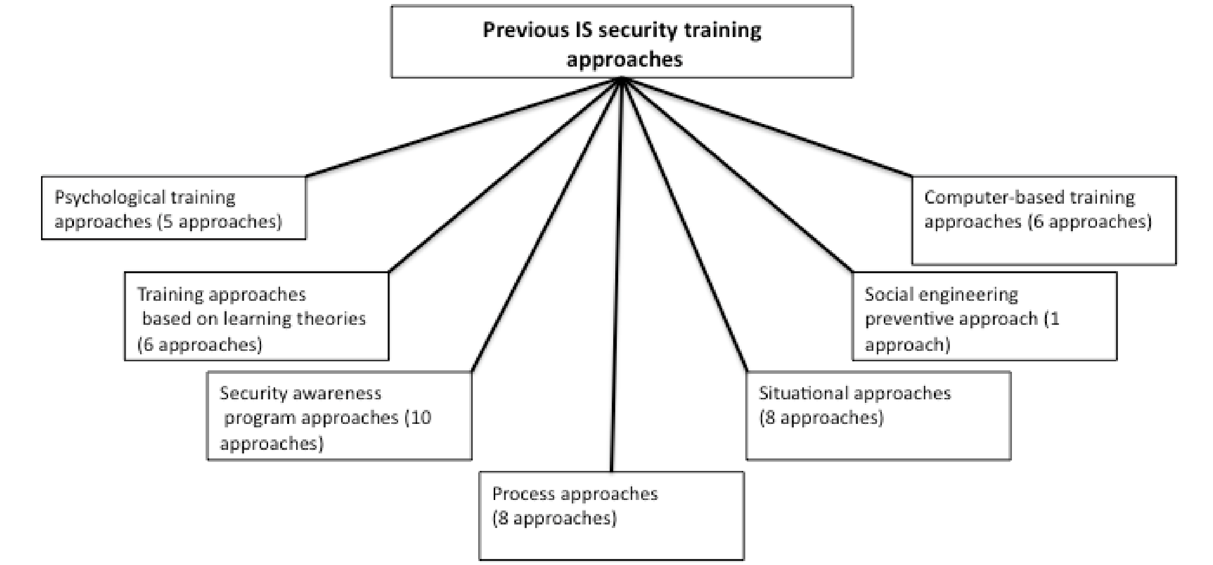

Previous IS security training approaches
Psychological training approaches (5 approaches)
Training approaches based on learning theories (6 approaches)
Security awareness program approaches (10 approaches)
Process approaches (8 approaches)
Situational approaches (8 approaches)
Social engineering preventive approach (1 approach)
Computer-based training approaches (6 approaches)

Figure 1. Categories of IS Security Training Approaches

Psychological training approaches (five approaches) and *training approaches based on learning theories* (six approaches) are based on theoretical concepts from the fields of psychology, social psychology, and education. *Security awareness program approaches* (10 approaches) view IS security training as a method for increasing employees' IS security awareness. *Security awareness programs* training is just one tool for increasing employees' compliance with IS security policies, the *process approaches* (eight approaches) introduce IS security training principles in a stepwise manner. While other approaches can be applied in any context, *context-specific approaches* (eight approaches) are especially designed for certain types of organizational settings, such as universities. While the previous approaches are oriented toward face-to-face learning, *computer-based training approaches* (six approaches) focus on e-learning approaches and computer games. Finally, while the other IS security training approaches are designed for improving employees' behavior in any area of IS security through training, the *social engineering preventive approach* (one approach) is focused on avoiding the phenomenon of social engineering in IS security training.

Table 1 presents seven categories, key findings, and the underlying theories[1] of each IS security training approach. As can be seen in Table 1, 19 of the 32 approaches are placed under only one of the seven categories presented in Figure 1. However, seven approaches are situated under two categories, and six approaches belong to three categories.

Table 1. Extant IS Security Training Approaches, Their Key Findings, and Underlying Theories

ISS training approaches	Category	Key findings	Underlying Theory
Cognitive processing approach (Puhakainen, 2006)	Training approaches based on learning theories, process approaches, and situational approaches	1. Stresses changes in IS security-related attitudes through cognitive processing (recognizing, understanding, and evaluating persuasive arguments). 2. Offers concrete guidance on how to achieve behavior changes. 3. Provides empirical evidence on the practical efficiency of IS security training.	Universal constructive instructional theory (Schott & Driscoll, 1997) and elaboration likelihood model (Petty & Cacioppo, 1986)

[1] The word theory is used here in a broad sense: if the IS security training approach includes any references towards applying a particular type of research (e.g., models, frameworks, or concepts), then we classify the approach as theory-based.

Table 1. Extant IS Security Training Approaches, Their Key Findings, and Underlying Theories (continued)

ISS training approaches	ISS training approaches	ISS training approaches	ISS training approaches
Constructive instruction approach (Heikka, 2008)	Training approaches based on learning theories, process approaches, and situational approaches	1. Emphasizes participants' thinking, interpretations, knowledge construction, and interaction with the environment. 2. Evaluates and reviews the impact of the IS security training on managers' security behaviors.	The systematic approach to training (Buckley & Cable, 1990) and constructivist learning principles (Fosnot & Perry, 2005)
Constructive scenario approach (Biros, 2004)	Training approaches based on learning theories, psychological training approaches, and situational approaches	1. Introduces scenario-based IS security training for teaching deception detection. 2. Mentions users' experiences and active construction of knowledge as essential factors in learning.	Signal detection theory (Klein et al., 1997) and constructivism.
Andragogical approach (Herold, 2005)	Training approaches based on learning theories, security awareness program approaches, and process approaches	1. Emphasizes learners' needs, former experiences, involving users, and improving employees' job performance as the main goals of learning. 2. Offers guidelines and practical examples to develop, implement, deliver, and evaluate IS security awareness and training.	Four basic principles of adult learning: readiness, experience, autonomy, and action (Knowles, 1950).
Cyber security game approach (Cone, Irvine, Thompson & Nguyen, 2007)	Training approaches based on learning theories, situational approaches, and computer-based training approaches	1. Suggests that actions, experiences, problem-solving skills, and critical thinking are essential factors in learning. 2. Introduces the use of a video game tool in training. 3. Examines IS security training and awareness policies in the target organization.	Learning principles in the area of games and simulations (e.g., Gee, 2005).
Pedagogical game approach (Greitzer, Kucher & Huston, 2007)	Training approaches based on learning theories, situational approaches, and computer-based training approaches	1. Incorporates cognitive and pedagogical principles in IS security training: well-connected knowledge structures, personally significant learning experiences, and reconstruction of knowledge. 2. Offers usability and training effectiveness assessments. 3. Presents suggestions for addressing deficiencies in the prevailing gaming context.	Discovery learning (Bruner, 1966; Herman, 1969), active or autonomous learning (e.g., Johnson et al., 1991), and constructionist learning theory

Table 1. Extant IS Security Training Approaches, Their Key Findings, and Underlying Theories (continued)

ISS training approaches	ISS training approaches	ISS training approaches	ISS training approaches
Social psychology oriented approach (Thomson & von Solms, 1998)	Psychological training approaches	1. Applies concepts of social psychology to create more effective training by influencing people's behaviors and/or attitudes. 2. Presents three methods for understanding and changing human behavior: a) directly change users' behavior regardless of their attitudes, knowledge, or feelings (e.g., instrumental learning), b) change attitudes through changes in behavior (e.g., self-persuasion), and c) change attitudes through persuasion.	A typical attitude system (Zimbardo & Leippe, 1991)
Motivation theory directive approach (Roper, Grau & Fischer, 2006)	Psychological training approaches	1. Offers practical guidance for developing and assessing security programs, model processes, and procedural checklists.	Expectancy theory, and the hierarchy of needs
Persuasive technology approach (Forget, Chiasson & Biiddle, 2007)	Psychological training approaches, and computer-based training approaches	1. Introduces an e-learning system based on persuasive technology to influence people's attitudes and behavior and to educate users of IS on the safe use of security measures. 2. Examines the effectiveness of the persuasive authentication framework.	A psychological framework on interactive computing systems (Fogg, 2003)
Social psychological approach (Kabay, 2002)	Psychological training approaches and security awareness program approaches	1. Applies social psychology to improve employees' information security beliefs, attitudes, and behavior. 2. Presents practical recommendations for IS security training to encourage people to be more inclined to approve of information security policies, the features of effective communication, and day-to-day security practices.	Schema, theories of personality, explanations of behavior, errors of attribution, intercultural differences, framing the reality, beliefs and attitudes, persuasion, encouraging initiatives, and group behavior.
Normative approach (Siponen, 2000)	Psychological training approaches	1. Addresses the need for normative approaches and motivation/behavioral theories in organizational IS security training. 2. Aims at making users internalize and commit to the organization's security guidelines.	The theory of intrinsic motivation (e.g., Deci, 1975) and TRA
Counteractive approach (McIlwraith, 2006)	Security awareness program approaches	1. Considers IS security training as an effective tool as part of the awareness program to reduce human error. 2. Offers practical strategies and techniques, measures awareness, and uses delivery media for implementing security awareness. 3. Considers that changes in behavior are the result of a decision-making process. 4. Includes five phases in an approach to the awareness process: managing by fact, goals and objectives, planning, implementation, and feedback.	-

Table 1. Extant IS Security Training Approaches, Their Key Findings, and Underlying Theories (continued)

ISS training approaches	ISS training approaches	ISS training approaches	ISS training approaches
Security ensuring approach (Peltier, 2000)	Security awareness program approaches	1. Considers the IS security awareness program as an element of an overall security program in an organization. 2. Has the goal of making employees aware of security policies, standards, procedures, and guidelines. 3. Discusses security awareness program goals, IS security training needs identification, program developments, methods for IS security training, and program presentations.	-
Communication oriented approach (Desman, 2002)	Security awareness program approaches	1. Presents instructions for building and evaluating an IS security awareness program in a step-by-step manner. 2. Has the goal of making employees aware of the value of the information, their responsibilities, and protection activities.	-
Promotional approach (Rudolph, Warshawsky & Numkin, 2002)	Security awareness program approaches	1. Considers IS security training to be a comprehensive and detailed action to teach employees knowledge and skills to perform effectively. 2. Has the goals of reinforcing the desired behavior and attitudes toward security, and changing undesired ones through repetition. 3. Offers practical principles for establishing IS security training that resemble commercial advertising and campaigns.	-
Stakeholder approach (Kovacich & Halibozek, 2003)	Security awareness program approaches	1. Introduces guidelines for developing and maintaining a corporate information security program and implementing security procedures. 2. Considers the IS security training program to be an important corporate security function to make all relevant actors responsible for the organization's information assets, aware of the ways to protect them, and in compliance with corporate practices.	-
Deterrence approach (Straub & Welke, 1998)	Security awareness program approaches, and situational approaches	1. Considers IS security awareness and training to be a part of their security program. 2. Uses a deterrent countermeasure to increase employees' knowledge of risks, policies, and sanctions in the organizational environment, and to provide a baseline for security planning and prevention activities.	Deterrence theory (Straub, 1990) and the model of managerial decision making (Simon, 1960)
Academic environment approach (Kajava & Siponen, 1997)	Security awareness program approaches, and situational approaches	1. Discusses the need for IS security awareness to create behavioral changes in the academic context. 2. Considers training, student education, and campaigning methods to increase IS security awareness and the level of security.	-
University environment approach (McCoy & Thurmond Fowler, 2004)	Security awareness program approaches, and situational approaches	1. Introduces an IS security awareness program to educate students and employees in the academic environment. 2. Has the training goals of changing people's attitudes and actions related to information security issues and developing metrics to measure the audience's knowledge level before and after the program implementation. 3. Concentrates on describing the planning process that includes determination of content, audience identification, selection of correct methods of delivery, and branding as well as monthly activities.	-

Table 1. Extant IS Security Training Approaches, Their Key Findings, and Underlying Theories (continued)

ISS training approaches	ISS training approaches	ISS training approaches	ISS training approaches
Preventive approach (Nosworthy, 2000)	Process approaches	1. Has the goal of making employees aware, trained, and motivated with respect to their security responsibilities and countermeasures in their daily work. 2. Offers practical instruction for the phases of the IS security training program: defining objectives, identifying requirements and training sources, developing and implementing the program, and monitoring and testing its effectiveness.	-
Strategic approach (Wilson & Hash, 2003)	Process approaches	1. Presents guidelines for the IS security training program at a strategic level for federal agencies and other organizations. 2. Suggests that the purpose of awareness is to change or reinforce users' security behavior. In turn, training aims at developing essential security skills and competencies for ordinary users.	-
Competence approach (Wilson, de Zafra, Pitcher, Tressler & Ippolito, 1998)	Process approaches	1. Addresses role- and performance-based IS security training, which emphasizes actual roles, responsibilities, and the individual needs of employees. 2.Aims to change employees' attitudes and the organizational culture concerning security, and provide training with information security knowledge and skills to all employees involved with IS. 3. Supports training needs identification, course development, and evaluation of learning effectiveness.	-
Operational controls approach (NIST, 1995)	Process approaches	1. Reviews computer security controls from management, operational, and technical viewpoints. 2. Considers IS security awareness, training, and education to be operational controls to improve employees' security attitudes and behavior. 3. Presents seven phases: a) identifying the scope, goals, and objectives, b) identifying the training staff, c) identifying the target audience, d) motivating the management and employees, e) administering the program, f) maintaining the program, and g) evaluating the program.	-
ISD approach (Hansche, 2001)	Process approaches	1. Provides an IS security training curriculum to meet job duties and roles. 2. Reviews phases of the traditional instructional system design (ISD) model: a) needs analysis and goal formation, b) design, c) development, d) implementation, and e) evaluation.	-
Traditional e-learning approach (Kajava, Varonen, Tuormaa & Nykänen, 2003)	Situational approaches and computer-based training approaches	1. Introduces a generic intranet-based e-learning approach for technically oriented specialists in the case organization. 2. Introduces technical, content-related, and pedagogical requirements for the learning environment, and handles presentation issues.	-

Table 1. Extant IS Security Training Approaches, Their Key Findings, and Underlying Theories (continued)

ISS training approaches	ISS training approaches	ISS training approaches	ISS training approaches
Hypermedia instruction approach (Shawn, Chen, Harris & Huang, 2009)	Situational approaches and computer-based training approaches	1. Examines organizational security awareness training in three types of online environments: hypermedia, multimedia, and hypertext. 2. Considers security awareness as three sequenced levels of abilities: users' perception, comprehension, and projection of information security risks. 3. Investigates the impact of information richness on the effectiveness of online IS security training approaches through statistical analysis of the collected data.	-
Policy creation approach (Gaunt, 1998)	Situational approaches	1. Discusses IS security training as part of the development and implementation of an IS security policy in the healthcare environment.	-
Healthcare environment approach (Furnell, Sanders & Warren, 1997)	Situational approaches	1. Introduces basic definitions of measures to establish the training and awareness framework with respect to specific training needs and actions within the healthcare environment. 2. Has the goal to make all employees know, understand, and accept security basics and procedures as part of their responsibilities and roles in the work environment.	-
Discursive approach and online tutorial approach (Cox, Connolly & Currall, 2001)	Situational approaches	1. Introduces three approaches for IS security awareness in the university environment: a discussion session, a checklist, and a Web-based tutorial. 2. Has the objective to increase users' understanding of security and motivate users to act in a secure manner. 3. Considers a discussion session as a discursive approach and a Web-based tutorial as an online tutorial approach in terms of IS security training, while a checklist represents written communication with respect to security issues.	-
Briefing approach (Markey, 1989)	Situational approaches	1. Introduces IS security training and awareness program including briefings for new employees, seminars for security officers, and briefings for directors.	-
Social engineering preventive approach (Mitnick & Simon, 2002)	Social engineering preventive approaches	1. Presents guidelines for the IS security training program and the implementation of customized security policies as prevention activities for social engineering. 2. Considers employees' awareness of security policies as the most effective issue to prevent social engineering. 2. Focuses on policies and procedures as well as on a continuous awareness program that is imperative for IS security to create changes in employees' behavior and attitudes.	-
Active e-learning approach (Furnell, Gennatou & Dowland, 2002)	Computer-based training approaches	1. Introduces a prototype software tool for self-paced IS security training, including three modes of operation: exploration mode (investigation of security measures and different types of security), evaluation mode (scenario-based testing), and author mode (creation of new scenarios).	-

To summarize the literature review of the extant IS security training approaches, while previous studies have echoed the importance of IS security training in organizations, no study has attempted to lay down fundamentals of IS security training, starting with issues such as identifying the fundamental nature of IS security training, and how it differs from other types of training. This is not a surprise, since only 12 out of the 32 IS security training approaches summarized in Table 1 include any kind of theory or theoretical concepts. Of these 12 theory-based approaches, six approaches apply learning theories (Puhakainen, 2006; Heikka, 2008; Biros, 2004; Herold, 2005; Cone et al., 2007; Greitzer et al., 2007); six approaches employ theories from the field of psychology or social psychology (Biros, 2004; Thomson & von Solms, 1998; Roper et al., 2006; Forget et al., 2007; Kabay, 2002; Siponen, 2000); and one approach uses criminology (Straub & Welke, 1998). The other IS security training approaches (n=20) do not include any theoretical foundations (Table 1). Similar findings are echoed by Puhakainen and Siponen (2010), who report the lack of pedagogical theories in the IS security training literature and highlight the need for IS security training studies based on proper pedagogical theories. We argue that before any pedagogical theory can be selected on which to base an IS security training approach, a meta-level examination of the fundamental nature of IS security training is needed. We maintain that only when we have an understanding of such fundamentals of IS security training we are in a position to select proper pedagogical theories on which to base IS security training approaches.

Therefore, we argue that IS security training needs a meta-theory that (i) lays down these elementary characteristics of IS security training, (ii) explains how these elementary characteristics shape IS security training principles in practice, and (iii) provides models on how IS security training practices can be evaluated pedagogically. We present such a theory next.

3. Toward a New Meta-Theory for Designing IS Security Training Approaches

Gregor (2006) distinguishes between five theory types in IS research: (1) analysis, (2) explanation, (3) prediction, (4) explanation and prediction, and (5) design and action. Niiniluoto (1993) calls the first four of these types descriptive (they explain, understand, or predict the world, human behavior, culture, etc.). He labels the last type of scientific enquiry “design science,” which focuses on how things ought to be in order to meet a certain goal (the technical norm in terms of von Wright, 1972). The descriptive theories are, therefore, interested in knowledge, and in the accuracy of information about the world, culture, man, society, etc. The correctness of the knowledge is typically estimated in terms of truth or truthlikeness (Niiniluoto, 1999). In the case of design and action (Gregor, 2006) or design science (Niiniluoto, 1993), success is not defined in terms of true or false but effectiveness related to intended use (Niiniluoto, 1993; von Wright, 1972).

Against this backdrop, we argue that the ultimate objective of IS security training (theory) is design and action (Gregor, 2006) or design science (Niiniluoto, 1993), since the objective is goal-oriented. That is, the aim of IS security training theory is to produce theoretically informed guidance on how to design effective training approaches. In this case, “effective” means that employees will comply with IS security policies. However, before such approaches can be developed, we need to understand the fundamental nature of IS security training, provided that it sets the fundamental direction for IS security training practices. To find a framework that allows us to define the fundamental characteristics of IS security training and explains how these characteristics have an effect on IS security training practices, we need a framework that is both descriptive and action guiding (design and action). To this end, Hare’s (1952, 1963, 1981) meta-theory of three levels of thinking is ideal. This theory is descriptive and prescriptive. As for the former, the theory describes maturity levels in relation to how people form action-guiding principles. We apply Hare’s meta-theory to sketch the structure of our new meta-theory for designing IS security training approaches (Figure 2).

The meta-level refers to fundamental questions, such as “What is IS security training?” and “How does IS security training differ from other types of training?” (Figure 1). The intuitive thinking level refers to conventional activities in practice. The critical thinking level, lying between the meta- and intuitive thinking levels, is needed to test the validity of our conventional actions and form new guidance in novel situations when needed (Hare, 1981). Via the critical thinking level, in our context, those at the intuitive level apply principles such as their education, upbringing, and personal experience to understand IS security training. People who simply follow their intuitive-level principles, without ever questioning them, reside at this level throughout their lives. For example, a practitioner engaging in IS security training who uses the same training method that his supervisor used when educating him, without ever questioning the validity of this method, stays at the level of intuitive thinking. However, when people critically ponder the validity and effectiveness of their conventional principles, they move to critical-level thinking. Such moves may be prompted by feedback from other people, self-critique, feedback from learners, or hints that the IS security training does not work as desired. At the critical level, people can form new imperatives and ways of acting with respect to IS security training, which they then implement at the level of intuitive thinking. This means that the principles at the intuitive level can be overridden; they can be modified, refined, or omitted (see Hare, 1981). Or in a case where two principles are in conflict, people can override one to follow the other. Next, we describe these levels of thinking, starting from the meta-level.

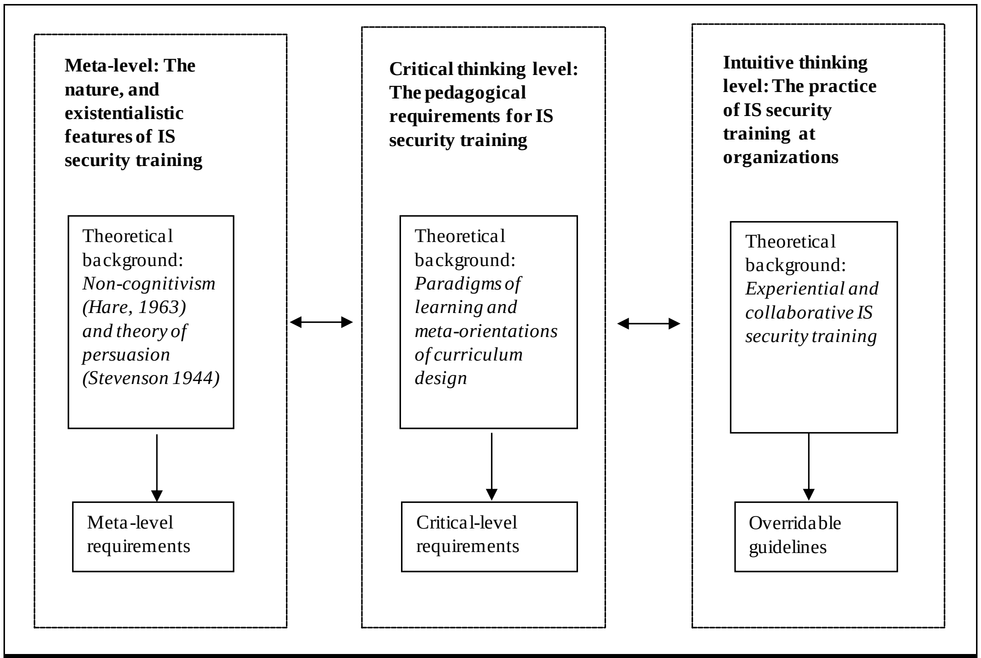

Meta-level: The nature, and existentialistic features of IS security training
Theoretical background: *Non-cognitivism (Hare, 1963) and theory of persuasion (Stevenson 1944)*
Meta-level requirements
Critical thinking level: The pedagogical requirements for IS security training
Theoretical background: *Paradigms of learning and meta-orientations of curriculum design*
Critical-level requirements
Intuitive thinking level: The practice of IS security training at organizations
Theoretical background: *Experiential and collaborative IS security training*
Overridable guidelines

Figure 2. A Framework for the Meta-Theory of Designing IS Security Training Approaches Based on Hare's Theory of Three Levels of Thinking (1952; 1963; 1981)

3.1. Meta-Level Thinking: The Nature and Existentialistic Features of IS Security Training

Meta-level thinking encompasses issues such as the meaning of learning in the context of IS security training or the fundamental characteristic of IS security training. Issues at this level are important because they help us to understand how IS security training differs from other types of training. We argue that it differs because of its nature and existentialistic features, which we discuss next.

3.1.1. The Fundamental Nature of IS Security Training

Based on non-cognitivism (Hare, 1963) and the theory of persuasion (Stevenson, 1944), we argue that the nature of IS security training is non-cognitive and persuasive. This nature contrasts with other types of training, such as university education, which is descriptive (hence, cognitive), provides scientific facts, and does not seek to influence learners' attitudes and behavior in the manner of persuasive training. IS security training is persuasive and non-cognitive because information procedures, similar to moral norms, require more normative training approaches than those employed in learning facts (Siponen, 2000). Indeed, compared to fact-telling educative strategies (presentation of the facts), persuasive approaches are more effective in situations where the level of commitment to change is low (Hayes 2010). This low level of employees' commitment to complying with IS security policies is widely mentioned in the literature (Siponen & Vance, 2010). IS security procedures are also non-cognitive because they are created within an organizational context, and not necessarily based on scientific or moral inquiry (as are the creation of facts and moral norms, respectively). Following non-cognitivism as a philosophical doctrine, IS security procedures are utterances expressing organizations' non-cognitive attitudes toward how employees ought to behave in a secure manner. The expressional side of IS security procedures resembles cognitivism at first sight, in that this procedure seems to have a true value, although it does not. Since IS security procedures are incapable of being objectively true or false, they are non-cognitive: They do not describe any factual features. For example, "This computer is red" is a cognitive statement, for which a truth-value can be resolved through scientific scrutiny. However an IS security procedure, such as "Do not share your passwords with peers" is not a fact; it does not have an objective truth-value.[2]

In addition to a non-cognitive and persuasive nature, other factors are characteristic of IS security training. While other types of organizational training for white-collar employees can be persuasive and non-cognitive, such as training on fire safety procedures the emphasis of IS security training is usually on daily work situations (Siponen & Vance 2010). For example, fire safety training for white-collar employees typically focuses on exceptional work situations, such as how to evacuate the building when there is a fire, but most IS security training focuses on routine work procedures, such as logging out of the computer every time the employees leave their computers (Siponen & Vance 2010; Puhakainen & Siponen 2010). While IS security training can also cover exceptional work situations (e.g., how to recover after an earthquake), such situations concern a limited number of employees, such as IT and IT security staff. Hence, IS security training for ordinary white-collar employees focuses on routine activities, and thus, should have relevance to employees' daily work (Puhakainen & Siponen, 2010).

3.1.2. Existentialistic Features of IS Security Training

Along with the persuasive and non-cognitive nature of IS security training, three existentialistic features are characteristic of the need for IS security training: (1) existence of security-sensitive organizational assets; (2) threats toward them; and (3) different technical, social, and organizational mechanisms for protecting the organization's assets (protection mechanisms) (modified from Siponen, Baskerville & Heikka, 2006). The absence of these features would make IS security training unnecessary. For example, if there are no assets of value in the organization, or if there are no threats to the organization, there is no need for IS security or for IS security training. Thus, IS security training must ensure that the employees understand the security-sensitive nature of organizational assets. If employees lack this understanding, the IS security training is meaningless and arbitrary from the viewpoint of the substance. IS security training also needs to introduce relevant threats to employees in a pedagogically meaningful manner. Finally, IS security training must be focused on achieving the objective of putting mechanisms in place that are able to protect security-sensitive organizational assets from threats. These three existentialistic features set the fundamental direction (general aim) of IS security training.

Related to these existentialistic features, IS security training has two characteristics that are in contrast to many other types of organizational training: (1) voluntariness vs. mandatoriness in using the protection mechanisms and (2) the intangible nature of the information security threats and assets. The first characteristic (voluntariness vs. mandatoriness) means that while the use of some protection mechanisms can be forced through technical solutions (e.g., restricting Internet access), and compliance with IS security procedures is typically mandatory (i.e., required in IS security policies), employees can bypass most protection mechanisms (e.g., leave their computer unlocked, send confidential e-mail without encryption, open links to infected websites). This is different from training in the use of the system, for example. If a new IS is deployed in an organization, the employees may have to use the system, because that may be the only way to perform their work. For instance, a travel agent may be forced to use a new travel system, whether he likes it or not.

The second characteristic is the intangible nature of IS security threats and assets, meaning that the consequences of IT and the lack of information security may be difficult for employees to see. This is different from fire safety, for example. Most people have seen a fire, but who has seen a password being cracked? In other words, compared to the IS security risks of an organization's

[2] This does not mean that there is no room for factual information in IS security training, e.g., persuasion can be based on facts about threats.

information assets, fire safety training, for example, concentrates on more concrete risks that can threaten organizations' facilities and employees' health or their lives. If employees do not understand the consequences of their actions, say, the negative consequences for selecting an easy to guess password, then why would they comply with IS security policies requiring passwords that are difficult to guess? Therefore, it is no surprise that IS security researchers have observed the difficulty employees have in understanding IS security assets and threats (Shawn et al., 2009).

From the discussion of the nature of IS security training, and the existentialistic features, which differentiate IS security training from other types of training, we arrive at the following meta-level requirements:

First meta-level requirement for IS security training approaches: An IS security training approach must be based on the understanding that the nature of IS security training is persuasive and non-cognitive for influencing employees' mainly routine work situations.

Second meta-level requirement for IS security training approaches: An IS security training approach must focus on the existentialistic features of IS security training, including understanding the voluntariness vs. mandatoriness in using the protection mechanisms, and the intangible nature of information security threats and assets.

We now focus on the preferred pedagogical requirements to be used in order to meet these two meta-level requirements for designing IS security training approaches.

3.2. Critical-Level Thinking

The critical-level thinking (Hare, 1981) applied to this context concerns selecting the proper pedagogical principles for carrying out IS security training in practice. Given that this study examines the preferred pedagogical principles for IS security training, the study scrutinizes paradigms of learning—behaviorism, cognitivism, constructivism, and social constructivism (Hung, 2001)—to find the most appropriate paradigm for this context. Meta-orientations are helpful for selecting the most suitable paradigm of learning for IS security training. In terms of Hare's (1981) work, these theories help us to determine the most appropriate critical-level requirements for IS security training approaches. Next, we illustrate this framework (learning paradigms and meta-orientations), and derive from it four pedagogical requirements at the critical level. We then analyze the extent to which the existing IS security training approaches meet these pedagogical requirements.

3.2.1. Paradigms of Learning and Features of Meta-Orientations

Compared to the paradigms of learning, meta-orientations allow us to more concretely examine IS security training approaches. Meta-orientations refer to the fundamental educational philosophy underlying any intentional interaction designed to facilitate learning and achieving educational goals (Miller & Seller, 1985; Cheung & Wong, 2002). Paradigms of learning and meta-orientations are interrelated; paradigms of learning form a theoretical basis for meta-orientations, which are used to analyze IS security training approaches. Table 2 summarizes the learning paradigms and features of meta-orientations.

Three meta-orientations—transmission, transaction, and transformation—have five dimensions. The first is the psychological context of learning. As can be seen from Table 2, different meta-orientations are linked with three paradigms of learning (behaviorism, cognitivism, constructivism and social constructivism): the transmission meta-orientation favors behavioristic principles, the transaction meta-orientation is influenced by cognitivism, and the transformation meta-orientation is linked with constructivism and social constructivism. The other dimensions are general aims (2), content (3), teaching methods (4), and evaluation of learning (5). Next, we discuss these dimensions starting from the general aims of IS security, because this dimension (Table 2) sets the overall direction for developing the training approach, including the other four dimensions of meta-orientations.

Table 2. Features of the Meta-Orientations of Curriculum Design (see MIller & Seller, 1985; Miller, 2007)

	Transmission	Transaction	Transformation	
1. Paradigm of learning as a psychological context	Behaviorism	Cognitivism	Constructivism	Social constructivism
2. General aims	Reception and mastery of pre-defined contents as objective knowledge	Development of cognitive abilities and problem-solving skills	Transformation of predominant beliefs and actions; personal change	Transformation of predominant beliefs and actions; communal change
3. Content	Subject-centered	Problem- or process-centered	Learner-centered	Community-centered
4. Teaching methods	Instructor-led approaches in order to transmit knowledge and provide external reinforcement	Focus on cognitive problem-solving and analysis	Focus on critical reflection of personal knowledge through collaboration or authentic problem solving to attain personal change	Focus on critical reflection of communal knowledge through collaboration or authentic problem-solving to attain communal change
5. Evaluation of learning	Observable performance through tests or competence-based evaluation	Adaptation of knowledge and acquisition of intellectual skills	Conversational forms of evaluation for individuals	Conversational forms of evaluation for groups

3.2.1.1. General Aims of IS Security Training

Recognizing the persuasive and non-cognitive nature of IS security training, and the existentialistic features of IS security training (training must be connected to protecting valuable assets from threats through specific means), we argue that the communal transformation meta-orientation is the preferred choice for IS security training.

While it is necessary that employees understand IS security procedures, the aims of IS security training are not simply to help employees remember and understand IS security procedures without providing an opportunity to analyze or reflect on information, as in transmission-oriented training (Miller, 2007; Miller & Seller, 1985). Transmission-oriented IS security training would involve a one-way communication of information to employees—"here are the IS security rules"—without any feedback, discussion, or activation of thinking processes. Such a transmission-oriented approach would be ideal for helping employees to remember and understand pre-determined content (facts, concepts, or values); however, given that IS security training is persuasive as discussed in section 3.1, it requires a more discursive and persuasive approach. Security guidelines must be justified, and employees need to see how the guidelines relate to work situations (Siponen, 2000). Hence, the general aims of transmission-oriented training are not suitable for IS security training.

Transaction-oriented training stresses cognitive adaptation through the use of problem-solving skills such as analyzing, synthesizing, evaluating, or applying knowledge (Miller, 2007; Miller & Seller, 1985). For example, a trainer could presents laws related to IS security, and then ask the learners to apply the laws in a predefined scenario that is not connected to the employees' work tasks. While such transaction-oriented training can be persuasive, the problem remains that a transaction-oriented approach does not emphasize that the learning situations must be connected to the employees' own working experiences. Consequently, the employees lose the connection of the training material to their own work tasks. Hence, the general aims of transaction-oriented training are not suitable for IS security training.

Transformation-oriented training is directed toward changing learners' beliefs and behavior (see Table 2). We argue that this is also the key purpose of IS security training: to change employees' IS security behavior in such a way that complying with IS security procedures becomes a natural part of the employees' daily activities (Siponen, 2000; Thomson et al., 2006); hence, the nature of IS security training is persuasive and cognitive. Even though IS security training can often include transmission- and transaction-oriented aims, such as delivering knowledge to employees or developing their cognitive abilities or problem-solving skills, these cannot be seen as the overall aims of training. Transformation-orientated training addresses the need to change behavior by connecting the learning issues, such as compliance with information security procedures, to employees' own work tasks and experiences. Hence, learning is based on learners' previous experiences (Miller & Seller, 1985). This is important since previous research shows that new knowledge is best constructed through previous experiences. To give an example of transformation-oriented IS security training on good password practices, the training would start with a discussion of the relevance of passwords as protection mechanisms in the employees' work situation. The trainer would make clear the assets that each employee protects by using passwords, and what the threats and implications are if someone cracks the employees' passwords. The training would further demonstrate what password cracking means, and how it happens using examples of the employees' passwords.

Finally, the transformation orientation includes two different directions for designing training: individual and communal. We emphasize the importance of the latter in IS security training, because we argue that IS security training is primarily directed toward creating a communal change in employees' IS security behavior—changing the work community's prevailing organizational work practices and developing the organizations' security culture (Dhillon, 2007)—rather than only an individual change (see Table 1). We argue that employees' IS security behavior consists of such shared organizational work practices, which, along with formal IS security policies, depend on an organization's unwritten culture, which defines what kinds of behavior are seen as acceptable and unacceptable (see Robbins, 1993). To influence such shared working practices, we argue that group-oriented training approaches are better than individual approaches, because group approaches help employees obtain richer knowledge and increased acceptance of the prescribed changes to their behavior (Robbins, 1993). For example, educators can organize a discussion section where learners present their own views on, say, why they should encrypt sensitive e-mails. Presentation of the different views of group members helps their peers understand different reasons for encrypting their e-mails and corrects their own misconceptions in the context of their work (e.g., "My e-mails do not contain sensitive information") and encourages higher acceptance of using e-mail encryption in their work. Keeping these issues in mind, we argue that the communal transformation meta-orientation is preferred for IS security training.

The general aims of the communal transformation meta-orientation set the direction for selecting other features of meta-orientations: psychological context, content, teaching method, and evaluation of learning (see Table 2). Next, we discuss the features of meta-orientation. In addition, we put forward corresponding pedagogical requirements for IS security training at the critical level derived from the communal transformation orientation as part of a meta-theory for designing IS security training.

3.2.1.2 Pedagogical Requirements for IS Security Training

(1) First Pedagogical Requirement for IS Security Training: Psychological Context

As the first pedagogical requirement for IS security training approaches derived from the communal transformation meta-orientation, the explicit psychological context—the learning paradigm behind the training approach—must be based upon a group-oriented theoretical approach to teaching and learning. This will guide training activities (see Fardanesh, 2006; Gibson, 2001; Hinsz, Vollrath & Tindale, 1997). Such group-oriented learning theory is needed for IS security training because it is primarily directed toward creating communal rather than personal change (see Table 2). This means that employees' compliance with IS security procedures at the individual level only is not enough to assure organizational success; rather, the target is communal-level change through communal (or collective) learning. Such communal learning develops the group's collective ability to act more effectively (or securely, in the case of IS security training) in a complex work environment, while individuals (or groups) are collaborating and learning from each other (Hayes, 2010). Depending on the situation, this may lead to collective refinement of the prevailing (IS security) rules or changing the employees' accepted ways of thinking and, further, behaving (Hayes, 2010; Argyris & Schön, 1978).

The transmission meta-orientation does not meet this requirement, as this meta-orientation emphasizes the stimulus-response system of learning in terms of behaviorism (see Miller & Seller, 1985). In turn, the transaction meta-orientation is psychologically oriented to cognitive psychology and cognitivism. Cognitivism, as an approach to learning, emphasizes individual development of cognition. These transmission and transaction meta-orientations consider learning only as an individual process in the psychological context. Thus, they do not represent a suitable learning approach for IS security training, which requires a communal and group-oriented learning approach. The communal group-oriented approach, ideally, leads to organizational improvement in the level of the overall IS security culture.

In addition, humanistic psychology (Maslow, 1970; Rogers, 1969), as the psychological context within the transformation meta-orientation (see Miller & Seller, 1985), emphasizes individual learning, and thus, for the aforementioned reasons, is not a suitable learning paradigm for IS security training. The humanistic approach to learning has much in common with the constructivist approach, as both emphasize the active role of the learner and the interactive character of learning. Humanism emphasizes self-actualization and self-transcendence (Miller & Seller, 1985), or growth and personal integrity (McNeil, 1981). Compared to humanism, constructivism is a more appropriate learning paradigm from which to construct meanings of events and ideas, to transform understanding (Ross, 2002), and to build a connection between a learner's existing knowledge and what he/she is expected to learn (Gagnon & Collay, 2006).

However, social constructivism, the second corresponding psychological context of the transformation orientation, meets this first pedagogical requirement, because it stresses social learning, the social viewpoint of learning processes, interactions, and knowledge (Palincsar, 1998). Because this learning paradigm offers a group-oriented theoretical approach, we argue that social constructivism is the most suitable learning paradigm for IS security training.

In addition to communal change being a general aim of IS security training rather than individual change (see the section General aim of IS security training), there are other justifications for considering social constructivism as the preferred approach for IS security training. First, studies in other areas have found that social learning influences a change in individuals' risk perceptions as well as in their protective behavior (e.g., Helleringer & Kohler, 2005; Douglas & Wildavsky, 1982). These are essential goals in IS security training. For instance, hightened understanding of risks related to selecting easy-to-guess passwords can be expected to lead employees to protect the valuable documents saved in their computers by complying with the organization's password procedures. Employing social learning in IS security training means including employees' collective experiences in the learning content (e.g., employees' shared experiences in IS security risks related to password use) and collaborative teaching and evaluation methods (e.g., discussion of the relevance of IS security risks related to password use in employees' work, and achieving mutual agreement to minimize the occurrence of these risks by adhering to password policies). We discuss content, teaching method, and evaluation of learning in more detail in the next sections.

Second, social constructivism includes several characteristics useful for motivating employees to change: user participation, involvement, and negotiated agreements (Nadler, 1993; Lines, 2004; Hayes, 2010).

Third, previous research reports that employees' IS security behavior is influenced by other people, which is consistent with the principles of social constructivism. For example, employees' compliance intentions or behavior is influenced by management and co-worker attitudes and behavioral expectations (Pahnila, Siponen & Mahmood, 2007; Herath & Rao, 2009), peer behavior (Herath & Rao, 2009), and active participation in workshops (Albrechtsen, 2007; Adams & Sasse, 1999).

(2) Second Pedagogical Requirement for IS Security Training: Content

As the second pedagogical requirement for IS security training derived from the communal transformation meta-orientation, the training content must be based on the learners' collective experiences and meaning perspectives (see Hmelo-Silver & Barrows, 2008). This is required because, to make IS security policies community-centered, understood, accepted, and implemented collectively (not just individually), training must include learners' shared perceptions of these policies in their own work.

Transmission-oriented content is not ideal for IS security training because such content does not involve the learners' collective experiences and meaning perspectives (hence, it does not meet the second pedagogical requirement). Rather, knowledge (content) is seen to be objective, unrelated to human subjectivity (Brody, 1998), and static (Miller, 2007). The content of transmission-oriented training is subject-centered (Miller & Seller, 1985; Miller, 2007). IS security training that introduces laws in the area of IS security without tailoring the training to the company's context and learners' experiences is an example of transmission-oriented training. Such training based on laws would be generic for all, and therefore, not connected to the work situations or work experiences of each learner.

The transaction orientation emphasizes problem-centered content mainly selected by the teacher, but also takes into account the learners' interests (Miller & Seller, 1985). This orientation stresses the learning process and cognitive process skills rather than the understanding of facts (Cheung & Wong, 2002). As an example of transaction orientation in the context of IS security training, learners may analyze information security policies or create classifications of information security threats and prevention activities provided in the literature. In addition, in the transaction orientation, the instructor uses concrete examples or questions in the training session to activate learners' cognitive processing of knowledge. However, the transaction-oriented training content does not emphasize communal and experiential characteristics, which are required for effective IS security training.

Learner-centered transformation-oriented training stresses learners' experiences and involvement in the community (Miller & Seller, 1985). Furthermore, as new knowledge emerges from the community through collaborative knowledge building (Hmelo-Silver & Barrows, 2008), the knowledge is community-centered. Thus, transformation meta-orientation content is based on the collective experiences and meaning perspectives of the learners, meeting the second requirement for IS security training. Using transformation-oriented training, the meaning and relevance of IS security laws are discussed within the context of the company's actual work situations. In addition, employees' experiences in this area are taken into account, because the substance of the training—laws, in this case—is based on learners' previous understanding. Finally, such employee experiences are shared and communicated during the training.

(3) Third Pedagogical Requirement for IS Security Training: Teaching Method

As the third pedagogical requirement for IS security training derived from the communal transformation meta-orientation, teaching methods must focus on collaborative learning in order to reveal and produce collective knowledge (see Mezirow, 1991; Palincsar, 1998; Dillenbourg, Baker, Blaye & O'Malley, 1996; Rochelle & Teacley, 1995). Such teaching methods are needed in IS security training because they enable communal change in employees' IS security attitudes and behavior (see Table 2).

This requirement is not met in transmission-oriented training, where the teaching method is a one-way distribution of knowledge, the teacher's role is directive, and learners are passive participants (Miller, 2007). In the context of IS security training, teaching methods characterized by the transmission orientation emphasize instructor-led activities to deliver security messages. The teacher presents security procedures to learners through different audio-visual means (e.g., face-to-face and computer-based presentations) without paying attention to learning processes, problem-solving assignments (transaction), or individual or communal reflection of experiences (transformation).

In the transaction orientation, teaching methods are not focused on collaborative learning in order to reveal and produce collective knowledge as required from IS security training. Instead, teaching methods focus on cognitive problem-solving through applications, analyses, and syntheses of the learning material (Bloom, 1956; Miller & Seller, 1985). In these cases, training includes cognitive problem-solving activities that are mainly defined by the teacher, and that demand active information processing by the learners. As an example in the context of IS security is training, students may be asked to recognize and classify IS security threats and prevention activities in imaginary scenarios created by the teacher that relate to predefined classifications in the IS security literature.

Transformation-oriented teaching methods, in contrast, make connections between learners and their actual working practices (Miller & Seller, 1985). Thus, learning occurs through critical reflection, authentic problem-solving, or communication. Critical reflection is when a person or a group of people ponder the validity of their actions, thoughts, and feelings in order to change them (Mezirow, 1991). Accordingly, in the context of IS security training, teaching methods that create communal knowledge must emphasize discussions concerning experiences, attitudes, and behaviors toward IS security issues. The communal creation of experiences includes collaboration (which engages each member of the group) in order to collectively solve a common problem or reach an agreement (Dillenbourg et al., 1996; Rochelle & Teacley, 1995). The goal of discussion is to reflect on collective experiences and achieve mutual understanding and agreement, which meets the third requirement for IS security training.

(4) Fourth Pedagogical Requirement for IS Security Training: Evaluation of Learning

As the fourth pedagogical requirement for IS security training derived from communal transformative meta-orientation, evaluation of learning should emphasize experiential and communication-based methods from the viewpoint of the learning community (see Miller & Seller, 1985; Birenbaum, 1996). These methods are preferred in IS security training because the goal of training is to construct collaborative knowledge (i.e., to mutually understand new IS security procedures).

Transmission-oriented training does not meet this goal, as the evaluation concentrates on an objective measurement of training goals with pre-defined responses. Examples of the evaluation representing the transmission orientation in the context of IS security training are formal exams, tests, or competence-based evaluations in authentic situations typically conducted after a training session. A web-based training evaluation asking learners about IS security procedures (e.g., a good password has more than 12 characters, “yes” or “no”) with multiple-choice-style answers is an example of a transmission-oriented evaluation of training.

As for transaction-oriented training, evaluation focuses on examining learners’ information processing through cognitive problem-solving tasks. Examples of transaction-oriented evaluation tasks in the context of IS security training include verbal or written exercises to analyze information or apply learned issues in a similar context. Thus, transaction-oriented teaching methods and evaluation tasks are highly similar in nature (see “Third pedagogical requirement for IS security training: Teaching method”). An example of this is case-based training, where employees are asked to point out how many IS security violations each case contains, and teachers assess whether the employees’ results are relevant according to some predefined criteria.

Evaluation in transformative training includes informal, experimental, and open-ended forms of evaluation for individuals or groups (Miller & Seller, 1985). Learners are active participants who share responsibility in the evaluation process through self-evaluation, reflection, collaboration, and continuous dialogue with the IS security trainer during the IS training sessions. The evaluation methods include feedback during work or assignments, group projects, peer evaluations, and interviews (Birenbaum, 1996). An example of an assignment could be one where the employees are asked to indicate how the training has improved their skills, knowledge, or behavior. Ideally, in transformative training, the learners and IS security trainers discuss such issues, and this communal sharing of knowledge results in new learning experiences. In this way, evaluation is a key part of the continuous learning process, not an end in itself. These evaluation methods are experiential and communication-based, and thus, fulfill the fourth requirement for IS security training. Next, we point out the extent to which the existing IS security training approaches meet these four requirements.

3.3. Existing IS Security Training Approaches and the Four Pedagogical Requirements

Thirty-two IS security training approaches have been developed aimed at improving employees' IS security behavior in the organizational context.[3] Table 3 shows the extent to which the existing IS security training approaches meet the four pedagogical requirements formulated earlier. To summarize, none of the IS security approaches meets all four pedagogical requirements. "X" means that an IS security training approach fulfills the requirement, and "–" signifies that the approach does not fulfill the requirement (for more details, see Appendix 1).

Table 3. The Degree to which Extant IS Security Training Approaches Meet the Four Pedagogical Requirements for IS Security Training Approaches

IS security training approaches	(1) Fulfills the requirement for the explicit psychological context	(2) Fulfills the requirement for the content	(3) Fulfills the requirement for teaching method	(4) Fulfills the requirement for evaluation of learning
Cognitive processing approach (Puhakainen, 2006)	-	X	X	X
Social psychological recommendations approach (Kabay, 2002)	-	X	X	-
Andragogical approach (Herold, 2005)	-	-	-	X
Strategic approach (Wilson and Hash, 2003)	-	-	-	X

Pedagogical requirements: (1) the explicit psychological context must be based upon the group-oriented theoretical approach of teaching and learning; **(2) the training content** must be based on collective experiences of the learners; **(3) teaching methods** must focus on collaborative learning in order to reveal and produce collective knowledge; and **(4) evaluation of learning** should emphasize experiential and communication-based methods from the viewpoint of the learning community.

Analyzed IS security training approaches, which do not fulfill any of the pedagogical requirements: Constructive instruction approach (Heikka, 2008); Constructive scenario approach (Biros, 2004); Cyber security game approach (Cone et al., 2007); Pedagogical game approach (Greitzer et al., 2007); Social psychology–oriented approach (Thomson & von Solms, 1998); Motivation theory directive approach (Roper et al., 2006); Persuasive technology approach (Forget et al., 2007); Normative approach (Siponen, 2000); Counteractive approach (McIlwraith, 2006); Security ensuring approach (Peltier, 2000); Communication-oriented approach (Desman, 2002); Promotional approach (Rudolph et al., 2002); Stakeholder approach, (Kovacich & Halibozek, 2003); Deterrence approach, (Straub & Welke, 1998); Academic environment approach (Kajava & Siponen, 1997); University environment approach (McCoy & Thurmond Fowler, 2004); Preventive approach (Nosworthy, 2000); Competence approach (Wilson et al., 1998); Operational controls approach (NIST, 1995); ISD approach (Hansche, 2001); Traditional e-learning approach (Kajava et al., 2003); Hypermedia instruction approach (Shawn et al., 2009); Policy creation approach (Gaunt, 1998); Healthcare environment approach (Furnell et al., 1997); Discursive approach and online tutorial approach (Cox et al., 2001); Briefing approach (Markey, 1989); Social engineering preventive approach (Mitnick & Simon, 2002) and; Active e-learning approach (Furnell et al., 2002).

[3] Studies on education for information security professionals are outside the scope of this review (e.g., Goel & Pon, 2006; Bishop, 2000; Romney, Higby, Stevenson, & Blackham, 2004; Ryan, 2003; Sharma & Sefchek, 2007). In addition, articles concentrating on evaluating training approaches (e.g., Kruger & Kearney, 2006; Martins & Eloff, 2001; Stanton, Stam, Mastrangelo, & Jolton, 2005; Dodge, Carver, & Ferguson, 2007) are omitted, because they focus only on how to measure the effectiveness of these approaches, not the actual development and implementation of training. In addition, articles referring to training as a part of an IS security awareness program are excluded if the characteristics of these training efforts are not described in detail (e.g., Bray, 2002; Information Security Forum, 2005; Leach, 2003; Murray, 1991; Olnes, 1994; Parker, 1999; Sasse, Brostoff, & Weirich, 2001; Spurling, 1995; Stacey, 1996; Telders, 1991).

One study (Puhakainen, 2006) meets the last three requirements, another (Kabay, 2002) meets the second and third requirements, and two (Herold, 2005; Wilson & Hash, 2003) meet the last requirement. However, the features of the existing IS security training approaches that fulfill these pedagogical requirements are not guided by the social constructivist learning paradigm or the instructional design approach. Therefore, these are considered to be only single features and not in the essence of the IS security training practice. Given that no existing IS security training approach meets all four pedagogical requirements, the following section advances an example of a new training approach that meets these four requirements.

3.4. Intuitive-level thinking: Example of an IS security training approach that meets the four pedagogical requirements

In the previous sections, we advanced a meta-theory for an IS security training approach, mirroring Hare's theory of three levels of thinking. Accordingly, we put forth two meta-level requirements: 1) An IS security training approach must be based on the understanding that the nature of IS security training is persuasive and non-cognitive; 2) An IS security training approach must focus on the existentialistic features of IS security training. These two requirements informed the search for pedagogical requirements at the critical-thinking level. As a result, we laid out four pedagogical requirements for IS security training approaches. This section demonstrates a potential pedagogical approach to IS security training that meets these four pedagogical requirements.

3.4.1. Searching for a Proper Instructional Design Approach Fulfilling the Pedagogical Requirements for IS Security Training

The first pedagogical requirement for IS security training is that the explicit psychological context of IS security training must be based upon the group-oriented theoretical approach to teaching and learning. In seeking candidate approaches that meet the first pedagogical requirement for IS security training, constructivist instructional design theories constitute ideal theoretical bases for designing IS security training, for two reasons. First, a constructivist instructional design theory is beneficial in training design because this theory expresses concrete instructions for training, unlike the four high-level pedagogical requirements derived from the social constructivist learning paradigm[4] (Yilmaz, 2008; Wasson, 1996). Second, constructivist instructional design approaches are also relevant for social constructivist instructional design. The key difference between them is that constructivism has the individual learner viewpoint and social constructivism emphasizes a social viewpoint toward learning with respect to general aims, content, teaching methods, and evaluation (see Table 2).

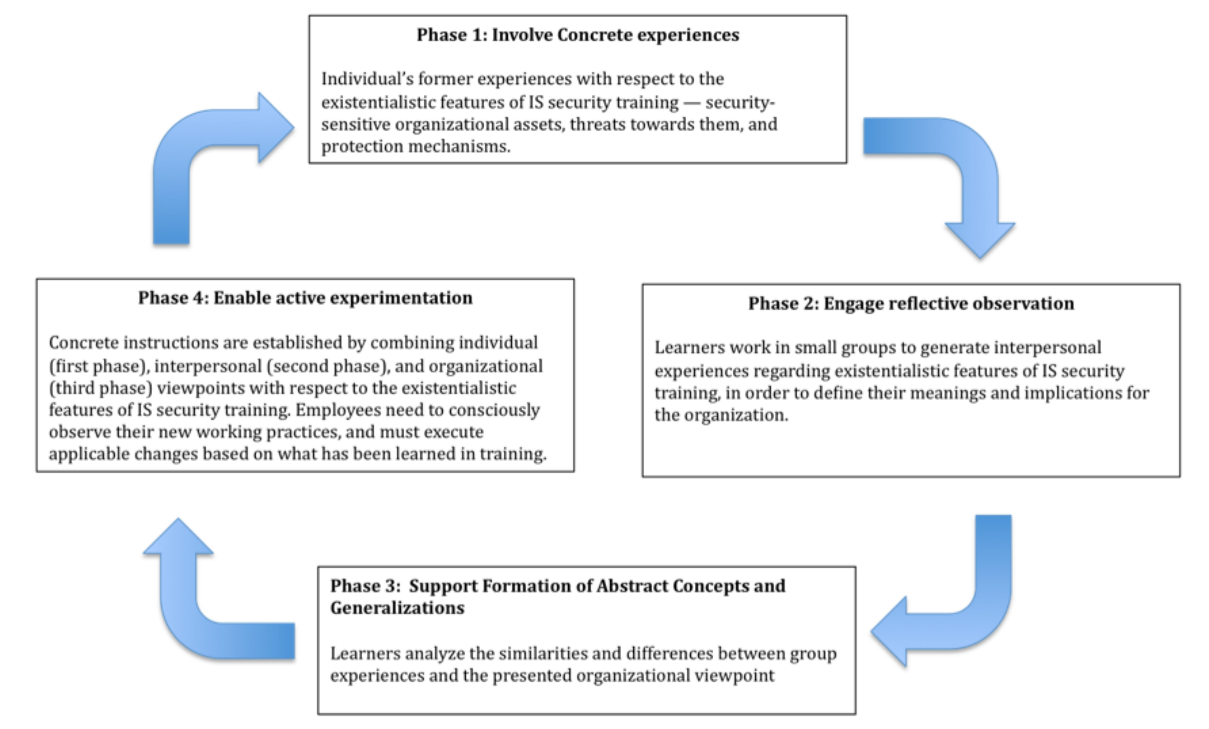
Of the alternative constructivist instructional design approaches (see Fardanesh, 2006; Kirschner, Sweller & Clark, 2006), we use experiential learning as an example to illustrate how to meet the four requirements, because it is the preferred learning approach in the organizational context (Pavlica, Holman, & Thorpe, 1998; Backström, 2004; Dixon, 1999); it is work-based learning (Honey & Mumford, 1992); and it achieves the raising of group consciousness, community action, and social change (Weil & McGill, 1989). Thus, we deem the experiential learning approach to be a suitable approach for changing employees' IS security attitudes and behaviors.

A leading experiential learning approach is Kolb's (1984) theory of experiential learning (see Tennant, 1997). We select this theory to form the instructional design part of the IS security training approach (which should meet the four pedagogical requirements). Because Kolb's theory of experiential learning does not address the social aspects of learning (Pavlica et al., 1998; Holman, Pavlica, & Thorpe, 1997), we add collaborative learning techniques (Barkley, Cross, & Major, 2005) to our IS security training approach, in order to achieve effective learning in groups. Collaborative learning has been reported to be effective for promoting achievement and productivity (Johnson, Maruyama, Johnson, Nelson, & Skon, 1981), and changing attitudes (Springer, Stanne, & Donovan, 1999). Next, we introduce the IS security training approach, combining experiential learning and collaborative learning techniques.

[4] This is the case since the four pedagogical requirements at the critical level are meta-requirements, i.e., high-level requirements for IS security training approaches.

3.4.2. The Experiential and Collaborative IS Security Training Approach

The learning approach involves four prescriptive guidelines based on Kolb's four-stage cycle (1984): (1) Involve Learners' Concrete Experiences, (2) Engage Reflective Observation, (3) Support Formation of Abstract Concepts and Generalizations, and (4) Enable Active Experimentation. These phases of the experiential learning cycle in the case of IS security training are summarized in Figure 3.



Phase 1: Involve Concrete experiences

Individual's former experiences with respect to the existentialistic features of IS security training — security-sensitive organizational assets, threats towards them, and protection mechanisms.

Phase 2: Engage reflective observation

Learners work in small groups to generate interpersonal experiences regarding existentialistic features of IS security training, in order to define their meanings and implications for the organization.

Phase 3: Support Formation of Abstract Concepts and Generalizations

Learners analyze the similarities and differences between group experiences and the presented organizational viewpoint

Phase 4: Enable active experimentation

Concrete instructions are established by combining individual (first phase), interpersonal (second phase), and organizational (third phase) viewpoints with respect to the existentialistic features of IS security training. Employees need to consciously observe their new working practices, and must execute applicable changes based on what has been learned in training.

Figure 3. Modification of Experiential Learning Cycle (Kolb, 1984; Gibson, 2001) in the Context of IS Security Training

Complemented by collaborative learning techniques (Barkley et al., 2005), Kolb's theory of experiential learning offers an instructional design approach analogous to collective cognition, which refers to the processing of information in groups (Gibson, 2001; Hinsz et al., 1997). Then, these four phases include certain processes to make changes in collective thinking and develop effective group decisions and actions. We argue that such a training approach stresses the experiences and collective activities of learners in order to achieve communal change. The particulars of this approach resemble the features of the transformation orientation and of social constructivism (previously presented in this article). Thus, this training approach fulfills the first pedagogical requirement for IS security training: The explicit psychological context of IS security training must be based upon the group-oriented theoretical approach to teaching and learning. Next, we describe each experiential learning phase in order to demonstrate how the experiential and collaborative IS security training approach meets the other three pedagogical requirements for IS security training.

(1) Involve Learners' Concrete Experiences

The learning cycle begins with concrete experiences (Kolb, 1984; Gibson, 2001) that form the basis for learning (see Figure 3). In IS security training, the concrete experiences at the initial phase of learning are previous experiences learners have had (see Fenwick, 2001; Dixon, 1999) with the existentialistic features of IS security training—security-sensitive organizational assets, threats toward them, and protection mechanisms. To illustrate this, let us assume that an organization finds insecure e-mail use by employees to be a problem. In this case, the employees' concrete experience with security-sensitive organizational assets (e.g., confidential documents), threats toward them (e.g., e-mail eavesdropping), and protection mechanisms (e.g., e-mail encryption) related to secure e-mail use will constitute the starting point for IS security training.

(2) Engage in Reflective Observation

The second phase, reflective observation (see Figure 3), occurs via retrieving, exchanging, and structuring groups' shared experiences (Kolb, 1984; Gibson, 2001). Then, employees can engage in discussions about their concrete experiences, which enable them to react to others' perspectives and practices (Honey & Mumford, 1992) and to map a causal relationship between their work practices and respective organizational consequences (Pavlica et al., 1998). In collaborative activities, learners generate rich descriptions and analyses through systematic and intentional conversations with others, which take into account learners' personal and interpersonal perspectives, former knowledge, and attitudes (Pavlica et al., 1998).

In practice, in the context of IS security training, learners work in small groups to generate interpersonal experiences regarding the existentialistic features of IS security training, in order to define the experiences' meanings and implications for the organization. For instance, if the topic of the training is to make employees' e-mail use more secure, their task is to consider what types of security-sensitive e-mail require protection, what protection mechanisms enable secure e-mail use, in general, which of these practices are valid in their own work, and what threats exist if these protection mechanisms are not followed. Thus, while this phase implements collective experiences as training content, the phase also involves groups' interpersonal perspectives toward the existentialistic features of IS security training. Hence, this phase meets the second pedagogical requirement.

Reflective observation of these collective experiences can be accomplished, for example, through the collaborative learning technique called Think-Pair-Share (Barkley et al., 2005), which is implemented as follows. First, learners think of existentialistic features with respect to secure e-mail use individually, and then share their ideas with a colleague to create a joint response. Next, pairs share their ideas in a group of four to expand common viewpoints (Lyman, 1981). Finally, the results are visually presented to the whole group by amalgamating them on the blackboard, a method that supports learners' understanding of different aspects and enhances their ability to build group consensus on the secure use of e-mail. Hence, teaching methods are focused on collaborative learning in the form of group discussions (i.e., Think-Pair-Share) in order to reveal and produce collective knowledge. Hence, this phase meets the third pedagogical requirement for IS security training: that teaching methods must focus on collaborative learning in order to reveal and produce collective knowledge.

(3) Support Formation of Abstract Concepts and Generalizations

The third phase, the formation of abstract concepts and generalizations (see Figure 3), involves negotiation, interpretation, and evaluation processes (Kolb, 1984; Gibson, 2001). In this phase, the meanings of collective experiences are interpreted in the organizational context by comparing them to organizational viewpoints (Honey and Mumford, 1992), as stated in the organization's written security policies. The instructor needs to introduce the organization's e-mail policies, related security-sensitive organizational assets, threats toward them, and protection mechanisms. Building on the aforementioned exercises in the previous phase (e.g., Think-Pair-Share), the learners analyze the similarities and differences between the group's experiences and the presented organizational viewpoint. This phase is an examination of the overlap between organizational regulations and employees' communal experiences. Some variations are possible in cases where existing policies and instructions do not reconcile with actual work practices.

Similar to the previous phase, this phase involves collective experiences as training content, thereby fulfilling the second pedagogical requirement: that the training content must be based on the learners' collective experiences. This phase also involves collaborative learning in the form of group discussion in order to reveal and produce collective knowledge; hence, this phase fulfills the third pedagogical requirement: that teaching methods must focus on collaborative learning in order to reveal and produce collective knowledge. However, compared to the previous phase, collective experiences are now expanded from the group to the organizational level, involving reflection of the organization's formal e-mail policies.

(4) Enable Active Experimentation

The last phase, active experimentation (see Figure 3), refers to integrating collective experiences in order to reach decisions and actions (Kolb, 1984; Gibson, 2001). In this phase, employees' experiences (which were previously described and analyzed) are now used to develop new organizational practices (Pavlica et al., 1998). To put this into the context of IS security training, and to take the secure use of e-mail as an example, concrete e-mail use instructions are established in a manner that solves the original problem—insecure e-mail use by employees—by combining individual (first phase), interpersonal (second phase), and organizational (third phase) viewpoints with respect to the existentialistic features of secure e-mail use.

The ultimate purpose of the fourth phase is to define how formal e-mail policies and instructions are actually experienced by employees, and how the policies can be applied by the learners. For example, the instructor can deliver written policies to learners with open spaces for learners' possible supplements and/or corrections. This document can also function as a “learning contract” that supports the transfer of employees' learned knowledge and attitudes (for example, to secure e-mail practices) (Kirkpatrick, 2006; Knowles, 1986).

As part of the last phase to ensure effective collective learning, learners need to be able to test their new understanding in practice (Backström, 2004). In addition to describing, analyzing, and creating organizational practices, learners are required to implement changes in their work (Pavlica et al., 1998). To validate a new practice in an organization, potential changes in the policies and instruction must be accepted by management. Employees need to consciously observe their e-mail use practices, and must execute applicable changes based on what they have learned in training. Finally, these new experiences are evaluated through group interviews, which are then used to evaluate the effectiveness of the training from the learners' perspective. If required, these new experiences can function as a starting point for a second learning cycle (Dixon, 1999).

A function of this phase is to put together the collective experiences of the learners regarding existentialistic features in the area of secure use of e-mail, which formed the content of the training in the presented example. A learning contract as a concrete form of this collective knowledge can again be created through collaborative learning techniques (e.g., Think-Pair-Share). This fourth phase of the experiential learning cycle also meets the second and third requirements for IS security training. At the same time, after employees have changed and observed their IS security practices related to the topic of the training (for example, e-mail use), learning is evaluated using the group interview. Then, the fourth pedagogical requirement for IS security training is also fulfilled: that evaluation of learning should emphasize experiential and communication-based methods from the viewpoint of the learning community. Table 4 illustrates the four phases of the experiential learning cycle in the context of IS security training.

Table 4. Phases of Experiential Learning Cycle (Kolb 1984; Gibson 2001) in the Context of IS Security Training

Phase	Description of the phase	Example in IS security training on the use of strong passwords
Phase 1: Concrete experiences	Employees' individual experiences regarding the following features in their work form the basis of learning: 1. Sensitive information (e.g., personnel data, business and strategic decisions, financial, customer, and R&D information); 2. IS security threats (e.g., loss of sensitive information due to unintentional information leak, IS security breach, virus infections); 3. Means to protect sensitive information from IS security threats (e.g., selecting strong passwords, encrypting e-mails, making regular backups)	Employees' experiences on secure passwords, which will be changed during the training, form the basis of learning: 1. What security-sensitive information in the employees' work environment requires password protection? 2. Which protection mechanisms constitute secure password use, and which of these practices are valid in employees' own work (and why)? 3. What threats exist if these protection mechanisms are not followed? For example, an HR secretary may think that only personnel information (1) needs to be secured with passwords to prevent other employees from seeing it (3), but does not recognize other areas of sensitive information or IS security threats in his work. In addition, he may not recognize why passwords need to be changed frequently or why selecting strong passwords is important (2).
Phase 2: Reflective observation	Learners work in small groups to share their experiences regarding secure working practices (see Phase 1). To be more precise, they describe and analyze employees' collective experiences with sensitive information, IS security threats, and ways to protect sensitive information from threats (see phase 1) in their work through a certain systematic discussion procedure called Think-Pair-Share.	1. Learners think about secure password practices individually (see phase 1). 2. They share their ideas with colleagues. 3. Pairs share their ideas in a group of four to expand common viewpoints. 4. These viewpoints are discussed and visually presented to all learners, e.g., via the blackboard. For example, through discussing their password experiences with a co-worker, a HR secretary may realize that he also has customer-related data in his laptop requiring password protection (2). In addition, in the group of four, he realizes that to prevent information theft, it might also be necessary to use password protection for confidential e-mails (3). Finally, because almost all groups stated that it is important not to share passwords with other people, the HR assistant becomes more convinced to follow this practice (4).
Phase 3: Formation of abstract concepts and generations	Through the systematic discussion method, learners analyze the possible differences between a group's collective experiences (formulated in phase 2) and the organization's written IS security policies, which provide guidelines for using different ways to protect sensitive information from IS security threats.	First, the instructor introduces the company's password procedures and justifies the protection of security-sensitive organizational assets from threats. Second, learners analyze the similarities and differences between group experiences and the password procedures through a discussion method described in a phase 2. For example, in contrast with the organization's IS procedures, an HR assistant did not find it necessary to use strong passwords, which was required by the company's IS security policies. After an illustration of the importance of using strong passwords, the employee becomes aware why he should use stronger passwords, and why they should be changed frequently.

Table 4. Phases of Experiential Learning Cycle (Kolb 1984; Gibson 2001) in the Context of IS Security Training (continued)

Phase	Description of the phase	Example in IS security training on the use of strong passwords
Phase 4: Active experimentation	Learners establish new procedures to protect sensitive information from IS security threats, use them in practice, and evaluate their practical suitability through group interviews.	First, the instructor delivers password use procedures to learners with open spaces for feedback. Original procedures supplemented with employees' comments function as a concrete form of employees' collective knowledge, and can again be created through a discussion method (e.g., Think-Pair-Share). All IS security policies need to be discussed, and their use should be supported so that employees will apply them. For example, as a result of the discussion, it is found that, although employees understand the rationale behind most password procedures, and are willing to comply with them, they think that it is inconvenient to remember multiple passwords and select strong passwords that need to be changed frequently. For that reason, easy selection of strong passwords should be supported, for example, through teaching password mnemonics. After training, employees need to observe their password use and execute changes based on what has been decided in the training. These new user experiences are evaluated through group interviews, and if required, these can form a starting point for a second learning cycle.

4. Discussion

This paper advanced a meta-theory for designing IS security training with three levels of thinking: meta-level, critical level, and intuitive level. Through this theory, we would like to highlight two findings. First, at the meta-level, this theory advances fundamental features of IS security training (its non-cognitive and persuasive nature, and existentialistic features) and formulates respective meta-level requirements. None of the existing studies in the area of IS security training has considered these features.

Second, at the critical-thinking level, based on these meta-level requirements and learning theories, we formulated four pedagogical requirements for effective IS security training. None of the existing IS security training approaches meets all four pedagogical requirements. Thus, as the second contribution, we advanced an example of IS security training, the experiential and collaborative IS security training approach, that meets these requirements and provides guidelines that can be overridden for IS security training at the intuitive level.

Based on these findings, we suggest three directions for future research.

4.1. Research Direction 1: Research Methodologies to Validate IS Security Training Approaches

Given the lack of empirical research on IS security training programs (Puhakainen & Siponen, 2010), we call for four levels of evaluations (Kirkpatrick, 2006) to validate IS security training approaches (these are also used to empirically study research directions 2 and 3): 1) user reactions; 2) learning (changes in attitudes, knowledge, thinking, or skills); 3) behavior (e.g., how learning is implemented in the organization); and 4) results (e.g., decreased frequency of accidents and improved productivity). To study users' reactions, learning, and behavior, training programs can use interviews, observations, and surveys. In addition, to study behavior, these programs can employ objective measures. For example, users' objective Internet use behavior can be studied from log files before and after training on the non-work-related use of the Internet. The objective measures, if available, can be used to study the results, as well. For example, the number of malware infections can be analyzed in the long term before and after IS security training on protection against malware. To study changes in thinking, we suggest the use of integrative complexity (Suedfeld, Tetlock, & Streufert, 1992). Integrative complexity assumes that the level of thought complexity can be changed by discussion or training (Myyry, 2002; Suedfeld et al., 1992). Thus, as a result of IS security training, learners are expected to analyze and solve information security-related problems in their work using more diverse perspectives.

Evaluation of the impact of IS security training at levels 2-4 (Kirkpatrick, 2006) requires a pre- and post-research design, with control and experimental groups. We also call for a post-then-pre research design with a control group. In the post-then-pre research design, in addition to pre- and post-measurements being taken, participants would be asked immediately after training how they judged their earlier behavior. The post-then-pre research design should correct participants' previously incorrect views because, after training, participants are expected to better understand the training issues (Robinson & Robinson, 1989; Mezoff, 1981).

4.2. Research Direction 2: Development of Critical-Level Principles

The meta-theory we presented in this paper explains why only a few of the 32 IS security training approaches developed so far are based on pedagogical theories and offer empirical evidence of practical usefulness (Puhakainen & Siponen, 2010). We explain this through three levels of thinking. It is normal for practitioners dealing with a phenomenon—here IS security training—to have their own beliefs, based on practical experiences and education. These beliefs reside at the intuitive level. When people realize that these beliefs may not be valid (in some situations) or are not optimal, their thinking matures beyond those thoughts toward the critical level where (Hare, 1981). While method engineering (Brinkkember, 1996; Kumar & Welke, 1992) and the contingency view in management science (Weill & Olson, 1989) have long recognized that there cannot be a universal "fit-one-fit all" principle, IS security training literature has not embraced this idea. Hence, scholars need to develop critical-level principles for selecting intuitive-level principles. There are three reasons why critical thinking is needed (Hare, 1981). First, we need to know the validity of our intuitive-level principles. Second, we need to know when general intuitive principles conflict in particular cases. Third, we need critical thinking to select the intuitive principles that we will use in a given IS security training scenario.

Hence, the aim of research direction 2 is the development of critical-level principles. These principles can be inferred by studying the validity of IS security training practices (at the intuitive level), within organizations, through the research setting described in research direction 1. When developing and testing such principles, paying attention to the context and the conditions under which the principles may be valid is important.

Another research issue is how to make a selection when the intuitive principles conflict in particular cases. Given that the aim of the critical level is to develop principles to solve situations where intuitive-level principles are in conflict, such critical-level principles should be developed. An authentic example of such a conflict is when there is a recognized need to implement IS security training, but strict deadlines for finalizing software products prevent the training (Puhakainen & Siponen, 2010). To address this issue, we also call for research on self-learning (e.g., through a web-based system), which employees can undertake at any time. Self-learning should be theory-based, and follow the research setting described in research direction 1. For example, research could compare the effectiveness (to which extent employees comply with IS security policies) and cost of the collaborative face-to-face approach based on transformation orientation versus social constructivism and the e-learning IS security training approach based on transmission-orientation and behaviorism.

4.3. Research Direction 3: Development of Evidence-Based Intuitive Level IS Security Training Principles

Future research should develop intuitive-thinking-level IS security training approaches that meet the four pedagogical requirements based on meta-level requirements and the social constructivist learning paradigm. This study suggested that the experiential learning approach could be used to satisfy the four critical-level requirements. In addition, IS security training approaches with different constructivist instructional design approaches should be developed and tested for different training topics and contexts. Implementing the four pedagogical requirements for IS security training should improve learners' understanding of security-sensitive organizational assets, impending threats, and protection mechanisms (cf., the existentialistic feature of IS security training). Against this backdrop, research should be conducted on how IS security training practices can be developed based on the existentialistic features. For example, regarding existentialistic features (the existence of security-sensitive organizational assets, threats toward them, and protection mechanisms), scholars could develop different exercises that attempt to increase employees' understanding of the assets they encounter in their daily work, threats toward these assets, and a mechanism to protect the assets. The effect of these techniques should be studied using the research setting described in research direction 1.

5. Conclusions

Employee non-compliance with IS security policies is considered one of the biggest threats to IS security. To solve this problem, researchers have introduced several training approaches in the IS security literature. Despite the recognized importance of having effective training, IS security training is largely a theoretically underdeveloped area. To fill this gap in research, we develop a new meta-theory to design IS security training approaches, based on Hare's theory of three levels of thinking. This meta-theory suggests that IS security training differs from other types of training and needs to be understood before pedagogical principles for IS security training can be selected. In addition, our meta-theory proposes four pedagogical requirements that must be satisfied by any IS security training approach. We review the existing IS security training approaches in light of these four requirements and find that no previous IS security training approach meets all these requirements. Finally, we demonstrate how an IS security training approach can meet these requirements.

The key contribution of the study is the introduction of the new meta-theory for IS security training, including four pedagogical requirements for designing IS security training approaches. Finally, we advance a research agenda based on the meta-theory for IS security training.

References

Adams, A., & Sasse, M. A. (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.

Argyris, C., & Schön, D. (1978). Organizational learning: A theory of action perspective. Reading, MA Addison Wesley.

Backström, T. (2004). Collective Learning. A Way over the Ridge to a New Organizational Attractor. *The Learning Organization, 11(6)*, 466 – 477.

Barkley, E.F., Cross, K.P., & Major, C.H. (2005). Collaborative Learning Techniques. A Handbook for College Faculty. San Francisco (CA): Jossey-Bass.

Birenbaum, M. (1996). Assessment 2000: Towards a pluralistic approach to assessment. In M. Birenbaum, & F. J. R. C. Dochy (Eds.), *Alternatives in assessment of achievements, learning processes and prior knowledge* (pp. 3 - 29). Boston/Dordrecht/London: Kluwer Academic Publishers.

Biros, D. P. (2004). Scenario-based training for deception detection. InfoSecCD '04. Proceedings of the 1 st annual conference on information security curriculum development, 32 – 36.

Bishop, M. (2000). Education in information security. IEEE Concurrency, 8(4).

Bloom, B. S. (1956). Taxonomy of educational objectives: Handbook 1: Cognitive domain. New York: David McKay Co. Inc.

Bray, T. J. (2002). Security actions during reduction in workforce efforts: What to do when downsizing information systems security. Informa*tion System security, 11(1),* 11 – 15.

Brinkkemper, S. (1996). Method engineering: Engineering of information systems development methods and tools. *Information and Software Technology, 38(4)*, 275-280.

Brody, C. M. (1998). The significance of teacher beliefs for professional development and cooperative learning. In C.M. Brody (Ed.), *Professional development for cooperative learning: Issues and approaches* (pp. 25 – 48). Albany: State University of New York Press.

Cheung, D., & Wong, H. (2002). Measuring teacher beliefs about alternative curriculum designs. *The Curriculum Journal, 13(2)*, 225 – 248.

Cone, B., Irvine, C., Thompson, M. F., & Nguyen, T. D. (2007). A video game for cyber security training and awareness. *Computers and Security, 26(1)*, 63 – 72.

Cox, A., Connolly, S., & Currall, J. (2001). Raising IS security awareness in the academic setting. VINE, 123(1), 11 – 16.

CSI Survey (2007). The 12th annual computer crime and security survey. Retrieved from: http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf. 3.2.2010

Derry, S. J., & DuRussel, L. A. (2000). Assessing knowledge construction in on-line learning communities. Retrieved from: http://www.eric.ed.gov/ERICDocs/data/ericdocs2sql/content_storage_01/0000019b/80/16/9c/cb.pdf. 88. 3.2.2011

Desman, M. B. (2002). Building an information security awareness program. Boca Raton, London, New York, Washington, D.C.: Auerbach Publications.

Dhillon, G. (2007). Principles of information systems security: Text and cases. New York: John Wiley and Sons.

Dillenbourg, R, Baker, M., Blaye, A., & O'Malley, C. (1996). The evolution of research on collaborative learning. In H. Spada, & P. Reimann (Eds.), *Learning in humans and machines. Towards an interdisciplinary learning science* (pp. 189 – 211). Oxford: Pergamon.

Dixon, N. M. (1999). The organizational learning cycle: How we can learn collectively? Second edition. Aldershot, England: Gower Publishing Limited.

Dodge Jr., R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. *Computers & Security, 26(1)*, 73 – 80.

Douglas, M., & Wildavsky, A. (1982). Risk and culture. An essay on the selection of technological and environmental dangers. Berkeley: University of California Press.

Fardanesh, H. (2006). A classification of constructivist instructional design models based on learning and teaching approaches. Retrieved from: http://www.eric.ed.gov/ERICWebPortal/custom/portlets/recordDetails/detailmini.jsp?_nfpb=t rueand_andERICExtSearch_SearchValue_0=ED491713andERICExtSearch_SearchType_0=noandaccno=ED491713. 3.2.2011

Fenwick, T. J. (2001). Experiential learning: A theoretical critique from five perspectives. Information Series No. 385. Retrieved from ERIC database (ED454418) Clearinghouse on Adult, Career, and Vocational Education. Center on Education and Training for Employment College of Education.

Forget, A., Chiasson, S, & Biddle, R. (2007). Persuasion as education for computer security. In T. Bastiaens, & S. Carliner (Eds.), Proceedings of World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education 2007 (pp. 822-829). Chesapeake, VA: AACE.

Furnell, S. M., Gennatou, M., & Dowland, P. S. (2002). A prototype tool for IS security awareness and training. *International Journal of Logistics Information Management, 15(5/6),* 352 – 357.

Furnell, S., Sanders, P. W., & Warren, M. J. (1997). Addressing information security training and awareness within the European healthcare community. Proceedings of Medical Informatics Europe '97. In Pappas, C., Maglaveras, N. and Scherrer, J.R. (Eds) Medical Informatics Europe '97. Amsterdam: IOS Press, 707 – 711.

Gagnon, G. W., & Collay, M. (2006). Constructivist learning design: Key questions for teaching to standards. Thousand Oaks (CA): Corwin Press.

Gaunt, N. (1998). Installing an appropriate information security policy. *International Journal of Medical Informatics, 49(1)*, 131 – 134.

Gibson, C. B. (2001). From knowledge accumulation to accommodation: Cycles of collective cognition in work groups. *Journal of Organizational Behavior, 22(2)*, 121 – 134.

Goel, S., & Pon, D. (2006). Innovative model for information assurance curriculum: A teaching hospital. *Journal on Educational Resources in Computing, 6(3),* 1 – 15.

Gregor, S. (2006). The nature of theory in information systems. *MIS Quarterly, 30(3)*, 611– 642.

Greitzer, F. L., Kucher, O. A., & Huston, K. (2007). Cognitive science implications for enhancing training effectiveness in a serious gaming context. *Journal of Educational Resources in Computing, 7(3)*, 1 – 16.

Hansche, S. (2001). Information system security training: Making it happen, Part 2. *Information Systems Security, 10(3)*, 51 – 70.

Hare, R. M. (1952). Language of morals. Oxford: Clarendon Press.

Hare, R. M. (1963). Freedom and reason. Oxford: Clarendon Press.

Hare, R. M. (1981). Moral thinking: Its levels, method, and point. Oxford: Clarendon Press.

Hayes, J. (2010). The theory and practice of change management. Third Edition. New York: Palgrave Macmillan.

Heikka, J. (2008). A constructive approach to information systems security training: An action research experience. Proceedings of the 14th Americas Conference on Information Systems (AMCIS), Toronto, Canada, August 14-17, 1 – 8.

Helleringer, S., & Kohler, H-P. (2005). Social networks, perceptions of risk, and changing attitudes towards HIV/AIDS: New evidence from a longitudinal study using fixed-effects analysis. *Population Studies, 59(3)*, 265 – 282.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106 – 125.

Herold, R. (2005). Managing an information security and privacy awareness and training program.Boston, MA: Auerbach Publications.

Hinsz, V. B., Vollrath, D. A., & Tindale, R. S. (1997). The emerging conceptualization of groups as information processors. *Psychological Bulletin, 121(1),* 43 – 64.

Hmelo-Silver, C. E, & Barrows, H. S. (2008). Facilitating collaborative knowledge building. *Cognition and Instruction, 26(1),* 48 – 94.

Holman, D., Pavlica, K., & Thorpe, R. (1997). Rethinking Kolb's theory of experiential learning in management education. *Management Learning, 28(2*), 135 – 148.

Honey, P., & Mumford, A. (1992). Manual of learning styles. 3rd edition. Maidenhead (UK): Peter Honey.

Hung, D. (2001). Theories of learning and computer-mediated instructional technologies. *Educational Media International, 38(4),* 281 – 287.

Information Security Forum (2005). The standard of good practice for information security. Version 4.1. Retrieved from: https://www.isfsecuritystandard.com/SOGP07/index.htm. 3.2.2011.

Johnson, D. W., Maruyama, G., Johnson, R., Nelson, D., & Skon, L. (1981). Effects of cooperative, competitive, and individualistic goal structure on achievement: A meta-analysis. *Psychological Bulletin, 89(1),* 47 – 62.

Kabay, M.E. (2002). Using social psychology to implement security policies. In S. Bosworth, & M.E. Kabay (Eds.) *Computer Security Handbook*, 4th edition. New York, NY, USA: John Wiley and Sons, Inc., 35.1 – 32.18

Kajava, J., & Siponen, M. T. (1997). Effectively implemented information security awareness - An example from university environment. Proceedings of IFIP-TC 11 (Sec'97/WG 11.1), 13th International Conference on IS Security: IS security Management - The Future, 105 – 114.

Kajava, J., Varonen, R., Tuormaa, E. J., & Nykänen, M. (2003). Information security training through e-learning – A small-scale perspective. Security e-Learning: Why, where and how. European Intensive Programme on Information and Communication Technologies Security, 28 – 39.

Kirkpatrick, D. L. (2006). Evaluating training programs: The four levels. 3rd edition. San Francisco (CA): Berrett-Koehler.

Kirschner, P. A., Sweller, J., & Clark, R. E. (2006). Why minimal guidance during instruction does not work: An analysis of the failure of constructivist, discovery, problem-based, experiential, and inquiry-based teaching. *Educational Psychologist, 41(2)*, 75 – 86.

Knowles, M. S. (1986). Using learning contracts. San Francisco: Jossey-Bass.

Kolb, D. A. (1984). Experiential learning. Experience as a source of learning and development. Englewood Cliffs (NJ): Prentice Hall.

Kovacich, G. L., & Halibozek, E. P. (2003). The manager's handbook for corporate security: Establishing and managing a successful assets protection program. USA: Butterworth-Heinemann.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers and Security, 25(4),* 289 – 296.

Kumar, K., & Welke, R. J. (1992). Methodology engineering: A proposal for situation-specific methodology construction. In W.W. Cotterman, & J.A. Senn (Eds.), *Challenges and Strategies for Research in Systems Development* (pp. 257 – 259). New York, NY: John Wiley.

Leach, J. (2003). Improving user security behaviour. *Computers & Security, 22(8)*, 685 – 692.

Lines, R. (2004). Influence of participation in strategic change: Resistance, organizational commitment and change goal achievement. *Journal of Change Management, 4(3),* 193 – 215.

Lyman, F. T. (1981). The responsive classroom discussion. In Anderson, A.S. (Ed.) Mainstreaming Digest, College Park, MD: University of Maryland College of Education.

Markey, E. (1989). Getting organizations involved in computer security: The role of security awareness. In W.J. Caelli (Ed.), *Computer security in the age of information* (pp. 83 – 85). Proceedings of the Fifth IFIP International Conference. North-Holland: Elsevier Science Publishers.

Martins, A., & Eloff, J. H. P. (2001). Measuring information security. Rand Afrikaans University, Department of Computer Science, 1 – 14. Retrieved from: http://academy.delmar.edu/Courses/ITSY2400/eBooks/InformationSecurity(Measuring).pdf. 10.3.2009.

Maslow, A. (1970). Motivation and personality. Third Edition. New York: Harper and Row.

McCoy, C., & Thurmond Fowler, R. (2004). You are the key to security: Establishing a successful security awareness program. Proceedings of the 32nd Annual ACM SIGUCCS Conference on User Services, 346 – 349.

McIlwraith, A. (2006). Information security and employee behaviour. How to reduce risk through employee education, training and awareness. Hampshire, England: Gower Publishing Limited.

McLean, K. (1992). Information security awareness – Selling the cause. Proceedings of the IFIP TC11, Eighth International Conference on Information Security: IT Security: The Need for International Cooperation, 179 – 193.

McLeod, G. (2003). Learning theory and instructional design. Learning Matters 2, 35 – 43. Retrieved from: http://courses.durhamtech.edu/tlc/www/html/Resources/learningmatters/learningtheory.pdf. 3.2.2011

McNeil, J. D. (1981). Curriculum. A comprehensive introduction. 2nd edition. Boston: Little, Brown and Company.

Mezirow, J. (1991). Transformative dimensions of adult learning. San Francisco: Jossey-Bass.

Mezoff, B. (1981). How to get accurate self-reports of training outcomes. *Training and Development Journal, 35(9)*, 56 – 61.

Miller, J. (2007). The holistic curriculum. 2nd edition. Toronto: OISE Press.

Miller, J. P., & Seller, W. (1985). Curriculum perspectives and practice. White Plains, NY: Longman Inc.

Mitnick, K. D., & Simon, W. L. (2002). The art of deception: Controlling the human element of security. New York, NY: John Wiley & Sons, Inc.

Murray, B. (1991). Running corporate and national security awareness programmes. Proceedings of the IFIP TC11 Seventh International Conference on IS Security, 203 – 207.

Myyry, L. (2002). Everyday value conflicts and integrative complexity of thought. *Scandinavian Journal of Psychology, 43(5),* 385 – 395.

Nadler, D. (1993). Concepts for the management of organizational change. In C. Mabey, & B. Mayon-White (Eds), *Managing change* (pp. 85 – 98). Second Edition. London: Paul Chapman.

National Institute of Standards and Technology (NIST) (1995). Technology Administration, U.S. Department of Commerce, An introduction to computer security: The NIST Handbook, NIST Special Publication 800-12. Retrieved from: http://all.net/books/standards/NIST-CSRC/csrc.nist.gov/publications/nistpubs/index.html. 10.3.2009.

Niiniluoto, I. (1993). The aim and structure of applied research. *Erkenntnis, 38 (1)*, 1 – 21.

Niiniluoto, I. (1999). Critical scientific realism. Oxford: Oxford University Press.

Nosworthy, J. D. (2000). Implementing information security in the 21st Century – Do you have the balancing factors? *Computers and Security, 19(4)*, 337 – 347.

Ølnes, J. (1994). Development of security policies. Computers and Security, 13(9), 628 – 636.

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).

Palincsar, A. S. (1998). Social constructivist perspectives on teaching and learning. *Annual Review of Psychology, 49,* 345 – 375.

Parker, D. B. (1999). Security motivation, the mother of all controls, must precede awareness. *Computer Security Journal, 15(4)*, 15 – 23.

Pavlica, K., Holman, D., & Thorpe, R. (1998). The manager as a practical author of learning. *Career Development International 3(7)*, 300 – 307.

Peltier, T. (2000). How to build a comprehensive security awareness program. *Computer Security Journal,* 16(2), 23 – 32.

Puhakainen, P. (2006). A design theory for information security awareness (Ph.D. Thesis, University of Oulu, Finland). Retrieved from: http://herkules.oulu.fi/isbn9514281144/isbn9514281144.pdf. 2.8.2011.

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

Robbins, S. P. (1993). Organizational behavior. Concepts, controversies, and applications. 6th edition. Englewood Cliffs (N. J.): Prentice Hall.

Robinson, D. G., & Robinson J. C. (1989). Training for impact: How to link training to business needs and measure the results. San Francisco: Jossey-Bass.

Rogers, C. R. (1969). Freedom to learn. Columbus (OH): Charles Merrill Publishing Company.

Romney, G. W., Higby, C., Stevenson, B. R., & Blackham, N. (2004). A teaching prototype for educating IT security engineers in emerging environments. Proceedings of the Fifth International Conference on Information Technology Based Higher Education and Training, 662 – 667.

Roper, C. A., Grau, J. A., & Fischer, L. F. (2006). Security education, awareness and training. From theory to practice. Burlington, MA: Elsevier Butterworth-Heinemann.

Roschelle, J., & Teacley, S. D. (1995). The construction of shared knowledge in collaborative problem solving. In C.E. O´Malley (Ed.), Computer-supported collaborative learning (pp. 69 – 97). Berlin, Germany: Springer Verlag.

Ross, O. T. (2002). Self-directed learning in adulthood: A literature review. Retrieved from: http://www.eric.ed.gov:80/PDFS/ED461050.pdf. 3.2.2011

Rudolph, K., Warshawsky, G., & Numkin, L. (2002). Security awareness. In S. Bosworth, & M.E. Kabay (Eds.), *Computer security handbook*, 4th edition (pp. 29.1. – 29.19). USA: John Wiley and Sons.

Ryan, J. J. C. H. (2003). Teaching information security to engineering managers. Proceedings of 33 rd ASEE/IEEE Frontiers in Education Conference, 1 – 6.

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

Sharma, S. K., & Sefchek, J. (2007). Teaching information systems security courses: A hands-on approach. *Computers & Security, 26(4)*, 290 – 299.

Shawn, R. S., Chen, C. C., Harris, A. L., & Huang, H. (2009). The impact of information richness on information security awareness training effectiveness. *Computers and Education, 52(1),* 92 – 100.

Siponen, M. T. (2000). A Conceptual foundation for organizational information security awareness. *Information Management and Computer Security, 8(1)*, 31 – 41.

Siponen, M., Baskerville, R., & Heikka, J. (2006). A design theory for secure information systems design methods. *Journal of the Association for Information Systems, 7(11)*, 725-770.

Siponen, M. T., Pahnila, S., & Mahmood, A. (2007). Employees' adherence to information security policies: An empirical study. Proceedings of the IFIP SEC2007, 14-16 May 2007, Sandton, Gauteng, South Africa.

Siponen, M., & Vance, A. (2010). Neutralization: New insight into the problem of employee information systems security policy violations. *MisQuarterly, 34(3),* 487 – 502.

Skinner, B. F. (1968). The technology of teaching. East Norwalk, CT: Appleton-Century-Crofts.

Springer, L., Stanne, M. E., & Donovan, S. (1999). Effects of small-group learning on undergraduates in science, mathematics, engineering, and technology: A meta-analysis. *Review of Educational Research, 69(1),* 21-51.

Spurling, P. (1995). Promoting security awareness and commitment. *Information Management & Computer Security, 3(2)*, 20 – 26.

Stacey, T. R. (1996). Information security program maturity grid. *Information System Security, 5(2),* 22 – 33.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviours. *Computers and Security, 24(2)*, 124 – 133.

Stevenson, C. (1944). Ethics and language. New Haven, CT: Yale University Press.

Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research 1(3),* 255-276.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22(4)*, 441 – 469.

Suedfeld, P., Tetlock, P., & Streufert, S. (1992). Conceptual/integrative complexity. In C.P. Smith, J.W. Atkinson, D.C. McClelland, & J. Veroff (Ed.), *Motivation and personality: Handbook of thematic content analysis* (pp. 393 – 400). Cambridge, England: Cambridge University Press.

Telders, E. (1991). Security awareness programs: A proactive approach. *Computer Security Journal, 7(2*), 57 – 64.

Tennant, M. (1997). Psychology and adult learning. Second Edition. London: Routledge.

Thomson, K. L., von Solms, R., & Louw, L. (2006). Cultivating an organisational information security culture. *Computer Fraud & Security, 2006(10*), 7 – 11.

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

Thorndike, E. L. (1911). Animal Intelligence. New York: Macmillan

Wright, G. H. von (1972). The varieties of goodness. London: Routledge & Kegan Paul.

Wasson, B. (1996). Instructional planning and contemporary theories of learning: Is this a self-contradiction? In P. Brna, A. Paiva, & J. Self (Eds.), Proceedings of the European Conference on Artificial Intelligence in Education (pp. 23 – 30). Lisbon: Colibri.

Weil, S., & McGill, I. (1989). Making sense of experiential learning. Diversity in theory and practice. Milton Keynes: Open University Press.

Weill, P., & Olson, M. H. (1989). An assessment of the contingency theory of management information systems, *Journal of Management Information Systems,6(1),* 59-85.

Wilson, M., de Zafra, D. E., Pitcher, S. I., Tressler, J. D., & Ippolito, J. B. (1998). Information technology security training requirements: A role- and performance-based model. NIST Special Publication 800-16. Retrieved from: http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf. 3.2.2011.

Wilson, M., & Hash, J. (2003). Building an information technology security awareness and training program. NIST Special Publication 800-50. Retrieved from: http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf. 3.2.2011

Yilmaz, K. (2008). Constructivism: Its theoretical underpinnings, variations, and implications for classroom instruction. *Educational Horizons, 86(3),* 161 – 172.

Appendix

With respect to meta-orientations of curriculum design, the results of a review of IS security training approaches are shown in Tables 5–8. In the tables, the term “inclusive” means that the IS security training approach named contains all the meta-orientations and corresponding learning paradigms. In turn, the term “exclusive” indicates that the approach contains only one kind of meta-orientation and a corresponding learning paradigm.

The first pedagogical requirement for future IS security training is that the learning theory behind the training approach, or the psychological context, must be based upon the group-oriented approach to teaching and learning (Fardanesh, 2006; Gibson, 2001; Hinsz et al., 1997). Only six of the 32 IS security approaches apply a learning theory at all; however, having a theoretical foundation is invaluable for effective training (e.g., McLeod, 2003). The six approaches that do apply theory consider learning only from the viewpoint of an individual learner: one approach comes exclusively from the transaction orientation (cognitivism), and five approaches derive from the transformation orientation (constructivism). Because none of the existing IS security training approaches is based on social constructivist learning theory, they are not effective or pedagogically meaningful educational practices in this sense (see Table 5).

Table 5. The Psychological Context of Learning in the Existing IS Security Training Approaches

Psychological context of learning within the IS security approaches			
Missing (26) *Social psychology-oriented approach* (Thomson & von Solms 1998), *Motivation theory directive approach* (Roper *et al.* 2006), *Social psychological recommendations approach* (Kabay 2002), *Normative approach* (Siponen 2000), *Deterrence approach* (Straub & Welke 1998), *ISD approach* (Hansche 2001), *Counteractive approach* (McIlwraith 2006), *University environment approach* (McCoy & Thurnmond Fowler 2004), *Security ensuring approach* (Peltier 2000), Academic environment approach (Kajava & Siponen 1997), *Communication oriented approach* (Desman 2002), *Promotional approach* (Rudolph *et al.* 2002), *Preventive approach* (Nosworthy 2000), *Stakeholder approach* (Kovacich & Halibozek 2003), *Strategic approach* (Wilson & Hash 2003), *Competence approach* (Wilson *et al.* 1998), *Policy creation approach* (Gaunt 1998), *Healthcare environment approach* (Furnell *et al.* 1997), *Social engineering preventive approach* (Mitnick & Simon 2002), *Discursive approach and online tutorial approach* (Cox et *al.* 2001), *Briefing approach* (Markey 1989), *Operational controls approach* (NIST 1996), *Active e-learning approach* (Furnel *et al.* 2002), *Traditional e-learning approach* (Kajava *et al.* 2003), *Persuasive technology approach* (Forget *et al.* 2007), *Hypermedia instruction approach* (Shawn et *al*. 2009)			
Transmission	**Transaction**	**Transformation**	
Behaviorism (0)	**Cognitivism (1)**	**Constructivism (5)**	**Social constructivism (0)**
Inclusive (0) -			
Exclusive (0) -	Exclusive (1) *Cognitive processing approach* (Puhakainen 2006)	Exclusive (5) *Constructive instruction approach* (Heikka 2008), *Constructive scenario approach* (Biros 2004), *Andragogical approach* (Herold 2005), *Cyber security game approach* (Cone *et al.* 2007) *Pedagogical game approach* (Greitzer *et al.* 2007)	Exclusive (0) -

The second pedagogical requirement for future IS security training is that the training content must be community-centered, i.e., based on learners' collective experiences and their perspectives (e.g., Kolb, 1984; Gibson, 2001). This is considered a feature of effective IS security training. Twenty-four of the 32 IS security training approaches include subject-centered content typical of behaviorism. In these approaches, the training content is presented without connections to learning processes, problem solving, or learners' experiences in the training situation. Further, 18 of the approaches include process- and/or problem-centered training content, which is typical of a transaction orientation and cognitivism, which emphasizes integration of new knowledge with existing knowledge structures or cognitive problem solving and analysis (e.g., Palincsar, 1998, 347). Process-centered content takes into account the cognitive processing of information (e.g., activation of learners' prior knowledge before a training session and engagement of analogies, case studies, or stories). Problem-centered content emphasizes cognitive problem-solving tasks (e.g., analysis and synthesis) as a part of training. Finally, 23 approaches include learner-centered content. In these approaches, the training content is partly created during a training session according to the learners' experiences and choices, which is typical of the transformation orientation and constructivism. Only two of these 23 approaches also include community-centered content typical of social constructivism, which stresses communal knowledge formulated during training: the communal relevance of the learning task (the cognitive processing approach of Puhakainen (2006)) and the existing corporate culture, expectations, and social schemata (the social psychological recommendation approach of Kabay (2002)). (See Table 6.)

Table 6. The Training Content in Existing IS Security Training Approaches

Training content within the IS security training approaches			
Transmission	**Transaction**	**Transformation**	
Behaviorism (24)	**Cognitivism (18)**	**Constructivism (23)**	**Social constructivism (2)**
Inclusive (12) *Social psychology oriented approach* (Thomson & von Solms 1998) *Motivation theory directive approach* (Roper *et al.* 2006) *Social psychological recommendations approach* (Kabay 2002) *Constructive scenario approach* (Biros 2004) *Andragogical approach* (Herold 2005) *ISD approach* (Hansche 2001) *Counteractive approach* (McIlwraith 2006) *Security ensuring approach* (Peltier 2000) *Competence approach* (Wilson *et al.* 1998) *Discursive approach and online tutorial approach* (Cox *et al.* 2001) *Social engineering preventive approach* (Mitnick & Simon 2002) *Traditional e-learning approach* (Kajava *et al.* 2003)			
Exclusive (7) *Deterrence approach* (Straub & Welke 1998) *Academic environment focused approach* (Kajava & Siponen 1997) *Stakeholder approach* (Kovacich & Halibozek 2003) *University environment approach* (McCoy & Thurmond Fowler 2004) *Preventive approach* (Nosworthy 2000) *Healthcare environment approach* (Furnell *et al.* 1997) *Briefing approach* (Markey 1989)	Exclusive (0)	Exclusive (4) *Normative approach* (Siponen 2000) *Policy creation approach* (Gaunt 1998) *Cyber security game approach* (Cone *et al.* 2007) *Active e-learning approach* (Furnell *et al.* 2002)	Exclusive (0)
Behaviorism + cognitivism (2) *Communication oriented approach* (Desman 2002) *Promotional approach* (Rudolph *et al.* 2002)			

Table 6. The Training Content in Existing IS Security Training Approaches (continued)

	Cognitivism + constructivism (4) *Cognitive processing approach* (Puhakainen 2006) *Pedagogical game approach* (Greitzer *et al.* 2007) *Persuasive technology approach* (Forget *et al*. 2007) *Hypermedia instruction approach* (Shawn *et al.* 2009)		
Behaviorism + constructivism (3) *Constructive instruction approach* (Heikka 2008) *Operational controls approach* (NIST 1996) *Strategic approach* (Wilson & Hash 2003)		Behaviorism + constructivism (3) *Constructive instruction approach* (Heikka 2008) *Operational controls approach* (NIST 1996) *Strategic approach* (Wilson & Hash 2003)	
			Social constructivism (2) *Cognitive processing approach* (Puhakainen 2006) *Social psychological recommendations approach* (Kabay 2002)

The third pedagogical requirement for future IS security training is that the teaching methods need to focus on critical reflection of collective knowledge and experiences through authentic problem solving or communication, i.e., they must include collaborative learning techniques in order to reveal and produce collective knowledge (e.g., Barkley et al., 2005). These techniques are preferred for effective IS security training. With respect to the teaching methods explored, 24 approaches represent the transmission orientation and behaviorism. These teaching/learning activities facilitate teachers in transmitting knowledge and learners in receiving knowledge or external reinforcement of their behavior. Nine of the 24 approaches employ transaction-oriented teaching methods. Teaching methods that represent the transaction orientation and cognitivism support the cognitive processing of information, implement activities of cognitive problem solving and analysis, or both. Finally, 23 approaches include teaching methods that represent the transformation orientation and constructivism. In these cases, the teaching methods emphasize the opportunities to reflect on one's own experiences, authentic problem solving, or both. Along with individual activities, 14 approaches representing transformative teaching methods also include solitary references to collaborative learning activities in the learning situation, such as role-playing exercises and scenario discussion (Thompson and von Solms, 1998; Roper et al., 2006; Heikka, 2008; Biros, 2004; Siponen, 2000; Herold, 2005; McIlwraith, 2006; Peltier, 2000; Wilson et al., 1998; Gaunt, 1998; Mitnick and Simon, 2002; Cox et al., 2001; Greitzer et al., 2007; Kajava et al., 2003). However, the purpose of the collaboration is to enhance individual learning, not to achieve socially constructed knowledge and emphasize the communal characteristic of learning. Therefore, teaching methods in these cases represent constructivism. Only two approaches also include collaborative teaching methods that emphasize the communal characteristic of learning. These two are Puhakainen's (2006) cognitive processing approach that seeks the communal relevance of a learning task through a team rehearsal and Kabay's (2002) social psychological recommendations approach that tries to reveal corporate culture and social views of reality through discourse. (See Table 7.)

Table 7. Teaching Methods in the Existing IS Security Training Approaches

Teaching method within the IS security training approaches			
Transmission	**Transaction**	**Transformation**	
Behaviorism (24)	**Cognitivism (9)**	**Constructivism (23)**	**Social constructivism (2)**
Inclusive (8) *Motivation theory directed approach* (Roper *et al.* 2006) *Andragogical approach* (Herold 2005) *Counteractive approach* (McIlwraith 2006) *ISD approach* (Hansche 2001) *Strategic approach* (Wilson & Hash 2003) *Operational controls approach* (NIST 1996) *Discursive approach and online tutorial approach* (Cox *et al.* 2001) *Competence approach* (Wilson *et al.* 1998)			
Exclusive (8) *Deterrence approach* (Straub & Welke 1998) *Communication oriented approach* (Desman 2002) *University environment approach* (McCoy & Thurmond Fowler 2004) *Preventive approach* (Nosworthy 2000) *Stakeholder approach* (Kovacich & Halibozek 2003) *Healthcare environment approach* (Furnell *et al.* 1997) *Briefing approach* (Markey 1989) *Promotional approach* (Rudolph *et al.* 2002)	Exclusive (0)	Exclusive (8) *Normative approach* (Siponen 2000) *Cognitive processing approach* (Puhakainen 2006) *Constructive instruction approach* (Heikka 2008) *Policy creation approach* (Gaunt 1998) *Cyber security game approach* (Cone *et al.* 2007) *Pedagogical game approach* (Greitzer *et al.* 2007) *Active learning approach* (Furnell *et al.* 2002) *Hypermedia instruction approach* (Shawn *et al.* 2009)	Exclusive (0)
Behaviorism + cognitivism (1) *Academic environment approach* (Kajava & Siponen 1997)			
Behaviorism + constructivism (7) *Social psychological recommendations approach* (Kabay 2002) *Constructive scenario approach* (Biros 2004) *Security ensuring approach* (Peltier 2000) *Social engineering preventive approach* (Mitnick & Simon 2002) *Persuasive technology approach* (Forget *et al.* 2007) *Social psychology oriented approach* (Thomson & von Solms 1998) *Traditional e-learning approach* (Kajava *et al.* 2003)		Behaviorism + constructivism (7) *Social psychological recommendations approach* (Kabay 2002) *Constructive scenario approach* (Biros 2004) *Security ensuring approach* (Peltier 2000) *Social engineering preventive approach* (Mitnick & Simon 2002) *Persuasive technology approach* (Forget *et al.* 2007) *Social psychology oriented approach* (Thomson & von Solms 1998) *Traditional e-learning approach* (Kajava *et al.* 2003)	
			Social constructivism (2) *Social psychological recommendations approach* (Kabay 2002) *Cognitive processing approach* (Puhakainen 2006)

The fourth pedagogical requirement for future IS security training is that informal, experimental, and open-ended forms of evaluation for groups need to be applied. This means that assessment of learning must emphasize experiential and communication-based methods from the viewpoint of the learning community (e.g., Derry and DuRussel, 2000). Transmission-oriented evaluation practices appear in 17 approaches. These evaluation practices include various ways to measure the repetition of knowledge (e.g., multiple-choice questions and security quizzes), or observe changes in a real or simulated working environment without instant feedback (competence-based evaluation). These are distinctive features of behaviorist evaluation practices. Typical evaluation of transaction and cognitivism is performed in five approaches, where the object of evaluation is adaptation of learned knowledge and problem solving through interactive exercises, case studies, or essay questions. In 15 approaches, features of the transformation orientation and constructivism are identified in the suggestions for conducting evaluation practices. Hence, these conversational evaluation practices are characterized as informal, experimental, and/ or open-ended. Typical evaluations include self-assessments, interviews, and feedback during the instruction. In addition, along with evaluating individual learners, three approaches stress communication as the purpose of evaluation, which is viewed as a feature of effective educational practice: corrective feedback during the group assignment (Puhakainen's (2006) cognitive processing approach), role-play scenarios and focus groups (Herold's (2005) andragogical approach), and group interviews (Wilson and Hash's (2003) strategic approach). (See Table 8.)

Table 8. Evaluation of Learning in the Existing IS Security Training Approaches

Evaluation of learning within the IS security training approaches			
Missing (10) *Social psychological recommendations approach* (Kabay 2002), *Normative approach* (Siponen 2000), *Deterrence approach* (Straub and Welke 1998), *Academic environment approach* (Kajava & Siponen 1997), *University environment approach* (McCoy & Thurmond Fowler 2004), *ISD approach* (Hansche 2001), *Policy creation approach* (Gaunt 1998), *Healthcare environment approach* (Furnell *et al.* 1997), *Discursive approach and online tutorial approach* (Cox *et al.* 2001), *Briefing approach* (Markey 1989)			
Transmission	**Transmission**	**Transmission**	
Behaviorism (17)	**Cognitivism (5)**	**Constructivism (15)**	**Social constructivism (3)**
Inclusive (2) *Competence approach* (Wilson *et al.* 1998) *Hypermedia instruction approach* (Shawn *et al.* 2009)			
Exclusive (5) *Security ensuring approach* (Peltier 2000) *Communication oriented approach* (Desman 2002) *Stakeholder approach* (Kovacich & Halibozek 2003) *Social engineering preventive approach* (Mitnick & Simon 2002) *Traditional e-learning approach* (Kajava *et al.* 2003)	Exclusive (0)	Exclusive (4) *Constructive instruction approach* (Heikka 2008) *Cyber security game approach* (Cone *et al.* 2007) *Active e-learning approach* (Furnell *et al.* 2002) *Persuasive technology approach* (Forget *et al.* 2007)	Exclusive (0)
Behaviorism + cognitivism (2) *Constructive scenario approach* (Biros 2004) *Operational controls approach* (NIST 1996)			
	Cognitivism + constructivism (1) *Pedagogical game approach* (Greitzer *et al.* 2007)		

Table 8. Evaluation of Learning in the Existing IS Security Training Approaches (continued)

Behaviorism + constructivism (8) *Social psychology oriented approach* (Thomson & von Solms 1998) *Motivation theory directive approach* (Roper *et al.* 2006) *Cognitive processing approach* (Puhakainen 2006) *Andragogical approach* (Herold 2005) *Counteractive approach* (McIlwraith 2006) *Promotional approach* (Rudolph *et al.* 2002) *Preventive approach* (Nosworthy 2000) *Strategic approach* (Wilson & Hash 2003)		Behaviorism + constructivism (8) *Social psychology oriented approach* (Thomson & von Solms 1998) *Motivation theory directive approach* (Roper *et al.* 2006) *Cognitive processing approach* (Puhakainen 2006) *Andragogical approach* (Herold 2005) *Counteractive approach* (McIlwraith 2006) *Promotional approach* (Rudolph *et al.* 2002) *Preventive approach* (Nosworthy 2000) *Strategic approach* (Wilson & Hash 2003)	
			Social constructivism (3) *Cognitive processing approach* (Puhakainen 2006) *Andragogical approach* (Herold 2005) *Strategic approach* (Wilson & Hash 2003)

About the Authors

Mari KARJALAINEN is a Ph.D. candidate in the Department of Information Processing Science at the University of Oulu, Finland. She has a Master' s degree in Education from the University of Oulu, Finland. Before joining her present position, she has worked as an adult educator and as a career counselor. Her research interests include IS security behavior and training.

Mikko SIPONEN is a Professor and the Director of the IS Security Research Centre in the Department of Information Processing Science at the University of Oulu, Finland. He is also a Vice-Head of the department. 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. In addition to his 70 conference articles, he has 37 published or forthcoming papers in journals, such as MIS Quarterly, Journal of the Association for Information Systems, European Journal of Information Systems, Information & Organization, Information Systems Journal, Communications of the ACM and IEEE Computer. He has served as a senior and associate editor for ICIS and ECIS. Currently, he sits on the editorial boards of EJIS and CAIS. Dr. Siponen has received over $5.4 million of research funding from corporations and numerous funding bodies.