11-30-2009

Towards a A New Meta-Theory for Designing IS Security Training Approaches

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

Mikko Siponen
The University of Oulu, msiponen@tols16.oulu.fi

芽|Sprouts Working Papers on Information Systems ISSN 1535-6078

Towards a A New Meta-Theory for Designing IS Security Training Approaches

Mari Karjalainen
The University of Oulu, Finland

Mikko Siponen
The University of Oulu, Finland

Abstract
Employee non-compliance with information systems (IS) security policies is a key concern for organisations. To tackle this problem, scholars have advanced several IS security training approaches. Despite the fact that the importance of having effective training is understood by scholars and practitioners, IS security training is largely a theoretically underdeveloped area. To this end, we advance a meta-theory for IS security training, based on Hareâ s theory of three levels of thinking. It is a meta-theory because it suggests that IS security training has certain fundamental characteristics which separate it from other forms of training, and it advances pedagogical requirements for the design and evaluation of IS security training approaches. After sketching this meta-theory, including four pedagogical requirements for IS security training approaches, we show that no existing IS security training approach meets all of these requirements. To this end, we put forth an IS security training approach which meets all these requirements. For scholars, this study offers new theoretical insights into the fundamental characteristics of IS security training; a set of principles for designing and evaluating IS security training approaches; and an agenda for future research on IS security training. For practitioners designing and implementing IS security training at organisations, this study offers principles for designing effective IS security training approaches in practice.

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

Permanent URL: http://sprouts.aisnet.org/9-53

Reference: Karjalainen, M., Siponen, M. (2009). "Towards a A New Meta-Theory for Designing IS Security Training Approaches," Proceedings > Proceedings of JAIS Theory Development Workshop . *Sprouts: Working Papers on Information Systems*, 9(53). http://sprouts.aisnet.org/9-53

TOWARDS A NEW META-THEORY FOR DESIGNING IS SECURITY TRAINING APPROACHES

ABSTRACT

Employee non-compliance with information systems (IS) security policies is a key concern for organisations. To tackle this problem, scholars have advanced several IS security training approaches. Despite the fact that the importance of having effective training is understood by scholars and practitioners, IS security training is largely a theoretically underdeveloped area. To this end, we advance a meta-theory for IS security training, based on Hare's theory of three levels of thinking. It is a meta-theory because it suggests that IS security training has certain fundamental characteristics which separate it from other forms of training, and it advances pedagogical requirements for the design and evaluation of IS security training approaches. After sketching this meta-theory, including four pedagogical requirements for IS security training approaches, we show that no existing IS security training approach meets all of these requirements. To this end, we put forth an IS security training approach which meets all these requirements.

For scholars, this study offers new theoretical insights into the fundamental characteristics of IS security training; a set of principles for designing and evaluating IS security training approaches; and an agenda for future research on IS security training. For practitioners designing and implementing IS security training at organisations, this study offers principles for designing effective IS security training approaches in practice.

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

1. INTRODUCTION

Employees' negligent behaviour towards information security policies is one of the biggest threats to IS security: if users do not comply with IS security policies, security solutions lose their usefulness (Kruger and Kearney, 2006). A common approach to improving employees' IS security behaviour is to motivate and persuade them to adhere to IS security procedures through IS security training (Puhakainen, 2006). While the need for IS security training is widely agreed upon by scholars and practitioners, previous research has noted that this area is largely theoretically underdeveloped (Puhakainen, 2006). Against this backdrop, we advance a meta-theory of IS security training approaches. This theory suggests that IS security training differs from other types of training, a fact which needs to be understood before pedagogical principles for IS security training can be selected. Our theory maintains, based on a review of paradigms of learning, that there are four pedagogical requirements which any IS security training approach must meet. We then review extant IS security training approaches, and conclude that no previous approach meets all these requirements. Finally, we illustrate how an IS security training approach can meet these requirements.

The results of this study are welcomed by both scholars and practitioners engaging in IS security training. For scholars, this paper offers a new theoretical contribution, the 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 to design IS security training approaches, and offers an agenda for future research. For practitioners, this study illustrates how to put our meta-theory to practical use by

offering important insights into how to improve IS security training in practice through the new theoretical framework.

The rest of the paper is organised as follows: At the beginning of the second section, a new meta-theory for designing IS security training approaches is advanced, including four pedagogical requirements for IS security training approaches. Extant IS security training approaches are then reviewed in the light of these requirements with the result 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 third section outlines implications for practice and research, and finally, the fourth section concludes the findings of the paper.

2. TOWARDS A NEW META-THEORY FOR DESIGNING IS SECURITY TRAINING APPROACHES

Gregor (2006) distinguishes five theory types in IS research: (1) analysis, (2) explanation, (3) prediction, (4) explanation and prediction, and (5) design and action. We argue that the ultimate objective of IS security training (theory) is "design and action", since its objective is goal-oriented. That is, the aim of IS security training theory is to design effective training approaches "effective" meaning that employees would comply with IS security policies. Like "design and action" types of theories (see Gregor, 2006) in general, we postulate that IS security training approaches should ultimately provide theoretically informed guidance on how to conduct effective IS security training in practice.

With respect to the theory viewed in terms of design and action, Hare (1952, 1963, 1981) suggests a meta-theory of three levels of thinking. This theory is prescriptive and descriptive. With regard to the latter, it describes potential maturity levels in relation to how people form action-guiding or

normative principles[1]. We apply Hare's meta-theory to sketch the structure of our new meta-theory for designing IS security training approaches (Figure 1).

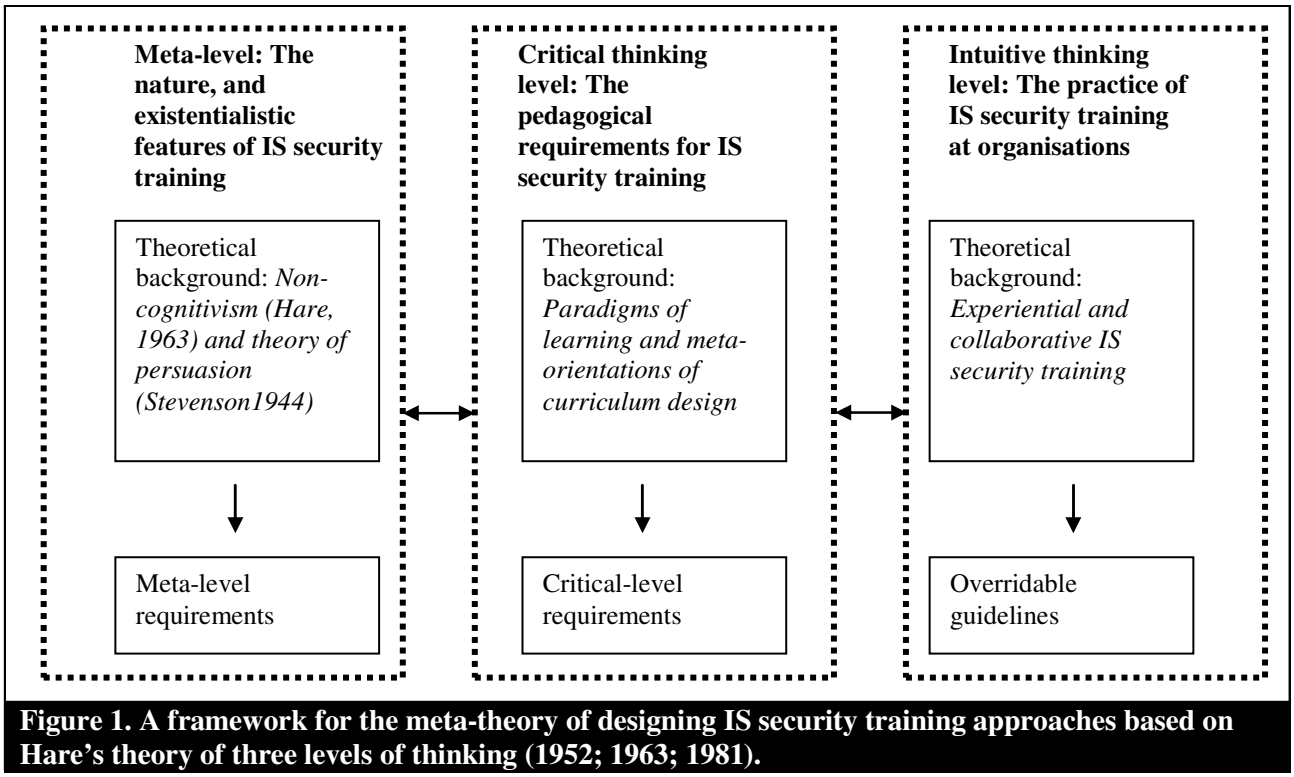

Figure 1. A framework for the meta-theory of designing IS security training approaches based on Hare's theory of three levels of thinking (1952; 1963; 1981).

In Figure 1, 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?" In turn, the intuitive thinking level means the customary or conventional activities in practice. The critical thinking level, lying between the meta- and intuitive thinking levels, is needed to test the validity of our ordinary/customary actions, and form new guidance in novel situations when needed (Hare, 1981). When applied to IS security training, Hare's idea is that people at the intuitive level, apply their learned principles to IS security training. These intuitive level principles are obtained, for example, through education, upbringing, and personal experience. People who simply follow their intuitive

[1] Hare's theory of universal prescriptivism has also prescriptive dimension by introduction of a logical decision making method, called "universalizability of moral judgement". This method is not necessary for our purposes; hence we omit the discussion of it from this study.

level principles, without ever questioning these, reside at the conventional level throughout their lives. To give an example, a practitioner engaging in IS security training, who uses the same training method that his supervisor used for educating him, without ever questioning the validity of these methods, stays at the level of intuitive thinking. However, when people critically ponder the validity and effectiveness of their customary 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 practical level are overridable; they can be modified, refined or omitted (see Hare 1981). Or in a case where two of our principles are in conflict, we can override (follow) one. Next, we describe these levels of thinking, starting from the meta-level.

2.1 Meta-level thinking: The nature and the 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 it has certain specific characteristics, namely its nature and existentialistic features. These will be discussed next.

First, it is important to understand the nature of IS security training, and how it differs from other types of training. Based on non-cognitivism (Hare, 1963) and theory of persuasion (Stevenson, 1944), we argue that the nature of IS security training is non-cognitive and persuasive. This is in contrast with other types of training, such as university education, which is descriptive (hence,

cognitive), provides scientific facts absolutely, and does not seek to influence learners' attitudes and behaviour in the manner of persuasive training. IS security training is persuasive and non-cognitive because its procedures are norms, per se, which require more normative training approaches than the learning of facts (Siponen, 2000). Another reason why IS security procedures are non-cognitive is that they are created within an organisational 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 organisations' non-cognitive attitudes towards how employees ought to behave in a secure manner. The expressional side of IS security procedures resembles cognitivism at first sight, in that it seems to have a true value, although it does not. This is the case since IS security procedures are incapable of being objectively true or false; hence, they are non-cognitive because they do not describe any factual feature. For example, "This computer is red" is a cognitive statement, for which a truth value can be resolved through scientific scrutiny. But a security procedure such as "Do not share your passwords with peers" is not a fact; it does not have an objective truth value.

Along with this persuasive and non-cognitive nature of IS security training, there are four existentialistic features of IS security training: (1) an existence of security-sensitive organisational assets; (2) threats towards them; and (3) different technical, social, organisational, and mechanisms for protecting the assets of the organisation (protection mechanisms) (modified from Siponen et al., 2006). Without the existence of these features, there is no need to have IS security training; hence, the label of existentialistic features. For example, if there are no assets of value in the organisation, or if there are no threats to the organisation, there is no need for IS security nor for IS security training. The first feature, an existence of security-sensitive organisational assets, means that IS security training should ensure that the employees understand these assets. If employees lack such an understanding, the IS security training is meaningless and arbitrary from the viewpoint of the

substance. The second feature means that there has to be a threat to these assets. Again, we argue that IS security training needs to introduce the relevant threats to the employees in a pedagogically meaningful manner. Finally, the third feature means that IS security training assumes that there are mechanisms in place that are able to protect security-sensitive organisational assets from threats, and that this training must be focused on achieving this objective. These three existentialistic features set the fundamental direction (general aim) of IS security training , in order to create a deeper understanding of the use of protection mechanisms to secure security-sensitive organisational assets from threats. In the most successful cases, changes in employees' understanding regarding existentialistic features also results in changes in their information security practices (Thomson et al., 2006).

From the discussion of the nature of the IS security training, and the existentialistic features, we arrived 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.

Second meta-level requirement for IS security training approaches: An IS security training approach must focus on the existentialistic features of IS security training.

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.

2.2 Critical level thinking: Paradigms of learning and features of meta-orientations

The critical level thinking in terms of Hare (1981) applied to this context, concerns the selection of proper pedagogical principles for carrying out IS security training in practice. Given that this study examines the preferred pedagogical principles for IS security training, it scrutinises paradigms of learning — behaviourism, cognitivism, constructivism, and social constructivism (Hung, 2001) — for finding the most appropriate paradigm for this context. In order to select the most suitable paradigm of learning for IS security training, it is helpful to apply the concept of meta-orientations. In terms of Hare (1981), 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-orientation), and derive from it four pedagogical requirements at the critical level. We then analyse the extent to which the existing IS security training approaches meet these pedagogical requirements.

Compared to the paradigms of learning, meta-orientations allow us to more concretely examine IS security training approaches. Meta-orientations represent basic orientations to the curriculum, which is any intentional interaction designed to facilitate learning, while imposing the meaning of experiences and achieving educational goals (Miller and Seller, 1985; Cheung and Wong, 2002). Paradigms of learning and meta-orientations are interrelated; paradigms of learning form a theoretical basis for meta-orientations, which are used to analyse IS security training approaches. Table 1 summarises the learning paradigms that are applied as theoretical frameworks and presents the practical features of meta-orientations in order to analyse IS security training approaches.

Table 1: Features of the meta-orientations of curriculum design (see Miller and Seller, 1985; Miller, 2001)

	Transmission	**Transaction**	**Transformation**	
Paradigm of learning as a psychological context	Behaviourism	Cognitivism	Constructivism	Social constructivism
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
Content	Subject-centred	Problem- or process-centred	Learner-centred	Community-centred
Teaching methods	Instructor-led approaches in order to transmit knowledge and provide external reinforcement	Focuses on cognitive problem-solving and analysis	Focuses on critical reflection of personal knowledge through collaboration or authentic problem solving to attain personal change	Focuses on critical reflection of communal knowledge through collaboration or authentic problem-solving to attain communal change
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

Three meta-orientations are used to select the explicit psychological context of learning, and the practical features of IS security training: content, teaching methods, and evaluation of learning. General aims are used as a means for selecting the most appropriate paradigm of learning in IS security training. The transmission meta-orientation resembles behaviourism, the transaction meta-orientation is based on cognitivism, and the transformation meta-orientation has strong similarities to constructivism and social constructivism. Thus, the paradigms of learning present the psychological contexts of the meta-orientations.

The four paradigms of learning — behaviourism, cognitivism, constructivism, and social constructivism — include specific directions and focus for educational practices. These four paradigms represent the psychological context of meta-orientations by combining all the features of

meta-orientations under a certain theoretical framework (see Table 1). The psychological context as an explicit learning paradigm should be applied to the training approach, because learning paradigms suggest fundamental directions and focus for educational practices, and thus are invaluable for effective and pedagogically meaningful training (Yilmaz, 2008; McLeod, 2003).

In reference to Table 1, general statements of aims represent an overall direction for development of the training approach. The content includes the subject matter, knowledge, skills, concepts, ideas, or topic areas. The teaching method (instruction) stresses interactions aimed at enhancing learning within the educational practices. Each meta-orientation also has a corresponding approach to evaluation procedures.

General aim as a descriptive feature of IS security training

General aims of training (see Table 1) are used as a fundamental feature for selecting the most appropriate paradigm of learning for IS security training. In transmission-oriented training, the general aims are to convey certain pre-defined contents (objective knowledge, facts, skills, concepts, and values) to students (Miller and Seller, 1985). A one-way flow of skills and knowledge through reading or listening, without the opportunity to analyse or reflect on information, is an example of transmission orientation (Miller, 2001). In turn, the general aims of transaction-oriented training are to obtain problem-solving skills through inquiring, analysing, synthesising, evaluating, or applying knowledge (Miller and Seller, 1985). This cognitive interaction emphasises analysis and thinking rather than synthesis and feeling (Miller, 2001). Thus, the general aims of training are clearly connected with the cognitive adaptation and application of knowledge — that is, of cognitive problem-solving. Finally, Miller and Seller (1985) argue that in transformation-oriented training, the general aims are expressed in relation to personal perceptions and experiences.

Reflective skills and personal appropriations of the content are required to attain personal and social (communal) change. According to this position, learning is aimed at transforming predominant beliefs and actions.

In this study, the general aim of transformation-orientation with respect to communal change is expected to be a fundamental feature of IS security training which sets the direction for other features of meta-orientations: psychological context, content, teaching method, and evaluation of learning (see Table 1). This expectation, with respect to the general aims, is based on meta-level requirements for IS security training: non-cognitive and persuasive nature and existentialistic features.

Recognising the persuasive and non-cognitive nature of IS security training (first meta-level requirement for IS security training approaches) as for the general aims of IS security training, we find that the transformation meta-orientation is the most suitable for IS security training. The general aims of IS security training are not to simply make employees remember and understand pre-determined contents (facts, concepts, or values) as general knowledge, in the manner of educational practices in transmission-oriented training. Neither is IS security training aimed at developing cognitive abilities, in the manner of educational practices in transaction-oriented training. Rather, the ultimate purpose of IS security training is to improve expertise concerning employees' knowledge, attitudes, and behaviours that is applicable to IS security issues within the organisation (Siponen, 2000). Therefore, learning is aimed at transforming predominant IS security beliefs and actions in order for them to become a natural part of employees' daily activities (Thomson, et al., 2006).

The existentialistic features of IS security training (second meta-level requirement for IS security training approaches) are closely related to the IS security policies, because information security policies are a common way of articulating these existentialistic features to the employees through constraining and prescribing employees' work behaviour (Thomson et al., 2006). In this paper, we assume that in order to maintain a secure work environment, these existentialistic features, and thus also information security policies, must be understood, accepted, and implemented collectively – not only individually (see Salomon & Perkins, 1998). This social aspect of learning emphasises organisations' or teams' level of acquisition of knowledge, understanding, skills, different cultures (Salomon and Perkins, 1998; Brown and Campione, 1994), organisational routines that include policies, practices, and belief systems (Levitt and March, 1988), or agreements that deal with operating procedures (Weick, 1979) as a target of learning. This is a relevant perspective in the area of IS security training because the general aims of training are closely tied to shared organisational work practices and related work communities, and an organisation's security culture is thereby developed (Dhillon, 2007; Thomson et al., 2006). For this reason, general aims regarding communal changes need to be emphasised. Organisational context, teams as learning units, and organisational routines (existentialistic features as IS security policies) as a target of learning, are considered to be communal characters of IS security training. These characteristics explain the reasons for selecting the proper nature of the general aim of IS security training.

Pedagogical requirements for IS security training

Based on the general aim of IS security training, we argue in the following sections that, in order to create communal change in the organisational context, the transformation meta-orientation and consequently, social constructivism, is the preferred theoretical basis for IS security training. As a consequence, it is necessary to emphasise social (or communal) viewpoints in regards to

psychological context, content, teaching methods, and evaluation of learning in order to enhance communal change in understanding existentialistic features of IS security training, Next, the meaning of these four features of meta-orientation in transmission, transaction, and transformation is explained. Also, pedagogical requirements for IS security training at the critical level derived from transformation orientation, are put forward as a part of a meta-theory for designing IS security training.

First pedagogical requirement for IS security training: Psychological context

The transmission meta-orientation represents mechanistic and natural science-based thinking, as well as behaviouristic psychology (Thorndike, 1911; Skinner, 1968) (see Miller and Seller, 1985). Thus, behaviourism is a psychological context in educational practices belonging to the transmission orientation. In turn, the transaction meta-orientation is psychologically oriented to developmental and cognitive psychology (Kohlberg and Mayer, 1972; Piaget, 196) (see Miller and Seller, 1985). Thus, cognitivism as an approach to learning that emphasises individual development of cognition, is the corresponding psychological context in transaction-oriented educational practices. Finally, the transformation meta-orientation can be traced back to humanistic psychology (Maslow, 1970; Rogers, 1969) (see Miller and Seller, 1985). The humanistic approach to learning has much in common with the constructivist approach, as both emphasise the active role of the learner and the interactive and communal character of learning. Humanism emphasises self-actualisation and self-transcendence (Miller and Seller, 1985), or growth and personal integrity (McNeil, 1981). In turn, constructivism is a more appropriate learning paradigm from which to construct meanings of events and ideas, to transform understandings (Ross, 2002), and to build a connection between a learner's existing knowledge and what he is expected to learn (Gagnon and Collay, 2006). Instead of considering learning as an individual process, social constructivism emphasises a social (or communal) viewpoint in the learning process (Palincsar, 1998). Thus,

constructivism and social constructivism are corresponding psychological contexts within the transformation orientation.

Constructivism and social constructivism have different theoretical origins. Constructivism is rooted in Piaget's (1985) socio-cognitive conflict theory, which explains the role of social interaction in the learning process from the viewpoint of individual learning (Palincsar, 1998). In turn, social constructivism is grounded on Vygotsky's (1978) socio-cultural theory, which considers individual thinking to be secondary to, and a derivative of, social interaction, and learning is considered to require interaction, negotiation, and collaboration. Social constructivism stresses the social viewpoint of learning processes, interactions, and knowledge. With respect to the descriptive features of IS security training, we argue that social constructivism is the most suitable learning paradigm. Thus, as a first pedagogical requirement for IS security training approaches, the explicit psychological context — that is, the learning paradigm behind the training approach — must be based upon a group-oriented theoretical approach to teaching and learning, which will guide training activities (see Fardanesh, 2006; Gibson, 2001; Hinsz et al., 1997).

Second pedagogical requirement for IS security training: Content

In the transmission orientation, knowledge (content) is seen to be objective, unrelated to human subjectivity (Brody, 1998), and static (Miller, 2001). Thus, transmission orientation focuses on pre-determined subjects (Miller and Seller, 1985) and is the dominant orientation in basic skill development and within traditional subject curriculums (Miller, 2001). The content of transmission-oriented training is subject-centred (Miller and Seller, 1985; Miller, 2001).

Transaction orientation emphasises problem-centred content mainly selected by the teacher, but also takes into account students' interests (Miller and Seller, 1985). In addition, this cognitive process orientation stresses the learning process and cognitive process skills rather than curriculum content and the acquisition of factual knowledge (Cheung and Wong, 2000). Thus, the content is also process-centred.

Concerning the scope of the content (or topic areas), transformation-oriented training stresses learners' experiences and involvement in the community, and is, therefore, considered to be learner-centred (Miller and Seller, 1985). New knowledge emerges from the community through collaborative knowledge building (Hmelo-Silver and Barrows, 2008). Thus, the content can also be community-centred. As with transaction orientation, the content is not separable from the teaching methods and is mainly formulated during the educational practice.

IS security policies and employee compliance within an organisation as a content of IS security training, are both dependent on environmental and communal factors, such as the prevailing organisational policies, the aims of the company, and the individual learner (see Cole and Engeström, 1993). In addition, they are influenced by the individual learner's roles, perspectives, values, and tacit beliefs (see Salomon and Perkins, 1998). Thus, in order to make the content of IS security training understood, accepted, and implemented collectively (not just individually), it must consist of employees' shared knowledge, attitudes, and behaviours concerning IS security issues in relation to its expected outcomes. Thus, as a second pedagogical requirement for IS security training, the content of the training must be based on the collective experiences and meaning perspectives of the learners (see Hmelo-Silver and Barrows, 2008).

Third pedagogical requirement for IS security training: teaching method

In transmission-oriented training, a teaching method is the educator's approach to spreading knowledge. Thus, the teacher's role is directive, and learners are passive participants (Miller, 2001). Teaching shapes the learner's responses through instructional procedures, such as modeling and reinforcement (Palincsar, 1998).

Training resembles a transaction when teaching methods focus on cognitive problem-solving through applications, analyses, and syntheses of the learning material (Bloom, 1956; Miller and Seller, 1985). In these cases, training includes cognitive problem-solving activities that are mainly defined by the teacher, and which demand active information processing from the learners.

According to Miller and Seller (1985), transformation-oriented teaching methods, in contrast, make connections between students and the real world, while making students aware of their thinking processes. Thus, they maintain that learning occurs through the critical reflection of information through authentic problem-solving or communication. In critical reflection, a person or a group ponders the validity of his actions, thoughts, and feelings in order to change these meaning perspectives (Mezirow, 1991).

In the context of IS security training, teaching methods that create communal experiences must be executed through discussions concerning experiences, attitudes, and behaviours towards security issues. The communal creation of experiences includes collaboration (which must engage each member of the group) in order to collectively solve the common problem or reach an agreement (Dillenbourg et al., 1996; Rochelle and Teacley, 1995). In this sense, differentiating personal teaching methods from communal ones is closely related to the general aims of training. For example, a discussion to support individual understanding can be considered a personal teaching

method. However, if the goal of the discussion is to reflect on collective experiences and to achieve mutual understanding and agreements, it can be considered a communal teaching method. Accordingly, as a third pedagogical requirement for IS security training, teaching methods must focus on collaborative learning in order to reveal and produce collective knowledge (see Mezirow, 1991; Palincsar, 1998; Dillenbourg et al., 1996; Rochelle and Teacley, 1995).

Fourth pedagogical requirement for IS security training: Evaluation of learning

In transmission-oriented training, the evaluation concentrates on the learner's observable performance or achievement through tests (Miller and Seller, 1985). Generally, evaluation pursues an objective measurement of training goals with pre-defined responses. Examples of 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.

In transaction-oriented training, evaluation stresses the adaptation of knowledge, development of intellectual skills (e.g., analysis and synthesis), and "the ability to assess concepts, theories and materials according to selected criteria" (Miller and Seller, 1985: 182; Bloom, 1956). Thus, evaluation focuses on examining learners' information processing through cognitive problem-solving tasks.

Evaluation in transformative training includes various conversational models, such as informal, experimental, and open-ended forms of evaluation for individuals or groups (Miller and Seller, 1985). Students are active participants who share responsibility in the evaluation process through self-evaluation, reflection, collaboration, and continuous dialogue with the teacher, and evaluation methods include feedback during work or assignments, group projects, peer evaluations, and

interviews (Birenbaum, 1996). When the goal of transformative training is to construct collaborative knowledge (in other words, to mutually understand new ideas and behavioural norms), evaluation must measure the presence, frequency, and quality of group interactions in discourse processes (Derry and DuRussel, 2000). Thus, as a fourth pedagogical requirement for IS security training, evaluation of learning should emphasise experiential and communication-based methods from the viewpoint of the learning community (see Miller and Seller, 1985; Birenbaum, 1996).

Existing IS security training approaches and the four pedagogical requirements

Existing IS security training approaches (N = 32) selected for the review include training and awareness activities in an organisational context. The goal of such training is to achieve organisation- and work-specific changes in employees' attitudes and behaviours. Hence, studies on education for information security professionals are outside the scope of this review (e.g., Goel & Pon 2006, Bishop 2000, Romney et al. 2004, Ryan 2003, and Sharma & Sefchek 2007). Also articles concentrating on the evaluation of training approaches (e.g., Kruger & Kearney 2006, Martins & Eloff 2001, Stanton et al. 2005, and Dodge et al. 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 programme 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 et al. 2001, Spurling 1995, Stacey 1996, and Telders 1991).

Table 2 shows the extent to which the extant IS security training approaches meet the four pedagogical requirements formulated in this section. To summarise, none of the IS security approaches meets all four pedagogical requirements. "X" means that an IS security training

approach fulfils the requirement, and "–" signifies that it does not fulfil it (For more details, see Appendix 1).

Table 2. The degree to which extant IS security training approaches meet the four pedagogical requirements for IS security training approaches.

IS security training approaches	(1) Fulfils the requirement for the explicit psychological context	(2) Fulfils the requirement for the content	(3) Fulfils the requirement for teaching method	(4) Fulfils 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 content** of training 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 emphasise experiential and communication-based methods from the viewpoint of the learning community.

Analysed IS security training approaches, which do not fulfil 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 and 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 and Halibozek, 2003); Deterrence approach, (Straub and Welke, 1998); Academic environment approach (Kajava and Siponen, 1997); University environment approach (McCoy and Thurmond Fowler, 2004); Preventive approach (Nosworthy, 2000); Competence approach (Wilson et al., 1998); Operational controls approach (NIST, 1996); ISD approach (Hansche, 2001); Traditional e-learning approach (Kajava et al., 2003); Hypermedia instruction approach (Shawn et al., 1998); 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 and Simon, 2002) and; Active e-learning approach (Furnell et al., 2002).

One study (Puhakainen, 2006) meets the last three requirements; another (Kabay, 2002) meets the second and third requirements; and two (Herold, 2005; Wilson and Hash, 2003) meet the last

requirement. However, features of existing IS security training approaches which fulfil these pedagogical requirements, are not guided by the social constructivist learning paradigm or instructional design approach. Therefore, they are considered to be only single features and not in the essence of the IS security training practice. This means that instead of an active communal production of knowledge and work practices, IS security training is directed towards adopting stable work practices (see Tuomi-Gröhn and Engeström 2003). Given that no existing IS security training approaches meet all four pedagogical requirements, the following section advances a new training approach which meets these four requirements.

2.3 Intuitive level thinking: Example of an IS security training approach meeting the four pedagogical requirements

In previous sections, we advanced a meta-theory for IS security training approaches, 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, four pedagogical requirements for IS security training approaches were laid down. This section demonstrates a potential pedagogical approach to IS security training, which meets these four pedagogical requirements.

Searching for a Proper Instructional Design Approach fulfilling the pedagogical requirements for IS security training

The first pedagogical requirement for IS security training argued that the explicit psychological context of IS security training must be based upon the group-oriented theoretical approach to teaching and learning. In seeking such candidate approaches that meet the first pedagogical

requirement for IS security training, constructivist instructional design theories are found to constitute ideal theoretical bases for designing IS security training. This is due to two reasons. First, a constructivist instructional design theory is beneficial in training design because it expresses concrete instructions for training, unlike the four high-level pedagogical requirements derived from the social constructivist learning paradigm[2] (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 a viewpoint of the individual learner and social constructivism emphasises a social viewpoint towards learning with respect to general aims, content, teaching methods, and evaluation (see Table 1).

Of the alternative constructivist instructional design approaches (see Fardanesh, 2006; Kirschner et al., 2006), experiential learning is preferred here, because it is considered to be the prevailing paradigm in adult education (Fenwick, 2001) and the preferred learning approach in the organisational context (Pavlica et al., 1998; Backström, 2004; Dixon, 1999). Furthermore, it has also been a successful learning approach aimed at attitudinal changes in other contexts, such as group consciousness-raising, community action, social change (Weil and McGill, 1989), and work-based learning (Honey and Mumford, 1992). Thus, we also deem the experiential learning approach to be a preferred approach for changing employees' IS security attitudes and behaviours.

A leading experiential learning approach is the theory of experiential learning by Kolb (1984). It acts as a foundation for modern experiential education and provides an effective framework for planning teaching and learning activities (Tennant, 1997). Hence, we select it to form the instructional design part of the IS security training approach (that should meet the four pedagogical

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

requirements). Because Kolb's theory of experiential learning does not address the social aspects of learning (Pavlica et al., 1998; Holman et al., 1997), we add collaborative learning techniques (Barkley et al., 2005) to our IS security training approach, in order to achieve effective learning in groups. Collaborative learning techniques are detailed practical descriptions that create effective group work assignments and engage students in collaborative learning when knowledge is socially produced and constructed by talking together and reaching agreements (Barkley et al., 2005). Collaborative learning has been reported to be effective, for example, for conceptual change (Rochelle, 1992), promoting achievement and productivity (Johnson et al., 1981), and improving attitudes towards the subject matter (Springer et al., 1999). Next, the IS security training approach, combining experiential learning and collaborative learning techniques, is introduced.

The Experiential and Collaborative IS Security Training Approach

A learning process is a four-stage cycle (Kolb, 1984). According to Gibson (2001), Kolb's phases of (individual) learning are analogous to phases of collective cognition: accumulation, interaction, examination, and accommodation (see Figure 2). Each of these phases includes certain processes to create changes in collective thinking and to develop effective group decisions and actions. Information processing at the group level in cognitive tasks (such as problem-solving, decision making, and inference) involves sharing information among group members, which creates learning outcomes at both the individual and group levels (Hinsz, 1997). These four phases of experiential learning can be seen as an example of the intuitive thinking level of the meta-theory for designing IS security training approaches.

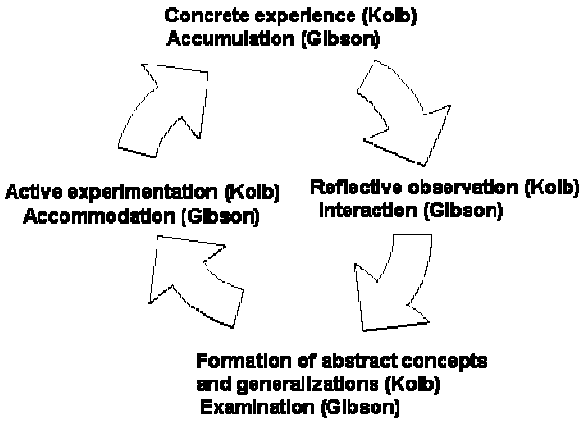

Figure 2. The experiential learning cycle and analogous phases of collective cognition (Kolb, 1984; Gibson, 2001).

Complemented by collaborative learning techniques (Barkley, 2005), the 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). Such a training approach stresses the experiences and collective activities of learners in order to achieve communal change. It resembles features of transformation orientation and of social constructivism (previously presented in this article). Thus, this training approach fulfils 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.

While the experiential and collaborative IS security training emphasises *the reflection of a common competence* as a content of training (see Backström, 2004), this framework also fulfils the second pedagogical requirement for IS security training: the content of training must be based on the collective experiences of the learners. In addition, while teaching method and evaluation are based on *a collective activity,* interactions among individual learners (see Backström, 2004), this framework also fulfils the third and fourth pedagogical requirements for IS security training:

teaching methods must focus on collaborative learning in order to reveal and produce collective knowledge, and evaluation of learning should emphasise experiential and communication-based methods from the viewpoint of the learning community.

As argued in this section, the selection of the experiential and collaborative theoretical approach for IS security training fulfils the first pedagogical requirement for IS security training. Next, each of the four phases of experiential learning (see Figure 2) is described in the context of IS security training in order to demonstrate in more detail, how the experiential and collaborative IS security training approach meets the other three pedagogical requirements for IS security training.

Involve Learners' Concrete Experiences

The learning cycle begins with concrete experiences (Kolb, 1984; Gibson, 2001), which form the basis for learning. In IS security training, the concrete experiences at the initial phase of learning are former experiences that the learner has encountered (see Fenwick, 2001; Dixon, 1999) with respect to the existentialistic features of IS security training — security-sensitive organisational assets, threats towards them, and protection mechanisms. Let us presume that an organisation finds insecure email use by employees to be a problem. In this case, the employees' concrete experience with the security-sensitive organisational assets (e.g., confidential documents), threats towards them (e.g., email eavesdropping) and protection mechanisms (e.g., email encryption) in regards to secure email use, will constitute the starting point for IS security training.

Individual learners' concrete experiences create a basis for realising pedagogical requirements for IS security training approaches in the following three phases, which include content based on the collective experiences of learners, and teaching methods involving collaborative learning. The

fourth phase also includes evaluation which emphasises experiential and communication-based methods from the viewpoint of the learning community. During the following three phases of experiential learning cycle, these individual concrete experiences will be modified as a result of collaborative reflection with respect to the collective experiences concerning the existentialistic features of IS security training.

Engage Reflective Observation

The second phase, reflective observation (or interaction), occurs via retrieving, exchanging, and structuring groups' shared experiences (Kolb, 1984; Gibson, 2001). Then, concrete experiences can be reflected through group discussions in order to react to others' perspectives and practices (Honey and Mumford, 1992), and to map a causal relationship between their work practices and respective organisational 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 existentialistic features of IS security training, in order to define their meanings and implications for the organisation. For instance, if the topic of the training is to make employees' use of email more secure, their task is to consider what kind of security-sensitive emails requires protection, what protection mechanisms constitute secure email use in general, which of these practices are valid in their own work and why, and what threats exist if these protection mechanisms are not followed. Thus, while this phase implements collective experiences

as a content of training, it also involves groups' interpersonal perspectives towards the existentialistic features of IS security training. Hence, it 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 email use individually, and then share their ideas with a partner 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, which supports learners' understanding of different aspects and enhances their ability to build group consensus on the secure use of email. 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: teaching methods must focus on collaborative learning in order to reveal and produce collective knowledge.

Support Formation of Abstract Concepts and Generalisations

The third phase, the formation of abstract concepts and generalisations, involves processes of negotiation, interpretation, and evaluation (Kolb, 1984; Gibson, 2001). In this phase, the meanings of collective experiences are interpreted in the organisational context by comparing them to the organisational viewpoints (Honey and Mumford, 1992), as stated in the organisation's written security policies. The instructor needs to introduce the organisation's email policies, related security-sensitive organisational assets, threats towards them, and protection mechanisms. Building on the aforementioned exercises in the previous phase (à la Think-Pair-Share), the learners analyse

the similarities and differences between group experiences and the presented organisational viewpoint. This phase is an examination of the overlap between organisational regulations and employees' communal experiences. Some variations are possible in cases where existing policies and instructions do not reconcile with actual work practices.

Similarly to the previous phase, this phase involves collective experiences as a content of training, thereby fulfilling the second pedagogical requirement: the content of training must be based on the collective experiences of the learners. It also involves collaborative learning in the form of group discussion in order to reveal and produce collective knowledge; hence, it fulfils the third pedagogical requirement: 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 group to organisational level involving reflection of the organisation's formal email policies.

Enable Active Experimentation

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

The ultimate purpose of the fourth phase is to define how formal email policies and instructions are actually experienced by employees, and how they can be applied by the learners. For example, rules, exceptional situations, and concrete procedures involving secure use of email are defined for all employees to follow. It is essential that learners receive this concrete training outcome in written form. For example, the instructor can deliver written policies to learners with open spaces for learners' possible correctives, supplements, and/or corrections. This document can also function as a 'learning contract', which supports the transfer of learned knowledge and attitudes of employees (for example, to secure email practices) (Kirkpatrick, 2005; 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, analysing, and creating organisational practices, learners are required to implement changes in their work (Pavlica et al., 1998). In order to validate a new practice in an organisation, potential changes in the policies and instruction must be accepted by management. Employees need to consciously observe their email use practices, and must execute applicable changes based on what has been 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 with respect to existentialistic features in the area of secure use of email, 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 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

with respect to the topic of the training (for example, email use), evaluation of learning is conducted using the group interview. Then, the fourth pedagogical requirement for IS security training is also fulfilled: evaluation of learning should emphasise experiential and communication-based methods from the viewpoint of the learning community.

3. DISCUSSION

Based on Hare's (1981) meta-theory of three level of thinking, a new meta-theory for designing effective IS security training approaches was developed in this study. At the meta-level, this theory advances fundamental features of IS security training (non-cognitive and persuasive nature, and existentialistic features), and formulates respective meta-level requirements. At the critical thinking level, based on these meta-level requirements and learning theories, four pedagogical requirements for effective IS security training based on social constructivism were formulated. As none of the existing IS security training approaches meets all four pedagogical requirements, we advanced a new IS security training approach, the experiential and collaborative IS security training approach, that meets these requirements and provides overridable guidelines for IS security training.

Based on our findings, we would like to highlight the following four avenues for further research on IS security training: 1) the development and implementation of IS security training approaches that meet the pedagogical requirements set in this study; 2) the execution of an empirical evaluation of the impact of IS security training at different levels while emphasising changes in employees' actual work behaviour; 3) the use of the control group or pre-then-post research design, along with the pre- and post-research design, to reliably and accurately measure the impact of the training; and 4) the measurement of the integrative complexity of thought in analysing the changes incited with regard to IS security behaviour. Next, these are discussed in more detail.

First, it has been argued in this paper that future research should develop IS security training approaches that meet the four pedagogical requirements, which were further based on meta-level requirements and the social constructivist learning paradigm. Such IS security training approaches should be developed and tested for different training topics and contexts.

Second, the impact of such social constructivist IS security training should be empirically evaluated in practice. It is expected that implementation of the four pedagogical requirements for IS security training formulated in this article should improve learners' understanding of security-sensitive organisational assets, impending threats, and protection mechanisms. This proposition can be tested through the execution of an empirical evaluation of the impact of IS security training. To this end, Kirkpatrick's (2005) four-level approach offers useful information for evaluating training approaches and is widely applied in diverse areas and in different types of organisations. These four levels represent a sequence of inter-related ways to evaluate training approaches, and consist of: 1) reactions (user satisfaction); 2) learning (changes in attitudes, knowledge, or skills); 3) behaviour (e.g., how learning is implemented in the organisation); and 4) results (e.g., decreased frequency of accidents and improved productivity).

While the general aim of IS security training, as described in this study, is to achieve communal changes in employees' information security work practices, the focus of the evaluations is mainly on the third (behavioural) level in terms of Kirkpatrick's model. However, Kirkpatrick (2005) and Robinson and Robinson (1989) claim that all levels of this model have relevance to the evaluation of training and should be implemented. While IS security training can affect learners' knowledge and skills relating to the achievement of more secure work practices, changes in behaviour also require support from the organisation's management. Thus, if no changes in employees' security

behaviour (third level) are achieved, further examination can reveal whether this situation is due to ineffective training at the first and second levels of evaluation, or problems with the organisational environment (e.g., work climate or lack of rewards). In turn, IS security training results (e.g., decreased frequency of accidents and improved productivity) denote positive outcomes at all previous levels, and such results are the ultimate reason for training in the first place.

An assessment of the impact of training at the second, third, and fourth levels of evaluation (Kirkpatrick, 2005) requires a pre- and post-research design where learners' work practices, mental abilities, knowledge, skills, or the number of incidents in the organisation, are measured both before and after IS security training, and compared in order to demonstrate possible changes therein (Robinson and Robinson, 1989).The third implication for future research on IS security training calls for a rigorous pre-then-post research design with a control group. A pre-then-post research design would more accurately reveal real changes and training benefits as compared with the conventional pre- and post- design (Mezoff, 1981; Howard, 1980). According to Robinson and Robinson (1989) and Mezoff (1981), in the pre-then-post research design, in addition to pre- and post-measurements being taken, participants would be asked immediately after training how they judged their earlier behaviour. They maintain that the pre-then-post research design should correct participants' previously incorrect views because, after training, they are expected to clearly understand the subject matter and the purpose of training.

Fourth, to evaluate the impact of IS security training, we also suggest the use of integrative complexity. According to Suefeld et al. (1992), it measures the complexity of mental abilities in terms of differentiation and integration, where differentiation refers to the perception of different perspectives, and integration to the conceptual connections among differentiated perspectives (e.g., trade-offs between alternatives). They maintain that integrative complexity has been successfully

applied in the past to investigate attitudinal changes and social perceptions, and to solve organisational problems. It assumes that the level of thought complexity can be changed by discussion, information gathering, or training (Myyry, 2002; Suefeld et al., 1992). Thus, it offers an opportunity to determine whether IS security training increases the integrative complexity of thoughts regarding IS security behaviour. As a result of IS security training, learners are expected to analyse and solve information security-related problems in their work using more diverse perspectives.

4. CONCLUSIONS

Employee non-compliance with IS security policies is considered to be one of the biggest threats to IS security. To solve this problem, several training approaches have been introduced in the IS security literature. Despite the recognised importance of having effective training, IS security training is largely a theoretically underdeveloped area. To fill this gap in research, a new meta-theory for designing IS security training approaches, based on Hare's theory of three levels of thinking, was put forward. 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. Also, the meta-theory proposed four pedagogical requirements, which any IS security training approach must meet. The existing IS security training approaches were then reviewed in the light of these four requirements. This review pointed out that no previous IS security training approach meets all these requirements. Finally, we demonstrated how an IS security training approach can meet these requirements.

The key contribution of the study was the introduction of the new meta-theory for IS security training, including four pedagogical requirements for designing IS security training approaches. In

addition, four avenues for future research were suggested. First, it was argued that future research should study the design and implementation of IS security training, based on the presented meta-theory for designing IS security training approaches. Second, there is a need to execute an empirical evaluation of the impact of IS security training at four levels of evaluation, while particularly emphasising changes in employees' security behaviour. Third, the control group or pre-then-post research designs, along with the pre- and post-research design could be used for the creation of reliable and accurate measurements of the impact of IS security training. Fourth, the measurement of the integrative complexity of thought could be useful in analysing changes in IS security behaviour.

5. REFERENCES

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. and Major, C.H. (2005). Collaborative Learning Techniques. A Handbook for College Faculty. San Francisco (CA): Jossey-Bass.

Birenbaum, M. (2000). Assessment 2000: Towards a Pluralistic Approach to Assessment. In Birenbaum, M. and Dochy, F.J.R.C. (Eds.) Alternatives in Assessment of Achievements, Learning Processes and Prior Knowledge. Boston/Dordrecht/London: Kluwer Academic Publishers, 3 – 29.

Biros, D.P. (2004). Scenario-Based Training for Deception Detection. InfoSecCD Conference, 32 – 36.

Bishop, M. (2000). Education in Information Security. IEEE Concurrency, 4 – 8.

Bloom, B.S. (1956). Taxonomy of Educational Objectives: Cognitive Domain. New York: McKay.

Bray, T.J. (2002). Security Actions During Reduction in Workforce Efforts: What to Do When Downsizing. Information System Security, 11(1), 11 – 15.

Brody, C.M. (1998). The Significance of Teacher Beliefs for Professional Development and Cooperative Learning. In Brody, C.M. (Ed.) Professional Development for Cooperative Learning. Albany: State University of New York Press, 25 – 48.

Brown, A. and Campione, J. (1994). Guided Discovery in a Community of Learners. In McGilly, K. (Ed.) Classroom Lessons: Integrating Cognitive Theory and Classroom Practice. Cambridge (MA): MIT Press, 227 – 270.

Cheung, D. and Wong, H. (2002). Measuring Teacher Beliefs About Alternative Curriculum Designs. The Curriculum Journal, 13(2), 225 – 248.

Cole, M. and Engeström, Y. (1993). A Cultural-Historical Approach to Distributed Cognition. In Salomon, G. (Ed.) Distributed Cognitions: Psychological and Educational Considerations. Cambridge (UK); New York; Melbourne: Cambridge University Press, 1 – 46.

Cone, B., Irvine, C., Thompson, M.F. and Nguyen, T.D. (2007). A Video Game for Cyber Security Training and Awareness. Computers and Security, 26(1), 63 – 72.

Cox, A., Connolly, S. and Currall, J. (2001). Raising IS Security Awareness in the Academic Setting. VINE, 123, 11 – 16.

Derry, S.J. and DuRussel, J.A. (2000). Assessing Knowledge Construction in On-Line Learning Communities. Available: http://www.eric.ed.gov/ERICDocs/data/ericdocs2sql/content_storage_01/0000019b/80/16/9c/cb.pdf. 88. 8.4.2009

Desman, M.B. (2002). Building Information Security awareness Program. USA: Auerbach Publications.

Dillenbourg, R, Baker, M., Blaye, A. and O`Malley, C. (1996). The Evolution of Research on Collaborative Learning. In Spada, H. and Reimann, P. (Eds.) Learning in Humans and Machines. Towards an Interdisciplinary Learning Science. Oxford: Pergamon, 189 – 211.

Dixon, N.M. (1999). Organizational Learning Cycle: How We Can Learn Collectively? Abindon, Oxon (GBR): Gower Publishing Limited.

Dhillon, G. (2007). Principles of Information Systems Security: Text and Cases. New York: John Wiley and Sons.

Dodge Jr., R.C., Carver, C. & Ferguson, A.J. (2007). Phishing for User Security Awareness. Computers & Security, 26, 73 – 80.

Fardanesh, H. (2006). A Classification of Constructivist Instructional Design Models Based on Learning and Teaching Approaches. Available: http://www.eric.ed.gov/ERICWebPortal/custom/portlets/recordDetails/detailmini.jsp?_nfpb=trueand_andERICExtSearch_SearchValue_0=ED491713andERICExtSearch_SearchType_0=noandaccno=ED491713. 24.4.2009

Fenwick, T.J. (2001). Experiential Learning. A Theoretical Critique from Five Perspectives. Information Series No. 385. ERIC Clearinghouse on Adult, Career, and Vocational Education. Center on Education and Training for Employment College of Education.

Forget, A., Chiasson, S. and Biddle, R. (2007). Persuasion as Education for Computer Security. In Richards, G. (Ed.) Proceedings of World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education, 822 – 829.

Furnell, S.M., Gennatou, M. and 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. and 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. and 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, 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. ACM Journal of 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. and Huston, K. (2007). Cognitive Science Implications for Enhancing Training Effectiveness in a Serious Gaming Context. ACM Journal of Educational Resources in Computing, 7(2), 1 – 16.

Hansche, S. (2001). Information System Security Training: Making It Happen, Part 2. Information Systems Security, 10(3), 51 – 70.

Hare, R.M. (1981). Moral Thinking: its Levels, Method, and Point. Oxford: Clarendon Press.

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

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

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), 1 – 8.

Herold, R. (2005). Managing an Information Security and Privacy Awareness and Training Program. Boca Raton: Auerbach Publications.

Hinsz, V.B., Vollrath, D.A. and Tindale, R.S. (1997). The Emerging Conceptualization of Groups as Information Processors. Psychological Bulletin, 121(1), 43 – 64.

Hmelo-Silver, C.E. and Barrows, H.S. (2008). Facilitating Collaborative Knowledge Building. Cognition and Instruction, 26(1), 48 – 94.

Holman, D., Pavlica, K. and Thorpe, R. (1997). Rethinking Kolb's Theory of Experiential Learning in Management Education. Management Learning, 28(2), 135 – 148.

Honey, P. and Mumford, A. (1992). Manual of Learning Styles. 3rd edition. Maudenhead (UK): P.Honey.

Howard, G.S. (1980). Response- Shift Bias: A Problem in Evaluating Interventions with Pre/Post Self Reports. Evaluation Review, 4(1), 93 – 106.

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. Available: https://www.isfsecuritystandard.com/SOGP07/index.htm. 10.3.2009.

Johnson, D.W., Maruyama, G., Johnson, R., Nelson, D., & Skon, L. (1981). Effects of Cooperative, Competetive, and Individual Goal Structure on Achievement: A Meta-Analysis. Psychological Bulletin, 89, 47 – 62.

Kabay, M.E. (2002). Using Social Psychology to Implement Security Policies. In: Bosworth, S. and Kabay, M.E. (Eds.) Computer Security Handbook, 4th edition. USA: John Wiley and Sons, Inc., 32.1 – 32.16.

Kajava, J. and Siponen, M.T. (1997). Effectively Implemented IS 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. and 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. (2005). Evaluating Training Programs: The Four Levels. 3rd edition. San Francisco (CA): Berrett-Koehler.

Kirschner, P.A., Sweller, J. and 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.

Kohlberg, L.N. and Mayer, R. (1972). Development as an Aim of Education. The Harvard Educational Review, 42, 449 – 496.

Kolb, D.A. (1984). Experiential Learning. Experience as a Source of Learning and Development. Englewood Cliffs (NJ): Prentice Hall.

Koschmann, T. (1996). (Ed.) CLCL: Theory and Practice of an Emerging Paradigm. Mahwah (NJ): Lawrence Erlbaum Associates.

Kovacich, G.L. and 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. and Kearney, W.D. (2006). A Prototype for Assessing Information Security Awareness. Computers and Security, 25, 289 – 296.

Leach, J. (2003). Improving User Security Behaviour. Computers & Security, 22(8), 685 – 692.

Levitt, B. and March, J.G. (1988). Organizational Learning. Annual Review of Sociology, 14, 319 – 340.

Lyman, F.T. (1981). The Responsive Classroom Discussion. In Anderson, A.S. (Ed.) Mainstreaming Digests. College Park: University of Maryland College of Education.

Markey, E. (1989). Getting Organizations Involved in Computer Security: The Role of Security Awareness. In Caelli, W.J. (Ed.) Computer Security in the Age of Information. Proceedings of the Fifth IFIP International Conference. North-Holland: Elsevier Science Publishers, 83 – 85.

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

Maslow, A. (1970). Motivation and Personality. New York: Harper and Row.

McCoy, C. and 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: Gower.

McLeod, G. (2003). Learning Theory and Instructional Design. Learning Matters 2, 35 – 43. Available: http://courses.durhamtech.edu/tlc/www/html/Resources/learningmatters/learningtheory.pdf. 1.4.2009

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.

Miller, J. (2001). The Holistic Curriculum. 2nd edition. Toronto: OISE Press.

Miller, J.P. and Seller, W. (1985). Curriculum. Perspectives and Practice. Toronto: Copp Clark Pitman.

Mitnick, K.D. and Simon, W.L. (2002). The Art of Deception. Controlling the Human Element of Security. Indianapolis: Wiley.

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. The Scandinavian Journal of Psychology, 43, 385 – 395.

National Institute of Standards and Technology (NIST) (1996). Technology Administration, U.S. Department of Commerce, An Introduction to Computer Security: The NIST Handbook, NIST Special Publication 800-12. Available: http://all.net/books/standards/NIST-CSRC/csrc.nist.gov/publications/nistpubs/index.html. 10.3.2009.

Nosworthy, J.D. (2000). Implementing Information Security in the 21st Century – Do You Have the Balancing Factors? Computers and Security, 19(4), 337 – 347.

Olnes, J. (1994). Development of Security Polices. Computers & Security, 13, 628 – 636.

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. and Thorpe, R. (1998). The Manager as a Practical Author of Learning. Career Development International, 3(7), 300 – 309.

Peltier, T. (2000). How to Build a Comprehensive Security Awareness Program. Computer Security Journal, 16(2), 23 – 32.

Piaget, J. (1985). The Equilibration of Cognitive Structures: The Central Problem of Intellectual Development. Chicago: University Chicago Press.

Piaget, J. (1963). The Origins of Intelligence in Children. New York: Norton.

Puhakainen, P. (2006). A Design Theory for Information Security Awareness. Ph.D. Thesis, University of Oulu, Finland.

Reigeluth, C.M. (1983). Instructional Design: What Is It and Why Is It? In Reigeluth, C.M. (Ed.) Instructional-Design Theories and Models. An Overview of Their Cultural Status. Hillsdale (NJ): Lawrence Erlbaum Associates, 3 - 36.

Robinson, D.G. and Robinson J.C. (1989). Training for Impact. How to Link Training to Business Needs and Measure the Results. San Francisco: Jossey-Bass.

Rochelle, J. (1992). Learning by Collaborating: Convergent Conceptual Change. Journal of the Learning Sciences. 2(3), 235 – 276.

Rochelle, J. and Teacley, S.D. (1995). The Construction of Shared Knowledge in Collaborative Problem Solving. In O´Malley, C.E. (Ed.) Computer-Supported Collaborative Learning. Berlin: Springer, 69 – 97. Available:

Rogers, C. (1969). Freedom to Learn. Columbus (OH): Charles Merrill.

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. and Fischer, L.F. (2006). Security Education, Awareness and Training. From Theory to Practice. Burlington: Elsevier Butterworth-Heinemann.

Ross, O.T. (2002). Self-Directed Learning in Adulthood: A Literature Review. Available: http://eric.ed.gov/ERICDocs/data/ericdocs2sql/content_storage_01/0000019b/80/19/ba/6b.pdf. 31.3.2009

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

Ryan, J.J.C.H. (2003). Teaching Information Security to Engineering Managers. Proceedings of 33 rd ASEE/IEEE Frontiers in Education Conference, 1 – 6.

Salomon, G. and Perkins, D.N. (1998). Individual and Social Aspects of Learning. Review of Research in Education, 23(1), 1 – 24.

Sasse, 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. and Huang, H. (2008). 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. and Heikka, J. (2006). A Design Theory for Secure Information Systems Design Methods. Journal of the Association for Information Systems, 7(7), 725-770.

Skinner, B.F. (1968). The Technology of Teaching. East Norwalk: Appleton-Century-Crofts.

Springer, L., Stanne, M.E., and 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). IS 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: Yale University Press.

Straub, D.W. and 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. and Streufert, S. (1992). Conceptual/Integrative Complexity. In Smith, C.P. (Ed.) Motivation and Personality: Handbook of Thematic Content Analysis. Cambridge, England: Cambridge University Press, 393 – 400.

Telders, E. (1991). Security Awareness Programs: A Proactive Approach. Computer Security Journal, 7(2), 57 – 64.

Tennant, M. (1997). Psychology and Adult Learning. London: Routledge.

Thomson, K.L., von Solms, R., and Louw, L. (2006). Cultivating an Organisational Information Security Culture. Computer Fraud & Security, Issue 10, October 2006, 7 – 11.

Thomson, M.E. and 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

Tuomi-Gröhn, T. and Engeström, Y. (2003). Conceptualizing Transfer: From Standard Notions to Developmental Perspectives. In Tuomi-Gröhn, T. and Engeström, Y. (Eds.) Between School and Work. New Perspectives on Transfer and Boundary-Crossing. Advanced in Learning and Instruction Series. Amsterdam: Pergamon, 19 – 38.

Vygotsky, L. (1978). Mind in Society: The Development of Higher Psychological Processes. In Cole, M., John-Steiner, V., Scribner, S. and Souberman, E. (Eds.) Cambridge (MA): Harvard University Press.

Wasson, B. (1996). Instructional Planning and Contemporary Theories of Learning: Is This a Self-Contradiction? In Brna, P., Paiva, A. and Self, J. (Eds.) Proceedings of the European Conference on Artificial Intelligence in Education. Lisbon: Colibri, 23 – 30.

Weick, K. (1979). The Social Psychology of Organizing. 2nd edition. Reading (MA); Menlo Park, (CA); London; Amsterdam; Don Mills, Onterio; Sydney: Addison Wesley Publishing Co.

Weil, S. and McGill, I. (1989). Making Sense of Experiential Learning. Milton Keynes: Open University Press.

Wilson, M., de Zafra, D.E., Pitcher, S.I., Tressler, J.D. and Ippolito, J.B. (1998). Information Technology Security Training Requirements: A Role- and Performance-Based Model. NIST Special Publication 800-16. Available: http://all.net/books/standards/NIST-CSRC/csrc.nist.gov/publications/nistpubs/index.html. 10.3.2009.

Wilson, M. and Hash, J. (2003). Building an Information Technology Security Awareness and Training Programme. NIST Special Publication 800-50. Available: http://all.net/books/standards/NIST-CSRC/csrc.nist.gov/publications/nistpubs/index.html. 10.3.2009

Yilmaz, K. (2008). Constructivism: Its Theoretical Underpinnings, Variations, and Implications for Classroom Instruction. Educational Horizons, 86(3), 161 – 172.

APPENDIX 1

With respect to meta-orientations of curriculum design, the results review of IS security training approaches are demonstrated in Tables 3 – 6. In Tables, the term inclusive means that such IS security training approaches represent all the meta-orientations and corresponding learning paradigms with respect to the handled feature of the meta-orientation. In turn, the term exclusive indicates that those approaches contain only one kind of meta-orientation and corresponding learning paradigm with respect to the handled feature of the meta-orientation.

The first pedagogical requirement for future IS security training is that the explicit psychological context, the learning theory behind the training approach, must be based upon the group-oriented theoretical approach of teaching and learning, which directs the training activities (Fardanesh 2006; Gibson 2001; Hinsz et al. 1997). Only six of 32 IS security approaches apply any learning theories. However, such theoretical foundation is invaluable for effective training (e.g., McLeod 2003). These six approaches consider learning only from the viewpoint of an individual learner: one approach is placed exclusively under the transaction orientation (cognitivism), and five approaches are placed under the transformation orientation (constructivism). Because none of IS security training approaches is based on social constructivist learning theory, IS security training approaches are not effective and pedagogically meaningful educational practices in this sense (see Table 3).

Table 3. The psychological context of learning in the existing IS security training approaches.

<table>
<tr><td colspan="4">Psychological context of learning within the IS security approaches</td></tr>
<tr><td colspan="4">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 2001b), 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 (Shaw et al. 2008)</td></tr>
<tr><td>Transmission</td><td colspan="2">Transaction</td><td>Transformation</td></tr>
<tr><td>Behaviourism (0)</td><td>Cognitivism (1)</td><td>Constructivism (5)</td><td>Social constructivism (0)</td></tr>
<tr><td colspan="4">Inclusive (0)
-</td></tr>
<tr><td>Exclusive (0)
-</td><td>Exclusive (1)
Cognitive processing approach
(Puhakainen 2006)</td><td>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)</td><td>Exclusive (0)
-</td></tr>
</table>

The second pedagogical requirement for future IS security training is that the content of training must be community-centred, i.e., based on collective experiences and perspectives of the learners (e.g., Kolb 1984; Gibson 2001), which is considered as a feature of effective IS security training. 24 of 32 IS security training approaches include subject-centred contents typical to behaviourism. In these approaches, the content of training is presented without connections to learning processes, problem solving, or experiences of the learners in the training situation. Further, 18 of the

approaches include process- and/or problem-centred content of training, which is typical to the transaction orientation and also cognitivism, which emphasizes integration of new knowledge with existing knowledge structures or cognitive problem solving and analysis (e.g., Palincsar 1998, 347). Process-centred contents take into account the cognitive processing of information (e.g., activation of learners' prior knowledge before a training session, engagement of analogies, case studies, or stories). Problem-centred contents emphasize cognitive problem solving tasks (e.g., analysis and synthesis) as a part of training. Finally, 23 approaches include learner-centred contents. In these approaches, the content of training is partly created during a training session according to the learners' experiences and choices, which is typical to the transformation orientation and constructivism. Only two of these twenty-three approaches also include community-centred contents typical to 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 4).

Table 4. The content of training in the existing IS security training approaches (Continues on the following page).

Content of training within the IS security training approaches			
Transmission	**Transaction**	**Transformation**	
Behaviourism (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 2001b) *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)
Behaviourism + cognitivism (2) *Communication oriented approach* (Desman 2002) *Promotional approach* (Rudolph *et al.* 2002)			
	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.* 2008)		

Behaviourism + constructivism (3) *Constructive instruction approach* (Heikka 2008) *Operational controls approach* (NIST 1996) *Strategic approach* (Wilson & Hash 2003)		Behaviourism + 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 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), which are preferred for effective IS security training. With respect to teaching methods, 24 approaches represent the transmission orientation and behaviourism. These teaching/learning activities facilitate teachers to transmit knowledge and learners to receive knowledge or external reinforcement of their behaviour. Nine of 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, teaching methods emphasize the opportunities to reflect on own experiences, authentic problem-solving, or both. Along with individual activities, 14 approaches representing the transformative teaching methods also include solitary references to the 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 character of learning. Therefore, teaching methods in these cases represent constructivism. Only two approaches also include collaborative teaching methods that emphasize the communal character of learning. These two are the cognitive processing approach of Puhakainen (2006) that seeks the communal relevance of a learning task through a team rehearsal and the social psychological recommendations approach of Kabay (2002) that tries to reveal corporate culture and social views of the reality through discourse. (See Table 5.)

Table 5. Teaching methods in the existing IS security training approaches (continues on the following page).

Teaching method within the IS security training approaches			
Transmission	**Transaction**	**Transformation**	
Behaviourism (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 2001b) *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.* 2008)	Exclusive (0)
Behaviourism + cognitivism (1) *Academic environment approach* (Kajava & Siponen 1997)			

Behaviourism + 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)		Behaviourism + 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 behaviourist 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 to conduct evaluation practices. Hence, these conversational evaluation practices are characterised to be informal, experimental, and/ or open-ended. Typical evaluations include self-assessments, interviews, and feedback during the instruction. In addition, along with evaluation of 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 (cognitive processing approach of Puhakainen (2006)), role-play scenarios and focus groups (andragogical approach of Herold (2005)), and group interviews (strategic approach of Wilson and Hash (2003)). (See Table 6.)

Table 6. Evaluation of learning in the existing IS security training approaches (Continues on the following page).

<table>
<tr><td colspan="4">Evaluation of learning within the IS security training approaches</td></tr>
<tr><td colspan="4">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 2001b), 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)</td></tr>
<tr><td>Transmission</td><td colspan="2">Transaction</td><td>Transformation</td></tr>
<tr><td>Behaviourism (17)</td><td colspan="2">Cognitivism (5)</td><td>Constructivism (15)</td><td>Social constructivism (3)</td></tr>
<tr><td colspan="4"><u>Inclusive (2)</u>
Competence approach (Wilson et al. 1998)
Hypermedia instruction approach (Shawn et al. 2008)</td></tr>
<tr><td><u>Exclusive (5)</u>
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)</td><td><u>Exclusive (0)</u></td><td><u>Exclusive (4)</u>
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)</td><td><u>Exclusive (0)</u></td></tr>
</table>

Behaviourism + cognitivism (2) *Constructive scenario approach* (Biros 2004) *Operational controls approach* (NIST 1996)			
	Cognitivism + constructivism (1) *Pedagogical game approach* (Greitzer *et al.* 2007)		
Behaviourism + 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)		Behaviourism + 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)

芽|Sprouts

Working Papers on Information Systems | ISSN 1535-6078

Office:
Sprouts
University of Amsterdam
Roetersstraat 11, Room E 2.74
1018 WB Amsterdam, Netherlands
Email: admin@sprouts.aisnet.org

芽|Sprouts