6-18-2022

ARE YOU AWARE OF YOUR COMPETENCIES? – THE POTENTIALS OF COMPETENCE RESEARCH TO DESIGN EFFECTIVE SETA PROGRAMS

Florian Rampold
University of Goettingen, florian.rampold@uni-goettingen.de

Florian Schütz
University of Goettingen, florian.schuetz@uni-goettingen.de

Kristin Masuch
University of Goettingen, kristin.masuch@uni-goettingen.de

Patricia Köpfer
University of Hohenheim, patricia.koepfer@uni-hohenheim.de

Julia Warwas
University of Stuttgart-Hohenheim, julia.warwas@uni-hohenheim.de

ARE YOU AWARE OF YOUR COMPETENCIES? – THE POTENTIALS OF COMPETENCE RESEARCH TO DESIGN EFFECTIVE SETA PROGRAMS

Research Paper

Rampold, Florian, University of Goettingen, Goettingen, Germany, florian.rampold@uni-goettingen.de

Schütz, Florian, University of Goettingen, Goettingen, Germany, florian.schuetz@uni-goettingen.de

Masuch, Kristin, University of Goettingen, Goettingen, Germany, kristin.masuch@wiwi.uni-goettingen.de

Köpfer, Patricia, University of Hohenheim, Stuttgart, Germany, patricia.koepfer@uni-hohenheim.de

Warwas, Julia, University of Hohenheim, Stuttgart, Germany, julia.warwas@uni-hohenheim.de

Abstract

Since the late 1990s, security education training and awareness (SETA) programs have become commonplace. Despite extensive research into the effective design of such programs and factors influencing compliance behavior, SETA programs tend not to be as effective as they should be. In order to tailor learning content as closely as possible to individual needs, vocational education relies on the modeling and measurement of competencies. We argue that this existing knowledge can be transferred to the information security domain. Therefore, we introduce a competence model from vocational education and consider it in the context of the information security domain. Subsequently, we conduct a structured literature review on conceptualization and effective SETA design and investigate to what extent the competence dimensions from vocational education are already considered in the SETA literature. Our results indicate that competence research can make an important contribution to adapting SETA programs to individual situational actions.

Keywords: SETA, Security Education Training and Awareness, Competence Model, Vocational Education

1 Introduction

Nowadays, many organizations face the challenge of protecting their security-related assets due to sophisticated cyber security attacks (Ahmad *et al.*, 2020). The human factor is often seen as the weakest link in the information security chain (Abawajy, 2014). This highlights the need for employees who are aware of potential security threats and have comprehensive information security competencies. To overcome this challenge, security education and training awareness (SETA) programs have been acknowledged as the key for employees' security-related behavior (Posey *et al.*, 2015; Thomson and Von Solms, 1998; Tsohou, Karyda, Kokolakis, *et al.*, 2015). In the first place, SETA is applied in organizations to build common information security knowledge and awareness

which is then utilized to develop skills and a deeper understanding of fundamental security concerns (Cram *et al.*, 2019; D'Arcy *et al.*, 2009; Furnell *et al.*, 2002). While its origin goes back to the late 1990s, it has become an important strategical concept of most organizations to secure information assets and promote security governance (D'Arcy and Hovav, 2009; Hu *et al.*, 2021; Posey *et al.*, 2015). However, security incidents and data breaches are rising, causing tremendous economic damage and information theft (ENISA, 2021). Both practice and recent research findings support that SETA programs tend to be less efficient than they are supposed to be (Alshaikh *et al.*, 2020; Hu *et al.*, 2021; Kirova and Baumoel, 2018; Tsohou, Karyda, Kokolakis, *et al.*, 2015). Recent literature has identified two main reasons for this circumstance.

The first research stream identifies non-compliant behavior and attitude of recipients of SETA campaigns as the main reason for failure. Hence, many previous research papers analyzed influencing factors of security-related behaviors to provide stakeholders with knowledgeable guidance (Albrechtsen and Hovden, 2010; Herath *et al.*, 2018; Hwang *et al.*, 2017; Jenkins *et al.*, 2013). In this context, Alshaik et al. (2020) argue the relevance of systematic guidelines and grounded behavioral theories to be crucial to steering the behavioral change of employees. Thus, several research papers examine theoretical foundations that promote strategic decisions supporting employees' attitudes towards security compliance (Kajzer *et al.*, 2014; Karjalainen and Siponen, 2011). The second research stream perceives the limited success of SETA programs in one-size-fits-all approaches which are not tailored to job-specific and qualification-related needs of individual learners (Hu *et al.*, 2021; McCoy and Fowler, 2004). This omits, in particular, the fact that employees exhibit different behaviors in dealing with the knowledge they have learned. Thus, SETA programs are differently suited for various employees and sometimes lead to better and worse security behavior. Although various research papers have identified that SETA programs should be tailored to the target audience (McCoy and Fowler, 2004) and initial knowledge (Caldwell, 2016; Peltier, 2005) limited research exists that proposes guidelines on how to implement SETA programs that consider the individual human capabilities and situational recommendations for action. This idea can be extended by the field of vocational education, where learning processes play a crucial role, and situational action is considered one of the key concepts for training competent people, especially employees. Several research studies in the vocational education domain have targeted this challenge by drawing on competence modeling and measuring (Klotz and Winther, 2016; Kunter *et al.*, 2009; Winther, 2010). In this context, Weinert's (2001) concept of professional action competence has gained acceptance for modeling and measuring competence. Following Weinert (2001), competence encompasses […] "cognitive *abilities* and *skills* available to or learnable by individuals to solve specific problems, and the associated *motivational* and *social* dispositions and skills to apply the problem solutions successfully and responsibly in variable situations." Hence, competence describes a valid concept defining prerequisites that are needed to perform a specific profession. The research on information security awareness has already identified basic constructs of vocational education *(awareness, knowledge, skills, attitude, and behavior)* that should contribute to the development of responsible employees. However, there is a lack of holistic consideration and implementation of the concepts of vocational competence, which could be an explanation for the failure of SETA programs.

In vocational education research, it is emphasized that it is important to address competencies comprehensively because competence is viewed as an overarching construct that has multiple dimensions and facets. Consequently, within this domain, it is distinguished between the competence to conceptually grasp given situations of action and the competence to act adequately in a specific situation (Winther, 2010). While SETA research focuses on behavioral changes in employee compliance and is predominantly concerned with motivational aspects, vocational competence includes conceptual, procedural, and utilizationalal dimensions (Greeno *et al.*, 1984). Therefore, we deem a holistic approach, which draws on competence, to be important and shed light on a multi-perspective of why the effectiveness of SETA programs is constrained in practice. This study, therefore, addresses the following research question:

How can knowledge from vocational competence research contribute to identifying and overcoming the inefficiency of SETA programs?

We, therefore, introduce a competence model from the vocational education domain and apply relevant constructs to the information security domain. We then conduct a structured literature review following Webster and Watson (2002) and vom Brocke et al. (2015) on SETA design recommendations and classify them towards dimensions of competence research. Therefore, we searched in four prominent databases of IS research (AISeL, EbscoHost, Elsevier ScienceDirect, ACM Digital) and identified 944 research papers. Based on the application of inclusion and exclusion criteria, our final result set yielded 57 relevant research articles. By doing so, we contribute to a theory-informed and conceptualized development process of SETA programs. Moreover, we deduce implications for literature and practice and highlight the importance of developing a holistic competence model that considers the individual necessities of information security. The paper is structured as follows: Section two provides foundations of the theoretical background such as previous SETA literature and vocational education competence research. In section three, we deduce our methodical research approach. Finally, we provide an in-depth analysis of SETA literature focusing on competence modeling and discuss the implications of our work.

2 Theoretical Background

2.1 SETA Research

Most practitioners and researchers have acknowledged the necessity of managing information security in organizations (Hu *et al.*, 2021). In general, the acronym SETA is composed of three standalone concepts, including security education, security training, and security awareness (Hu *et al.*, 2021). As Hu et al. (2021) conclude in their structured literature review, these concepts are mixed and unclear. Therefore, we refer to their elaborated working definition stating that SETA can be understood as continued engagement of organizations to raise employee security consciousness and provide general security knowledge and skills to address security threats and risks (Hu *et al.*, 2021).

Previous literature has addressed two superordinate fields of research in the context of SETA programs. The first major research stream has investigated influencing factors for security-related behavior of employees on the individual level (Albrechtsen and Hovden, 2010; Cram *et al.*, 2019; D'Arcy *et al.*, 2009; Herath *et al.*, 2018; Hwang *et al.*, 2017). These studies mainly analyze the effectiveness of SETA programs in terms of behavioral change and attitudes that drive security compliance. In these terms, a wide range of empirical theories has been applied to examine why employees behave non-compliant. Some exemplary theories that are applied to explain security behavior are the protection motivation theory (Dhillon *et al.*, 2020; Posey *et al.*, 2015), theory of planned behavior (Jenkins *et al.*, 2013), theory of reasoned action, and deterrence theory (D'Arcy *et al.*, 2009; Herath *et al.*, 2018). An extensive review of these theories can be found in Hu et al. (2021) and Cram et al. (2019). A meta-analysis by Cram et al. (2019) suggests that attitude, personal norms, ethics, and normative beliefs have an increasingly high impact on security policy compliance. On the contrary, punishment and rewards are relatively ineffective to contribute towards compliant employee behavior. The second research stream concentrates on the conceptual foundation and/or effective design of SETA programs on an organizational level (Tsohou, Karyda, Kokolakis, *et al.*, 2015). This includes guidance on specifying the contents, external and internal factors of success, and the delivery mode (Hansche, 2001; Karjalainen and Siponen, 2011; May, 2008; Puhakainen and Siponen, 2010). In the following, we present some of the most important findings. Puhakainen and Siponen (2010) and Hansche (2001) emphasize the need for top management support. They conclude that management support is crucial through various internal organizational channels (Puhakainen and Siponen, 2010). McCrohan et al. (2010), Goode et al. (2018) and Tse et al. (2013) work out the necessity of providing comprehensive and fitted contents. Several studies could also show the need to consider different training durations (Albrechtsen and Hovden, 2010; Thomson and Von Solms, 1998). Abawajy (2014) compares different modes of SETA delivery and derives that different types of delivery methods (text-based, video-based, game-based) should be combined for maximized success. A minor stream of SETA research has also dealt with concepts that target security competence. Lin and Kunnathur

(2013) build a theory of end-user information security competence to shed light on how to produce competent security end-users. Their roadmap considers ethics and perceptions, knowledge and skills, and behavior which eventually lead to compliant information security behavior. Similarly, Kaur et al. (2021) examine the effect of enhanced security competence on information security job performance. They differentiate between two dimensions of competence: tacit and explicit knowledge. Another competence-oriented approach is utilized by Pike (2021). The author introduces competency-based education (CBE) to the IS security domain. CBE enables conveying information based on the individual capabilities of learners. In terms of security competence, this information includes knowledge, skills, and abilities defined by the NIST framework. Tarwireyi et al. (2011) develop a competence measurement questionnaire for students to choose secure passwords. Their main objective is to investigate different levels of competence for varying terms of study.

These research streams inform our paper in several aspects. First, it becomes evident that human behavioral aspects are relevant to implementing SETA programs successfully. In particular, the following important drivers are identified here and should not be ignored: attitude, personal norms, and normative beliefs. In addition, there are already approaches that address the conceptual and design level of SETA programs and attribute great importance to them. However, when looking at this research, it becomes clear that organizational factors for effective design are researched, but concepts for building effective SETA programs are missing. Although a minor research stream considers security competencies, the term competence is either not regarded as a multidimensional construct or does not explain how competence can be acquired to behave IT-secure. Tarwireyi et al. (2011) conceptualize a competency-based questionnaire that mainly covers declarative knowledge of participants. Kaur et al. (2021) regard tacit and explicit knowledge as competence dimensions which are both forms of declarative competence without relation to the situational requirements for action. We, therefore, study the fundamentals of the vocational education domain, which has been proven to be suitable for competence modeling in different application domains (Achtenhagen and Winther, 2008; Winther, 2010).

2.2 Competence Modeling

In recent years, the term competence has become widely accepted in discussions about the goals and outcomes of professional learning processes (Winther, 2010). Depending on the social system (politics, economy, science), the concept of competence is associated with different notions of constructs (Winther, 2010). Consequently, there exists no general definition of competence (Winther, 2010). Since the domain of vocational education is highly related to orientational action taking in vocational learning contexts (Winther, 2010), which also relates to learning and education processes conveyed by SETA programs, we refer to the most applied definition in the domain. Following this definition, we define competence as [..] “the cognitive abilities and skills available to or learnable by individuals to solve specific problems and the associated motivational and social dispositions and skills to use the problem solutions successfully and responsibly in variable situations” (Weinert, 2000). Hence, the competence definition applied in this work is highly contextual, focusing on how competence is learnable. Moreover, competence is understood as contextual dispositions related to specific situations and action requirements (Winther, 2010). Following this argumentation, successful action taking requires situational knowledge. These contextual dispositions have been transferred to multiple elemental parts of competence by Greeno et al. (1984). The authors differentiate between three cognitive dimensions of competence: *conceptual, procedural, and utilizational* competence. Conceptual competence can be understood as [...] “rule-based, abstract knowledge in a domain, which is translated into a specific plan of action that becomes effective in the specific action. A central element of this competence component is learned rules, formed according to cognitive assumptions depending on prior knowledge” (Winther, 2010). Instead, procedural competence [..] “refers to the procedures and skills that are needed to apply conceptual knowledge in specific situations of action” (Winther, 2010). Finally, utilizational or interpretational competence [..] “comprises the ability to recognize situations for action in a regulative way, i.e. to assess situational features and individual

target features and relate them to each other. This competence component thus covers the interaction with the context and the construction of the situation as an evaluation process“ (Winther, 2010).

The argumentation following Greeno et al. (1984) indicates that competence is highly dependent on context. Winther (2010) states that human action is influenced by a specific situation in a particular context. Hence, they conclude that competence always involves motivational and volatile efforts to cope with the confronted requirements of action. The specific situational action needs to be analyzed regarding necessary processes and skills required in multiple varying types of vocational action taking (Kunter *et al.*, 2009) to understand how competence can be built. Therefore, the vocational education domain defines models that conceptualize different competence dimensions. One promising model for IS domain is the structural vocational competence model by Achtenhagen & Winther (2008) (Figure 1).

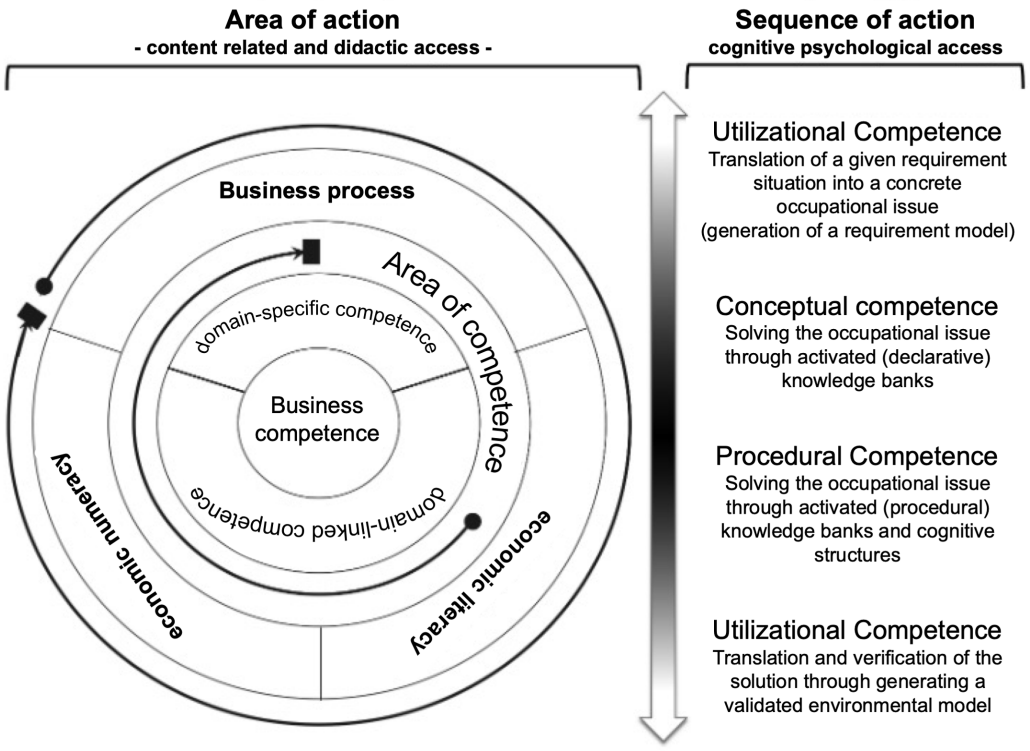

Figure 1. Vocational Education Competence Model (Achtenhagen and Winther, 2008)

Its main idea is to differentiate between areas of actions on the one hand and sequences of actions on the other hand. Regarding areas of action, Achtenhagen and Winther (2008) distinguish between domain-linked and domain-specific competence. Domain-linked competencies refer to applicable general competencies that support handling requirements within the domain. The vocational education domain includes the domain-linked areas of economic literacy and economic numeracy, which represent the general knowledge and skills to pursue a vocational or commercial profession successfully. Whereas economic literacy covers the ability to comprehend and participate in economic contexts, economic numeracy captures basic mathematical knowledge and skills of concrete business processes (Klotz and Winther, 2016; Winther, 2010). Next to domain-linked competencies, domain-specific competencies play an important role in terms of the proposed competence model. Domain-specific competence refers to concrete situational actions required in specific job-related professions. Thus, they are directly related to business processes. A business process is defined as job-specific situational action, characterized by its level of requirements and options for action taking (Winther, 2010). In terms of information security, such a business process can be understood as a particular security incident requiring a situational response in the personal working environment (Winther,

2010). Both the domain-linked and domain-specific competence are considered to have sub-components (conceptual, procedural, utilizational competence), which come to action when a particular issue in the working environment arises (Winther, 2010). As a starting point, situational requirements need to be recognized, including possible solutions. This is a crucial step to fully react in a meaningful way towards the situation. The domain-linked and specific declarative knowledge (conceptual competence) needs to be applied considering the general and functional, learned skills and procedures (procedural competence). In the last step, the solution to overcome the identified problem has to be evaluated in terms of the situational requirements. This step, therefore, relates the initial requirement set with the solution space and requires an evaluation and interpretation process (utilizational competence) (Winther, 2010).

This research informs our study in multiple aspects. First, the vocational education domain highlights the importance of considering different dimensions of competence. Second, these are interrelated and take varying situational actions into account. This enables the design of SETA programs beyond one-size-fits-all approaches that target the individual situation and job-specifics. The model of commercial education competence covers both the three dimensions applied as a sequence of action for solving occupational issues and the specific area of action. Therefore, we argue that the competence model by Achtenhagen and Winther (2008) can be applied to the IS security domain. Each business process in the model is understood as a possible security incident, and the sequence of action with its three competence dimensions is contextualized to IT-secure behavior. Since the situational context, including different options for action taking, is strongly emphasized to develop vocational competence, we stress the need to analyze the perception of competence in SETA literature.

3 Methodology

3.1 Literature Search

In order to get a broad overview of guidelines on effective SETA design and conceptualization, a structured literature review is conducted that follows the approach of Webster and Watson (2002) and vom Brocke et al. (2015). This approach aims to identify current state-of-the-art research in the information security awareness domain. The result of a literature review is strongly dependent on the actual search process. Vom Brocke et al. (2015) state that the literature search process in information systems (IS) research could often be complex and overwhelming due to a vast research foundation. Several steps have to be considered, such as the applied search process, data sources, the type of coverage, and the search technique (vom Brocke *et al.*, 2015). Since the research topic follows a clear structure, a sequential approach has been chosen. This fact implies that the literature search is defined at the beginning of the review and not repeated iteratively (vom Brocke *et al.*, 2015). Data sources have been selected for the literature search in the next step. As vom Brocke et al. (2015) elaborate, different types of available data sources exist. As a result, several prominent IS research and economics databases have been selected. These include Elsevier ScienceDirect, EbscoHost, ACM Digital Library, AISeL. In particular, the search focuses on seminal works in the field of information security awareness. Following vom Brocke et al. (2015), the most common approaches combine keyword searches with forward and backward searches. Both can be applied to extend the result of research papers that have been collected in terms of keyword search. According to vom Brocke et al. (2015), the objective of the backward approach is to identify as many relevant papers from the list of references that result from publications of the keyword search. In contrast, the forward approach aims to find papers that have cited other related papers resulting from the search process (vom Brocke *et al.*, 2015; Webster and Watson, 2002). As this literature review aims to give a comprehensive overview covering state-of-the-art solutions in terms of recommendations for effective SETA design, several criteria have been identified that narrow the literature search process to a decent degree. First, the publication date is between 1998 and 2021. Second, the search terms are part of the abstract, keywords, or title. Third, the publication was made in a peer-reviewed journal or conference to ensure a high standard of scientific quality. Lastly, the language of the research paper is English. Since

selecting the search parameters has a crucial influence on the outcome of the literature search, the combination of various search terms has been tested among different databases before the actual keyword search started (vom Brocke *et al.*, 2015). The final search string consists of a combination of SETA-related terms together with a focus on security competence research. The forward search resulted in 944 potential publications. After gathering the results from the mentioned databases, the outcome was analyzed by title, abstract, and screening of the paper's main contributions to filter for publications covering suggestions for SETA design, implementation, development, or programs. By doing so, the data set diminished to 160 publications. Subsequently, a backward search ensured that relevant literature for the search process but not identified through the keyword search was added to the result set. In this process, a total of 18 additional papers were identified. These mainly emerge from an existing literature review of Hu et al. (2021). Lastly, we defined exclusion criteria only to consider publications relevant to our analysis. We excluded publications if they met one of the following criteria. First, we excluded empirical research that targets the impact of SETA programs on employees' compliance behavior. Second, technical publications without conceptual or design focus have been sorted out. In total, the literature search process resulted in 57 relevant research articles that have been included in the analysis of approaches covering conceptualization and design of SETA programs. The overall search process is summarized in Figure 2.

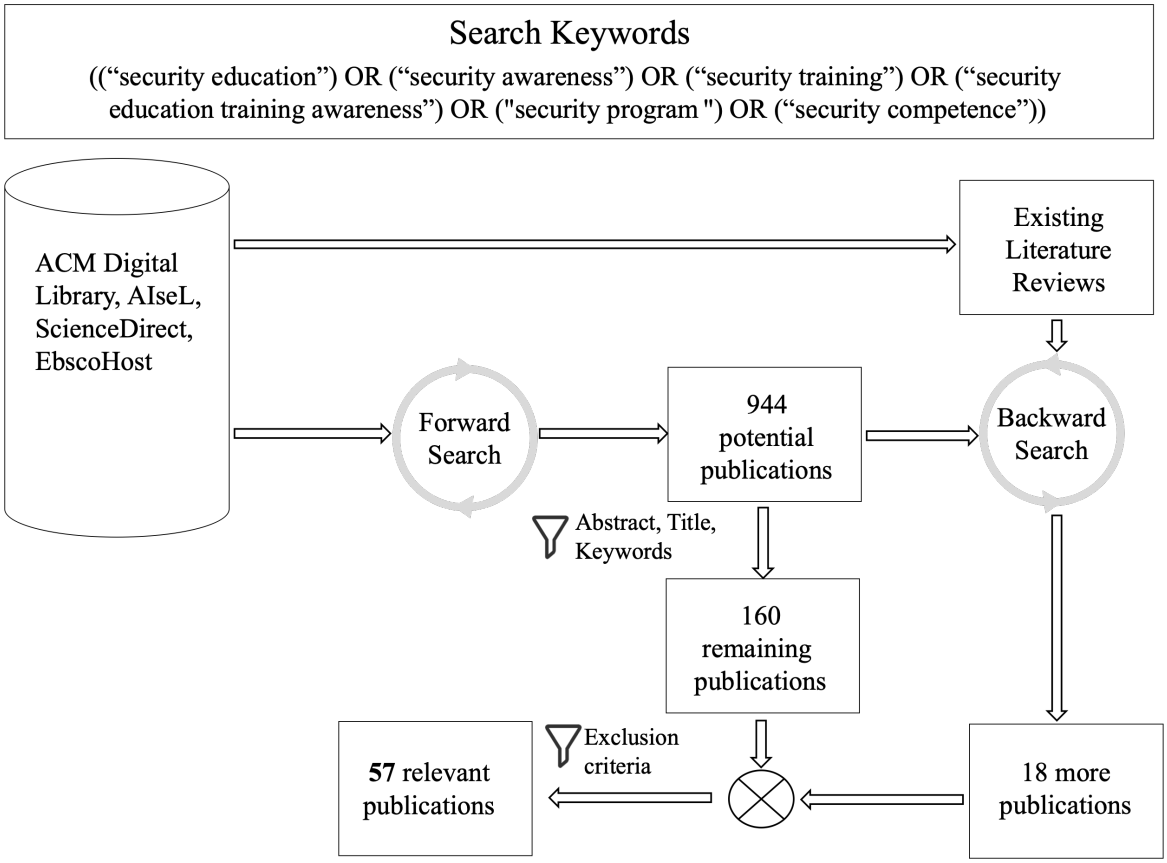

Figure 2. Literature Search Process

3.2 Coding Process

After the relevant papers were collected and identified, they were coded by two independent researchers. This involved analyzing the SETA literature regarding its perception and application of competence dimensions. All 57 research papers were categorized according to competence dimensions in vocational education. Referring to Greeno et al.'s (1984) definition and Winther's (2010)

interpretation given in chapter two, we classified competence dimensions. Table 1 provides examples from the SETA studies to illustrate the coding process. As it can be observed, we took the definition of each competence dimension as a reference to analyze conceptualization and design SETA literature.

Competence Dimension	Examples
Conceptual Competence	"Security awareness contains two equally important pieces. The first piece is the dissemination of accurate, current and appropriate knowledge of policy to individuals."(Wolf et al., 2011)
	„Another explanation for the lack in perceived responsibilities could be missing knowledge about the content of the ISP." (Bauer et al., 2017)
Procedural Competence	"One of the fundamental reasons for this is that people are not naturally equipped with the skills, instincts and behaviours required to ensure appropriate protection and so need support in order to help them understand what they should be doing and learn how to do it." (Furnell and Vasileiou, 2017)
	"Therefore, when individuals are aware of their ability to control security threats by using strong passwords, it is hypothesized that they will be more likely to use strong passwords than those individuals who are not aware of their ability to do so."(McCrohan et al., 2010)
Utilizational Competence	"When it is expected from someone to apply knowledge in the information security area, the type of problem should be known in order to execute the required procedures and to choose the best strategy for solving the problem." (Kruger et al., 2011) "People should be able to implement expertise in different contexts." (Kruger et al., 2011)
	[..] "scenario based learning: helps the participants think and suggest possible solutions to particular situations [..]" (Yasin et al., 2019)

Table 1. Examples from the SETA studies illustrate the coding process.

4 Literature Analysis and Synthesis

4.1 Classification of Competence Dimensions

The following section deals with the result of the literature search. As already stated, we categorized SETA literature that targets the conceptualization and effective design on their perception of the development of competencies. No research paper frames competence dimensions when addressing necessary concepts that contribute to effective training and designs. To better understand recommendations for effective SETA design, we created a concept matrix covering each combination of addressed competence dimensions by previous SETA literature (Table 2). Nearly all papers (57 publications) identified the need to establish conceptual competence by referring to security training which provides general and content-specific knowledge. Interestingly, if a paper identified procedural or utilizational competence to be relevant, it also addressed the conceptual competence dimension. In fact, a few research papers stressed the importance of providing this knowledge based on particular roles and responsibilities of employees within the organization (Amankwa *et al.*, 2014; Johnson, 2006; Katsikas, 2000; Stewart and Lacey, 2012; Tse *et al.*, 2013). According to Winther (2010) conceptual competence requires knowledge and learned rules to be specific to situational requirements. However, this fact is left untouched by the majority of researchers.

Nevertheless, a few papers exclusively acknowledged parts of conceptual competence to be relevant. This includes a scope of research papers (12 publications) giving relevant recommendations for effective SETA design and knowledge acquisition but leaving out options on how to build skills and evaluation processes for situational action-taking. May (2008), for example, gives strong recommendations on the design of information security awareness programs, such as making them

personal, short, and interesting. Stewart and Lacey (2012) highlight the importance of focusing on pre-existing beliefs, cultural factors, and the type of audience when designing SETA programs. Bauer et al. (2017) emphasize the reason for the lack of perceived responsibilities in missing knowledge about SETA content. Besides the conceptual competence dimension, acknowledgment of procedural competence has been a crucial subject of previous SETA literature. Many researchers addressed the conceptual dimension in accordance with the procedural component (21 publications). Most research papers refer to the development of skills as vital to cope with security threats (see Table 2). However, current research lacks in explaining how skills can be formed and if developed skills should vary in different situations of action. Furnell and Vasileiou (2017) argue that security training is necessary to produce security skills and competencies, whereas Wu et al. (2012) state that SETA programs need to go beyond creating procedural knowledge to impact behavioral change.

From a perspective of the vocational education domain, utilizational competence has two facets. Firstly, it is utilized to recognize the specific situational requirements in a problem context to construct a model of the environment. Secondly, it is applied to evaluate and translate the solution space after conceptual and procedural knowledge have been deployed to deal with an occupational issue (Winther, 2010). Therefore, we analyzed SETA literature towards both individual facets. If a paper addresses the need to (1) convey topics that are adapted to job roles or responsibilities and/or (2) understand the learned practices and apply them in the profession, we identified the utilizational competence dimension as being met to a limited extent. This arises from two reasons: First, (1) implies that varying situational actions are involved within the evaluation process of countermeasures when employees are faced with security incidents. However, we argue that situational action-taking also varies within different job roles and responsibilities. Second, (2) acknowledges the importance of applying knowledge and skills in a specific profession but leaves out the situational context. Following vocational education research, application and evaluation processes are always related to situational requirements, demanding situational actions (see section 2.2).

Publications that fall under this classification are, e.g., Amankawa et al. (2014), Katsikas (2000), Dodge et al. (2007), and Bauer et al. (2017). Amankawa (2014) and Katsikas (2000) stress the need to adopt SETA programs to be suited to the roles and responsibilities of employees. Johnson (2006), Tse et al. (2013), and Wu et al. (2012) emphasize this fact by pointing out the necessity of adopting training programs to the target audience with prioritized topics. Instead, Kennedy (2016) highlights a crucial concept of competence research by elaborating that employees should be able to relate new situations to known contexts. The author concludes that once such a behavior is established, people can apply the knowledge more efficiently and meaningfully (Kennedy, 2016). Tarwireyi et al. (2011) refer to the conscious learning competence model to create competence-based questions for measuring password security among students. However, they consider a student competent if they can choose a good password. In terms of the competence model by Achtenhagen and Winther (2008), this addresses only the conceptual and procedural dimensions of competence. However, the only publications that consider the utilizational competence dimension in its full understanding are Greitzer et al. (2007), Yasin et al. (2019), Lin and Kunnathur (2013), and Kruger et al. (2011). Yasin et al. (2019) propose a scenario-based learning approach to drive employees' awareness, knowledge, and skills. Kruger et al. (2011) refer to three cognitive skills, which provide the foundations for a successful learning process. These are (1) knowledge, processes, and concepts, (2) capabilities to apply to the knowledge, processes, and concepts, and (3) the ability to reason. All three cognitive categories are related to the introduced competence dimensions. Whereas the first component covers conceptual and procedural competence, the second and third categories establish the reference to the particular situational context of behavior.

Author	Competence Dimension			Total
	Conceptual Competence	Procedural Competence	Utilizational Competence	
AlMindeel and Martins (2021), Alshaik et al. (2020), Amankawa (2014), Bauer et al. (2017), Dincelli and Chengalur-Smith (2020), Dodge et al. (2007), Goode et al. (2018), Johnson (2006), Katsikas (2000), Karjalainen and Siponen (2011), Kennedy (2016), Peltier (2005), Tarwireyi et al. (2011), Thomson and von Solms (2006), Tse et al. (2013), Tsohu et al. (2015), Waly et al. (2012), Wu et al. (2012)	x	x	(x)	18
Greitzer et al. (2007), Yasin (2019), Kruger et al. (2011), Lin and Kunathur (2013)	x	x	x	4
Abawajy (2014), Aboutabl (2006), Alshaikh et al. (2020), Caldwell (2016), Conklin (2006), Furnell and Vasileiou (2017), Gkioulos and Chowdhury (2021), Hart et al. (2020), Hu and Meinel (2004), Kaur et al. (2021), Kirova and Baumoel (2018), Konak (2014), Kruger and Kearney (2006), McCrohan et al. (2010), Pike (2021), Shaw et al. (2009), Silic and Lowy (2020), Thomson and von Solms (1998), Tschackert and Ngamshuriyaroj (2019), Tsohou et al. (2008), Tsohou et al. (2015)	x	x		21
Abdul et al. (2015) , Caputo et al. (2014), Jenkins et al. (2013), Kajzer (2014), May (2008), Mensch and Wilkie (2011), McCoy and Fowler (2004), Gandhi (2017), Pérez-González et al. (2019), Stewart and Lacey (2012), Wiley et al. (2020), Wolf et al. (2011)	x			12
Hansche (2001), Spurling (1995)				2
				57

Table 2. Analyzed Literature regarding Competence Dimensions.

4.2 Synthesis of the Literature Analysis

Our analysis indicates that few research papers refer to a holistic view of competence dimensions as an important building block for effective SETA designs. However, no paper has explained what competence as an overall principle can be understood as. Accordingly, previous research identified components of competence dimensions to a limited extent. Whereas many papers consider conceptual and procedural competence, utilizational competence which requires evaluation of the situational requirements to deduce the correct action response is barely defined. Although several research papers argue that employees are individual learners who require different methods (Abawajy, 2014) and responsibility related content (Bauer *et al.*, 2017; Furnell and Vasileiou, 2017; Peltier, 2005), there is still a lack of research that recognizes situational requirements and actions as decisive for individuals learning performance and behavior.

Yasin (2019) and Kruger et al. (2011) provide guidance for situational action taking but neglect to relate different aspects of competence development to sequential actions. The competence model of commercial education, introduced in section two, picks up both the area of action, focusing on domain-linked and domain-specific knowledge and the need to apply these dimensions to the particular situational requirements. Additionally, addressing general security-related topics in SETA programs, we highlight the necessity of preparing employees for varying situational requirements. Therefore, we provide an example of integrating the three proposed competence dimensions from the vocational education domain to the IS security domain (see Table 3). The illustration covers the contextualization of the competence dimensions to the IS domain with a basic phishing example for two different job profiles. In this context, the situational situation of action varies while the applied steps to act compliant are similar. The example distinguishes between the job-role secretary and office staff. While secretaries are more likely to be exposed to CEO frauds, office staff are more often the target of spear-phishing attacks. Hence, the situational area of action varies and must be relatable to the employees' daily working routine.

Applied Competence Model (Achtenhagen and Winther, 2008)	**Dimensions contextualized to the IS domain**	**Applied to Phishing**
Situational Area of Action	The situational area of action describes the setting that relates to the job-specific context, which is jeopardized by security threats	Secretary: CEO Fraud Office Staff: Spear-Phishing
Utilizational Competence Translation of a given requirement situation into a concrete occupational issue	The employee accurately identifies a security threat and what it consists of.	The employee recognizes that they are confronted with a phishing email. They are also aware that the situation requires active intervention.
Conceptual Competence Solving the occupational issue through activated (declarative) knowledge banks	The employee accurately recognizes what the consequences will be if the security threat is not addressed.	Possible consequences are: Information Theft/Economic loss
Procedural Competence Solving the occupational issue through activated (procedural) knowledge banks and cognitive structures	From a variety of more or less suitable action options (measures) to avert threats, the employee selects the option for action (measure) that (a) is generally following safety guidelines and (b) is the most appropriate in the respective security threat situation.	Selection of a valid prevention strategy. One possible solution could be: Report to the direct supervisor and IT security officer (2) that the employee has received an untrustworthy mail including the exact facts and hints how they recognized it and (3) forward it in the secured area (4) and delete it.
Utilizational Competence Translation and verification through generating a validated environmental model	The employee proceeds in a planned, professional, and goal-oriented manner; can thus provide a valid justification for the chosen security strategy.	I chose to forward the email to the IT security officer in the secured area for two reasons. First, this way, they can open the email without it being a serious risk. Second, they can decide to conduct further actions
	The employee can implement the chosen strategy.	The employee needs to show that they can handle a phishing email. This can be achieved in this use case by phishing simulations.

	The employee evaluates the effectiveness of the implemented measure and, if necessary and possible, carries out appropriate follow-up actions.	Depending on the chosen strategy, the employee needs to understand why the reaction to a phishing email has been appropriate or not.

Table 3 Competence Dimensions applied to the Security Context

5 Discussion

5.1 Implications to Literature

Our research contributes to the existing SETA literature in multiple ways. First, our literature-based classification suggests that many researchers acknowledge concepts for the conceptual and procedural competence for the effective design of SETA programs. However, utilizational competence assumes that competent employees emerge from constantly training in specific situational actions. Research from the vocational education domain indicates competence to be generalizable over similar situations. In fact, the more competence is independent of a specific context, the better and easier it can be transferred in a generalized form to other contexts in different settings (Winther, 2010). However, situational action taking in working environments of varying security threats and incidents is likely to be context-specific. In contrast to other performance dispositions (e.g., intelligence), competencies are strongly bound to specific contexts (Winther, 2010). The more context-specific the scope of application, the more likely they require experience with the respective contexts (Winther, 2010). Conversely, we argue that SETA programs need to be designed over different situational actions to build competence in the first place. This requires addressing training in a sequence of actions, including the conceptual, procedural, and utilizational competence components. Especially the utilizational competence dimension has been barely focused on by previous research, although it contributes to successful competence building in the vocational education domain. Therefore, we argue that more research should theorize about how SETA can be designed to address situational actions on the one hand and take job-specific needs and qualifications into account, on the other hand. In addition, the perspective of competence modeling in vocational education and training is expanded by a new, highly relevant field of security. It can be shown that basic ideas of the research are already available, but the universality of the concepts is not yet given.

5.2 Implications to Practice

The findings add to the literature and help organizations rethink and optimize their SETA programs in the future by learning from vocational education. It becomes clear that today's SETA programs do not allow for holistic training, which might be a reason why the security behavior of employees is not adequate despite various measures. Accordingly, competence models could be used to improve the holistic approach. In addition, companies would have the opportunity to consult professional education researchers and adapt their SETA programs for the necessary competencies of their employees. In this turn, the practice could learn even more aspects from vocational education and thus enable employees to develop necessary competencies. In addition to the need to fully design SETA programs when in use, vocational education also calls for the need to measure competencies in advance of SETA program implementation.

5.3 Limitations & Opportunities for Future Research

Structured literature reviews highly depend on the applied search terms and data sources (vom Brocke *et al.*, 2015). Although the index terms have been iteratively refined, the result from the search process can strongly vary when replaced with similar terms (vom Brocke *et al.*, 2015). Moreover, the search

process is limited to English keywords, whereas inclusion and exclusion criteria depend on the defined scope of the researchers. Furthermore, although two independent researchers developed the categories for the literature analysis, it cannot be guaranteed that there were no other vital aspects that might belong to another category. Moreover, the applied competence model leaves out aspects of motivational behavior. We deliberately concentrated on content and process-related development and implementation of SETA programs. A holistic competence model for information security needs to incorporate volatile and motivational components to design effective SETA guidance. Future research should enhance and adapt the vocational education competence model to the information security domain. In the next step, a holistic framework for competence modeling has to be developed. Based on different situations requiring employee action (security incidents and threats), it needs to be tested if such a model can contribute to practice. We, therefore, plan to conduct interviews with organizations. Secondly, we stress the need to measure competencies in advance of the implementation of SETA programs. As several previous research papers have identified, one-size-fits-all approaches can be a reason for the inefficiency of SETA programs. The vocational education domain stresses the importance of competence measurement for several reasons. First, they provide guidance on learnings and allow the forecast of future learning curves. Second, they contribute to offering customized training offers related to situational action-taking. Also, competence measurement can contribute to recognizing the initial level of competence before SETA programs are implemented in organizations (Winther, 2010).

6 Conclusion

In this research study, we analyzed conceptual and design-focused SETA literature in-depth and analyzed it towards competence dimensions of vocational education research. Our results indicate that the different facets of competence have mainly been regarded as standalone concepts. Although most of the previous literature acknowledges conceptual and procedural knowledge as a crucial building block for effective SETA programs, the utilizational dimension is only addressed to a limited extent or not at all. This paper, therefore, contributes to the SETA research in several ways. Firstly, we found that concepts of competence research in the vocational education domain are not fully reflected in the information security context. Hence, we suggest transferring this existing knowledge on producing competent professionals to the SETA context. In particular, this refers to the need to consider situational requirements in the first place. Secondly, we contribute to the literature by classifying different concepts that are closely related to competence but often mixed. We, therefore, hope that our analysis sheds light on possible reasons why SETA programs might fail in practice apart from motivational issues.

Acknowledgement

This research paper has been developed as part of the research project “ITS.kompetent” funded by the German Federal Ministry for Economic Affairs and Climate Action. We would like to thank the Federal Ministry for Economic Affairs and Climate Action for the support.

References

Abawajy, J. (2014), “User preference of cyber security awareness delivery methods”, *Behaviour and Information Technology*, Vol. 33 No. 3, pp. 237–248.

Aboutabl, M.S. (2006), “The CyberDefense laboratory: A framework for information security education”, *Proceedings of the 2006 IEEE Workshop on Information Assurance*, Vol. 2006, pp. 55–60.

Achtenhagen, F. and Winther, E. (2008), “Wirtschaftspädagogische Forschung zur beruflichen Kompetenzentwicklung”, *Kompetenzerfassung in Pädagogischen Handlungsfeldern Theorien, Konzepte Und Methoden*, N. Jude, J. Hartig, E. Klieme, Bonn, Berlin: BMBF, pp. 117–140.

Ahlan, A.R., Lubis, M. and Lubis, A.R. (2015), "Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures", *Procedia Computer Science*.

Ahmad, A., Desouza, K.C., Maynard, S.B., Naseer, H. and Baskerville, R.L. (2020), "How integration of cyber security management and incident response enables organizational learning", *Journal of the Association for Information Science and Technology*, Vol. 71 No. 8, pp. 939–953.

Albrechtsen, E. and Hovden, J. (2010), "Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study", *Computers and Security*, Elsevier Ltd, Vol. 29 No. 4, pp. 432–445.

AlMindeel, R. and Martins, J.T. (2021), "Information security awareness in a developing country context: insights from the government sector in Saudi Arabia", *Information Technology and People*, Vol. 34 No. 2, pp. 770–788.

Alshaikh, M., Naseer, H., Ahmad, A. and Maynard, S.B. (2020), "Toward sustainable behaviour change: An approach for cyber security education training and awareness", *27th European Conference on Information Systems - Information Systems for a Sharing Society, ECIS 2019*, pp. 1–14.

Amankwa, E., Loock, M. and Kritzinger, E. (2014), "A conceptual analysis of information security education, information security training and information security awareness definitions", *9th International Conference for Internet Technology and Secured Transactions, ICITST 2014*, Infonomics Society, pp. 248–252.

Bauer, S., Bernroider, E.W.N. and Chudzikowski, K. (2017), "Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks", *Computers and Security*, Elsevier Ltd, Vol. 68, pp. 145–159.

vom Brocke, J. V., Simons, A., Riemer, K., Niehaves, B., Plattfault, R. and Cleven, A. (2015), "Standing on the shoulders of giants: Challenges and recommendations of literature search in Information Systems research", *Communications of the Association for Information Systems*, Vol. 37 No. 9, pp. 205–224.

Caldwell, T. (2016), "Making security awareness training work", *Computer Fraud and Security*, Elsevier Ltd, Vol. 2016 No. 6, pp. 8–14.

Caputo, D.D., Pfleeger, S.L., Freeman, J.D. and Johnson, M.E. (2014), "Going spear phishing: Exploring embedded training and awareness", *IEEE Security and Privacy*, Vol. 12 No. 1, pp. 28–38.

Conklin, A. (2006), "Cyber defense competitions and information security education: An active learning solution for a capstone course", *Proceedings of the 39th Hawaii International Conference on System Sciences*, Vol. 9 No. C, pp. 1–6.

Cram, W.A., D'Arcy, J. and Proudfoot, J.G. (2019), "Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance", *MIS Quarterly: Management Information Systems*, Vol. 43 No. 2, pp. 525–554.

D'Arcy, J. and Hovav, A. (2009), "Does one size fit all? Examining the differential effects of IS security countermeasures", *Journal of Business Ethics*, Vol. 89 No. 1, pp. 59–71.

D'Arcy, J., Hovav, A. and Galletta, D. (2009), "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach", *Information Systems Research*, Vol. 20 No. 1, pp. 79–98.

Dhillon, G., Talib, Y.Y.A. and Picoto, W.N. (2020), "The mediating role of psychological empowerment in information security compliance intentions", *Journal of the Association for Information Systems*, Vol. 21 No. 1, pp. 152–174.

Dincelli, E. and Chengalur-Smith, I.S. (2020), "Choose your own training adventure: designing a gamified SETA artefact for improving information security and privacy through interactive storytelling", *European Journal of Information Systems*, Taylor & Francis, Vol. 29 No. 6, pp. 669–687.

Dodge, R.C., Carver, C. and Ferguson, A.J. (2007), "Phishing for user security awareness", *Computers and Security*, Vol. 26 No. 1, pp. 73–80.

ENISA. (2021), *ENISA Threat Landscape 2021*, *EU for Cybersecurity*

Furnell, S. and Vasileiou, I. (2017), "Security education and awareness: just let them burn?", *Network Security*, Elsevier Ltd, Vol. 2017 No. 12, pp. 5–9.

Furnell, S.M., Gennatou, M. and Dowland, P.S. (2002), "A prototype tool for information security awareness and training", *Logistics Information Management*, Vol. 15 No. 5/6, pp. 352–357.

Gandhi, A. (2017), "Quantitative assessment of information security awareness on informatics students in a university", *ACM International Conference Proceeding Series*, pp. 346–350.

Gkioulos, V. and Chowdhury, N. (2021), "Cyber security training for critical infrastructure protection: A literature review", *Computer Science Review*, Elsevier Inc., Vol. 40, pp. 1–20.

Goode, J., Levy, Y., Hovav, A. and Smith, J. (2018), "Expert assessment of organizational cybersecurity programs and development of vignettes to measure cybersecurity countermeasures awareness", *Online Journal of Applied Knowledge Management*, Vol. 6 No. 1, pp. 67–80.

Greeno, J.G., Riley, M.S. and Gelman, R. (1984), "Conceptual competence nd children's scounting", *Cognitive Psychology*, Vol. 16 No. 1, pp. 94–143.

Greitzer, F.L., Kuchar, O.A. and Huston, K. (2007), "Cognitive science implications for enhancing training effectiveness in a serious gaming context", *ACM Journal on Educational Resources in Computing*, Vol. 7 No. 3, pp. 1–16.

Hansche, S. (2001), "Information System Security Training: Making It Happen: Part 2 of 2", *Information Systems Security*, Vol. 10 No. 1, pp. 1–9.

Hart, S., Margheri, A., Paci, F. and Sassone, V. (2020), "Riskio: A Serious Game for Cyber Security Awareness and Education", *Computers and Security*, Elsevier Ltd, Vol. 95

Herath, T., Yim, M.S., D'Arcy, J., Nam, K. and Rao, H.R. (2018), "Examining employee security violations: moral disengagement and its environmental influences", *Information Technology and People*, Vol. 31 No. 6, pp. 1135–1162.

Hu, J. and Meinel, C. (2004), "Tele-Lab 'IT-Security' on CD: Portable, reliable and safe IT security training", *Computers and Security*, Vol. 23 No. 4, pp. 282–289.

Hu, S., Hsu, C. and Zhou, Z. (2021), "Security Education, Training, and Awareness Programs: Literature Review", *Journal of Computer Information Systems*, Taylor & Francis, Vol. 00 No. 00, pp. 1–13.

Hwang, I., Kim, D., Kim, T. and Kim, S. (2017), "Why not comply with information security? An empirical approach for the causes of non-compliance", *Online Information Review*, Vol. 41 No. 1, pp. 2–18.

Jenkins, J.L., Durcikova, A. and Mary, B. (2013), "Simplicity is bliss: Controlling extraneous cognitive load in online security training to promote secure behavior", *Journal of Organizational and End User Computing*, Vol. 25 No. 3, pp. 52–66.

Johnson, E.C. (2006), "Security awareness: Switch to a better programme", *Network Security*, Vol. 2006 No. 2, pp. 15–18.

Kajzer, M., Darcy, J., Crowell, C.R., Striegel, A. and Van Bruggen, D. (2014), "An exploratory investigation of message-person congruence in information security awareness campaigns", *Computers and Security*, Elsevier Ltd, Vol. 43, pp. 64–76.

Karjalainen, M. and Siponen, M. (2011), "Toward a New Meta-Theory for Designing Information Systems (IS) Security Training Approaches", Vol. 12 No. 8, pp. 518–556.

Katsikas, S.K. (2000), "Health care management and information systems security: Awareness, training or education?", *International Journal of Medical Informatics*, Vol. 60 No. 2, pp. 129–135.

Kaur, J., Dhillon, G. and Picoto, W.N. (2021), "AIS Electronic Library (AISeL) The role of organizational competence on information security job performance", *WISP 2021 Proceedings*, Vol. 9.

Kennedy, S.E. (2016), "The pathway to security-mitigating user negligence", *Information and Computer Security*, Vol. 24 No. 3, pp. 255–264.

Kirova, D. and Baumoel, U. (2018), "Factors that Affect the Success of Security Education, Training, and Awareness Programs: A Literature Review", *Journal of Information Technology Theory and Application (JITTA)*, Vol. 19 No. 4, pp. 56–83.

Klotz, V.K. and Winther, E. (2016), "Zur Entwicklung domänenverbundener und

domänenspezifischer Kompetenz im Ausbildungsverlauf: Eine Analyse für die kaufmännische Domäne", *Zeitschrift Fur Erziehungswissenschaft*, Vol. 19 No. 4, pp. 765–782.

Konak, A., Clark, T.K. and Nasereddin, M. (2014), "Using Kolb's Experiential Learning Cycle to improve student learning in virtual computer laboratories", *Computers and Education*, Elsevier Ltd, Vol. 72, pp. 11–22.

Kruger, H.A., Drevin, L., Flowerday, S. and Steyn, T. (2011), "An assessment of the role of cultural factors in information security awareness", *2011 Information Security for South Africa - Proceedings of the ISSA 2011 Conference*, IEEE, pp. 1–7.

Kruger, H.A. and Kearney, W.D. (2006), "A prototype for assessing information security awareness", *Computers and Security*, Vol. 25 No. 4, pp. 289–296.

Kunter, M., Klusmann, U. and Baumert, J. (2009), "Professionelle Kompetenz von Mathematiklehrkräften : Das COACTIV-Modell", *Lehrprofessionalität - Bedingungen, Genese, Wirkungen Und Ihre Messung*, O. Zlatkin-Troitschanskaia, ol K. Beck, D. Sembill, R. Nickolaus, R.Mulder, pp. 153–165.

Lin, C. and Kunnathur, A.S. (2013), "Toward developing a theory of end user information security competence", *19th Americas Conference on Information Systems, AMCIS 2013 - Hyperconnected World: Anything, Anywhere, Anytime*, Vol. 5 No. 2006, pp. 3578–3587.

May, C. (2008), "Approaches to user education", *Network Security*, Vol. 2008 No. 9, pp. 15–17.

McCoy, C. and Fowler, R.T. (2004), "'You Are the Key to Security': Establishing a Successful Security Awareness Program", *Proceedings of the 32nd Annual ACM SIGUCCS Conference on User Services*, pp. 346–349.

McCrohan, K.F., Engel, K. and Harvey, J.W. (2010), "Influence of awareness and training on cyber security", *Journal of Internet Commerce*, Vol. 9 No. 1, pp. 23–41.

Mensch, S. and Wilkie, L. (2011), "Information Security Activities of College Students: An Exploratory Study", *Academy of Information and Management Sciences Journal*, Vol. 14 No. 2, pp. 91–116.

Peltier, T.R. (2005), "Implementing an information security awareness program", *Information Systems Security*, Vol. 14 No. 2, pp. 37–49.

Pérez-González, D., Preciado, S.T. and Solana-Gonzalez, P. (2019), "Organizational practices as antecedents of the information security management performance: An empirical investigation", *Information Technology and People*, Vol. 32 No. 5, pp. 1262–1275.

Pike, R. (2021), "Enhancing cybersecurity capability in local governments through competency-based education", *Proceedings of the Annual Hawaii International Conference on System Sciences*, Vol. 2020-Janua, pp. 2019–2025.

Posey, C., Roberts, T.L. and Lowry, P.B. (2015), "The impact of organizational commitment on insiders motivation to protect organizational information assets", *Journal of Management Information Systems*, Routledge, Vol. 32 No. 4, pp. 179–214.

Puhakainen, P. and Siponen, M. (2010), "Improving employees' compliance through information systems security training: An action research study", *MIS Quarterly: Management Information Systems*, Vol. 34 No. 4, pp. 757–778.

Shaw, R.S., Chen, C.C., Harris, A.L. and Huang, H.J. (2009), "The impact of information richness on information security awareness training effectiveness", *Computers and Education*, Elsevier Ltd, Vol. 52 No. 1, pp. 92–100.

Silic, M. and Lowry, P.B. (2020), "Using Design-Science Based Gamification to Improve Organizational Security Training and Compliance", *Journal of Management Information Systems*, Routledge, Vol. 37 No. 1, pp. 129–161.

Spurling, P. (1995), "Promoting security awareness and commitment", *Information Management & Computer Security*, Vol. 3 No. 2, pp. 20–26.

Stewart, G. and Lacey, D. (2012), "Death by a thousand facts: Criticising the technocratic approach to information security awareness", *Information Management and Computer Security*, Vol. 20 No. 1, pp. 29–38.

Tarwireyi, P., Flowerday, S. and Bayaga, A. (2011), "Information security competence test with regards to password management", *2011 Information Security for South Africa - Proceedings of*

the ISSA 2011 Conference.
Thomson, K.L. and von Solms, R. (2006), "Towards an Information Security Competence Maturity Model", *Computer Fraud and Security*, Vol. 2006 No. 5, pp. 11–15.
Thomson, M.E. and Von Solms, R. (1998), "Information security awareness: Educating your users effectively", *Information Management and Computer Security*, Vol. 6 No. 4, pp. 167–173.
Tschakert, K.F. and Ngamsuriyaroj, S. (2019), "Effectiveness of and user preferences for security awareness training methodologies", *Heliyon*, Elsevier Ltd, Vol. 5 No. 6, pp. 1–10.
Tse, W.K.D., Hui, M.H., Lam, S.T., Mok, Y.C., Oei, W.C., Tang, K.L. and Yau, X.L. (2013), "Education in IT Security: A Case Study in Banking Industry", *GSTF Journal on Computing (JoC)*, Vol. 3 No. 3.
Tsohou, A., Karyda, M. and Kokolakis, S. (2015), "Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs", *Computers and Security*, Elsevier Ltd, Vol. 52, pp. 128–141.
Tsohou, A., Karyda, M., Kokolakis, S. and Kiountouzis, E. (2015), "Managing the introduction of information security awareness programmes in organisations", *European Journal of Information Systems*, Vol. 24 No. 1, pp. 38–58.
Tsohou, A., Kokolakis, S., Karyda, M. and Kiountouzis, E. (2008), "Investigating information security awareness: Research and practice gaps", *Information Security Journal*, Vol. 17 No. 5–6, pp. 207–227.
Waly, N., Tassabehji, R. and Kamala, M. (2012), "Measures for improving information security management in organisations: the impact of training and awareness programmes", *UK Academy for Information Systems Conference Proceedings 2012*, pp. 1–10.
Webster, J. and Watson, R.T. (2002), "Analyzing the Past to Prepare for the Future: Writing a Literature Review.", *MIS Quarterly*, Vol. 26 No. 2, pp. xiii–xxiii.
Weinert, F.E. (2000), "Lehren und Lernen für die Zukunft - Ansprüche an das Lernen in der Schule", *Pädagogische Nachrichten Rheinland-Pfalz*, Vol. 2, pp. 1–16.
Wiley, A., McCormac, A. and Calic, D. (2020), "More than the individual: Examining the relationship between culture and Information Security Awareness", *Computers and Security*, Elsevier Ltd, Vol. 88, pp. 1–8.
Winther, E. (2010), *Kompetenzmessung in Der Beruflichen Bildung*, Bertelsmann, Bielefeld, Germany.
Wolf, M., Haworth, D. and Pietron, L. (2011), "Measuring An Information Security", *Review of Business Information Systems – Third Quarter 2011*, Vol. 15 No. 3, pp. 9–22.
Wu, Y.A., Guynes, C.S. and Windsor, J. (2012), "Security Awareness Programs", *Review of Business Information Systems (RBIS)*, Vol. 16 No. 4, pp. 165–168.
Yasin, A., Liu, L., Li, T., Fatima, R. and Jianmin, W. (2019), "Improving software security awareness using a serious game", *IET Software*, Vol. 13 No. 2, pp. 159–169.