Rising like a Phoenix: Emerging from the Pandemic and Reshaping Human Endeavors with Digital Technologies ICIS 2023

Cybersecurity and Privacy

Dec 11th, 12:00 AM

Triad or Error? Introducing Three Basic Dimensions of Competence as a Driving Force for Information Security Performance

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

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

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

Simon Trang
University of Paderborn, simon.trang@wiwi.uni-goettingen.de

Recommended Citation

Rampold, Florian; Masuch, Kristin; Warwas, Julia; and Trang, Simon, "Triad or Error? Introducing Three Basic Dimensions of Competence as a Driving Force for Information Security Performance" (2023). *Rising like a Phoenix: Emerging from the Pandemic and Reshaping Human Endeavors with Digital Technologies ICIS 2023*. 11.
https://aisel.aisnet.org/icis2023/cyber_security/cyber_security/11

Triad or Error? Introducing Three Basic Dimensions of Competence as a Driving Force for Information Security Performance

Completed Research Paper

Florian Rampold
University of Goettingen
Platz der Goettinger Sieben 5
37073 Goettingen, Germany
florian.rampold@uni-goettingen.de

Kristin Masuch
University of Goettingen
Platz der Goettinger Sieben 5
37073 Goettingen, Germany
kristin.masuch@uni-goettingen.de

Julia Warwas
University of Hohenheim
Fruwirthstr. 47
70599 Stuttgart
julia.warwas@uni-hohenheim.de

Simon Thanh-Nam Trang
University of Paderborn
Warburger Str. 100
33098 Paderborn
simon.trang@uni-paderborn.de

Abstract

As security incidents such as data breaches have dramatically increased in recent years, companies have acknowledged the utmost importance of implementing SETA (Security, Education, Training, and Awareness) programs. Although there has been much effort in designing these programs as effectively as possible, many security incidents are caused by employee misconduct. In this study, we shed light on the basic dimensions of information security competence (ISC) that employees need to efficiently improve their performance in dealing with security threats. Using a competence model from the field of vocational education, we conceptualize information security competence as a multidimensional construct. We then empirically test the impact of information security competence on information security performance in a study with 234 participants. Our results suggest that a differentiated view of competence is necessary, first, to improve employee performance in dealing with security threats and, second, to develop SETA programs that address employee vulnerabilities.

Keywords: *Information Security Competence, Vocational Education and Training, SETA, Information Security Performance*

Introduction

The worldwide spending on organizational information security has dramatically increased in the last two decades. While security investments in technical and organizational measures grow moderately, the relative proportion of human-caused information security breaches is extraordinarily high (Gartner, 2022). A recent joint report of Stanford University and the security firm Tessian shows that up to 88% of security breaches are human-enabled (Tessian, 2020). According to Verizon (2020), 22% percent of data breaches in 2020 involved phishing attacks. As AI-based capabilities such as Chat GPT become more sophisticated, hackers are expected to have an effortless time designing phishing attacks almost indistinguishable from real messages. Organizations spend a lot of time and resources to address this issue by building effective security education, training, and awareness (SETA) programs (D’Arcy & Hovav, 2009; S. Hu et al., 2021; Posey et al., 2015). These cover a wide range of delivery methods, from micro-training (e.g., short video clips, posters, flyers, and E-mails) to sophisticated educational information security policy (ISP) training (e.g., long-term instructional training, e-learning platforms, and on-site ISP training) (Boss et al., 2015; Puhakainen & Siponen, 2010). Although IT professionals have made great efforts to educate employees about information security compliance and behavior, the previously mentioned statistics suggest that SETA programs are only partially effective in preparing employees for various security threats in their work context. (IBM Security, 2019). We can identify two possible main drivers for this circumstance.

First, SETA programs fail to effectively change employees' commitment to engage in information security behaviors. In these terms, IS research in the information security domain has investigated antecedents influencing employees' information security compliance behavior. These determinants constitute motivational and affective dimensions of competent, particularly responsible (security) behavior at the workplace. However, they mainly stimulate the attitudes and commitment toward organizational information security (e.g., punishment severity (Johnston et al., 2015), normative beliefs (Herath & Rao, 2009), and rewards (Bulgurcu et al., 2010)).

Second, SETA programs fail to develop the dimensions of information security competence (ISC) needed to transfer knowledge into daily practice. As a result, employees are committed to protecting their company's information security but occasionally fail to do so. *Imagine an employee who has a high attitude toward information security. The employee recently attended a video-based phishing training and understands the concerns related to falling for phishing and the consequences it can pose for the employer. However, one day, the employee receives a message from a person via the firmwide collaboration tool. Apparently, the person works in the same company, but the person is unknown to the employee. The message prompts to provide the password for a file called customer data.* In this context, the employee can fail to overcome the threatening situation in two ways. First, the employee does not recognize being confronted with a malicious attacker, or second, the employee chooses an insufficient strategy to mitigate the security threat (such as ignoring the message). Although s/he is motivated to follow the regulations of the ISP of the company, the employee fails to show the desired behavior since specific knowledge about the function and implementation of specific measures and their appropriate and confident application in different work situations is lacking (Rausch et al., 2019).

In other words, being committed to attaining certain standards of IT-secure behavior is an important motivational prerequisite but insufficient for performing appropriately if declarative knowledge (about ISP facts and rules) and procedural knowledge (of how to use these facts and rules) are missing (Lau & Roeser, 2002). Accordingly, the extent to which SETA programs develop/promote different knowledge components as at least equally important determinants of performance in handling security threats presents an indispensable evaluation criterion for these programs. Although the literature on performance in IS security is scarce, some studies have conceptualized it as a measurement construct in phishing literature. However, the performance measure is limited to past success in detecting phishing (Chen et al., 2020; Wang et al., 2016, 2017).

Research in the field of Vocational education and training (VET), on the other hand, has a long-standing tradition in modeling and assessing drivers of employees' performance at the workplace, which together form the concept of competence (Seeber, 2016; Winther, 2010). Competence thus presents an integrated set of knowledge and skills as well as motivational and volitional prerequisites residing in an individual (Rausch et al., 2019). It functions as a multifaceted, latent disposition that translates into observable, situated behavior (Blömeke et al., 2015). From this perspective, performance can be defined as the process by which individuals make use of their respective cognitive resources (Lau & Roeser, 2002; Rausch et al., 2019). With an emphasis on cognitive resources, Greeno et al. (1984) distinguish three dimensions of competence (conceptual, procedural, and interpretative competence) – a classification adopted by researchers in the VET domain (Gibson, 2008; Klotz et al., 2015). When adopting this classification for reviewing SETA-design recommendations, Rampold et al. (2022) find that rule-based security knowledge and concepts (conceptual competence) as well as the procedures and skills required to apply security-specific knowledge (procedural competence) are often present. In contrast, guiding employees to assess the situational demands to counter security threats adequately (interpretative competence) has mostly been neglected. Although there have been advancements in the IS domain to capture ISC through questionnaires, these commonly follow a unidimensional approach (Bulgurcu et al., 2010; Parsons et al., 2014). This can be problematic against the background of a multidimensional perspective of competence determining performance. Based on these considerations, we pose the following research question: *How does a multidimensional perspective on ISC affect information security performance on the employee level?*

To answer this RQ, we introduce a basic competence model from the VET domain as a theoretical lens and apply the relevant constructs to the information security domain. Therefore, we propose three basic and distinct constructs (conceptual, procedural, and interpretative ISC) as individual, cognitive resources when handling security threats. We developed a self-assessment instrument covering these constructs with 9 measurement items. Afterward, the items were evaluated and refined based on a card-sorting assignment following the guidelines of Moore and Benbasat (1991). In the next step, we tested the reliability and validity of the items based on the assessment of 100 employees. Finally, the conceptualization of ISC was tested empirically in a study with 260 participants with past phishing handling success as a performance measure. Our results suggest that conceptual ISC can be distinguished empirically from action-oriented ISC (covering procedural and interpretative dimensions as a second-order construct) and that it has a strong positive effect on information security performance.

We contribute to the information security IS literature in at least two ways. First, we open a new research perspective on functionally different yet connected determinants of information security performance. We, therefore, provide an insight into the dimensions of competence that are necessary to cope with varying security threats in the daily working situations of employees. Second, we link to the research stream that seeks to explain why some SETA programs might fall short of their expectations. In these terms, our results suggest that distinct dimensions of ISC need to be considered equally to enhance the information security performance potential of employees.

Theoretical Background

Reviewing Central Concepts of Competence as Dispositions to Performance

Competence was first discussed in the US during the 1970s (Blömeke et al., 2015). Since then, competence has been mainly understood in two different ways. Traditionally, it has been viewed as a "characteristic that is causally related to criterion-referenced effective and/or superior performance in a job or situation" (Spencer & Spencer, 1993, p. 9). Following this definition, competence can be observed by directly assessing the behavior of individuals in real-world situations to infer from performance criteria to extant competence (behavioral perspective). Cognitive structures and processes, as well as motivational orientations or affective tendencies, are underlying drivers that enable observable behavior (Blömeke et al., 2015). However, when limiting measures of competence strictly to observations of behavior (i.e. performance), it becomes difficult to account for the unique contribution of the different facets of competence that steer this behavior in the first place (Corno et al., 2001). Consequently, the second perspective is based on the analytical assessment of several *cognitive, affective, and motivational* resources that sum up to an overall construct of competence and, when used conjointly in an achievement-related situation, result in high performance. This complementary approach stresses that competence can be understood as a person's dispositional repertoire for behaving in high accordance with the demands and standards of a focal domain (e.g., in a particular profession). Competence embraces the person's repertoire of knowledge, skills, and traits as opposed to their many practical applications in real-world situations (e.g., in the various typical tasks of that profession; Klotz et al. 2015). Thus, both perspectives converge in the assumption that competence involves "the latent cognitive and affective-motivational underpinning of domain-specific performance in varying situations" (Blömeke et al., 2015, p. 3) and performance usually displays indicators of these dispositions to an outside observer, although there might be situations in which the person refrains from employing all of his/her behavioral resources. Hence, we understand competence as multidimensional and highly context-sensitive in this research paper. While the cognitive part of competence (knowledge and skills) is regarded as the cornerstone of competent action-taking, motivational and affective dispositions are commonly seen as reinforcing problem-solving capacities (Rausch et al., 2019).

When assessing competence in VET contexts, the main goal is to identify starting points (even deficits) to promote particular cognitive, affective, and motivational resources and to document competence gains (growing dispositions for high performance) of individuals or groups during this developmental process (Klotz et al., 2015; Blömeke et al., 2015). Competence assessment is mainly applied to address the gap between the current state of required dispositions and the desired levels of competence in the focal domain (Seeber, 2016; Winther, 2010). Exemplary domains include the modeling and measurement of the competence of medical health staff. (Warwas et al., 2023). The assessment process starts with thoroughly analyzing the underlying domain, including information about job-related tasks, in order to extract the demands of professional action situations as reliably as possible (Seeber, 2016). Schuetz et al. (2023) showcase how the analysis of the domain translates to the information security context.

We can leverage these findings in the following way: Competence is a complex construct encompassing knowledge, skills, as well as affective and motivational traits. As affective and motivational resources for engaging in IS behaviors have been investigated thoroughly in IS research (see Cram et al., 2019), we concentrate on delineating the cognitive dimensions of competence in our present work. We draw on Greeno et al.'s (1984) distinction between three cognitive dimensions of competence (conceptual, procedural, and interpretative competence). Conceptual competence encompasses the ability to retrieve factual knowledge and learned rules in a specific action situation *(What)*. Procedural competence refers to the ability to select and execute domain-related actions and procedures concerning a particular situation *(How)*. Finally, interpretative competence compromises the ability to understand the requirements of different situations as a cognitive evaluation process *(When and Where)*. This interpretational component includes, firstly, the ability to recognize the requirements of the necessary actions in a given situation (Klotz et al., 2015). Secondly, an appropriate solution strategy has to be found and evaluated in light of the situational conditions and goals (Greeno et al., 1984; Winther, 2010).

These concepts have two implications for considering competence in the security context. First, ISC goes beyond knowing rules and regulations, such as using strong passwords and reporting security incidents. The ability to identify and cognitively evaluate specific requirements of a situation (interpretative competence) is assumed by Greeno et al. (1984) to be a separate dimension of competence. This implies that individuals should not only possess knowledge about security principles and rules (conceptual ISC) and how to apply them (procedural ISC) but also be able to assess whether and how to respond best to a security threat (interpretative ISC).

Notions of Competence and Performance in Extant Literature

In the following, we will discuss how competence has been considered a measurement construct in the IS security literature, focusing on the cognitive dimensions of competence. Following Greeno et al. (1984) these are knowledge or skill-based and refer to the understanding and application of rules and facts in a domain. These knowledge and skills translate to performance when they are retrieved and combined in a given requirement or real-world situation (Winther 2010). To get an impression of commonly applied constructs in nomological networks for security-related behavior that capture the construct, we analyzed the IS security literature in terms of the three (conceptual, procedural, and interpretative) ISC dimensions that inform our research. As a sound basis for reviewing related literature, we take up the references in the comprehensive meta-analysis by Cram et al. (2019) that deals with antecedents of information security compliance. Below, we will present our main findings.

We can observe that previous research addresses conceptual ISC in several ways. Multiple research papers leverage Information Security Awareness (ISA) as an essential antecedent of information security compliance behavior. Bulgurcu et al. (2010) defined ISA as employees' general knowledge of information security and policies, including the potential consequences of security-related misbehavior. ISA encompasses two facets: General ISA and ISP Awareness. While General ISA refers to abstract knowledge about security threats and their consequences, ISP Awareness measures employees' general knowledge about the rules and regulations within an organizational context. During the last decade, the construct has been mainly applied to measure conceptual ISC in nomological networks (Park et al., 2017). Commonly, these approaches leverage conceptual ISC as a direct antecedent of information security compliance behavior or as part of a nomological network with mediating factors and security or compliance behavior as a dependent variable (Bulgurcu et al., 2010; Park et al., 2017). ISP knowledge has also been conceptualized in several other measurement scales (McCormac et al., 2017; Parsons et al., 2014). Based on the Knowledge-Attitude-Behavior (KAB) model, Parsons et al. (2013) developed a security-related measurement scale encompassing knowledge, attitude, and behavioral items contextualized to the security domain. Another strand of literature identifies SETA Awareness as a conceptual security component. In these terms, D'Arcy et al. (2009) developed a scale for assessing users' SETA program awareness which has been utilized in quantitative empirical studies as an antecedent of security compliance behavior in multiple studies (Lowry et al., 2015; Sommestad et al., 2015). However, the scale only captures the knowledge of the existence of SETA programs in the organization, not the content of security programs, such as information about security threats or countermeasures. Other related constructs that have been applied to the IS security context include fear appeals (perceived threat severity, perceived threat susceptibility, and perceived response efficacy). In their nature, they are antecedents of one's commitment and belief in the usefulness of general security rules and policies. For instance, threat severity is usually related to one's perception of the consequences if the ISP is not followed or specific security incidents arise (such as the spilling of passwords) (Cram et al., 2019; Johnston et al., 2015). Threat susceptibility considers the risks and potential entry points that attackers can exploit (Herath & Rao, 2009). However, both constructs do not necessarily capture knowledge about the consequences or risks of misbehavior but are more likely related to what extent the individual considers security regulations important and relevant. Moreover, response efficacy refers to the effectiveness of countermeasures or responses in mitigating security threats (Cram et al., 2019). It emphasizes the importance of countermeasures but does not assess the specific knowledge about countermeasures in general.

As procedural ISC is defined as the procedures and skills necessary to apply conceptual knowledge (Greeno et al. 1984), it focuses on the ability to execute security-related behaviors. When measured from self-reported statements, it often relates to the conceptualization of information security-related self-efficacy Bandura (1986). Since self-efficacy refers to one's perception of being able to perform certain behaviors (Bandura (1986)), it often utilizes one's belief in their skills or abilities. It is important to note that procedural ISC focuses on the specific procedures and actions required to respond to a security threat, whereas IS security self-efficacy is a more general belief in one's ability to adhere to an organization's specific security policies. While self-efficacy is a driver of an individual's commitment to perform a certain behavior, procedural competence is the activated knowledge of how to handle a task (Alexander et al., 1991; Lau & Roeser, 2002). In the IS security context, self-efficacy has been conceptualized in manifold ways. Most research papers considering self-efficacy relate the construct to one's self-perception of successfully coping with the ISP (Bulgurcu et al., 2010; D'Arcy & Lowry, 2019; Siponen et al., 2014). Workman et al. (2008) instead defined self-efficacy in terms of the ability to implement security measures. Lastly, we reviewed interpretative competence as a construct in IS security literature. Although there have been advancements to capture the construct, they solely focus on the identification process of security threats (Ng et al. 2009; Sheng et al. 2010) but not in a sense of interpreting the situation as an evaluation process to develop an appropriate counter-strategy.

As performance is an outcome measure of competence in VET research, we also investigated how information security performance has been considered in extant IS security literature. Therefore, we conducted a literature review using the search terms ("information security performance" or information security job performance" or "security performance") in the AIS library. Our search yielded 16 publications. However, most of these studies investigate security performance on the organizational level. In these terms, it is either understood as the operational efficiency and effectiveness of security processes (Naseer et al., 2016) or measured as the capabilities of organizations to prevent security breaches (Kwon & Johnson, 2018; Li et al., 2021). On the individual level, Lebek et al. (2014) define it as a bidimensional construct composed of employee security compliance and security participation. Thus, they adapt a security in-role and security extra-role behavior perspective on performance. In other studies, it has been primarily leveraged to measure employees' detection success of security threats (especially for phishing emails) (Chen et al., 2020). The findings inform our research as follows. Although competence has been regarded theoretically in IS security research, previous research lacks a differentiated conceptualization of the cognitive dimensions of competence of individual employees in the IS security context. While some conceptual and procedural competence facets are represented in security measure scales, the interpretative dimension has been mainly overlooked. Especially the ability to assess the situation of action and the interpretation of the contextual demands to choose the most suitable counter-reaction to a security threat has not been covered by existing measurement scales. We argue that it is crucial to conceptualize and measure an individual's ability to recognize a security threat and how best to mitigate it when the outcome variable of interest is performance. Similar to the concept of competence, information security performance has been mainly captured at the organizational level. Although few studies have considered performance in empirical IS security research, the measure is restricted to the detection success of security threats.

The Relationship between ISC and Information Security Performance

Viewing Competence Models as a Theoretical Lens

The distinction between conceptual, procedural, and interpretative competence as an individual disposition for performance has been applied in various contexts in the VET domain. In these models, it is assumed that success in solving a task or problem depends on the availability of different measurable dimensions of competence (Winther, 2010). One prominent example is the competence model by Winther (2010); see also Klotz et al., 2015. It utilizes the previously introduced three competence dimensions originally developed by Greeno et al. (1984) and has been initially developed to measure the competencies in the working context of commercial employees. The model considers three distinct dimensions of competence in the sense of a series of actions. The first dimension is processing learning and work requirements by using activated declarative knowledge (conceptual competence). This is done to gain a holistic and functional understanding of domain-related ideas. The second dimension is the selection and execution of domain-specific strategies and the application of knowledge acquired in domain (procedural competence). Finally, the third dimension involves constructing a solution that aligns best with the requirements of the situation (interpretative competence) (Winther, 2010). This process of deciding and evaluating gauges the success of the chosen strategies and thus includes the overall understanding of the situational requirements (typically reflected in distinct tasks) of the domain (Winther, 2010). With respect to information security at the workplace, these tasks or requirements are particular security incidents that employees are confronted with. Winther (2010) further combines the two dimensions of procedural and interpretative competence into one overarching action-oriented competence. This assumption aligns with cognitive psychology research, as interpretative competence is sometimes understood as a complementary facet of procedural competence (Gibson, 2008). Figure 1 depicts the relationship.

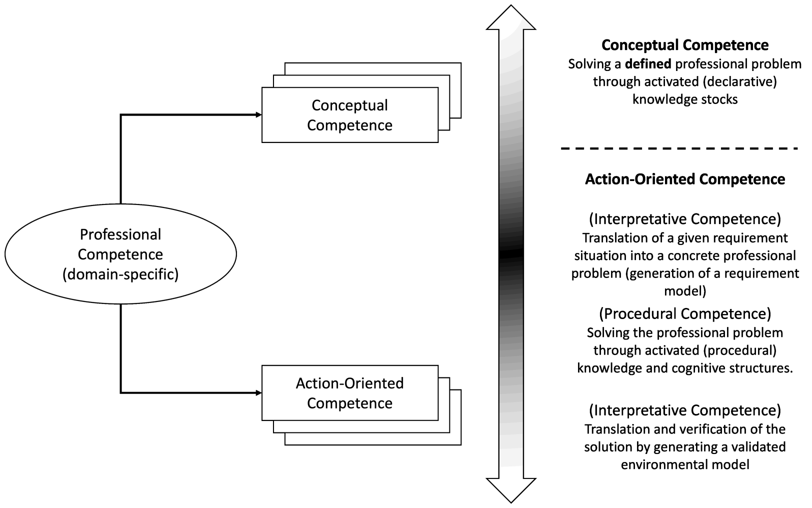
Professional
Competence
(domain-specific)
Conceptual
Competence
Action-Oriented
Competence
Conceptual Competence
Solving a defined professional problem through activated (declarative) knowledge stocks
Action-Oriented Competence
(Interpretative Competence)
Translation of a given requirement situation into a concrete professional problem (generation of a requirement model)
(Procedural Competence)
Solving the professional problem through activated (procedural) knowledge and cognitive structures.
(Interpretative Competence)
Translation and verification of the solution by generating a validated environmental model

Figure 1. Competence Model based on Winther (2010)

The competence model informs our research in the following way. Dealing effectively with the requirements of a situation is processual and involves sequences of connected cognitive operations. In other words, someone who misses the correct interpretation of the context when confronted with a task cannot construct a proper solution. Moreover, conceptual competence forms the basis for solving a task that can only be sufficient when the procedural and interpretative actions align with the situational requirements. With its dual (or, respectively triad) view on competent action in a specific domain, we argue that this basic competence model can be transferred to the domain of counter-acting information security threats.

The Competence Model as a Theoretical Lens for the Information Security Domain

To transfer the competence structure model of Winther (2010) to the information security domain, we applied several steps presented in the following. Based on the classification framework of Greeno et al. (1984), we argue that a competent person needs to possess all three dimensions of competence. As our literature review revealed that the procedural and interpretative components of ISC have been insufficiently addressed, we follow several steps to develop items to measure each dimension of our ISC model. In these terms, we first specified the domain of interest for the construct, second, generated items informed by extant literature, and third, assessed the content validity of the items. Finally, we conducted a pretest to explore the developed items' loadings and reliability and then conducted one study to show the application of the constructs in a nomological network (MacKenzie et al., 2011).

We first applied a top-down approach and initiated the three dimensions as first-order constructs following our theoretical viewpoint of the competence model by Winther (2010). Based on our definition of conceptual ISC, the construct encompasses factual knowledge about security threats and general knowledge about measures to contain security threats. The procedural ISC construct includes the skills to select and apply conceptual security knowledge in the specific action (Winther, 2010). At last, we transferred the interpretative ISC dimension to the application case of handling security threats. Following the established definition, to fulfill this dimension, an individual needs to (1) recognize the situational elements of security threats and (2) situationally decide on the optimal course of action to mitigate security threats. Since the focal construct of ISC is multidimensional, items for each subdimension had to be formulated. As discussed in chapter 2, we searched the literature for existing items. In these terms, the items of conceptual ISC were inspired by the general ISA construct of Bulgurcu et al. (2010). In total, 20 items were created to measure all the facets of the focal construct. To capture multiple facets of conceptual ISC, we split the construct into the knowledge of consequences, characteristics, and countermeasures of security threats. For conceptual ISC 12 items were built, and four items each were built for procedural and interpretative ISC.

After the construction process, a face validity check was conducted since most items had been developed from the experience of two IS security researchers and one expert in the field of vocational education. We included two persons, one external person with a high educational background in grammar and the English language, and one IS information security expert. We instructed the persons of the face validity check not to rank or rate the items but to verify the comprehensibility, wording, and grammar (MacKenzie et al., 2011). Five items were unclear or not worded well in the first iteration of the face validity check. We, therefore, reworded the items. Once the face validity check was completed, the predefined constructs with their items were subjected to a card-sorting test following the guidelines of Moore and Benbasat (1991). The card sorting assignment was conducted to check for the content validity of the created measurement items. Content validity refers to the degree to which the items of a measurement scale represent the generalizable scope of the content (MacKenzie et al., 2011; Straub et al., 2004). Two conditions should apply: First, each item needs to be a representative piece of the entire content area of the construct. Second, all items together should represent the construct's whole content domain (MacKenzie et al., 2011). At first, we selected 12 raters to identify items that were supposed to measure the same constructs. Therefore, the raters received all items in randomized order on index cards. They then built as many constructs as they thought would be reasonable based on the wording and content of the items. As all of the conceptual ISC items are supposed to measure different facets of information security knowledge, we expected the raters to construct either three constructs or one composed construct. Afterward, the raters labeled each construct and were advised to provide feedback on the clarity and separability of the found constructs. Two raters did not specify any descriptions or identifiers for the items. Thus, we excluded them from the sorting task. Interestingly, all other raters could provide accurate descriptions of the intended constructs. All except one participant built two distinct constructs to measure procedural and interpretative ISC as intended. As expected, most raters built one single construct or three constructs for conceptual ISC. Two items in the conceptual ISC construct were mixed with other facets of the construct. These items were slightly reworded based on the rater's feedback. The results of the sorting task by the raters emphasize the initial assumption that the three facets (knowledge about consequences, countermeasures, and characteristics of security threats) are conceptually different and cover separate aspects of conceptual security knowledge. Hence, they define the meaning of the construct and are not interchangeable (Jarvis et al., 2003). We, therefore, measure conceptual ISC as a formative construct. As a result, we only kept three indicators (one for each facet) based on the rater's assessments and feedback. Instead, we expected the two first-order constructs (procedural and interpretative ISC) to be reflective constructs. This applies for two reasons. First, we expect the indicators to be correlated, and second, the indicators to be independent of the meaning of the superordinate construct. (Jarvis et al., 2003). Also, the second-order construct (action-oriented ISC) has first-order factors as reflective indicators following the previous line of reasoning.

We created a pretest with 100 participants to evaluate the psychometric validity and reliability of the new ISC constructs. The main objective of the pretest was to evaluate the comprehensibility of the items, the reliability test, and check if the items loaded to their intended constructs (MacKenzie et al., 2011). In addition, we collected data for a performance measure using an adapted scale for the past phishing handling success of Chen et al. (2020) (see Table 5). We then evaluated the formative construct conceptual ISC.

Therefore, we followed the guidelines of Hair et al. (2021) for validating formative constructs. First, we assured that the construct fulfills convergent validity. Hence, we tested whether the formatively measured construct is highly correlated with one single reflective item capturing the same construct. The path coefficient exceeded the critical threshold of 0.708 (Hair et al., 2021). Second, we assessed the outer weights between the indicators and conceptual ISC: indicator 1 (knowledge about consequences) β-=0.297, p = 0.191; indicator 2 (knowledge about countermeasures) β-=0.222, p = 0.347; indicator 3 (knowledge about characteristics) β-=0.580, p= 0.008. Hair et al. (2021) highlight that if the indicator weights are not significant, this does not indicate a poor measurement model. Instead, they advise examining the absolute contribution of a formative indicator by assessing the loading of the indicators. The indicator loadings are significant with sufficient t-statistics (indicator 1: β-=0.875, t-value=10.735 p <0.001; indicator 2: β-=0.833, t-value=9.421, p <0.001; indicator 3: β-=0.957, t-value=20.608, p <0.001). Based on the evaluation criteria for formative constructs, we investigated the variance inflation factors (VIF) of the conceptual ISC construct. All values were well below the threshold of 3.33 (Diamantopoulos & Siguaw, 2006). Secondly, we evaluated the items in terms of the validity and reliability of the first-order reflective constructs (procedural and interpretative ISC). We, therefore, submitted the items of the reflective constructs to exploratory factor analysis (EFA) (settings: principal component analysis, Promax rotation with Kaiser normalization) (Hair et al., 2014) to observe if the items loaded to the two intended constructs. The results (see Table 6 in the appendix) showed that all first-order dimensions were unidimensional, as intended. Afterward, we conducted a confirmatory factor analysis (CFA). The initial CFA suggested a high correlation of the error terms between one indicator from the procedural and one of the interpretative ISC dimensions. We, therefore, removed one item from each dimension of the analysis. The second CFA resulted in good scores based on the defined cut-off criteria for model fit based on Hu and Bentler (1999) (see Table 6). Table 1 depicts our final measurement model, including three items for each dimension of ISC.

Second Order	**First Order**	**First-Order Items**
	Conceptual ISC (formative)	I possess knowledge about the associated consequences of [*security threats].*
		I know measures to combat [*security threats].*
		I am familiar with the characteristics of [*security threats].*
Action-Oriented ISC (reflective)	Procedural ISC (reflective)	When I have chosen measures to mitigate a [*security threat]*, I can implement them.
		After selecting a counterstrategy against a [*security threat]*, I can take the necessary steps to apply it.
		Once I have decided on a counterstrategy against a [*security threat]*, I can take the necessary actions to execute it.
	Interpretative ISC (reflective)	Based on the identification of the situational characteristics of a [*security threat]*, I can develop the best solution to combat the threat.
		By identifying a [*security threat]* according to situation-specific elements, I can determine the most effective strategy to counter it.
		As a result of recognizing the situational characteristics of a [*security threat]*, I can devise a solution that will be most effective to mitigate it in the situation.

Table 1. Final Measurement Items

To assess the reliability of the constructs, we also evaluated Cronbach's alpha, which was above the commonly suggested threshold of 0.7, implying high reliability (Nunnally, 1978). We also assessed discriminant validity by using the Fornell–Larcker criterion (Fornell & Larcker, 1981), which was also fulfilled. Moreover, we assessed the Heterotrait–Monotrait (HTMT) ratio of correlations and found them to be below the threshold of 0.85. Afterward, we concluded our measurement items to be reliable for further analysis.

Applying the Competence Dimensions to the Information Security Domain

Subsequent to the adaption of the competence structure model by Winther (2010) to the information security domain, we show how it can be applied to investigate the effect of ISC on information security performance. Figure 2 depicts the underlying research model. The competence model by Winther (2010) which informs our research model views the interplay of the facets of competence to be interconnected and interactive in nature. This implies that the ability to cope with a given situation depends on the availability of the different dimensions of competence.

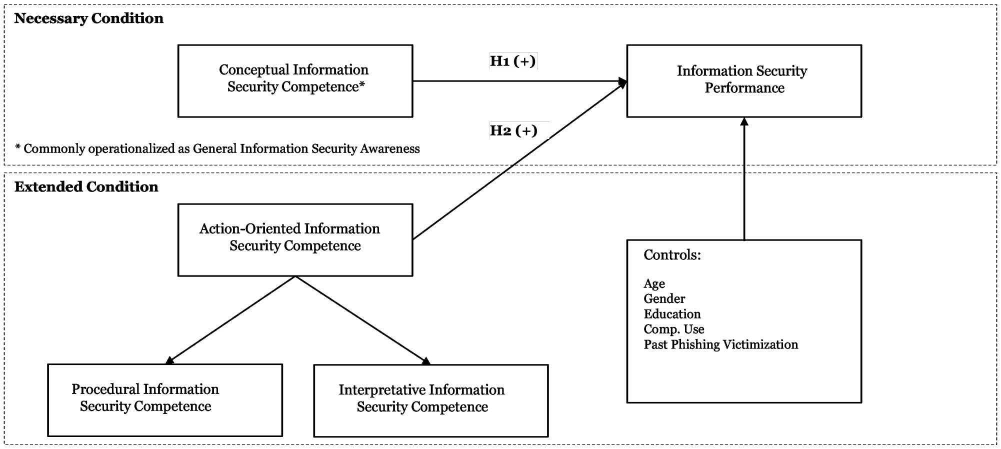
Necessary Condition
Conceptual Information Security Competence*
H1 (+)
Information Security Performance
H2 (+)
* Commonly operationalized as General Information Security Awareness
Extended Condition
Action-Oriented Information Security Competence
Controls:
Age
Gender
Education
Comp. Use
Past Phishing Victimization
Procedural Information Security Competence
Interpretative Information Security Competence

Figure 2. Research Model

Imagine someone who faces a phishing attack. In the process, all three types of competence are required. First, the person must know the different forms of phishing, the indicators, consequences, and countermeasures to mitigate the attack (conceptual competence). The person must be able to apply his or her knowledge (procedural competence) to overcome the threatening situation. This includes the selection and application of a countermeasure. Finally, interpretative competence is needed to differentiate when to use a specific countermeasure that is appropriate to the situation (Alexander et al., 1991). Based on these considerations, different levels of the fulfillment of each dimension of competence lead to successful action-taking. Therefore, two types of conditions can be derived that lead to high-performance levels.

The Necessary Condition

While procedural and interpretive competence require a meaningful understanding of concepts (such as rules) and their application, it is possible to know the "what" of a particular task in a domain without the more detailed context of how and when to utilize it (Alexander et al., 1991). As McCormick (1997) and Glaser (1984) describe, conceptual knowledge is essential for effectively using procedural knowledge in problem-solving. Accordingly, research studies in cognitive psychology have shown that the minimum criterion for high-performance levels depends on an accessible and extensive conceptual knowledge base (Alexander & Judy, 1988; Chi, 1981). Hence, a certain amount of facts and rules is necessary to choose, combine, and evaluate strategies. Thus, content knowledge serves as the foundation for strategy development; without this knowledge, the ability to develop strategies is limited at best and impossible at worst (Alexander & Judy, 1988). When transferring this relationship to the context of successfully handling security threats, it becomes apparent that without a strong conceptual knowledge base (knowledge of characteristics, countermeasures, and consequences that can result from poor behavior), all downstream steps, such as selecting and implementing a counterstrategy appropriate to the situation, can only be successful to a limited extent. Therefore, conceptual ISC should be a necessary condition for showing domain-specific performance. However, the mastery of a task also depends strongly on the difficulty of a demanding situation (Winther 2010). Depending on the difficulty of handling a possibly faced security threat, conceptual ISC may be sufficient to cope with the situation leading to acceptable performance. Based on these arguments, we derive the following hypothesis:

H1: Employees' Conceptual ISC has a *positive* effect on Information Security Performance.

The Extended Condition

As noted previously, a minimal knowledge base in the domain is a necessary but not sufficient condition for the effective use of procedural and interpretative knowledge (Alexander & Judy, 1988). Yet, there is evidence in extant literature that individuals often fail to develop efficient strategies when dealing with a domain-specific task. Results from cognitive psychology research indicate that conceptual knowledge falls short when individuals lack the strategic competence that activates or operates the conceptual knowledge (Reys & Rybolt, 1982; Schoenfeld, 1987). In these terms, research in VET has revealed that individual performance is largely shaped by how they perceive and assess a situation (Pintrich & De Groot, 1990; Pressley et al., 1987). To make informed decisions about adequate solution strategies, conceptual knowledge about a topic must be assembled and utilized through its application (Winther 2010). Thus, conceptual knowledge structures are elementary, but someone well-trained in a domain can transfer this conceptual knowledge to specific situations of action. Moreover, Winther (2010) points out that if the specific elements characterizing the requirements to cope with the situation are misinterpreted, it becomes more challenging for the individual to develop an appropriate solution for the problem context. Following this line of reasoning, employees who know about phishing attacks (including the characteristics, countermeasures, and consequences of inadequate behavior) but do not situationally know how and which countermeasures to take will likely fail to recognize and/or take the required steps to mitigate them. Hence, we argue that procedural and interpretative competence can contribute to the utilization of domain-specific (conceptual) competence resulting in higher performance levels. As action-0riented ISC is composed of both constructs, we propose the following:

H2: Employees' Action-Oriented ISC *positively* affects Information Security Performance.

Method

Survey Design

A cross-sectional survey design was applied to test our research model. To enable the participants to assess their competence best, they were asked to put themselves in a fictitious scenario. In the scenario, the participants were employees of the NextBigOffice firm. They were given a name and additional information, such as the work environment, the boss' name, and the tools and work tasks they perform in the company. Then they were shown three different phishing attacks that differed in nature and characteristics. The first threat contained an email that appeared to be sent from Microsoft. Participants were asked to verify their accounts again. Otherwise, it would be blocked within the next 12 hours. Attentive subscribers could tell from the sender and the link address in the email that the email was phishing. The second threat was a Microsoft Teams message supposedly sent by the boss of NextBigOffice company. In the message, an attachment was sent asking the subject to review the plan costs. Participants identified a potential phishing attack based on the link and the differing company email from their boss. In addition, the message was classified as external. The third threat was a private message via LinkedIn in which a person pretended to be a colleague. Each participant then had the time to determine for themself if they were confronted with one or multiple phishing attacks. Afterward, they were told that all three threats were phishing attempts. We followed the scenario-based approach to enable participants to reflect on their own capabilities in handling phishing attacks. Moreover, evaluations of one's own competence need to be grounded in realistic situations (Winther 2010). In the next stage, the participants were asked to self-evaluate their competence in handling these or related phishing attacks, which they were confronted with in their real-world jobs. Finally, they were prompted to assess their past phishing handling success as the performance-related outcome measure in the last three months. All items were measured on a 7-point Likert scale (1 = Strongly disagree, 7 = Strongly agree).

Data Collection and Sampling

Three experts reviewed the questionnaire before the survey was conducted. This ensured high comprehensibility and a logical structure of the questionnaire. The review led to minor changes in the wording and the length of the scenario descriptions. As study participants, we included persons who were fully employed, fluent English speakers, and had been at least once confronted with a phishing attack in their previous working life. This ensured that participants were able to put themselves in the situation appropriately. Subsequently, the participants were asked about all variables of interest. Additionally, two attention checks were designed to control for high quality in the respondent's clicking behavior. After excluding data records due to quality criteria such as missing data, 234 completed questionnaires could be used for statistical analysis. The average age of participants was 41 years, and 51% of participants were female, while the other 49% were male. 87% of participants received at least one phishing training in their working life. 27.97% specified that their highest degree is high school, 47.03 % had a college degree, 20.34% of participants had a bachelor's degree, and the remaining 4.66% indicated to have a master's degree or equivalent.

Results

Measurement Validation

In order to evaluate our research model, we used structural equational modeling (SEM) with Partial-Least Squares (PLS) analysis for mainly two reasons. First, our SEM model includes a formative construct, and second, it supports the modeling of a second-order reflective construct (Hair et al., 2021) Initially, we evaluated the reliability and validity of conceptual ISC as a formative construct. As we validated convergent validity in the pretest data, we limited the evaluation to first assessing the outer weights and factor loadings and second evaluating the VIF. Although the outer weight of CISC1 is not significant, the factor loading is greater than 0.5. Also, the VIF for all indicators is below the critical threshold of 3.33. The results can be seen in Table 2.

Constructs	ID	Weight		Loading	VIF
		Estimate	p-value		
Conceptual ISC	CISC1	0.103	0.612	0.705	1.727
	CISC2	0.449	**0.011***	0.877	1.829
	CISC3	0.574	**0.001****	0.929	2.100

Note: * p<0.05; ** p<0.01; *** p<0.001; all p-values that indicate a significance at α < .05 are bolded

Table 2. Formative Measurement Model Results

As a second step, we assessed the reliability and validity of the first-order reflective constructs and the dependent variable. Table 3 shows the results of the measurement validation of the reflective constructs.

	ID	Loading	CR	CA	AVE	PISC	IISC	PHS
PISC	PISC1	0.931	0.966	0.947	0.904	**0.951**		
	PISC2	0.965						
	PISC3	0.957						
IISC	IISC1	0.941	0.959	0.937	0.887	0.796	**0.942**	
	IISC2	0.947						
	IISC3	0.938						
PHS	PHS1	0.960	0.968	0.951	0.911	0.481	0.381	**0.954**
	PHS2	0.955						
	PHS2	0.948						

Note: AVE = Average Variance Extracted; CR = Composite Reliability; CA = Cronbach's Alpha; PISC = Procedural ISC; IISC = Interpretative ISC; PHS = Past Phishing Handling Success

Table 3. Reflective Measurement Model Results

First, all factor loadings are above the threshold of 0.7 and thus fulfill convergent validity. Moreover, composite reliability exceeds the cut-off criterion of 0.7 (Fornell & Larcker, 1981; Nunnally & Bernstein, 1994). As a next step, we investigated the AVE and found that it is well above 0.5 for all constructs (MacKenzie et al., 2011). Lastly, we evaluated the HTMT of each variable and the fulfillment of the Fornell-Larcker criterion in the research model. All scores were below the strict threshold of 0.85 (Henseler et al., 2015). Furthermore, for each construct the square root of the AVE was greater than the correlation with other constructs. Lastly, we evaluated the reliability and validity of the second-order construct action-oriented ISC. All reliability and validity criteria were above the recommended thresholds (Factor loading: PISC: 0.959, IISC: 0.935; CR: 0.921; CA:0.887; AVE:0.897). In order to rule out potential common method bias in our data, we conducted the Harmann one-single-factor test. Based on the results, the total variance explained by one factor was 43.5% (below the threshold of 50%) (Podsakoff & Organ, 1986). Additionally, we utilized the marker variable technique to check for common method variance. The highest correlation of our marker variable (i.e., "I like the color blue") with the research variables is 0.2, suggesting that common method bias is not a concern for our study.

Structural Model Analysis

We applied the structural model to handling phishing attacks to highlight the relationship between the dimensions of ISC and information security performance. The performance construct has been conceptually measured by past phishing handling success. This construct was adapted from the past phishing detection success construct operationalized by (Chen et al., 2020) and developed by (Bose & Leung, 2007) (see Table 5 in the appendix). The model includes the following demographic control variables (age, gender, and education), and control variables that are directly related to handling phishing attacks (daily computer usage and past phishing victimization). To evaluate our measurement model, we applied the disjoint two-stage approach using SmartPLS4, following the guidelines of Sarstedt et al. (2019). As a common practice, we used the bootstrapping re-sampling method with 5000 samples to evaluate the path estimations. Before we interpreted the path coefficients, we assessed the model fit. The SRMR is 0.035, indicating a good fit (Hu and Bentler, 1999). Table 4 shows the results of the path estimations.

Path	**β-value**	**t-value**	**p-value**
Independent variable (Direct effect)			
Conceptual ISC → Past Phishing Handling Success	0.255	2.798	**0.005****
Action-Oriented ISC → Past Phishing Handling Success	0.271	2.610	**0.009****
Controls			
Age → Past Phishing Handling Success	0.018	0.252	0.801
Gender → Past Phishing Handling Success	-0.002	0.019	0.985
Education → Past Phishing Handling Success	0.071	1.259	0.208
Computer Usage → Past Phishing Handling Success	-0.045	0.847	0.397
Past Phishing Victimization → Past Phishing Handling Success	0.155	1.211	0.226

Note: * p<0.05; ** p<0.01; *** p<0.001; all p-values that indicate a significance at α < .05 are bolded

Table 4. Results of the PLS-SEM Model Estimation

Our analysis indicated that none of the control variables significantly affected past phishing handling success. The PLS-SEM results indicate that the model accounts for a substantial amount of explained variance. The model explains 26 % of the variance of past phishing handling success. The data confirm H1 in our research model. An employee's conceptual ISC positively affects information security performance. Regarding H2, our findings support the assumption that an employee's action-oriented ISC positively affects information security performance.

Discussion

Drawing on research in the field of VET, we assumed that ISC is multi-dimensional. Our results indicate that both conceptual ISC and action-oriented ISC influence information security performance (measured as self-reported success in handling phishing attacks). Our data thus reinforce the impression that ISC is an important driver of information security performance, which has been neglected in previous literature. The path coefficients indicate that conceptual and action-oriented ISC are equally important in explaining the variance in the phishing handling success of employees. This result aligns with the theoretical assumptions that each competence dimension makes a unique contribution to handling phishing attacks effectively. It also enforces our initial conceptualization of conceptual ISC as a necessary condition for information security performance and action-oriented ISC as an extended condition.

Our work has several implications for IS security literature. First, we have extended the General ISA concept which is acknowledged to enhance employees' compliance behavior. While "knowing-what" (conceptual competence) has been considered as an antecedent of security-related outcomes in prior literature, we are among the first to shed light on the "knowing-how (procedural competence) and the "know-how-to-decide-what-to-do-and-when-knowledge" (interpretative competence) (Gibson, 2008). Therefore, we utilize the competence model by Winther (2010) as a theoretical point of view in the information security context.

Second, we introduce a new measurement scale to assess this basic model of ISC at the employee level. The measurement items were tested in two studies with 360 participants in total. Hence, our measurement tool can be contextualized to varying security threats (such as social engineering, password policies, and ransomware attacks). As a self-assessment instrument, it can function as the first indicator to locate security-related knowledge gaps in employees. It can then be leveraged to evaluate the effectiveness of SETA programs. Considering greater discourse on human-caused misbehavior, the importance of acquiring insights into ISC on the individual level constantly increases. Our new perspective on assessing these competencies can offer methodical foundations that go beyond measuring conceptual security knowledge. Third, we link to the research stream that addresses why some SETA programs might fall short of their expectations. Our results indicate that the basic dimensions of ISC contribute jointly to enhanced information security performance. Although we have not shown in this study how each of the three competence dimensions can be trained efficiently, we propose that different types of SETA interventions (such as micro-trainings and educational ISP training) may stimulate the acquisition of ISC differently.

Next to contributions to literature, our study holds several important implications for practitioners. In recent years, we can observe a massive trend of companies investing in cybersecurity (Gartner, 2022). This includes technical as well as organizational measures. Therefore, these companies are interested in understanding the security-related knowledge gaps of their employees better. Practitioners can integrate the instrument into their set of evaluation instruments for the effectiveness of their SETA programs. In the practical context, a wide variety of training formats exists, such as different forms of security micro-trainings (intranet messages, email notices, videos, flyers, and posters) and educational ISP training (real-world simulations, onsite training courses) (Boss et al., 2015; Puhakainen & Siponen, 2010). However, it can be challenging for decision-makers to select the measures that balance budget constraints with meeting employees' knowledge gaps from these formats. Thus, our measurement constructs allow corporate decision-makers to gauge their employees' ISC and qualification requirements in an orienting step prior to training selection. Our conceptualization of different dimensions of ISC enables them to align their decisions with qualification needs. For instance, if employees fall short in procedural competence, training in applying security knowledge or, more specifically, applying measures to combat security threats might be beneficial. If employees show weak spots in interpretative ISC, the SETA program should possibly be more tailored to specific contexts of potentially emerging security threats. In this study, we have shown that security threats differ in the scope and context they appear. Hence, the characteristics that indicate this form of attack vary. Moreover, the counterstrategy to mitigate security threats is dependent on the setting it is embedded in. Security-competent individuals can differentiate between these contexts and make informed decisions about the necessary steps to combat these situations and to self-improve their behavior for future action taking. Fostering interpretative ISC might also require designing examples of security threats in the training programs as realistically as possible. On the one hand, a social media marketing manager will likely need more training in dealing with potential phishing attacks spread through social media channels. On the other hand, back-office employees must be more likely be prepared to recognize phishing via email and collaboration tools.

Our study has limitations that are described in the following. First, the study is based on a survey that deals with the specific security threat of phishing. To ensure a high level of relevance for the target group we surveyed only fully employed participants who have been confronted with a phishing attack at least once in their working lives. Furthermore, we used examples of phishing that have been acknowledged by participants to be very realistic (mean: 5.27). However, the external validity of our study could be increased by conducting the study with real phishing attacks. In these terms, conducting interventions using fake phishing emails sent to the participant's email addresses would be interesting. Similarly, the measurement of information security performance can be enhanced when using longitudinal data. Second, we collected cross-sectional survey data to validate the relationship between ISC and information security performance. We plan to utilize our measurement constructs to prove their applicability in online experiments. Third, we generalize the effect found in our study as it was only conducted with a sample in the U.S.A.. Fourth, to achieve stable results in terms of validity and reliability the measurement scale needs to be applied to other security threats beyond the handling of phishing attacks. Lastly, we assessed ISC and information security performance from self-reported statements. As a future research agenda, we highlight the necessity to investigate how each competence dimension conceptualized in this work can be stimulated through different types of SETA interventions.

Conclusion

In this research paper, we have conceptualized the basic dimensions of ISC. Our results show that existing measurement scales do not account for the ability to cognitively evaluate specific demands of a situation. Our conceptualization of ISC suggests that both the effect of conceptual ISC and the effect of action-oriented ISC have a significant impact on information security performance. While conceptual ISC has been leveraged as an antecedent of information security compliance in previous literature, we show that action-oriented ISC is an important factor that additionally drives the performance of employees.

Acknowledgments

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

Alexander, P. A., & Judy, J. E. (1988). The Interaction of Domain-Specific and Strategic Knowledge in Academic Performance. *Review of Educational Research*, *58*(4). **https://doi.org/10.3102/00346543058004375**

Alexander, P. A., Schallert, D. L., & Hare, V. C. (1991). Coming to Terms: How Researchers in Learning and Literacy Talk About Knowledge. *Review of Educational Research*, *61*(3), 315–343. **https://doi.org/10.3102/00346543061003315**

Bandura, A. (1986). Social Foundations of Thought and Action: A Social Cognitive Theory. *Englewood Cliffs*, *1986*(23–28).

Blömeke, S., Gustafsson, J. E., & Shavelson, R. J. (2015). Beyond dichotomies: Competence viewed as a continuum. *Zeitschrift Fur Psychologie / Journal of Psychology*, *223*(1), 3–13. **https://doi.org/10.1027/2151-2604/a000194**

Bose, I., & Leung, A. C. M. (2007). Unveiling the Mask of Phishing: Threats, Preventive Measures, and Responsibilities. *Communications of the Association for Information Systems*, *19*. **https://doi.org/10.17705/1CAIS.01924**

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors. *MIS Quarterly*, *39*(4), 837–864. **https://doi.org/10.25300/MISQ/2015/39.4.5**

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 523–548. **https://doi.org/10.2307/25750690**

Chen, R., Gaia, J., & Rao, H. R. (2020). An examination of the effect of recent phishing encounters on phishing susceptibility. *Decision Support Systems*, *133*, 113287. **https://doi.org/10.1016/j.dss.2020.113287**

Chi, M. T. (1981). *Knowledge development and memory performance*. Springer.

Corno, L., Cronbach, L. J., Kupermintz, H., Lohman, D. F., Mandinach, E. B., Porteus, A. W., & Talbert, J. E. (2001). *Remaking the Concept of Aptitude: Extending the Legacy of Richard E. Snow*. Routledge. **https://doi.org/10.4324/9781410604521**

Cram, W. A., D’Arcy, J., & Proudfoot, J. G. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly*, *43*(2), 525–554. **https://doi.org/10.25300/MISQ/2019/15117**

D’Arcy, J., & Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security countermeasures. *Journal of Business Ethics*, *89*(1), 59–71. **https://doi.org/10.1007/s10551-008-9909-7**

D’Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79–98. **https://doi.org/10.1287/isre.1070.0160**

D’Arcy, J., & Lowry, P. B. (2019). Cognitive-affective drivers of employees’ daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*, *29*(1), 43–69. **https://doi.org/10.1111/isj.12173**

Diamantopoulos, A., & Siguaw, J. A. (2006). Formative versus reflective indicators in organizational measure development: A comparison and empirical illustration. *British Journal of Management*, *17*(4), 263–282. **https://doi.org/10.1111/j.1467-8551.2006.00500.x**

Fornell, C., & Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research*, *18*(1), 39. **https://doi.org/10.2307/3151312**

Gartner. (2022). Information security spending worldwide from 2017 to 2023, by segment (in million U.S: dollars). *In Statista.* **https://www.statista.com/statistics/790834/spending-global-security-technology-and-services-market-by-segment/**

Gibson, K. (2008). Technology and technological knowledge: A challenge for school curricula. *Teachers and Teaching*, *14*(1), 3–15. **https://doi.org/10.1080/13540600701837582**

Glaser, R. (1984). Education and thinking: The role of knowledge. *American Psychologist*, *39*(2), 93. **https://psycnet.apa.org/doi/10.1037/0003-066X.39.2.93**

Greeno, J. G., Riley, M. S., & Gelman, R. (1984). Conceptual competence nd children's counting. *Cognitive Psychology*, *16*(1), 94–143.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2014). Pearson new international edition. *Multivariate Data Analysis, Seventh Edition. Pearson Education Limited Harlow, Essex.*

Hair, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2021). *A primer on partial least squares structural equation modeling (PLS-SEM)*. SAGE.

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, *43*, 115–135. **https://link.springer.com/article/10.1007/s11747-014-0403-8**

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125. **https://doi.org/10.1057/ejis.2009.6**

Hu, L., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal*, *6*(1), 1–55. **https://doi.org/10.1080/10705519909540118**

Hu, S., Hsu, C., & Zhou, Z. (2021). Security Education, Training, and Awareness Programs: Literature Review. *Journal of Computer Information Systems*, 1–13. **https://doi.org/10.1080/08874417.2021.1913671**

IBM Security. (2019). Cost of a Data Breach Report. *IBM Security*, 76.

Jarvis, C. B., MacKenzie, S. B., & Podsakoff, P. M. (2003). A Critical Review of Construct Indicators and Measurement Model Misspecification in Marketing and Consumer Research. *Journal of Consumer Research*, *30*(2), 199–218. **https://doi.org/10.1086/376806**

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). *An Enhanced Fear Appeal Rhetorical Framework: Leveraging threats to the human asset trough sanctioning rhetoric*. MIS Quarterly *39*(1), 113–134.

Klotz, V. K., Winther, E., & Festner, D. (2015). Modeling the Development of Vocational Competence: A Psychometric Model for Economic Domains. *Vocations and Learning*, *8*(3), 247–268. **https://doi.org/10.1007/s12186-015-9139-y**

Kwon, J., & Johnson, M. E. (2018). Meaningful healthcare security: Does meaningful-use attestation improve information security performance? *MIS Quarterly*, *42*(4), 1043–1068. **https://doi.org/10.25300/MISQ/2018/13580**

Lau, S., & Roeser, R. W. (2002). Cognitive Abilities and Motivational Processes in High School Students' Situational Engagement and Achievement in Science. *Educational Assessment*, *8*(2), 139–162. **https://doi.org/10.1207/S15326977EA0802_04**

Lebek, B., Guhr, N., & Breitner, M. H. (2014). Transformational Leadership and Employees' Information Security Performance: The Mediating Role of Motivation and Climate. *ICIS 2014 Proceedings. 21.* **https://aisel.aisnet.org/icis2014/proceedings/ISSecurity/21/**

Li, H., Yoo, S., & Kettinger, W. J. (2021). The Roles of IT Strategies and Security Investments in Reducing Organizational Security Breaches. *Journal of Management Information Systems*, *38*(1), 222–245. **https://doi.org/10.1080/07421222.2021.1870390**

Lowry, P. B., Posey, C., Bennett, R. B. J., & Roberts, T. L. (2015). Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies. *Information Systems Journal*, *25*(3), 193–273. **https://doi.org/10.1111/isj.12063**

MacKenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. *MIS Quarterly: Management Information Systems*, *35*(2), 293–334. **https://doi.org/10.2307/23044045**

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and Information Security Awareness. *Computers in Human Behavior*, *69*, 151–156. **https://doi.org/10.1016/j.chb.2016.11.065**

McCormick, R. (1997). Conceptual and procedural knowledge. *International Journal of Technology and Design Education*, *7*, 141–159. **https://doi.org/10.1023/A:1008819912213**

Moore, G. C., & Benbasat, I. (1991). Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation. *Information Systems Research*, *2*(3), 192–222. **https://doi.org/10.1287/isre.2.3.192**

Naseer, H., Maynard, S., & Ahmad, A. (2016). Business analytics in information security risk management: The contingent effect on security performance. *Research-in-Progress Papers. 13*. **https://aisel.aisnet.org/ecis2016_rip/13**

Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory* (3rd ed). McGraw-Hill.

Park, E. H., Kim, J., & Park, Y. S. (2017). The role of information security learning and individual factors in disclosing patients' health information. *Computers & Security*, *65*, 64–76. **https://doi.org/10.1016/j.cose.2016.10.011**

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers and Security*, *42*(May), 165–176. **https://doi.org/10.1016/j.cose.2013.12.003**

Pintrich, P. R., & De Groot, E. V. (1990). Motivational and self-regulated learning components of classroom academic performance. *Journal of Educational Psychology*, *82*(1), 33–40. **https://doi.org/10.1037/0022-0663.82.1.33**

Podsakoff, P. M., & Organ, D. W. (1986). Self-reports in organizational research: Problems and prospects. *Journal of Management*, *12*(4), 531–544. **https://doi.org/10.1177/014920638601200408**

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders motivation to protect organizational information assets. *Journal of Management Information Systems*, *32*(4), 179–214. **https://doi.org/10.1080/07421222.2015.1138374**

Pressley, M., Borkowski, J. G., & Schneider, W. (1987). *Cognitive strategies: Good strategy users coordinate metacognition and knowledge*.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, *34*(4), 757–778. **https://doi.org/10.2307/25750704**

Rampold, F., Schütz, F., Masuch, K., Köpfer, P., & Warwas, J. (2022). Are you aware of your competencies? – The potentials of competence research to design effective SETA programs. *ECIS 2022 Research Papers. 134.*, 1–17.

Rausch, A., Kögler, K., & Seifried, J. (2019). Validation of Embedded Experience Sampling (EES) for Measuring Non-cognitive Facets of Problem-Solving Competence in Scenario-Based Assessments. *Frontiers in Psychology*, *10*, 1200. **https://doi.org/10.3389/fpsyg.2019.01200**

Reys, R. E., & Rybolt, J. F. (1982). Processes Used by Good Computational Estimators. *Journal for Research in Mathematics Education*, *13*(3), 183–201. **https://doi.org/10.5951/jresematheduc.13.3.0183**

Sarstedt, M., Hair, J. F., Cheah, J.-H., Becker, J.-M., & Ringle, C. M. (2019). How to Specify, Estimate, and Validate Higher-Order Constructs in PLS-SEM. *Australasian Marketing Journal*, *27*(3), 197–211. **https://doi.org/10.1016/j.ausmj.2019.05.003**

Schoenfeld, A. H. (1987). What's all the fuss about metacognition? *Cognitive Science and Mathematics Education*, 189–215.

Schuetz, F., Rampold, F., Köpfer, P., Mann, D., Trang, S., Masuch, K., & Warwas, J. (2023). *Bridging the Gap between Security Competencies and Security Threats: Toward a Cyber Security Domain Model*. 10. **https://hdl.handle.net/10125/103375**

Seeber, S. (2016). Vom Domänenmodell zum Kompetenzmodell: Konturen eines Assessmentdesigns zur Messung beruflicher Fachkompetenzen bei Medizinischen Fachangestellten. In *Bwp@ Berufs-und Wirtschaftspädagogik online* (pp. 1–25).

Siponen, M., Adam Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information and Management*, *51*(2), 217–224. **https://doi.org/10.1016/j.im.2013.08.006**

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Information & Computer Security*, *23*(2), 200–217. **https://doi.org/10.1108/ICS-04-2014-0025**

Spencer, L. M., & Spencer, S. M. (1993). *Competence at work: Models for superior performance*. NY: Wiley & Sons.

Straub, D., Boudreau, M.-C., & Gefen, D. (2004). Validation Guidelines for IS Positivist Research. *Communications of the Association for Information Systems*, *13*(1), 24. **https://doi.org/10.17705/1CAIS.01324**

Tessian. (2020). *Psychology of Human Error 2020*. https://www.tessian.com/research/the-psychology-of-human-error/

Verizon. (2020). *Data Breach Investigations Report*. **https://www.verizon.com/business/resources/reports/2020-data-breach-investigations-report.pdf**

Wang, J., Li, Y., Columbia College, & The University of Texas at San Antonio. (2016). Overconfidence in Phishing Email Detection. *Journal of the Association for Information Systems*, *17*(11), 759–783. **https://doi.org/10.17705/1jais.00442**

Wang, J., Li, Y., & Rao, H. R. (2017). Coping Responses in Phishing Detection: An Investigation of Antecedents and Consequences. *Information Systems Research*, *28*(2), 378–396. **https://doi.org/10.1287/isre.2016.0680**

Warwas, J., Vorpahl, W., Seeber, S., Krebs, P., Weyland, U., Wittmann, E., Wilczek, L., & Strikovic, A. (2023). Developing and validating an online situational judgment test on the stress coping competence of nursing apprentices. *Empirical Research in Vocational Education and Training*, *15*(1), 5. **https://doi.org/10.1186/s40461-023-00145-x**

Winther, E. (2010). *Kompetenzmessung in der beruflichen Bildung*. Bertelsmann.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*(6), 2799–2816. **https://doi.org/10.1016/j.chb.2008.04.005**

Appendix

Constructs and Items
Past Phishing Handling Success (based on Chen et al. 2020) I had been successful in combating phishing attacks in the past three months. I had defeated most phishing attacks that I encountered in the past three months. I had been able to handle phishing attacks and not fall for them in the past three months.

Table 5. Past Phishing Handling Success Measurement

	EFA			**CFA**		
Item ID	**Factor 1**	**Factor 2**	**Cronbach's Alpha**	**Factor Loading**	**Model Fit**	
					Fit Index	**Value**
PISC1	0.05	**0.86**	0.916	0.934	X^2/df	1.14 < 3
PISC2	-0.02	**0.88**		0.857	SRMR	0.023 < 0.08
PISC3	-0.02	**0.91**		0.872	RMSEA	0.038 < 0.06
PISC4 (removed)	0.18	**0.76**		-	TLI	0.995 > 0.95
IISC1	**0.76**	0.13	0.876	0.908	CFI	0.997 > 0.95
IISC2	**0.82**	0.01		0.838		
IISC3 (removed)	**0.88**	-0.01		-		
IISC4	**0.80**	0.04		0.773		
Note: The CFA has been conducted using PISC1, PISC2, PISC3, IISC1, IISC2, IISC4						

Table 6. Results of the EFA and CFA Pretest Data