Received 17 March 2025
Revised 21 May 2025
Accepted 21 May 2025

Developing and testing a framework for matching distinct personality types with information security awareness methods

Satu Bjorn, Veronika Jashari, Ella Kolkowska and Shang Gao
Department of Informatics, Orebro University, Orebro, Sweden

Abstract

Purpose – This study aims to develop and test a framework to associate learning styles and social influencing vulnerabilities with different personality types in the context of tailoring information security awareness (ISA) methods for people with different personality types.

Design/methodology/approach – The framework was developed following directed content analysis and applied to match distinct personality types with ISA methods identified through a systematic literature search. The directed content analysis was conducted in two parts: a) Describe and identify keywords for the DISC (dominance [D], inducement [I], submission [S] and compliance [C]) personality types, Kolb's learning styles and Cialdini's social influencing principles; b) Identify the relationships between personality types, learning styles and social influencing vulnerabilities and create the PLS (i.e. personality types, learning styles and social influencing vulnerabilities) framework. As a result, four relationships are identified for each distinct personality type in the PLS framework.

Findings – The study has theoretically demonstrated the framework's feasibility of finding best-matched ISA methods for distinct personality types, considering their linked learning style and social influencing vulnerabilities.

Research limitations/implications – The study provides two main theoretical contributions: 1) PLS framework: presenting the relationship of personality types with their linked learning style and their social influencing vulnerabilities; 2) Examples of matching distinct personality types with ISA methods, including suggestions for a theoretically best matched ISA method. Therefore, this study contributes to building a sound theoretical ground for tailoring ISA methods for people with different personality types. In addition, the derived keywords are helpful to capture a good understanding of the different dimensions of the selected theories. Furthermore, following the examples provided in this paper, the developed PLS framework can be used as a base for managers to use ISA methods for people with different personality types in organizations.

Practical implications – Furthermore, following the examples provided in this paper, the developed PLS framework can be used as a base for managers to employ ISA methods for people with different personality types in organizations.

Originality/value – To the best of the authors' knowledge, this study is the first of its kind in developing and testing a framework for matching distinct personality types with information security awareness methods.

Keywords Information security awareness methods, Personality types, Learning styles, Social influencing vulnerabilities, Information security awareness (ISA)

Paper type Research paper

Information & Computer Security
Vol. 34 No. 2, 2026
pp. 246-272
Emerald Publishing Limited
2056-4961
DOI 10.1108/ICS-03-2025-0091

1. Introduction

Information is an essential asset in organizations and must be protected to not affect its confidentiality, integrity and availability (Kritzinger and Smith, 2008). Previous studies (e.g. Mouton *et al.*, 2016; Murray *et al.*, 2024; Stahl *et al.*, 2012) indicated that many organizational information security incidents were due to the exploitation of human elements, and a large number of information security breaches are caused by employees (Khatib and Barki, 2020). A common reason for security breaches in organizations is employees' lack of information security awareness (ISA) (Parsons *et al.*, 2014; Soomro *et al.*, 2016). ISA is in research perceived and managed in different ways, and there is no common definition, method and approach of ISA, as it is a socially constructed concept (Tsohou *et al.*, 2008). ISA tends to focus on the extent to which an employee understands the importance and implications of information security policies, rules and guidelines, and the extent to which they behave in accordance with these policies, rules and guidelines (Kruger and Kearney, 2006).

Different ISA delivery methods (ISA methods) such as classes, workshops, educational emails, posters and gamification have been proposed to rise employees' information security awareness in the organization. The different ISA methods may be combined in an ISA program. The main goal with an ISA program is to give employees skills that help them identify, disable and report any malicious attempts by attackers (Aldawood and Skinner, 2019c). However, an individual's knowledge of information security is not the sole factor that determines his/her security behavior (Schutz, 1982). Different people may respond differently to a specific ISA method, depending on their personality (e.g. risk-taker vs. cautious), learning preferences or perception of the situation, which would have an influence on their security behavior.

Although there are many existing studies on ISA methods (e.g. Alyami *et al.*, 2024; Khando *et al.*, 2021; Pahlavanpour and Gao, 2024), there is still a lack of research on how to adjust ISA programs to the targeted audiences (Hu *et al.*, 2022). Previous studies suggested that an individual's personality played an important role in understanding information security behaviors (Aharony *et al.*, 2020; Flowerday and Van der Schyff, 2019; Hadlington *et al.*, 2019), and ISA methods should be adjusted to individual employee personality type (Hadlington *et al.*, 2019). Furthermore, previous studies also indicated that personality types are influenced in different ways by social influencing principles (e.g. Alkış and Temizel, 2015) and that ISA is improved when training is provided in line with an individual's preferred learning style (Pattinson *et al.*, 2020). However, to our knowledge, none of the previous studies have theoretically addressed matching distinct personality types with existing ISA methods by considering learning styles and social influencing vulnerabilities.

Therefore, the aim of the study is to develop and test a framework to associate learning styles and social influencing vulnerabilities with different personality types in the context of tailoring ISA programs by matching distinct personality types with ISA methods. The framework was initially presented at the HAISA2024 conference (i.e. Jashari *et al.*, 2024). This paper extends the conference paper by testing the framework to tailor ISA programs for targeted audiences.

The rest of the paper is organized as follows. The related work is presented in Section 2. Section 3 describes the theoretical background for forming the foundation for the framework development. Section 4 illustrates the research method. The developed framework is presented in Section 5. In Section 6, we describe ISA methods identified in the literature review and in Section 7, we show how the PLS framework can be used to much distinct

personality types with ISA methods. This is followed by discussion and conclusion in Section 8.

2. Related work

According to the literature, the ISA methods are often randomly chosen and applied without considering the targeted audiences (Haeussinger and Kranz, 2017). This in turn leads to users' unwillingness to actively participate in ISA training (Micallef and Arachchilage, 2017) and results in insufficient knowledge and ISA that do not sustain (Reinheimer *et al.*, 2020).

A recent literature review (Hu *et al.*, 2022) found that content in an ISA program needs to be adjusted to the targeted audiences (Tsohou *et al.*, 2015) and to the knowledge level of the users (Tse *et al.*, 2013). Since personally adjusted ISA training has a higher chance of being successful, various scholars emphasize the importance of tailoring ISA programs, for instance, by dividing employees into smaller groups according to their preferences and information security skills (Caldwell, 2016). Previous studies have also shown that learner-centered, contextually based and group-oriented security programs are effective in improving employees' security behavior (Bauer *et al.*, 2017). The delivery methods included in an ISA program are also of importance and need to be chosen with consideration of the target group's preferences and capabilities (Hu *et al.*, 2022). Moreover, previous studies (i.e. Abawajy, 2014; Hart *et al.*, 2020) show that different ISA delivery methods (e.g. conventional and game-based) have different effects and therefore should be adapted differently for different target groups. Furthermore, previous studies suggest that factors such as culture (Wiley *et al.*, 2020) or/and personal characteristics, for example conscientiousness and agreeableness, may explain the variance in employees' security awareness (Kajzer *et al.*, 2014).

Past research indicates that one important factor influencing ISA and information security behavior is an individual's personality type (Pattinson *et al.*, 2015). Therefore, individual differences such as personality types (Glaspie and Karwowski, 2017) need to be considered to choose relevant ISA delivery methods and provide effective ISA programs (Hadlington *et al.*, 2019). Furthermore, previous research shows that personality types are influenced in different ways by social influencing principles (Alkış and Temizel, 2015) and that ISA is improved when training is provided in line with an individual's preferred learning style (Pattinson *et al.*, 2020).

Although previous studies show that ISA is influenced by an individual's personality type (Hadlington *et al.*, 2019), and that personality types are influenced by social influencing principles (Alkış and Temizel, 2015), as well as that ISA is improved when training is provided in line with an individual's preferred learning style (Pattinson *et al.*, 2020), none of the previous studies has combined these three theoretical backgrounds to support tailoring of ISA methods to targeted audiences. The current study contributes to previous research by suggesting and testing a theoretical framework combining distinct personality types with learning styles and social influencing vulnerabilities. In this way, this study also addresses the call made by many researchers (e.g. Abraham and Chengalur-Smith, 2019) for more theory-grounded approaches to ISA programs.

3. Theoretical background

3.1 Personality types

Personality types do not fully explain human behavior; however, they provide a means for describing how individuals are different from one another and give a foundation

from which future behavior can be predicted (Funder, 1994). DISC personality types (i.e., DISC model) are developed from the DISC theory introduced by Marston (1928). The DISC theory divides individual emotional behavior into four different dimensions of dominance (D), inducement (I), submission (S) and compliance (C). These dimensions have evolved over the years, with certain terms being refined. For example, "influencing" dimension has been proposed instead of "inducement," and "submission" dimension is alternatively referred to as "steady." The following four personality types in the context of DISC theory: dominant, influencing, steady and compliant. The theory identifies that the emotions and behaviors of a normal person come from an individual's sense of self in interaction with the environment (Alshehri *et al.*, 2018). The DISC model, similarly, as other personality models, has been criticized in the literature mainly for reducing human behavior into simplistic categories that do not fully capture all important aspects of personality in different contexts and cultures.

We have chosen the DISC model for this study because it is considered to be widely used for the assessment of personality types, and it provides enough information for lecturers to deliver teaching material to students that suits their personalities (Agung and Yuniar, 2016). The DISC model has been widely used by over 50 million people and is one of the oldest and validated assessments for personality types (Puccio and Grivas, 2009). We believe that using the DISC model for adjusting security awareness education for users can be a valuable approach because 1) the DISC model categorizes individuals based on their behavioral tendencies, which can help tailor security awareness messages to different user groups; 2) by understanding users' communication preferences and behavioral styles, security awareness education can be made more relevant and relatable, increasing engagement and information retention; 3) the DISC model emphasizes observable behavior, making it potentially useful for promoting specific behavioral changes in security practices. Tailoring educational content to match users' behavioral styles may encourage better adherence to security guidelines.

3.2 Learning styles

Previous studies indicated that personality types can give rise to different learning capabilities (Busato *et al.*, 1998), and a tailored individual training with a matched learning style was able to enhance an individual's ISA level in a positive manner (Pattinson *et al.*, 2020). Felder (1996) defined an individual's learning style as "characteristic strengths and preferences in the ways they take in and process information." Pattinson *et al.* (Pattinson *et al.*, 2020) found that an individual's level of ISA was increased if the received training was matched with an individual's preferred learning style. Several models have been developed to explain learning styles. For instance, Gardner (Gardner, 1993) developed the multiple intelligences on the following eight identified intelligences that are required for real-world activities: musical, kinesthetic, logical–mathematical, spatial, linguistic, interpersonal, intrapersonal and naturalist. Moreover, the developed VARK model by Fleming (Fleming, 2011) can assess an individual's learning preferences across four different perceptual modalities: visual (V), aural (A), read/write (R) and kinaesthetic (K). Furthermore, Kolb's learning style inventory (LSI) (Kolb, 2014) contains four basic learning types: accommodating, diverging, assimilating and converging.

The suggested learning style models above have been used in previous studies in information security management. For instance, Kolb's model has been used to combine pedagogical practices and cybersecurity modelling to support dynamically adaptive training procedures (Hatzivasilis *et al.*, 2020). In addition, Konak (2018) proposed a curriculum and a pedagogical

approach to expose K–12 students to cybersecurity concepts and skills, where inspiration has been taken from Kolb's model. The findings above demonstrated that having a good understanding of learners' learning styles would contribute to improving learners' learning outcomes. A tailored ISA program with a matched learning style would contribute to an improved individual's ISA level. In this study, Kolb's learning style is adopted to further explore the associated learning styles with different personality types in the context of tailoring ISA methods for different individuals.

3.3 Social influencing vulnerabilities

Another factor affected by individual differences is social influence (Parsons *et al.*, 2019). Social influence refers to attitude or behavior change caused by external pressure that is either real or imagined (Cialdini, 2009). Cialdini and Trost (1998) indicated that social influence can be used to foster growth and move people away from negative habits and in more positive directions, thereby creating the conditions for new change opportunities. There are some suggested principles that explain social influence. For instance, Cialdini (2009) proposed six principles of influence: authority, commitment, liking, reciprocity, scarcity and social proof.

The suggested social influencing principles can be used to convince people to act and think in a wanted way (Cialdini, 2009). These suggested influencing principles have been used in previous information security research. For instance, Parsons *et al.* (2019) developed a social influence framework based on Cialdini's six principles of influence to examine the success of various email phishing attacks. In addition, Wright *et al.* (2014) applied Cialdini's six principles of influence to investigate the relative effectiveness of phishing strategies. Therefore, it is necessary to also consider social influencing principles used by attackers in ISA programs.

In this study, Cialdini's six social influencing principles are selected to explore the associated social influencing vulnerabilities with different personality types in the context of tailoring ISA methods for different individuals. These principles could provide an explanation for why some people are more likely to be vulnerable to a cyberattack (Parsons *et al.*, 2019).

4. Research method

The PLS framework was developed according to a directed content analysis approach, which aims to validate or extend conceptually a theoretical framework or theory (Hsieh and Shannon, 2005). The framework was then tested in the context of tailoring ISA programs by matching distinct personality types with ISA methods. Figure 1 illustrates the methods applied in this study. Firstly, the directed content analysis was used to create the PLS framework (see Section 4.1). Secondly, the created PLS framework was applied to match distinct personality types with ISA methods identified through a systematic literature search (see Section 4.2).

4.1 Development of the framework – directed content analysis

The keywords describing DISC personality types, Kolb's learning styles and Cialdini's social influencing principles were primarily retrieved from the theories' original descriptions, namely, the DISC theory (Marston, 1928), the learning styles (Kolb and Kolb, 2005) and the social influencing principles (Cialdini, 2009).

To further enrich the data and increase our understanding of the theories and their use, we conducted a search for empirical studies using the three theories. The empirical studies were retrieved by searching in the following five databases: IEEE Xplore, ACM Digital Library,

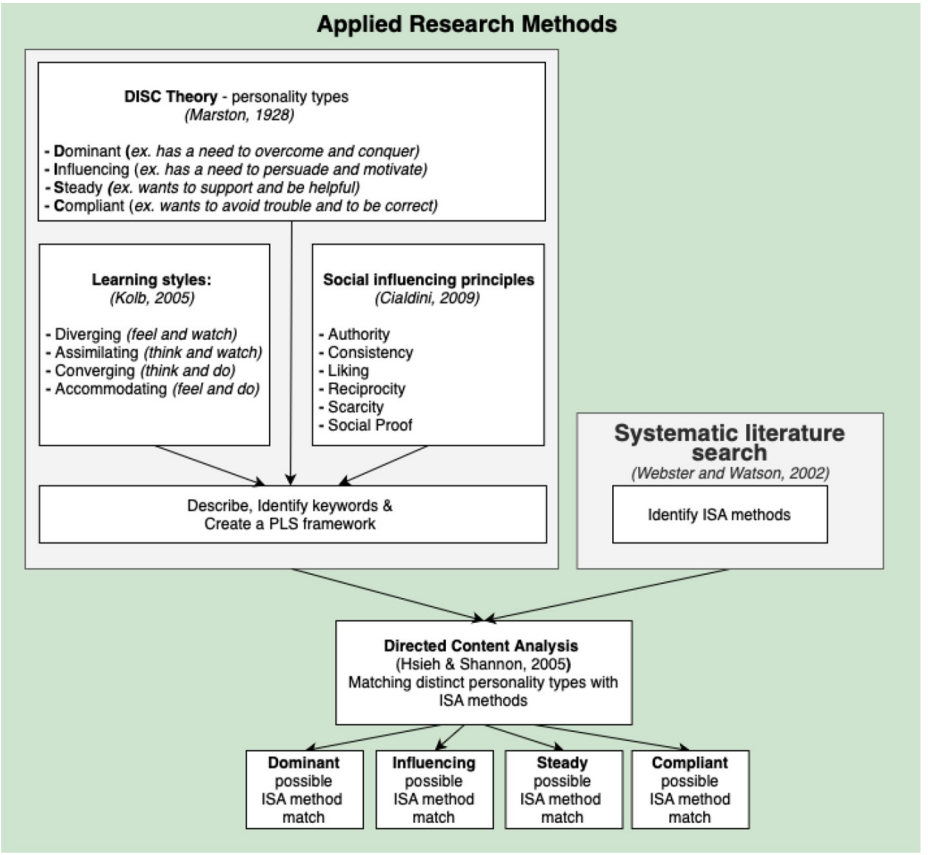

Figure 1. The research methods applied in this research
Source: Created by authors 1 and 2

Elsevier Science Direct, Emerald Insight and Google Scholar. The papers were selected if they included character traits on DISC personality types, Kolb's learning styles and Cialdini's social influencing principles. Studies that did not contain traits were excluded. The search strings used included the following keywords: DISC model, DISC theory, DISC personality types, DISC personality traits, Kolb's learning styles, Kolb's learning traits, Kolb's program, Kolb's method, Cialdini's social influencing principles, Cialdini's principles and Cialdini's principle of influence and have applied the theories empirically.

A directed content analysis (Hsieh and Shannon, 2005) was used to interpret the theoretical data on the DISC theory (Marston, 1928), learning styles (Kolb and Kolb, 2005) and social influencing principles (Cialdini, 2009) collected in the previous step. Following the directed content analysis (Hsieh and Shannon, 2005), the theories were described under their categories of types, styles or principles as defined in the following theories:

- personality types: dominant, influencing, steady and compliant;
- learning styles: diverging, assimilating, converging and accommodating; and

- social influencing principles: authority, consistency, liking, reciprocity, scarcity and social proof.

The next step of the analysis was to read through the retrieved theoretical data from the search and highlight descriptive paragraphs, sentences or keywords of each personality type, learning styles and social influencing principles, as shown in Figure 2.

The goal of the directed approach is to extend conceptually a theoretical framework (Hsieh and Shannon, 2005) and form new categories "X" as seen in Figure 3, which in our case meant to find a relationship between DISC personality types, learning styles and social influencing principles, and to form the PLS framework, as described in detail in section 5.

4.2 Matching distinct personality types with information security awareness methods

The framework was then applied to match distinct personality types with ISA methods identified through a systematic literature search following Webster and Watson (2002).

The following keywords were used for the literature search:

("Cyber security awareness" AND training) OR ("Cyber security awareness" AND education) OR ("Cyber security awareness" AND program) OR ("Cyber security awareness" AND method) OR ("Information security awareness" AND training) OR ("Information security awareness" AND education) OR ("Information security awareness" AND program) OR ("Information security awareness" AND method).

The selected databases for the literature search were IEEE Xplore, ACM Digital Library, Elsevier Science Direct, Emerald Insight and Google Scholar. Note: The Google Scholar

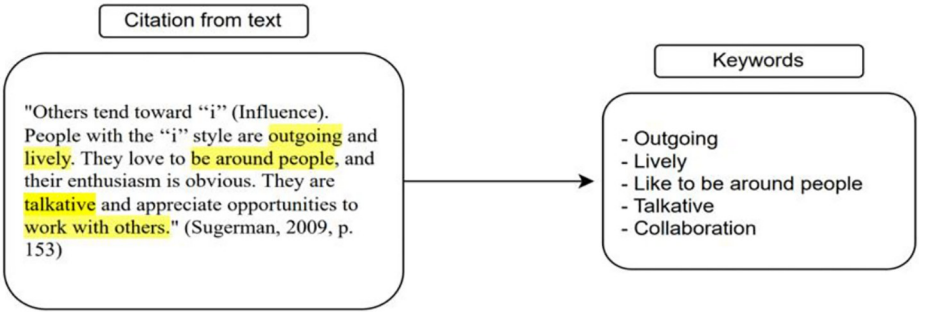

Figure 2. An example of keyword extraction
Source: Created by authors 1 and 2

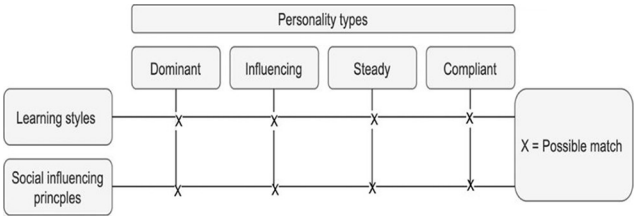

Figure 3. Forming new categories x from the three theories
Source: Created by authors 1 and 2

database search string only searched in the title due to the huge amount of irrelevant hits returned. In contrast, the other databases searched across all metadata (such as title, abstract and indexing terms). These five databases were chosen as they are among the leading electronic databases (Nasir *et al.*, 2019) and are widely used in information security research (Cram *et al.*, 2017). Both journal and conference papers were chosen, as Siponen and Oinas-Kukkonen (2007) indicate that both have a broad coverage of information security efforts and security topics. The search included articles published from 2000 onward, as studies before 2000 (Siponen, 2000) rarely provided detailed descriptions of ISA methods and instead emphasized the importance of considering social aspects in information security (Wood and Banks, 1993).

To ensure that retrieved articles contained information on ISA methods, we applied the inclusion criterion, where the title needs to contain one of the following phrases: 1) information security or cyber security; 2) training, education, program or method; 3) such as conventional (email, newsletter and poster), instructor-led (classroom, seminar and workshop), game-based, online or web-based methods (Abawajy, 2014; Ghazvini and Shukur, 2017). The retrieved papers were downloaded and reviewed for descriptions of ISA methods, and only those containing such descriptions were selected for the study. Furthermore, a backward search (Webster and Watson, 2002) identified an additional 20 papers. In total, 54 papers were included (see Appendix).

The PLS framework was used as glasses when looking at the selected articles in Appendix to find how different factors such as personality types, learning styles and social influencing principles can be combined or matched with ISA methods. As shown in Figure 4, the coding of these articles was done in a four-step process, called "sentence unit," "condensed sentence unit," "subcategory" and "code" (Graneheim and Lundman, 2004).

The sentence unit was used to gather sentences or paragraphs from the selected articles. All information (e.g. abstract, introduction, background, method, results and conclusion) in articles was used to find information. The focus of the sentence unit was to find descriptions of ISA methods that explain, for example, what the method is used for and its characteristics. The sentence unit was then decoded further through condensing the sentence by summarizing the ISA methods' key characteristics. The key characteristics were later decoded by deciding its subcategory, with that said, its keywords. The subcategory (keywords) was then linked with keywords found in the PLS framework to decide the personality type that can be matched with the ISA method. An extract of the conducted coding is shown below (see Table 1).

The coding of the articles was divided among the first two authors. The results of the coding were later checked and confirmed by both authors. Based on the ISA method citations, six ISA method groups were created by the authors, namely, conventional, instructor-led, group discussion, video-based, computer and mobile-based and game-based methods (see Section 6). For example, as seen in Table 1, "Computer games" was grouped under the game-based method, as the description was similar to other game-based methods

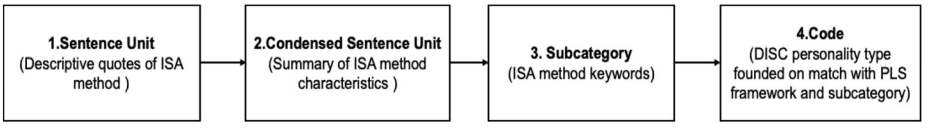

Figure 4. Coding process
Source: Created by authors 1 and 2

Table 1. An extract of the conducted coding

Sentence unit *(Descriptive quotes of the ISA method)*	Condensed sentence unit *(Summary of ISA method characteristics)*	Subcategory *(ISA method keywords)*	Code *(DISC personality type founded on match with PLS framework and subcategory)*
"Computer *games* are approaches that provide direct interaction with the player interface to produce visible reactions towards the game device or computer and encourage diversion, play, and competition […] Video games have many benefits; it improves the imagination and logical thinking of the players. It also helps to teach collaboration between players. […] Game-based Learning provides a combination of motivation, simulation, engagement, adaptivity, collaboration, and data collection […] challenging games." (Alserri *et al.*, 2018, p. 1351, 1352, 1354)	An ISA method that is interactive, competitive, collaborative, challenging, engaging and motivative	Interactive Competitive Collaborative Challenging Engaging Motivative	*Dominant* (Solve issues, problem solving, likes challenges, competitive, converging – solving issues, decision-making skills *Influencing* (Interaction, collaboration, accommodating learning style)

Source(s): Created by authors 1 and 2

found in the ISA method citations. Section 7 presents the results of matching the four distinct DISC personality types with the ISA methods found in the systematic literature search.

5. PLS framework

Firstly, as described in the previous section, the selected theories were carefully described, then for each theory, a set of keywords was identified and listed. These keywords were used to create the framework that describes the relationship or link found among DISC personality types, Kolb's learning styles and Cialdini's social influencing principles. Secondly, the developed PLS framework is presented in Section 5.4. Space restrictions do not allow us to present the thorough process of identifying the keyword for each theory; therefore, in each subsection, we just present the identified keywords for each theory.

5.1 The DISC theory

The DISC theory, first introduced by (Marston, 1928), divides individual emotional behavior into four different dimensions of: dominant, influencing, steady and compliant. The theory identifies that the emotions and behaviors of a normal person comes from an individual's sense of self in interaction with the environment (Alshehri *et al.*, 2018):

- *Keywords dominant:* aggressive, blunt, bottom-line-oriented, change environment, competitive, confident, confrontative, control, deals with problems, dominance, direct, dominate, fast-mover, forceful, get immediate results, likes challenges, more powerful than other, predominate, prevail, strong-willed, results oriented, straight to point, superiority, task-oriented;
- *Keywords influencing:* affiliation, collaboration, friendly, dislikes to be ignored, entertain others, enthusiasm, extroverts, influence, independent, interaction, lead, likes to share ideas, lively, likes to give opinion, optimistic, outgoing, persuasive, pleasing, process oriented, sociable, talkative;
- *Keywords steady:* calm approach, casual, deliberate, dislikes changes, dislikes quick decision, follow commands, good listeners, help people, humble, likes stable environments, logical, organized, obedient, loyal, likes close ended questions, logical solutions, modest, patient, predictable, secure environments, service oriented, structured, submissive, yield power/authority; and
- *Keywords compliant:* accuracy, adapt to environment, analytical, business like, conformity, complacent, compliant, comply, courteous, detail-oriented, diminution, fears being wrong, following those having a superior power, independent, logic, readjust, task-oriented.

5.2 Kolb's learning styles

Kolb's LSI is based on the Experiential Learning Theory (ELT), which is a comprehensive theory of learning and development (Kolb, 2014). According to Kolb and Kolb (2005), the LSI is an educational tool to help increase individuals' understanding of the process of learning from experience and to understand their approach to learning. Learning style in ELT is defined as a social psychological concept that is only partly determined by personality. Individuals who are tested on the LSI show many different patterns of scores. However, research using the tool has identified four basic learning styles: diverging, assimilating, converging and accommodating (Kolb and Kolb, 2005). The keywords identified for these learning styles are described next:

- *Keywords diverging:* brainstorming, collaboration, communicative, feelings, gather information, helpful, introverted, listen, observer, open-minded, valuation skills, work in groups;
- *Keywords assimilating:* concise, explore analytical models, have time to think, introverted, logical, lectures, soundness, systematic planning, understand wide range of information, watching, work on their own;
- *Keywords converging:* apply what they have learned, decision skills, dominant in the technology field, extroverted, make decisions, practical, think, simulation, solve problems; and
- *Keywords accommodating:* action skills, challenging experiences, extroverted, field work, gut feeling, hands-on experience, relies on people, set goals, test, work with others.

5.3 Cialdini's principles of social influence

Cialdini (2009) introduces six principles of social influence: authority, consistency, liking, reciprocity, scarcity and social proof. These principles are used universally in human interactions

to influence and to convince people to do, act and think the way one wants (Cialdini, 2009). Keywords for the six principles of social influence are presented next:

(1) *Keywords authority:* authority, fear, follow commands, obedient, readily;

(2) *Keywords consistency:* consistent, commitment, compliance, rules, trap;

(3) *Keywords liking:* association, extroverted, familiarity, liking, positive, social, trust;

(4) *Keywords reciprocity:* attention, compliance, depth, favor, not wanting to be disliked, obliged, repay;

(5) *Keywords scarcity:* impulsivity, limited availability, reactance, scarcity; and

(6) *Keywords social proof:* actions/behavior of others, follow, mimic, observe, similarity, social evidence.

5.4 PLS framework

This section presents a PLS framework, illustrating the four distinct DISC personality types with their linked learning style and their identified social influencing vulnerabilities. Table 2 illustrates how the relationship for dominant, DISC personality type, its learning style and social influencing vulnerabilities was found through the keywords presented in the above sections. The same procedure was repeated for each DISC personality type, but the page limit allows us to only show one example.

The PLS framework in Figure 5 is a summary of all identified relationships, without the descriptions of how the relationship was made, as illustrated in Table 2. In summary, the following relationships were identified for each distinct personality type:

- Dominant: has a *converging* learning style and is vulnerable against the *authority* and *scarcity* social influencing principles;
- Influencing: has an *accommodating* learning style and is vulnerable to the *liking* and *reciprocity* social influencing principles;
- Steady: has a *diverging* learning style and is vulnerable to the *authority, consistency* and *social proof* social influencing vulnerabilities; and
- Compliant: has an *assimilating* learning style and is vulnerable to the *authority, consistency and social proof* social influencing principles.

6. Information security awareness methods

This section presents the ISA methods found in the systematic literature search and directed content analysis, described in the method section. The ISA methods have been grouped by similarity under the six headings of conventional, instructor-led, group discussion, video-based, computer and mobile-based and game-based methods.

6.1 Conventional method

The conventional ISA methods include emails, posters and newsletters in print or electronic format (Abawajy, 2014). These methods are a flexible way to convey one or more messages to a large or targeted audience, that can consume the information in their own time (Abawajy, 2014; Khan *et al.*, 2011a). One of the drawbacks with these methods is that the message may be ignored or not understood (Abawajy, 2014).

Table 2. Dominant personality framework

	Learning style				Social influencing vulnerability					
	Diverging	Assimilating	Converging *(Think and do)*	Accommodating	Authority	Consistency	Liking	Reciprocity	Scarcity	Social proof
DOMINANT	–	–	The *dominant* personality is task-oriented (Jones and Hartley, 2013), they like challenges (Angood, 2017), like to get straight to the point, get immediate results (Beamish, 2005) and are more likely to change and shape the environment (Puccio and Grivas, 2009). This means that they have a learning style similar to *converging* as they are best at solving issues, like new ideas and are extroverted with decision-making skills (Kolb and Kolb, 2005)	–	The *dominant* personality is described as confident (Beamish, 2005) and a fast mover (Jones and Hartley, 2013). They can therefore be influenced by the *authority* principle, where people are likely to stop thinking and start reacting when a legitimate authority gives them commands (Cialdini, 2009), especially if in fear of losing some privileges (Workman, 2008) or control over something, as the *dominant* personality sees themselves as more powerful than others (Puccio and Grivas, 2009)	–	–	–	The *dominant* personality is known to be a fast mover (Jones and Hartley, 2013) and gets straight to the point (Beamish, 2005). This means that the *dominant* personality is likely to be influenced by *scarcity*, which is linked to reactance and impulsivity (Workman, 2008)	–

Source(s): Created by authors 1 and 2

	Learning style				Social influencing vulnerability					
	Diverging	Assimilating	Converging	Accommodating	Authority	Consistency	Liking	Reciprocity	Scarcity	Social Proof
Dominant			v		v				v	
Influencing				v			v	v		
Steady	v				v	v				v
Compliant		v			v	v				v

Figure 5. PLS Framework
Source: Created by authors 1 and 2

6.2 Instructor-led method

The instructor-led ISA method is a formal top-down approach using an expert to disseminate information to the attendees (e.g. Abawajy, 2014; Khan *et al.*, 2011a) in a classroom (e.g. Dupuis and Gordon, 2018; Stefaniuk, 2020), brown-bag seminars or online sessions (Cone *et al.*, 2006). This approach creates an interactive relationship between instructor and student providing timely answers to questions (Abawajy, 2014; Mathoosoothenen *et al.*, 2017) and giving the instructor the opportunity to modify instructions accordingly (Abawajy, 2014), as the success of this method is dependent on the instructor to engage the audience (Cone *et al.*, 2006). This method can be criticized for not giving hand-on experience (Dupuis and Gordon, 2018). A variant of the method is a brain-compatible teaching technique where students can move around the classroom and address multiple modes of learning (Reid *et al.*, 2011).

6.3 Group discussion method

According to Khan *et al.* (2011b) and Stefaniuk, (2020), the group discussion ISA method can be used to discuss different ISA-related issues. Albrechtsen and Hovden (2010) explain that users have the possibility to reflect on their working situation. These reflections are later discussed in smaller groups (Albrechtsen and Hovden, 2010). The groups can be between 15 and 20 people, where the purpose is to share knowledge and experience with each other (Khan *et al.*, 2011b; Stefaniuk, 2020). The strategy of group discussion is to motivate them in workshop environments while increasing their IS attention and intention (Khan *et al.*, 2011b). The group discussions (workshops) are interactive and enhance collective reflections, group work, experience transfer (e.g. Abawajy, 2014; Khan *et al.*, 2011b), motivation, attention and awareness level (Khan *et al.*, 2011b).

6.4 Video-based method

Video clips or video-based ISA methods provide security knowledge in an interactive way (Chmura, 2017) and provide visual and audio learning for users (Abawajy, 2014). Users can study the content independently (Aldawood and Skinner, 2018), learn whenever they have time (Stefaniuk, 2020) and at their own pace (Abawajy, 2014; Chmura, 2017). Video clips are also flexible and effective since they can be watched and re-watched whenever it is needed (Abawajy, 2014).

6.5 Computer and mobile-based method

The computer and mobile-based ISA method offers training that is flexible (e.g. Abawajy, 2014; Cone *et al.*, 2006), self-paced (e.g. Abawajy, 2014; Abraham and Chengalur-Smith, 2019), learner-controlled (Abraham and Chengalur-Smith, 2019) and repeatable (Dupuis and Gordon, 2018). The training is often online (Abawajy, 2014; Mathoosoothenen *et al.*, 2017) in the form of e-learning (Gundu and Flowerday, 2013), broadcasting, online discussion, blogging, videos, social media sites (Mathoosoothenen *et al.*, 2017) and can also be in sandbox labs offering users hands-on experience, using imaging (Dupuis and Gordon, 2018) or on mobile platforms (Abawajy, 2014). One of the drawbacks with these methods is that it is passive, can become unchallenging, provide no dialogue for questions (Cone *et al.*, 2006; Khan *et al.*, 2011b) and users try to complete sessions with minimal time and thought (Cone *et al.*, 2006).

6.6 Game-based method

There are different types of definitions for game-based ISA methods. Some of these definitions are gamification (e.g. Qusa and Tarazi, 2021), games (e.g. Chmura, 2017) or serious games (e.g. Mettler and Pinto, 2015).

Game-based methods are used for alternative or active learning (Dupuis and Gordon, 2018; Lugnet *et al.*, 2020; Mettler and Pinto, 2015) and provide an interactive way for users to educate themselves in various security topics (Alotaibi *et al.*, 2017) (Holdsworth and Apeh, 2017) or simulated environments (Ghazvini and Shukur, 2018; Tioh *et al.*, 2019). This interactive approach engages and motivates users while exploring a risk-free environment during the learning process (Ghazvini and Shukur, 2018; Qusa and Tarazi, 2021). Learning becomes an active and meaningful process (Hart *et al.*, 2020), potentially influencing impulsive behaviors by stimulating achievement and competition (Cone *et al.*, 2006; Holdsworth and Apeh, 2017). Games also aid problem-solving in resource-limited scenarios (Cone *et al.*, 2006) and track users' progression through points and rankings, fostering competition (Alotaibi *et al.*, 2017; Tioh *et al.*, 2019). Users are motivated to reach in-game goals and follow security rules (Nagarajan *et al.*, 2012).

Some games promote collaboration, such as card games (Aldawood and Skinner, 2019b; Lugnet *et al.*, 2020; Yasin *et al.*, 2018), which enhance teamwork and decision-making through dialogue and creativity (Lugnet *et al.*, 2020). These games improve security awareness, particularly against social engineering attacks (Aldawood and Skinner, 2019b). Games can also be addictive and engaging, effectively increasing information security awareness (Chmura, 2017; Khan *et al.*, 2011b). Their combination of knowledge and entertainment fosters commitment (Alotaibi *et al.*, 2017; Lugnet *et al.*, 2020) and allows experimentation in risk-free environments (Qusa and Tarazi, 2021). Challenges within these games enhance problem-solving (Abawajy, 2014; Lugnet *et al.*, 2020; Mettler and Pinto, 2015) and critical thinking (Cone *et al.*, 2006; Labuschagne *et al.*, 2011), improving decision-making skills (Aldawood and Skinner, 2019b; Ghazvini and Shukur, 2017).

7. Matching DISC personality types with information security awareness methods

This section presents the results of matching the four distinct DISC personality types with the ISA methods found in the systematic literature search (using the analysis and coding described in section 4.2). Section 7.1 illustrates the analysis and presents the best-matched ISA methods for the dominant personality with the help of converging learning style and social influencing vulnerabilities. The same procedure was repeated for each DISC personality type, but the word limit allows us to only show one example. Sections 7.2–7.4 summarize the results of the matching for the other DISC personality types. Figures 6–9

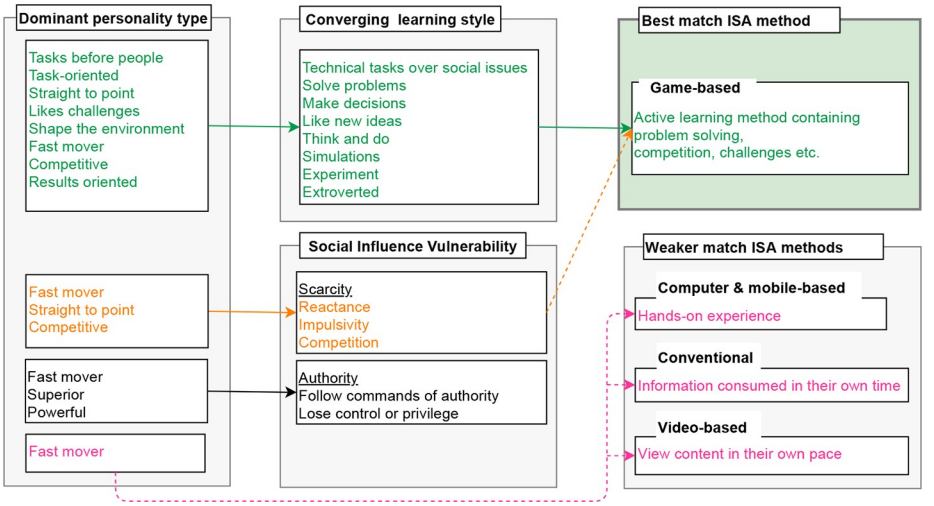

Figure 6. Dominant personality analysis match
Note(s): —> indicates a stronger link, whereas - - -> represents a weaker link
Source: Created by authors 1 and 2

illustrate the best match ISA method(s) for DISC personality types, through their linked learning style and social influencing vulnerabilities. The figures also include other ISA methods that can be linked with each personality type, but the match is weaker.

7.1 Analysis of matching of dominant personality type with the information security awareness methods – an example

Figure 6 depicts the best matched ISA method for the dominant personality with the help of converging learning style and social influencing vulnerabilities (scarcity and authority), which were earlier linked with dominant personality presented in the PLS framework.

7.1.1 An example of analysis of best-matched information security awareness method for the dominant personality. Kolb and Kolb (2005) explain that a person with a converging learning style is more likely to think and do, which can be related to game-based ISA methods that are used as active learning by doing, rather than solely listening, or reading (Mettler and Pinto, 2015). The converging style prefers to work with simulations, to experiment, and likes new ideas (Kolb and Kolb, 2005), which the game emphasizes by offering a simulated environment with different scenarios (Ghazvini and Shukur, 2018; Tioh *et al.*, 2019) and at the same time offering a risk-free environment that can be explored (e.g. Ghazvini and Shukur, 2017; Qusa and Tarazi, 2021). Furthermore, problems are solved throughout the game with limited resources, which is especially attractive to people with short attention spans (Cone *et al.*, 2006). This can be linked to the dominant personality being a fast-mover (Jones and Hartley, 2013) and their converging style when it comes to solving problems (Kolb and Kolb, 2005). Games allow users to activate their competition instinct (e.g. Alserri *et al.*, 2018; Tioh *et al.*, 2019) by keeping track of their individual progression when it comes to level, points, and rankings (Cone *et al.*, 2007). Competition and individual progression in games can be drawn by the dominant personality as they are competitive (Beamish, 2005) and results-oriented (Sugerman, 2009).

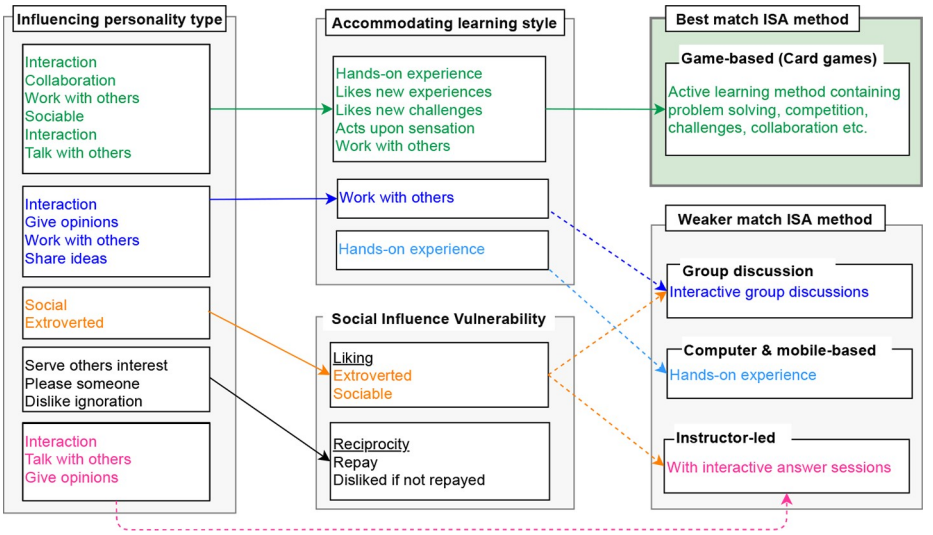

Figure 7. Influencing personality analysis match
Note(s): ⇒ indicates a stronger link, whereas ---> represents a weaker link
Source: Created by authors 1 and 2

As games are addictive in nature (Holdsworth and Apeh, 2017), they can catch users' attention and raise their ISA (e.g. Chmura, 2017; Khan *et al.*, 2011b) and at the same time challenge them (e.g. Aldawood and Skinner, 2018, 2019b). These challenges enhance problem-solving (Lugnet *et al.*, 2020), their critical thinking (Cone *et al.*, 2007) and their decision-making (Ghazvini and Shukur, 2018). People with a dominant personality are therefore more likely to be engaged in a game as they like challenges (Beamish, 2005) and have a converging learning style where they like decision making and solving problems (Kolb and Kolb, 2005). Card games are another form of game-based ISA method, where collaboration is included (Alserri *et al.*, 2018) and where multiple players play in competing teams (Lugnet *et al.*, 2020). Card games contain challenging situations that enhance decision-making skills (Aldawood and Skinner, 2019b), which can be linked with the dominant personality who likes challenges and is competitive (Beamish, 2005). It can also be linked to the converging learning style where people like to solve problems, have decision-making skills and are extroverted (Kolb and Kolb, 2005).

The dominant personality is influenced by the scarcity social influencing principle as they are fast movers and competitive (Jones and Hartley, 2013). This means that competitive games are more likely to influence individuals with a dominant personality in a positive way (Ferreira *et al.*, 2015), as scarcity influences people by reactance, impulsivity and competition (Workman, 2008).

7.1.2 Weaker matched information security awareness methods. The dominant personality is a fast mover (Jones and Hartley, 2013) and can be linked to computer and mobile-based, conventional and video-based ISA methods as they are flexible (Abawajy, 2014). The computer and mobile-based ISA methods, however, are often unchallenging (Cone *et al.*, 2006), which is a drawback to the dominant personality liking challenges (Beamish, 2005). Furthermore, the dominant personality through its converging learning

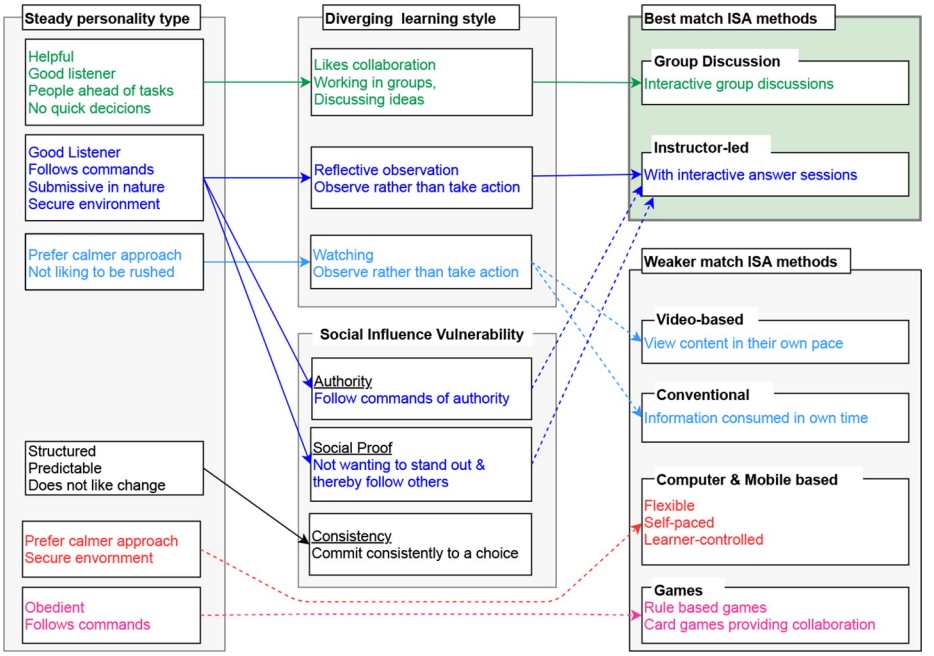

Figure 8. Steady personality analysis match
Note(s): → indicates a stronger link, whereas → represents a weaker link
Source: Created by authors 1 and 2

style prefers practical assignments and practical applications (Kolb and Kolb, 2005) and is therefore less likely to learn from the conventional and video-based methods. This means that the conventional, computer and mobile, and video-based ISA methods are not well suited for the dominant personality, even though we have one keyword match.

7.1.3 Summary. From the above analysis, a game-based ISA method is most suitable for the dominant personality given their matched converging learning style. Furthermore, the dominant personality is more likely to be influenced by authority and scarcity social influencing principles, where the scarcity also can point to the direction of game-based method to guide the dominant personality to raise ISA.

7.2 Summary of matching of influencing personality type with the information security awareness methods

Figure 7 depicts the best-matched ISA methods for the influencing personality with the help of accommodating learning style and social influencing vulnerabilities (liking and reciprocity), which were earlier linked with influencing personality presented in the PLS framework.

7.2.1 Summary. From our analysis, card game methods are most suitable for the influencing personality given their matched accommodating learning style. The influencing personality is more likely to be influenced by the liking and reciprocity social influencing principles, where the liking can point to the direction of instructor-led and group discussion methods to guide the influencing personality to raised ISA.

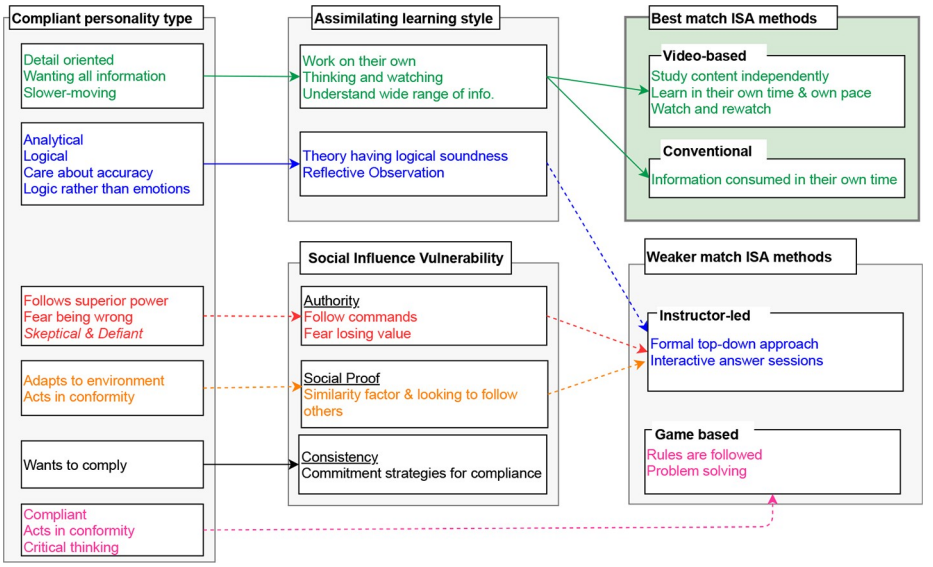

Figure 9. Compliant personality analysis match
Note(s): → indicates a stronger link, whereas → represents a weaker link
Source: Created by authors 1 and 2

7.3 Summary of matching of steady personality type with the information security awareness methods

Figure 8 depicts the best matched ISA methods for the steady personality with the help of diverging learning style and social influencing vulnerabilities (authority, social proof and consistency), which were earlier linked with the steady personality presented in the PLS framework.

7.3.1 Summary. From our analysis, the instructor-led and group discussions ISA methods are seen as most suitable for the steady personality given their matched diverging learning style. Furthermore, the steady personality is more likely to be influenced by authority, consistency, and social proof social influencing principles, where the authority and social proof can point to the direction of the instructor-led method to guide the steady personality to raised ISA.

7.4 Summary of matching of compliant personality type with the information security awareness methods

Figure 9 depicts the best matched ISA methods for the compliant personality with the help of assimilating learning style and social influencing vulnerabilities (authority, social proof and consistency), which were earlier linked with steady personality presented in the PLS framework.

7.4.1 Summary. From our analysis, the video-based and conventional ISA methods are seen as more suitable for the compliant personality given their matched assimilating learning style. Furthermore, the compliant personality is more likely to be influenced by authority, consistency and social proof social influencing principles, where the authority and social proof can point to the direction of the instructor-led method to guide the compliant personality to raised ISA, but there are some conflicts involved.

8. Discussions and conclusion

8.1 Theoretical contribution

This study developed and tested a framework, named the PLS framework, to associate learning styles and social influencing vulnerabilities with distinct personality types. The theoretical contributions are described as follows.

Firstly, this study contributes to the existing studies on ISA methods. The existing studies on ISA methods tend to focus on proposing and developing ISA methods (e.g. Abawajy, 2014). Previous studies also indicate that content in ISA training needs to be adjusted to the targeted audiences (Tsohou *et al.*, 2015) and to the knowledge level of the users (Tse *et al.*, 2013). However, there is a lack of studies on the matching between personality types and ISA methods. Pattinson *et al.* (2020) find that by adapting training to the preferred learning styles or learning preferences of an individual, the individual level of ISA would improve. Their study does, however, not consider distinct personality types. The types of employees are instead differentiated by age and gender (Pattinson *et al.*, 2020). Based on the existing theories, this study developed a PLS framework that illustrates the relationship of each distinct personality type from the DISC theory with a learning style from Kolb's LSI. In addition, the framework links each personality type with social influencing vulnerabilities from Cialdini's principles of social influence. This is valuable since previous research argues that personality types are influenced in different ways by Cialdini's social influencing principles (Alkış and Temizel, 2015). Therefore, this study contributes to building a sound theoretical ground for tailoring ISA methods for people with different personality types. For instance, personality types can be considered to design more effective ISA programs for different individuals in an organization.

Secondly, the derived keywords from the selected theories (i.e., the DISC theory, Kolb's LSI and Cialdini's principles of social influence) have been used to develop the PLS framework. The derived keywords are helpful to capture a good understanding of the different dimensions of the selected theories. The identified keywords contribute to the existing knowledge base on personality types.

Thirdly, the method for building the framework by using a keywords approach following a directed content analysis approach by Hsieh and Shannon (2005) can also be applied to associate with some other alternative theories. The PLS framework is built on the DISC theory, Kolb's LSI and Cialdini's principles of social influence, but the implementation of the directed approach can be used as a guide for other researchers in building a new framework with other theories for a different research purpose.

Fourthly, in this study, we theoretically matched distinct DISC personality types with different ISA methods using the PLS framework. Through our analysis, we also identified the best-matched ISA method(s) for each personality type. The study found that for some personality types, such as steady and compliant, more than one ISA method could be considered a best match. In contrast, for dominant and influencing personalities, only one best-matched ISA method could be determined. Additionally, previous literature studies (e.g. Khando *et al.*, 2021) have highlighted the popularity and importance of applying gamification or gamified concepts in ISA methods. However, our study shows that no single method suits all personality types. It is important to apply a tailored approach when it comes to employing ISA methods in organizations. Furthermore, weaker associations with other ISA methods were identified for all four personality types. These matches were considered weaker when they involved conflicting elements or were directly linked through a single personality trait. For example, the dominant personality's association with conventional, video-, computer- and mobile-based ISA methods was deemed weak, as the match was made without considering the associated learning style or social influence vulnerabilities.

The proposed best-matched ISA methods for the distinct DISC personality types contribute to the existing literature on tailored ISA methods for individuals with different personality traits. Previous studies (e.g. Hadlington *et al.*, 2019) have emphasized the need to adapt information security training and awareness methods to individual employee personality types, as individuals react differently to information security threats.

8.2 Practical implications

Earlier studies (e.g. Pattinson *et al.*, 2020) indicate that ISA and associated security behavior are influenced by an individual's personality type, and ISA methods therefore need to be adapted. Prior research has focused on individual differences such as age, gender and preferred learning style to improve ISA, whereas this study investigated how distinct DISC personality types (Marston, 1928) can be matched with existing ISA methods by considering both learning styles (Kolb and Kolb, 2005) and social influencing vulnerabilities (Cialdini, 2009).

In the study, we were able to theoretically link the DISC personality types with a learning style and their social influencing vulnerabilities, presented in a PLS framework. The main implication this research offers to practitioners is the PLS framework, that is showing the relationships of the distinct DISC personality types with a learning style and their social influencing vulnerabilities. The proposed PLS framework can be used as a base for managers to employ ISA methods for people with different personality types in organizations. Furthermore, the PLS framework can also be used to assist organizations in formulating enhanced training and education materials for their employees.

In this study, we also tested the PLS framework to theoretically match distinct personality types with ISA methods using a set of relevant papers from the literature. Both the best-matched and weaker-matched ISA methods for each personality type have been identified. The collection of these matched ISA methods can serve as a reference for organizations when selecting ISA methods. Organizations may consider offering multiple ISA methods to effectively enhance their employees' ISA. However, they also need to evaluate the costs associated with implementing various ISA methods and assess the return on investment. In addition, it is important to recognize that individuals may exhibit personality traits that place them between two or more personality types. Organizations should take such mixed personality traits into account when planning the implementation of ISA methods.

8.3 Conclusion

This study developed and tested a framework, named PLS, to associate learning styles and social influencing vulnerabilities with different personality types in the context of tailoring ISA methods for people with different personality types. Both best-matched and weaker-matched ISA methods have been identified for each personality type. According to the results, game-based methods have been suggested as the best-matched ISA method for the dominant personality. For the influencing personality, game-based methods, specifically card games, have been identified as the best match. Group discussions and instructor-led methods have been suggested as the most suitable ISA methods for the steady personality. Meanwhile, video-based and conventional methods have been identified as the best-matched ISA methods for the compliant personality.

8.4 Limitations and future studies

We are also aware of some limitations of this study. This provides some opportunities for future studies. Firstly, although we used some existing theories to develop the PLS framework, there are some other alternative theories (e.g. the big five personality) that could have been used

instead. Researchers could investigate the possibility of using other theories to redevelop and complement the framework in the future. Secondly, apart from the directed approach by Hsieh and Shannon (2005), other content analysis methods could also be applied to the collected theoretical data. Thirdly, the applicability of the proposed PLS framework has only been tested theoretically using a set of papers from the literature. However, we have not measured the effectiveness and efficiency of the suggested best-matched ISA methods for the distinct personality types in practice.

In the future, we plan to further validate the effectiveness and efficiency of the suggested best-matched ISA methods for distinct personality types in real organizational settings.

References

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

Abraham, S. and Chengalur-Smith, I. (2019), "Evaluating the effectiveness of learner controlled information security training", *Computers and Security*, Vol. 87, p. 101586.

Agung, A.A.G. and Yuniar, I. (2016), "Personality assessment website using DISC: a case study in information technology school", 2016 International Conference on Information Management and Technology (ICIMTech).

Aharony, N., Bouhnik, D. and Reich, N. (2020), "Readiness for information security of teachers as a function of their personality traits and their assessment of threats", *Aslib Journal of Information Management*, Vol. 72 No. 5.

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

Aldawood, H. and Skinner, G. (2018), "Educating and raising awareness on cyber security social engineering: a literature review", 2018 IEEE international conference on teaching, assessment, and learning for engineering (TALE), *Wollongong, Australia*, 4-7 December 2018.

Aldawood, H. and Skinner, G. (2019b), "Challenges of implementing training and awareness programs targeting cyber security social engineering", 2019 cybersecurity and cyberforensics conference (ccc), *Melbourne, Australia*, 8-9 May 2019.

Aldawood, H. and Skinner, G. (2019c), "Reviewing cyber security social engineering training and awareness programs—pitfalls and ongoing issues", *Future Internet*, Vol. 11 No. 3, p. 73.

Alkış, N. and Temizel, T.T. (2015), "The impact of individual differences on influence strategies", *Personality and Individual Differences*, Vol. 87, pp. 147-152.

Alotaibi, F., Furnell, S., Stengel, I. and Papadaki, M. (2017), "Enhancing cyber security awareness with mobile games", 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST), *Cambridge, United Kingdom*, 11-14 December.

Alserri, S.A., Zin, N.A.M. and Wook, T. (2018), "Gender-based engagement model for serious games", *International Journal on Advanced Science, Engineering and Information Technology*, Vol. 8 No. 4, pp. 1350-1357.

Alshehri, K.A., Alshamrani, H., Alharbi, A., Alshehri, H., Enani, M., Alghamdi, M. and Hassanien, M. (2018), "The relationship between personality type and the academic achievement of medical students in a Saudi medical school", *International Journal of Community Medicine and Public Health*, Vol. 5 No. 8, pp. 3205-3211.

Alyami, A., Sammon, D., Neville, K. and Mahony, C. (2024), "Critical success factors for security education, training and awareness (SETA) programme effectiveness: an empirical comparison of practitioner perspectives", *Information and Computer Security*, Vol. 32 No. 1, pp. 53-73, doi: 10.1108/ICS-08-2022-0133.

Angood, P.B. (2017), "Uncertainty, ambiguity and DiSC: a contrast", *Physician Leadership Journal*, Vol. 4 No. 4, pp. 6-8.

Bauer, S., Bernroider, E.W. 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*, Vol. 68, pp. 145-159.

Beamish, G. (2005), "How chief executives learn and what behaviour factors distinguish them from other people", *Industrial and Commercial Training*, Vol. 37 No. 3, pp. 138-144.

Busato, V.V., Prins, F.J., Elshout, J.J. and Hamaker, C. (1998), "The relation between learning styles, the big five personality traits and achievement motivation in higher education", *Personality and Individual Differences*, Vol. 26 No. 1, pp. 129-140.

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

Chmura, J. (2017), "Forming the awareness of employees in the field of information security", *Journal of Positive Management*, Vol. 8 No. 1, pp. 78-85.

Cialdini, R.B. (2009), *Influence: The Psychology of Persuasion*, HarperCollins e-books, New York, NY, available at: https://books.google.se/books?id=5dfv0HJ1TEoC

Cialdini, R.B. and Trost, M.R. (1998), "Social influence: social norms, conformity and compliance".

Cone, B.D., Irvine, C.E., Thompson, M.F. and Nguyen, T.D. (2007), "A video game for cyber security training and awareness", *Computers and Security*, Vol. 26 No. 1, pp. 63-72.

Cone, B.D., Thompson, M.F., Irvine, C.E. and Nguyen, T.D. (2006), "Cyber security training and awareness through game play", Security and Privacy in Dynamic Environments: *Proceedings of the IFIP TC-11 21st International Information Security Conference (SEC 2006), Karlstad, Sweden*, 22-24 May 2006.

Cram, W.A., Proudfoot, J.G. and D'arcy, J. (2017), "Organizational information security policies: a review and research framework", *European Journal of Information Systems*, Vol. 26 No. 6, pp. 605-641.

Dupuis, M. and Gordon, C. (2018), "Evaluating prevalence, perceptions, and effectiveness of cyber security and privacy education, training, and awareness programs", The Colloquium for Information Systems Security Education, New Orleans, LA, USA, 11 June 2018.

Felder, R.M. (1996), "Matters of style", *ASEE Prism*, Vol. 6 No. 4, pp. 18-23.

Ferreira, A., Coventry, L. and Lenzini, G. (2015), "Principles of persuasion in social engineering and their use in phishing", International Conference on Human Aspects of Information Security, Privacy, and Trust, *Lesvos, Greece*, 1-3 July 2015.

Fleming, N.D. (2011), *Teaching and Learning Styles: VARK Strategies*, IGI global, PA.

Flowerday, S. and Van der Schyff, K. (2019), "Social media surveillance: a personality-driven behaviour model", *Journal of Economic and Financial Sciences*, Vol. 12 No. 1, pp. 1-9.

Funder, D.C. (1994), "Explaining traits", *Psychological Inquiry*, Vol. 5 No. 2, pp. 125-127.

Gardner, H. (1993), *Multiple Intelligences: The Theory in Practice*, Basic books, New York, NY.

Ghazvini, A. and Shukur, Z. (2017), "A framework for an effective information security awareness program in healthcare", *Int. J. Adv. Comput. Sci. Appl*, Vol. 8, pp. 193-205.

Ghazvini, A. and Shukur, Z. (2018), "A serious game for healthcare industry: information security awareness training program for Hospital Universiti Kebangsaan Malaysia", *International Journal of Advanced Computer Science and Applications*, Vol. 9 No. 9.

Glaspie, H.W. and Karwowski, W. (2017), "Human factors in information security culture: a literature review", International Conference on Applied Human Factors and Ergonomics, AHFE 2017, *Los Angeles*, 17-21 Jul 2017.

Graneheim, U.H. and Lundman, B. (2004), "Qualitative content analysis in nursing research: concepts, procedures and measures to achieve trustworthiness", *Nurse Education Today*, Vol. 24 No. 2, pp. 105-112.

Gundu, T. and Flowerday, S. (2013), "Ignorance to awareness: towards an information security awareness process", *SAIEE Africa Research Journal*, Vol. 104 No. 2, pp. 69-79.

Hadlington, L., Popovac, M., Janicke, H., Yevseyeva, I. and Jones, K. (2019), "Exploring the role of work identity and work locus of control in information security awareness", *Computers and Security*, Vol. 81, pp. 41-48.

Haeussinger, F. and Kranz, J. (2017), "Antecedents of employees' information security awareness-review, synthesis, and directions for future research", The 25th European Conference on Information Systems (ECIS2017), *Guimarães, Portugal*, 5-10 June 2017.

Hart, S., Margheri, A., Paci, F. and Sassone, V. (2020), "Riskio: a serious game for cyber security awareness and education", *Computers and Security*, Vol. 95, p. 101827.

Hatzivasilis, G., Ioannidis, S., Smyrlis, M., Spanoudakis, G., Frati, F., Goeke, L., Hildebrandt, T., Tsakirakis, G., Oikonomou, F. and Leftheriotis, G. (2020), "Modern aspects of cyber-security training and continuous adaptation of programmes to trainees", *Applied Sciences*, Vol. 10 No. 16, p. 5702.

Holdsworth, J. and Apeh, E. (2017), "An effective immersive cyber security awareness learning platform for businesses in the hospitality sector", 2017 IEEE 25th International Requirements Engineering Conference Workshops (REW), *Lisbon*, 4-8 September 2017.

Hsieh, H.-F. and Shannon, S.E. (2005), "Three approaches to qualitative content analysis", *Qualitative Health Research*, Vol. 15 No. 9, pp. 1277-1288.

Hu, S., Hsu, C. and Zhou, Z. (2022), "Security education, training, and awareness programs: literature review", *Journal of Computer Information Systems*, Vol. 62 No. 4, pp. 752-764.

Jashari, V., Björn, S., Kolkowska, E. and Gao, S. (2024), "A framework for matching distinct personality types with information security awareness methods", *International Symposium on Human Aspects of Information Security and Assurance, Skövde, Sweden*, 9-11 July 2024.

Jones, C.S. and Hartley, N.T. (2013), "Comparing correlations between four-quadrant and five-factor personality assessments", *American Journal of Business Education (AJBE)*, Vol. 6 No. 4, pp. 459-470.

Kajzer, M., D'Arcy, 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*, Vol. 43, pp. 64-76.

Khan, B., Alghathbar, K.S. and Khan, M.K. (2011a), "Information security awareness campaign: an alternate approach", Information Security and Assurance: International Conference, ISA 2011, *Brno, Czech Republic*, 15-17 August 2011.

Khan, B., Alghathbar, K.S., Nabi, S.I. and Khan, M.K. (2011b), "Effectiveness of information security awareness methods based on psychological theories", *African Journal of Business Management*, Vol. 5 No. 26, p. 10862.

Khando, K., Gao, S., Islam, S.M. and Salman, A. (2021), "Enhancing employees information security awareness in private and public organisations: a systematic literature review", *Computers and Security*, Vol. 106, p. 102267.

Khatib, R. and Barki, H. (2020), "An activity theory approach to information security non-compliance", *Information and Computer Security*, Vol. 28 No. 4, pp. 485-501.

Kolb, D.A. (2014), *Experiential Learning: Experience as the Source of Learning and Development*, FT press, NJ.

Kolb, A.Y. and Kolb, D.A. (2005), "The Kolb learning style inventory-version 3.1 2005 technical specifications", *Boston, MA: Hay Resource Direct*, Vol. 200 No. 72, pp. 166-171.

Konak, A. (2018), "Experiential learning builds cybersecurity self-efficacy in K-12 students", *Journal of Cybersecurity Education, Research and Practice*, Vol. 2018 No. 1, p. 6.

Kritzinger, E. and Smith, E. (2008), "Information security management: an information security retrieval and awareness model for industry", *Computers and Security*, Vol. 27 Nos 5/6, pp. 224-231.

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.

Labuschagne, W., Burke, I., Veerasamy, N. and Eloff, M. (2011), "Design of cyber security awareness game utilizing a social media framework", 2011 Information Security for South Africa, *Johannesburg, South Africa*, 15-17 August 2011.

Lugnet, J., Ericson, Å., Lundgren, M. and Wenngren, J. (2020), "On the design of playful training material for information security awareness", The Sixth International Conference on Design Creativity (ICDC 2020), *Oulu*, 26-28 August 2020.

Marston, W.M. (1928), *Emotions of Normal People*, Kegan Paul Trench Trubner and Company Limited, New York, NY.

Mathoosoothenen, V.N., Sundaram, J.S., Palanichamy, R.A. and Brohi, S.N. (2017), "An integrated real-time simulated ethical hacking toolkit with interactive gamification capabilities and cyber security educational platform", *Proceedings of the 2017 International Conference on Computer Science and Artificial Intelligence*, *Jakarta*, 5-7 December 2017.

Mettler, T. and Pinto, R. (2015), "Serious games as a means for scientific knowledge transfer-A case from engineering management education", *IEEE Transactions on Engineering Management*, Vol. 62 No. 2, pp. 256-265.

Micallef, N. and Arachchilage, N.A.G. (2017), "Changing users' security behaviour towards security questions: a game based learning approach", 2017 Military Communications and Information Systems Conference (MilCIS), *Canberra*, 14-16 November 2017.

Mouton, F., Leenen, L. and Venter, H.S. (2016), "Social engineering attack examples, templates and scenarios", *Computers and Security*, Vol. 59, pp. 186-209.

Murray, G., Falkeling, M. and Gao, S. (2024), "Trends and challenges in research into the human aspects of ransomware: a systematic mapping study", *Information and Computer Security*, doi: 10.1108/ICS-12-2022-0195.

Nagarajan, A., Allbeck, J.M., Sood, A. and Janssen, T.L. (2012), "Exploring game design for cybersecurity training", 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), *Bangkok*, 27-31 May 2012.

Nasir, A., Arshah, R.A., Hamid, M.R.A. and Fahmy, S. (2019), "An analysis on the dimensions of information security culture concept: a review", *Journal of Information Security and Applications*, Vol. 44, pp. 12-22, doi: 10.1016/j.jisa.2018.11.003.

Pahlavanpour, O. and Gao, S. (2024), "A systematic mapping study on gamification within information security awareness programs", *Heliyon*, Vol. 10 No. 19, p. e38474, doi: 10.1016/j.heliyon.2024.e38474.

Parsons, K., Butavicius, M., Delfabbro, P. and Lillie, M. (2019), "Predicting susceptibility to social influence in phishing emails", *International Journal of Human-Computer Studies*, Vol. 128, pp. 17-26.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C. (2014), "Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q)", *Computers and Security*, Vol. 42, pp. 165-176, doi: 10.1016/j.cose.2013.12.003.

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A. and Calic, D. (2015), "Factors that influence information security behavior: an Australian web-based study", International Conference on Human Aspects of Information Security, Privacy, and Trust, *Lesvos*, 1-3 July 2015.

Pattinson, M., Butavicius, M., Lillie, M., Ciccarello, B., Parsons, K., Calic, D. and McCormac, A. (2020), "Matching training to individual learning styles improves information security awareness", *Information and Computer Security*, Vol. 28 No. 1, pp. 1-14.

Puccio, G. and Grivas, C. (2009), "Examining the relationship between personality traits and creativity styles", *Creativity and Innovation Management*, Vol. 18 No. 4, pp. 247-255.

Qusa, H. and Tarazi, J. (2021), "Cyber-hero: a gamification framework for cyber security awareness for high schools students", IEEE 11th annual computing and communication workshop and conference (CCWC), *Las Vegas, NV*, 27-30 January 2021.

Reid, R., Van Niekerk, J. and Von Solms, R. (2011), "Guidelines for the creation of brain-compatible cyber security educational material in Moodle 2.0", 2011 Information Security for South Africa, *Johannesburg*, 15-17 August 2011.

Reinheimer, B., Aldag, L., Mayer, P., Mossano, M., Duezguen, R., Lofthouse, B., Von Landesberger, T. and Volkamer, M. (2020), "An investigation of phishing awareness and education over time: when and how to best remind users", Sixteenth symposium on usable privacy and security (SOUPS 2020), Virtual Conference, August 10–11, 2020.

Schutz, A. (1982), "Collected papers. M. Nijhoff".

Siponen, M.T. (2000), "A conceptual foundation for organizational information security awareness", *Information Management and Computer Security*, Vol. 8 No. 1, pp. 31-41, doi: 10.1108/09685220010371394.

Siponen, M.T. and Oinas-Kukkonen, H. (2007), "A review of information security issues and respective research contributions", *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, Vol. 38 No. 1, pp. 60-80.

Soomro, Z.A., Shah, M.H. and Ahmed, J. (2016), "Information security management needs more holistic approach: a literature review", *International Journal of Information Management*, Vol. 36 No. 2, pp. 215-225.

Stahl, B.C., Doherty, N.F. and Shaw, M. (2012), "Information security policies in the UK healthcare sector: a critical evaluation", *Information Systems Journal*, Vol. 22 No. 1, pp. 77-94.

Stefaniuk, T. (2020), "Training in shaping employee information security awareness", *Entrepreneurship and Sustainability Issues*, Vol. 7 No. 3, p. 1832.

Sugerman, J. (2009), "Using the DiSC® model to improve communication effectiveness", *Industrial and Commercial Training*, Vol. 41 No. 3, pp. 151-154.

Tioh, J.-N., Mina, M. and Jacobson, D.W. (2019), "Cyber security social engineers an extensible teaching tool for social engineering education and awareness", 2019 IEEE Frontiers in Education Conference (FIE), *Covington, KY*, 16-19 Oct 2019.

Tse, W.D., Hui, M., Lam, S., Mok, Y., Oei, W., Tang, K. and Yau, X. (2013), "Education in IT security: a case study in banking industry", *GSTF Journal on Computing (JoC)*, Vol. 3 No. 3, pp. 1-10.

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*, Vol. 52, pp. 128-141.

Tsohou, A., Kokolakis, S., Karyda, M. and Kiountouzis, E. (2008), "Investigating information security awareness: research and practice gaps", *Information Security Journal: A Global Perspective*, Vol. 17 Nos 5/6, pp. 207-227.

Webster, J. and Watson, R.T. (2002), "Analyzing the past to prepare for the future: writing a literature review", *MIS Quarterly*, pp. xiii-xxiii.

Wiley, A., McCormac, A. and Calic, D. (2020), "More than the individual: examining the relationship between culture and information security awareness", *Computers and Security*, Vol. 88, p. 101640.

Wood, C.C. and Banks, W.W. Jr, (1993), "Human error: an overlooked but significant information security problem", *Computers and Security*, Vol. 12 No. 1, pp. 51-60.

Workman, M. (2008), "Wisecrackers: a theory-grounded investigation of phishing and pretext social engineering threats to information security", *Journal of the American Society for Information Science and Technology*, Vol. 59 No. 4, pp. 662-674.

Wright, R.T., Jensen, M.L., Thatcher, J.B., Dinger, M. and Marett, K. (2014), "Research note—influence techniques in phishing attacks: an examination of vulnerability and resistance", *Information Systems Research*, Vol. 25 No. 2, pp. 385-400.

Yasin, A., Liu, L., Li, T., Wang, J. and Zowghi, D. (2018), "Design and preliminary evaluation of a cyber security requirements education game (SREG)", *Information and Software Technology*, Vol. 95, pp. 179-200.

Further reading

Al Awawdeh, S. and Tubaishat, A. (2014), "An information security awareness program to address common security concerns in IT unit", 2014 11th International Conference on Information Technology: New Generations.

Al-Daeef, M.M., Basir, N. and Saudi, M.M. (2017), "Security awareness training: a review", *Proceedings of the world congress on engineering*.

Aldawood, H. and Skinner, G. (2019a), "An academic review of current industrial and commercial cyber security social engineering solutions", *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy*.

Alshaikh, M., Naseer, H., Ahmad, A. and Maynard, S.B. (2019), "Toward sustainable behaviour change: an approach for cyber security education training and awareness", The 27th European Conference on Information Systems (ECIS), *Stockholm and Uppsala, Sweden*, 8-14 June 2019.

Bada, S.O. and Olusegun, S. (2015), "Constructivism learning theory: a paradigm for teaching and learning", *Journal of Research and Method in Education*, Vol. 5 No. 6, pp. 66-70.

Cooper, M.H. (2008), "Information security training: lessons learned along the trail", *Proceedings of the 36th annual ACM SIGUCCS fall conference: moving mountains, blazing trails*.

Da Veiga, A. (2015), "An information security training and awareness approach (ISTAAP) to instil an information Security-Positive culture", HAISA.

Denning, T., Lerner, A., Shostack, A. and Kohno, T. (2013), "Control-Alt-Hack: the design and evaluation of a card game for computer security awareness and education", *Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security*.

Filipczuk, D., Mason, C. and Snow, S. (2019), "Using a game to explore notions of responsibility for cyber security in organisations", Extended abstracts of the 2019 CHI conference on Human Factors in Computing Systems.

Fung, C.C., Khera, V., Depickere, A., Tantatsanawong, P. and Boonbrahm, P. (2008), "Raising information security awareness in digital ecosystem with games-a pilot study in Thailand", 2008 2nd IEEE International Conference on Digital Ecosystems and Technologies.

Furnell, S.M., Gennatou, M. and Dowland, P.S. (2002), "A prototype tool for information security awareness and training", *Logistics Information Management*, Vol. 15 Nos 5/6, pp. 352-357.

Ghazvini, A. and Shukur, Z. (2016), "Awareness training transfer and information security content development for healthcare industry", *International Journal of Advanced Computer Science and Applications*, Vol. 7 No. 5, p. 70549.

Gondree, M. and Peterson, Z.N. (2013), "Valuing security by getting {[d0x3d!]}: experiences with a network security board game", 6th Workshop on Cyber Security Experimentation and Test (CSET 13).

Granic, I., Lobel, A. and Engels, R.C. (2014), "The benefits of playing video games", *American Psychologist*, Vol. 69 No. 1, p. 66.

Gundu, T. and Flowerday, S.V. (2012), "The enemy within: a behavioural intention model and an information security awareness process", 2012 information security for South Africa.

Herr, C. and Allen, D. (2015), "Video games as a training tool to prepare the next generation of cyber warriors", *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research*.

Koskinen, J.A. and Kelo, T.O. (2009), "Pure e-learning course in information security", *Proceedings of the 2nd International Conference on Security of Information and Networks*.

Lee, J.J. and Hammer, J. (2011), "Gamification in education: what, how, why bother?", *Academic Exchange Quarterly*, Vol. 15 No. 2, p. 146.

Monk, T., Van Niekerk, J. and Von Solms, R. (2009), "Concealing the medicine: information security education through game play", ISSA.

Oyelami, J. and Ithinh, N. (2013), "'People are the answer to security': establishing successful information security awareness training (ISAT) program in organization", *International Journal of Computer Science and Information Security*, Vol. 11 No. 8, pp. 1-8.

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

Shapi'i, A. and Ghulam, S. (2016), "Model for educational game using natural user interface", *International Journal of Computer Games Technology*, Vol. 2016 No. 1, p. 6890351.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L.F., Hong, J. and Nunge, E. (2007), "Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish", *Proceedings of the 3rd symposium on Usable privacy and security*.

Shostack, A. (2014), "Elevation of privilege: drawing developers into threat modeling", 2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14).

Tschakert, K.F. and Ngamsuriyaroj, S. (2019), "Effectiveness of and user preferences for security awareness training methodologies", *Heliyon*, Vol. 5 No. 6, p. e02010.

Appendix. The list of the included articles from the literature search

(Abawajy, 2014; Abraham and Chengalur-Smith, 2019; Al Awawdeh and Tubaishat, 2014; Al-Daeef *et al.*, 2017; Albrechtsen and Hovden, 2010; Aldawood and Skinner, 2018, 2019a, 2019b; Alotaibi *et al.*, 2017; Alshaikh *et al.*, 2019; Bada and Olusegun, 2015; Chmura, 2017; Cone *et al.*, 2007; Cone *et al.*, 2006; Cooper, 2008; Da Veiga, 2015; Denning *et al.*, 2013; Dupuis and Gordon, 2018; Filipczuk *et al.*, 2019; Fung *et al.*, 2008; Furnell *et al.*, 2002; Ghazvini and Shukur, 2016, 2018; Gondree and Peterson, 2013; Granic *et al.*, 2014; Gundu and Flowerday, 2013; Gundu and Flowerday, 2012; Hart *et al.*, 2020; Herr and Allen, 2015; Holdsworth and Apeh, 2017; Kajzer *et al.*, 2014; Khan *et al.*, 2011a, 2011b; Koskinen and Kelo, 2009; Labuschagne *et al.*, 2011; Lee and Hammer, 2011; Lugnet *et al.*, 2020; Mathoosoothenen *et al.*, 2017; Mettler and Pinto, 2015; Monk *et al.*, 2009; Nagarajan *et al.*, 2012; Oyelami and Ithinh, 2013; Puhakainen and Siponen, 2010; Qusa and Tarazi, 2021; Reid *et al.*, 2011; Shapi'i and Ghulam, 2016; Sheng *et al.*, 2007; Shostack, 2014; Stefaniuk, 2020; Tioh *et al.*, 2019; Tschakert and Ngamsuriyaroj, 2019; Yasin *et al.*, 2018)

Source: Created by author

Corresponding author

Ella Kolkowska can be contacted at: ella.kolkowska@oru.se