The critical success factors for Security Education, Training and Awareness (SETA) program effectiveness: a lifecycle model

Received 11 July 2022
Revised 20 December 2022
8 February 2023
Accepted 9 February 2023

Areej Alyami, David Sammon, Karen Neville and Carolanne Mahony
Business Information Systems Department, Cork University Business School, University College Cork, Cork, Ireland

Abstract

Purpose – This study explores the critical success factors (CSFs) for Security Education, Training and Awareness (SETA) program effectiveness. The questionable effectiveness of SETA programs at changing employee behavior and an absence of empirical studies on the CSFs for SETA program effectiveness is the key motivation for this study.

Design/methodology/approach – This exploratory study follows a systematic inductive approach to concept development. The methodology adopts the "key informant" approach to give voice to practitioners with SETA program expertise. Data are gathered using semi-structured interviews with 20 key informants from various geographic locations including the Gulf nations, Middle East, USA, UK and Ireland.

Findings – In this study, the analysis of these key informant interviews, following an inductive open, axial and selective coding approach, produces 11 CSFs for SETA program effectiveness. These CSFs are mapped along the phases of a SETA program lifecycle (design, development, implementation and evaluation) and nine relationships identified between the CSFs (within and across the lifecycle phases) are highlighted. The CSFs and CSFs' relationships are visualized in a Lifecycle Model of CSFs for SETA program effectiveness.

Originality/value – This research advances the first comprehensive conceptualization of the CSFs for SETA program effectiveness. The Lifecycle Model of CSFs for SETA program effectiveness provides valuable insights into the process of introducing and sustaining an effective SETA program in practice. The Lifecycle Model contributes to both theory and practice and lays the foundation for future studies.

Keywords SETA program, Effectiveness, Security, CSFs, Key informant, Lifecycle model

Paper type Research paper

1. Introduction

Cybersecurity and securing information systems assets has never been more important than it is today in an ever more connected and pervasive digital world (Khando *et al.*, 2021). In fact, the cybersecurity market size is expected to surpass US$400bn by 2027 (Lake, 2022). The devastating effects of cyber-attacks are well documented, therefore, despite security best practices being widely known *"people routinely fail to protect their digital assets"* (Haney and Lutters, 2021, p. 485). Furthermore, with the number of cyber-attacks also increasing each year, *"adequate cybersecurity measures are becoming a necessary venture for companies of all shapes and sizes"* (Lake, 2022). Organizations use various strategies to safeguard their information systems and information assets against security threats. However, a Security

Information Technology & People
Vol. 36 No. 8, 2023
pp. 94-125
Emerald Publishing Limited
0959-3845
DOI 10.1108/ITP-07-2022-0515

Education, Training and Awareness (SETA) program is one of the most prominent strategies used for controlling information security (IS) security threats and protecting information assets, and many researchers recommend establishing a SETA program as part of the organization's overall IS/cyber security strategy (Alshaikh *et al.*, 2018; Kirova and Baumöl, 2018; Tsohou *et al.*, 2015; D'Arcy *et al.*, 2009). In fact, a Google search of "Security Education, Training, and Awareness programmes" provides an array of results to choose from, including training course options, industry insights and academic research studies. While several SETA program definitions can be found in the literature, despite their variability, they all hold the employee central in their focus. Therefore, a SETA program is most often viewed as an educational process that is designed to reduce the number of accidental security breaches that occur due to a lack of employee awareness of IS security issues/threats (Whitman and Mattord, 2008; D'Arcy *et al.*, 2009; Puhakainen and Siponen, 2010; Han *et al.*, 2017; Alshaikh *et al.*, 2018; Barlow *et al.*, 2018; Yoo *et al.*, 2018; Dhillon *et al.*, 2020).

The significance of SETA programs is widely accepted by both academics and practitioners (Alshaikh *et al.*, 2018; Tsohou *et al.*, 2015; D'Arcy *et al.*, 2009; Wilson and Hash, 2003). Based on a review of the literature, SETA programs typically address the following: [1] provides individuals with knowledge regarding organizational IS security threats (AlMindeel and Martins, 2020; Dhillon *et al.*, 2020; Alshaikh *et al.*, 2019; Yoo *et al.*, 2018; Bulgurcu *et al.*, 2010; Mahmood *et al.*, 2010; D'Arcy *et al.*, 2009); [2] clarifies existing technical and procedural countermeasures available to individuals (Silic and Lowry, 2020; Pastor *et al.*, 2010); [3] highlights the organizational sanctions faced by individuals for security policy violations (Cram *et al.*, 2019; Barlow *et al.*, 2018; Herath *et al.*, 2018; Karjalainen *et al.*, 2013; Puhakainen and Siponen, 2010; Siponen and Vance, 2010) and [4] improves individuals awareness of their roles and responsibilities in protecting the organization's information assets (Tsohou *et al.*, 2015; Lebek *et al.*, 2014; Tsohou *et al.*, 2012; Karjalainen and Siponen, 2011; D'Arcy *et al.*, 2009).

Despite the prominence of SETA programs for organizational IS security, "*only a small portion of practitioners*" claim that their SETA programs are "*very effective*" (Hu *et al.*, 2021, p. 1). Furthermore, Talib *et al.* (2010) have observed that while some organizations claim to measure the effectiveness of their SETA programs, no actuals are provided as to the level of effectiveness. It is reported that poor SETA program effectiveness is linked to the programs failure to achieve its goal of impacting positively on employee security-related behaviors (Alshaikh *et al.*, 2021; Hu *et al.*, 2021; He and Zhang, 2019; Alshaikh *et al.*, 2019). A lack of a "*systematic understanding*" of the "*nature of SETA programmes*" and their impacts on "*security-related beliefs*" is viewed as a possible reason for this lack of effectiveness (Hu *et al.*, 2021, p. 1). In fact, Alshaikh *et al.* (2021, p. 1) argue that existing SETA programs are "*suboptimal*" as they "*aim to improve employee knowledge acquisition rather than behavior and belief.*" Therefore, more theorizing and conceptual clarity is needed in investigating the effectiveness of SETA programs (c.f. Alshaikh *et al.*, 2021; Hu *et al.*, 2021; Kirova and Baumöl, 2018; Puhakainen and Siponen, 2010), given the organizational challenge. For example, organizations put security policies in place and strive to ensure that employees are aware of IS security threats and behave in a way that mitigates against IS security risks. Typically, these organizations manage their approach to IS security on a continuous basis in an effort to cultivate a compliant culture among employees.

Further leveraging this need for conceptual clarity, research is still required on the design, development, implementation and evaluation phases of the SETA program lifecycle (Alyami *et al.*, 2020; Alshaikh *et al.*, 2018). For example, where empirical studies investigating the effectiveness of SETA programs exist, they fail to examine all phases of the SETA program lifecycle (design, development, implementation and evaluation), tending to focus more on one or two of the lifecycle phases (c.f. Puhakainen and Siponen, 2010;

Okenyi and Owens, 2007; Silic and Lowry, 2020; Rantos *et al.*, 2012). Therefore, while there are several guidelines from academia available to organizations to support the introduction of SETA programs, a question remains about the theoretical grounding and empirical evidence available, in current literature, around these guidelines, when it comes to "*developing an effective SETA programme to change employee behaviour*" (Alshaikh *et al.*, 2021, p. 2). In effect, despite the fact that there is a growing volume of research around SETA programs, there is still limited research of "*practical value*" available on "*organisational strategies to improve*" SETA programs, with recommendations to guide the development of SETA programs being "*fragmented and dispersed*" and not cumulative in nature (Alshaikh *et al.*, 2021, p. 3). Therefore, through leveraging the SETA program lifecycle phases, this paper sets out to address this research need by exploring the following **research questions**:

RQ1. What are the critical success factors (CSFs) for SETA program effectiveness? and

RQ2. How are these CSFs related to each other?

These CSFs are mapped against the phases of the SETA program lifecycle and the relationships identified between the CSFs are highlighted. The CSFs and their relationships are visualized in a Lifecycle Model of the CSFs for SETA program effectiveness.

The paper is organized as follows: Section 2 presents a background to the study; Section 3 describes the methodology, particularly the data gathering and data analysis techniques used; Section 4 presents the findings which identify the CSFs for SETA program effectiveness (RQ1) and the relationships between these CSFs (both *within* and *across* the SETA program lifecycle phases) (RQ2); Section 5 presents an evaluation of our findings (visualized as a Lifecycle Model) against the existing literature and, lastly, section 6 presents the conclusions and contributions of the research.

2. Background

Existing research on SETA programs suggests that their role is "*complex*" and many can have "*intended and unintended outcomes*" (Reeves *et al.*, 2021, p. 8). However, where cybersecurity professionals deliver organizational SETA programs to improve cybersecurity behavior "*they are often poorly received by employees*" and "*employee behaviour continues to be the primary cause of cyber vulnerabilities*" (Reeves *et al.*, 2021, p. 1). Therefore, the extent to which SETA programs "*succeed in producing positive outcomes remains unclear*" (Reeves *et al.*, 2021, p. 1). Whether this is because of organizational security policy, security management frameworks, employee behavior or employee awareness or a multiplicative effect of all these areas, it is something that still needs to be unpacked.

IS/cyber security researchers "*consistently argue*" that organizations need SETA programs "*to raise employees' awareness of security risk, and to provide them with the required skills and knowledge to comply with security policy*" (Alshaikh *et al.*, 2021, p. 1). However, it's increasingly clear from the IS/cyber security literature that the effectiveness of a SETA program "*requires ongoing voluntary compliance from employees*" (Pham *et al.*, 2019, p. 134). Therefore, the organizational challenge is to develop engaging SETA programs "*to promote and maintain the requisite user behaviors to increase cybersecurity*" (Pham *et al.*, 2019, p. 134). In fact, according to He and Zhang (2019, p. 249) "*many organisations cybersecurity training and awareness programmes fail to achieve their goals.*" While the reasons provided suggest a sense of "*security fatigue*" (He and Zhang, 2019, p. 249) or "*advice fatigue*" (Reeves *et al.*, 2021, p. 1) for employees, where "*employees feel bored*" and "*lack enthusiasm to participate*" (He and Zhang, 2019, p. 249) in such SETA programs. Furthermore, this sense of employee "security fatigue" comes at a significant organizational cost, where, despite significant investment in SETA programs, the "*rate of unintended breaches of security* *directives is still increasing"* with *"70% of security incidents"* attributed to employee non-compliance with security policy (Alshaikh *et al.*, 2021, p. 1). This reality can better qualify the reason why the market for cybersecurity awareness training is anticipated to increase to a value of US$12.1bn by 2027, representing a compound annual growth rate (CAGR) of 45.6% from 2022 to 2027 (Global Market Estimates, 2022).

IS/cyber security is best viewed as *"multidisciplinary in nature"* where the non-technical (human) aspect plays as major a part as the technical aspect (Khando *et al.*, 2021, p. 2). Indeed, Khando *et al.* (2021, p. 2) suggest that organizations invest significant amounts in *"technological countermeasures"* as they *"continuously struggle to maintain the security of their information assets,"* but they also highlight that it is simply not enough. In short, humans are found to be one of the *"weakest links"* in attempts to secure information systems assets and human errors are the *"direct and/or indirect cause of the majority of security incidents"* (Khando *et al.*, 2021, p. 2). In fact, Alotaibi *et al.* (2016, p. 661) argue that providing education and training to systems users is essential *"to increase awareness about cybersecurity"*; however, they also stress that the mode of education delivery *"has to be effective in creating an impact on users"* to ensure behavioral change. In fact, it is this absence of behavioral change that leads to a questioning of SETA program effectiveness. For example, Talib *et al.* (2010) argue that employees who receive IS/cyber security training are more aware of a great variety of IS/cyber security issues/threats and the training also has a positive effect on their actual practices; however, they further highlight that not all practices are positively impacted to the same degree which causes concern around the overall effectiveness of SETA programs. Therefore, *"simply undertaking training or having an awareness of an issue does not necessarily imply practice"* (Talib *et al.*, 2010, p. 200). Extant research also suggests that learning about security *"in a more active sense"* is better than *"simply reading reference material"* (Furnell *et al.*, 2002, p. 357). In fact, Alotaibi *et al.* (2016, p. 661) also argue that serious games (as part of a games-based learning approach) *"are proved to be effective tools for training and achieving a behavioural change."* Therefore, building a balance of technical and non-technical competencies in cybersecurity within organizations can be seen as critical to progress the effectiveness of an organizational SETA program.

3. Research methodology

To fulfill the research objective and answer the research questions, this research follows an exploratory design. As agreed by Marshall and Rossman (1989), the purpose of an exploratory research approach is to investigate a little-understood phenomenon. Therefore, being inspired by features of the Gioia Methodology, which is positioned as a *"systematic inductive approach to concept development"* (Gioia *et al.*, 2012, p. 17) and assumes that *"the organisational world is socially constructed"* (Gioia *et al.*, 2012, p. 17), we aim to conceptualize the practitioner voice and not *"substitute practitioners' understandings for theory"* (Markus and Rowe, 2021, p. 273). As a result, in data collection there is a need to *"give extraordinary voice to informants, who are treated as knowledgeable agents"*; while in data analysis there is a need to maintain *"the integrity of 1*st *order (informant-centric) terms"* during initial data coding and further *"organise 1*st*-order codes into 2*nd*-order (theory-centric) themes"* (Gioia *et al.*, 2012, p. 18). We embrace the Gioia Methodology because it encourages originality in our theorizing where what we already know does not limit *"what we can know"* (Gioia *et al.*, 2012, p. 16). In using the Gioia Methodology, we are looking to develop new concepts linked to how organizations organize themselves to deliver more effective SETA programs.

The CSFs for SETA program effectiveness are the outcome of this exploratory inductive-theorizing research approach. Furthermore, interpretive qualitative research is an appropriate research design to apply when exploring CSFs and several scholars have investigated and explored CSFs in IS by applying qualitative methods (c.f. Alhassan *et al.*, 2019). For the purposes of this research, CSFs are defined as "*key areas where things must go right in order to successfully achieve objectives and goals*" (Bullen and Rockart, 1981, p. 9). In essence, their continuing popularity is linked to their most valued characteristic of simplicity as a statement of focus and action (Alyami *et al.*, 2022). It is argued that CSFs are an established approach for providing guidance as a "*popular simplification mechanism to assist managers*" (Borman and Janssen, 2013, p. 86). This explains why CSFs have been widely investigated and used in IS research and in practice over the last three decades, thereby making sense of problems by identifying the factors that could influence business activities and outcomes (c.f. Alhassan *et al.*, 2019).

3.1 Data gathering

In this research, we adopt the "key informant" approach for data gathering and engage with key informants through semi-structured interviews. A key informant is an expert in a particular field who is highly experienced and knowledgeable. According to Marshall (1996), the five criteria for selecting a key informant are as follows: (1) knowledge (the informant should have a depth of information and experience of the phenomenon); (2) willingness (the informant must be willing to communicate and share their knowledge and experience); (3) communicability (the informant should be able to transfer their knowledge in a way that is understandable to the interviewer); (4) impartiality (the informant should be unbiased and any relevant biases must be disclosed beforehand to the interviewer) and (5) role in community (the informant should understand how their role contributes to an understanding of the phenomenon). Therefore, key informants were selected based on their position, experience and professional knowledge about IS/cyber security, particularly SETA program effectiveness.

Interviews are considered one of the most suitable data gathering techniques for collecting rich and detailed data from industry experts (Koh and Tan, 2011; Marshall and Rossman, 1989) and are a typical data-gathering technique with the key informant approach (Whittaker, 2012; Barker *et al.*, 2005). The semi-structured interview is suited to explore new ideas, capture new phenomena and identify the rich contextualized detail of complex concepts. In total, 20 individual semi-structured interviews were conducted with selected key informants from various geographic locations which included the Gulf nations (Saudi Arabia, United Arab Emirates, Qatar and Kuwait), the Middle East (Egypt and Lebanon), USA, UK and Ireland. Table 1 provides a list of the key informants' current role, years of experience, industry sector, qualifications and interview duration. The key informants were recruited through (1) prior knowledge of, and working relationships with, practitioners currently active in IS/cyber security; (2) speakers at practitioner conferences and webinars and (3) LinkedIn connections.

In this study, we conduct a series of semi-structured interviews where each key informant reveals their experiences (positive and negative) with delivering SETA programs. In particular, we are most interested in exploring two sides of a key informant's SETA program experience, namely the "*what*" and the "*how*" across the SETA program lifecycle phases (*design, development*, *implementation* and *evaluation*). This simply translates as "what" action they need to take and "how" they enable that action in their role (leading a SETA program). These actions are also in the context of the key informant striving for the best possible outcome (an effective SETA program). Therefore, all the interviews started by introducing the objective of the research. Each interviewee was then asked to provide a brief summary of their background. Thereafter, topics relating to the factors critical to the success of SETA programs throughout the lifecycle phases (*design, development, implementation and evaluation*) were discussed. See Appendix A for the Interview Guide used.

Table 1. The key informants' current role, years of experience, country, industry sector, qualifications and interview duration

KI #	Country	Role	Sector	Experience (years)	Qualification (education/professional accreditation)	Interview duration (minutes)
1	Saudi Arabia	IS security consultant	Education	>12 years	PhD (Security Software Design)	60
2	Saudi Arabia	CISO (chief information officer)	Fintech	~8 years	BSc (Computing) CEH and CISSP	45
3	Saudi Arabia	Supervisor in the cybersecurity department	Education	10 years	PhD (Cyber Security Management) ISO27001	55
4	Kuwait	Cyber security leader	Oil and Gas	~22 years	PhD (Management and Operations) Cybersecurity Influencer	60
5	Lebanon	Governance and risk management compliance manager	Banking	10 years	BSc (Computer Information Systems) CISA, CISM, CRISC and CIPM	40
6	Qatar	Senior manager for governance risk and compliance	Telecommunications	12 years	MSc (Cyber Security) CISM, ISO27001	45
7	UAE	InfoSec training lead	IT Services (SME)	10 years	BSc (Computer Software Engineering)	40
8	UAE	Consultant in IS security	IT Services (SME)	>17 years	MBA CISSP, ISO27001 and CRISC	50
9	Saudi Arabia	CISO (chief information officer)	Petrochemicals and Chemicals	15 years	MSc (Information Security) ISOC	55
10	Kuwait	CISO (chief information officer	Oil and Energy	8 years	MSc (Computer Engineering)	40
11	USA	Consultant in IS security	Financial Services and Education	20 years	BSc (Computer Information Systems) Certified SANS Instructor	60
12	UK	CISO (chief information officer)	IT Services	~20 years	MSc (Information Security) CISSP, CISM and ISO27001	55
13	USA	Director for cyber leadership and strategy solutions	IT Services	25 years	MBA (Information Security Management) CISM	45
14	Kuwait	Head of information security governance	IT Services	20 years	MSc (Information Security) CISM, ISO270001	50
15	Saudi Arabia	Cyber security consultant	Computer and Network Security	10 years	PHD (Cyber Security) CISM	60

(*continued*)

Table 1.

KI #	Country	Role	Sector	Experience (years)	Qualification (education/professional accreditation)	Interview duration (minutes)
16	Egypt	Head of cyber security	Banking	20 years	MSc (Business Information Technology) C|CISO, CISM, CRISC and ISO27001	55
17	UK	Security Awareness Manager	Banking	15 years	MSc (Information Security and Privacy)	50
18	USA	Director of Security Awareness	Computer and Network Security	>20 years	MBA Certified SANS Instructor	45
19	Ireland	Senior lecture in IS security	Education	17 years	PhD (IS Security Management)	45
20	Ireland	IT security officer	Education	21 years	MBA (Technology and Management)	50

Source(s): Table legend for professional accreditation
●CEH: Certified Ethical Hacker
●ISO27001: International Standard (Information Security Management Systems)
●CISA: Certified Information Systems Auditor
●CISM: Certified Information Security Management
●CRISC: Certified in Risk and Information Systems Control
●CIPM: Certificate in Investment Performance Measurement
●CISSP: Certified Information Systems Security Professional
●ISOC: Industrial Security Oversight Certification
●SANS: SysAdmin, Audit, Network and Security
●C|CISO: Certified Chief Information Security Officer
Author's own creation/work

Interviews took place over seven months (between April 2021 and October 2021) and ranged in duration from 40 to 60 min with an average duration of 50 min. Due to the coronavirus disease 2019 (COVID-19) restrictions, all interviews were conducted virtually through MS Teams. All participant engagement and research data management practices have been approved under institutional ethical approval (UCC ethical approval number: Log 2021 - 024). The interviews were conducted in two languages: Arabic and English. Four interviews from the Middle East were originally done in Arabic and translated into English by the lead author. The remaining 16 interviews were conducted in English. All the interviews were transcribed line by line and checked against the voice recordings, where necessary, to ensure the accuracy of the interview transcription process.

3.2 Data analysis

Data analysis is a crucial step in qualitative research (Leech and Onwuegbuzie, 2008). Its main purpose is to develop an understanding of the phenomenon of interest (Kawulich, 2004). In this research we adopt an inductive open, axial and selective coding approach as part of our qualitative data analysis. This approach to coding allows us "*to communicate and connect with the data to facilitate the comprehension of the emerging phenomena and to generate theory grounded in the data*" (Basit, 2003, p. 152). Therefore, during *open coding* we aim to generate concepts/categories from field data (c.f. Walsham, 2006) through a "*process of breaking down, examining, comparing, conceptualizing, and categorizing data*" (Strauss and Corbin, 1990, p. 61). Moving through the open coding process affords us the opportunity to identify the key ideas hidden within the key informant interview data (concepts/categories) and related to the phenomenon of interest (c.f. Bhattacherjee, 2012). Furthermore, during *axial coding* (the second reading of the data), we are thinking systematically about the data in order to link the emergent categories and form relationships (c.f. Alhassan *et al.*, 2019; Bhattacherjee, 2012; Dezdar and Sulaiman, 2009; Strauss and Corbin, 1990). Finally, during *selective coding* we tell the story of the core categories that emerge (c.f. Strauss and Corbin, 1990).

For this research, the open, axial and selective coding process took place over a 13-month period (from May 2021 to May 2022). The tempo with which the key informant interviews were completed dictated the tempo with which the coding of the data progressed. There was also a constant reflection back to the literature (e.g. SETA program effectiveness and SETA program lifecycle) throughout the inductive coding process. During the coding process, the research team followed "*collaborative reflection*" to offer a "*diversity of perspectives*" and challenge assumptions (c.f. Olmos-Vega *et al.*, 2022, pp. 5-6). These research team discussions maintained the ongoing accuracy and consistency of the codes/concepts being generated through the coding process while also allowing for a constant comparative analysis effort and consolidation of the codes/concepts into higher-order categories. This afforded the other members of the research team the opportunity to provide an external challenge to the lead author (giving a somewhat more "objective" view to the lead author – having not been "in the weeds" coding each interview transcript).

During *open coding*, this collaborative reflection, between the four-member research team, took place on four specific occasions, as follows: June 2021 (discussing the codes generated across 3 interviews), July 2021 (discussing the codes generated across 6 interviews), September (discussing the codes generated across 15 interviews) and October 2021 (discussing the codes generated across all 20 interviews). To enable this collaborative reflection, the lead author transcribed each key informant interview and generated a structured transcript, which they then coded (reading the transcript sentence by sentence and following an inductive open coding approach). The open coding procedure for the 20 key informant interviews resulted in 212 coded excerpts relating to the factors impacting on the effectiveness of a SETA program. These 212 coded excerpts led to the emergence of 15 categories mapped across the 4 SETA program lifecycle phases. Specifically, the code/category distribution is as follows: **design** phase: 95 coded excerpts across 8 categories, **development** phase: 27 coded excerpts across 4 categories; **implementation** phase, 50 coded excerpts across 5 categories and **evaluation** phase: 40 coded excerpts across 3 categories. Thereafter, unpacking the categories with at least five key informant voices (25% coverage) led to: [i] the removal of four categories (reducing the number of coded excerpts to 187) and [ii] the emergence of the CSFs (11 remaining categories) for SETA program effectiveness. The category with the highest coding frequency and key informant voices across each of the SETA program lifecycle phases is as follows: **design** phase – 22 coded excerpts in the "*Assessment Needs*" category (extracted from 18 key informants), **development** phase – 14 coded excerpts in the "*Communication*" category (extracted from 12 key informants), **implementation** phase – 28 coded excerpts in the "*Communication Channel*" category (extracted from 17 key informants) and **evaluation** phase – 24 coded excerpts in the "*Periodic Assessment*" category (extracted from 20 key informants). See Table 2 for an analysis across all 11 CSFs and Appendix B for the distribution of contributing key informants to CSFs (ranked in descending order).

Table 2.
Key informant frequency and coded excerpt distribution for each CSF

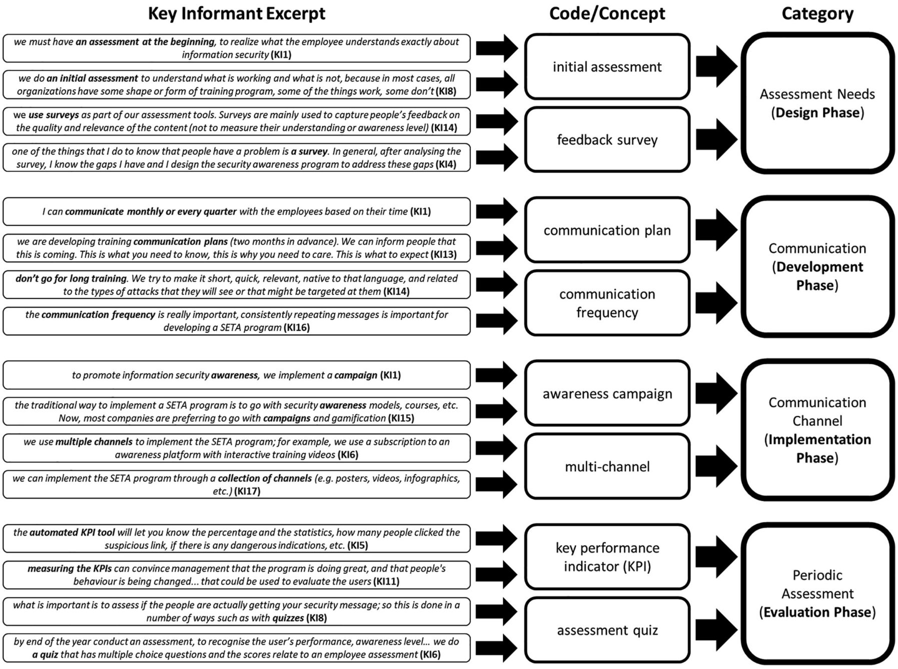
Lifecycle phase	CSF (ranked order within lifecycle phase)	Category	Coded excerpts	KI frequency	CSF rank
Design	**CSF-DS1:** Conduct an Initial Assessment of Employee Security Awareness	Assessment Needs	22 (12%)	18 (90%)	2
	CSF-DS2: Know Your Audiences to Ensure Content Suitability	Target Audiences	21 (11%)	18 (90%)	3
	CSF-DS3: Make a Yearly Plan to Align Goals and Objectives	Goal/Objective	16 (9%)	16 (80%)	5
	CSF-DS4: Design for Cultural Context and Employee Cultural Diversity	Culture	14 (7%)	14 (70%)	6
	CSF-DS5: Adhere to Organizational Security Policy and the "Law of the Land"	Policy	11 (6%)	11 (55%)	9
	CSF-DS6: Build Security Awareness Campaigns	Communication	11 (6%)	9 (45%)	11
Development	**CSF-DV1:** Sustained Communication of Relevant Messages	Communication	14 (7%)	12 (60%)	8
Implementation	**CSF-IM1:** Apply Diverse Methods to Deliver Security Awareness Messages	Communication Channel	28 (15%)	17 (85%)	4
	CSF-IM2: Motivate Employees to Engage in Security Awareness	Motivation	11 (6%)	11 (55%)	10
Evaluation	**CSF-EV1:** Maintain Quarterly Evaluation of Employee Performance	Periodic Assessment	24 (13%)	20 (100%)	1
	CSF-EV2: Measure Employee Reporting of Security Incidents	Incident Indication	15 (8%)	14 (70%)	7
Total			187 (100%)	20 (100%)	

Source(s): Authors' own creation/work

From November 2021 to January 2022, the analysis of the open coding outputs produced the initial list of 11 CSFs for SETA program effectiveness. These CSFs emerged as a result of grouping similar codes/concepts into higher-order, more abstract concepts, called categories. Again, through embracing collaborative reflection, the lead author shared these CSFs on three specific occasions as follows: November 2021 (discussing the codes/category and narrative generated for the first CSF), December 2021 (discussing the codes/categories and narratives generated for all 11 CSFs) and January 2022 (discussing the 2nd draft narratives for all 11 CSFs). See Figure 1 for a sample of our open coding.

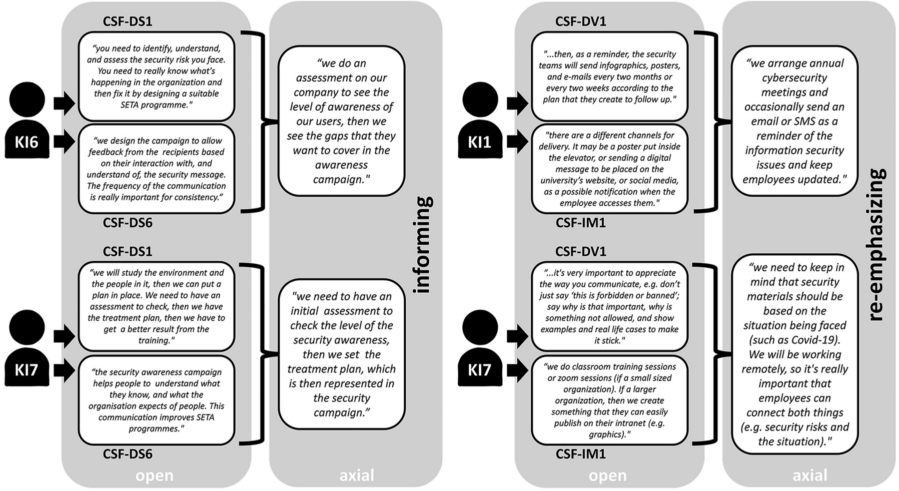
As part of our *axial coding* approach, which took place from February 2022 to May 2022, we identified several relationships between the CSFs (categories) generated during open coding. These relationships were identified where a coded excerpt (from a key informant) was linked to more than one CSF (as part of open coding), thereby suggesting a potential relationship being explained by a key informant. We deemed this relationship as relevant if it suggested a "cause and effect" type relationship was present in their story of achieving SETA program effectiveness. Again, we embraced collaborative reflection, where the lead author and 2nd author shared their interpretations of the prospective CSF relationships, on an almost fortnightly basis, throughout the four-month period. See Figure 2 for a sample of our axial coding.

Finally, our effort at *selective coding* allows us to tell a compelling theorizing story around the outputs (the 11 CSFs for SETA program effectiveness and the 9 relationships between these CSFs). See Figure 3 for our Lifecycle Model of CSFs for SETA program effectiveness. The genesis of our model is similar in nature to that of the relationships between the building blocks of the digital transformation process proposed by Vial (2019). For example, the arrows


Key Informant Excerpt
Code/Concept
Category
we must have an assessment at the beginning, to realize what the employee understands exactly about information security (KI1)
we do an initial assessment to understand what is working and what is not, because in most cases, all organizations have some shape or form of training program, some of the things work, some don't (KI8)
we use surveys as part of our assessment tools. Surveys are mainly used to capture people's feedback on the quality and relevance of the content (not to measure their understanding or awareness level) (KI14)
one of the things that I do to know that people have a problem is a survey. In general, after analysing the survey, I know the gaps I have and I design the security awareness program to address these gaps (KI4)
initial assessment
feedback survey
Assessment Needs (Design Phase)
I can communicate monthly or every quarter with the employees based on their time (KI1)
we are developing training communication plans (two months in advance). We can inform people that this is coming. This is what you need to know, this is why you need to care. This is what to expect (KI13)
don't go for long training. We try to make it short, quick, relevant, native to that language, and related to the types of attacks that they will see or that might be targeted at them (KI14)
the communication frequency is really important, consistently repeating messages is important for developing a SETA program (KI16)
communication plan
communication frequency
Communication (Development Phase)
to promote information security awareness, we implement a campaign (KI1)
the traditional way to implement a SETA program is to go with security awareness models, courses, etc. Now, most companies are preferring to go with campaigns and gamification (KI15)
we use multiple channels to implement the SETA program; for example, we use a subscription to an awareness platform with interactive training videos (KI6)
we can implement the SETA program through a collection of channels (e.g. posters, videos, infographics, etc.) (KI17)
awareness campaign
multi-channel
Communication Channel (Implementation Phase)
the automated KPI tool will let you know the percentage and the statistics, how many people clicked the suspicious link, if there is any dangerous indications, etc. (KI5)
measuring the KPIs can convince management that the program is doing great, and that people's behaviour is being changed... that could be used to evaluate the users (KI11)
what is important is to assess if the people are actually getting your security message; so this is done in a number of ways such as with quizzes (KI8)
by end of the year conduct an assessment, to recognise the user's performance, awareness level... we do a quiz that has multiple choice questions and the scores relate to an employee assessment (KI6)
key performance indicator (KPI)
assessment quiz
Periodic Assessment (Evaluation Phase)

Source(s): Author's own creation/work

Figure 1.
A sample of our open coding (a snapshot of the highest frequency categories across the four lifecycle phases)



“you need to identify, understand, and assess the security risk you face. You need to really know what's happening in the organization and then fix it by designing a suitable SETA programme."

“we design the campaign to allow feedback from the recipients based on their interaction with, and understand of, the security message. The frequency of the communication is really important for consistency.”

“we do an assessment on our company to see the level of awareness of our users, then we see the gaps that they want to cover in the awareness campaign."

“we will study the environment and the people in it, then we can put a plan in place. We need to have an assessment to check, then we have the treatment plan, then we have to get a better result from the training."

“the security awareness campaign helps people to understand what they know, and what the organisation expects of people. This communication improves SETA programmes."

"we need to have an initial assessment to check the level of the security awareness, then we set the treatment plan, which is then represented in the security campaign.”

"...then, as a reminder, the security teams will send infographics, posters, and e-mails every two months or every two weeks according to the plan that they create to follow up."

"there are a different channels for delivery. It may be a poster put inside the elevator, or sending a digital message to be placed on the university’s website, or social media, as a possible notification when the employee accesses them."

“we arrange annual cybersecurity meetings and occasionally send an email or SMS as a reminder of the information security issues and keep employees updated."

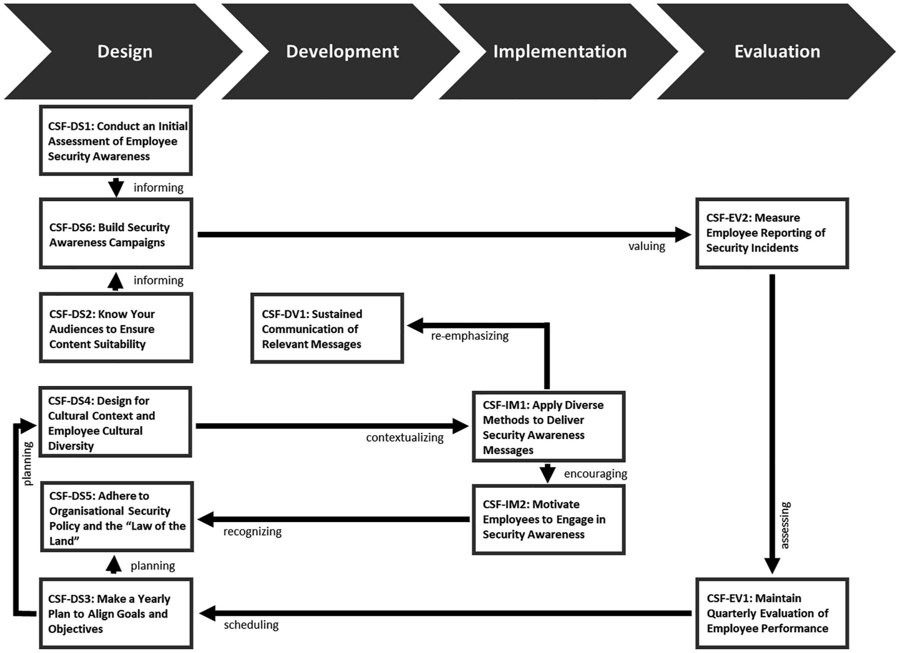
“...it's very important to appreciate the way you communicate, e.g. don’t just say ‘this is forbidden or banned’; say why is that important, why is something not allowed, and show examples and real life cases to make it stick."

“we do classroom training sessions or zoom sessions (if a small sized organization). If a larger organization, then we create something that they can easily publish on their intranet (e.g. graphics)."

“we need to keep in mind that security materials should be based on the situation being faced (such as Covid-19). We will be working remotely, so it's really important that employees can connect both things (e.g. security risks and the situation)."

Source(s): Author’s own creation/work

Figure 2.
A Sample of our axial coding (a snapshot of the *within* phase and *across* phase CSF relationships)


Design
Development
Implementation
Evaluation
CSF-DS1: Conduct an Initial Assessment of Employee Security Awareness
informing
CSF-DS6: Build Security Awareness Campaigns
valuing
CSF-EV2: Measure Employee Reporting of Security Incidents
informing
CSF-DS2: Know Your Audiences to Ensure Content Suitability
CSF-DV1: Sustained Communication of Relevant Messages
re-emphasizing
CSF-DS4: Design for Cultural Context and Employee Cultural Diversity
contextualizing
CSF-IM1: Apply Diverse Methods to Deliver Security Awareness Messages
planning
encouraging
CSF-DS5: Adhere to Organisational Security Policy and the “Law of the Land”
recognizing
CSF-IM2: Motivate Employees to Engage in Security Awareness
assessing
planning
CSF-DS3: Make a Yearly Plan to Align Goals and Objectives
scheduling
CSF-EV1: Maintain Quarterly Evaluation of Employee Performance

Source(s): Author’s own creation/work

Figure 3.
The Lifecycle Model of CSFs for SETA program effectiveness

“detail an overarching sequence of relationships” described by the key informants, as opposed to presenting *“a statistical relationship or a causality found in variance models”* (Vial, 2019, p. 122). In the next section, we discuss the research findings which are then presented as a Lifecycle Model of CSFs for SETA program effectiveness.

4. Findings: the CSFs and the CSF relationships

In this section, we set about answering our research questions (based on our analysis of the 20 key informant interviews). In section 4.1, we present the 11 CSFs for SETA program effectiveness (RQ1). In section 4.2, we present 9 relationships between the CSFs *within* (4) and *across* (5) the SETA program lifecycle phases (*design*, *development*, *implementation* and *evaluation*) (RQ2). As highlighted in Table 2, our analysis revealed six CSFs relating to the design phase, one CSF relating to the development phase, two CSFs relating to the implementation phase and two CSFs relating to the evaluation phase. The 11 CSFs and the 9 relationships are visualized in the Lifecycle Model of CSFs for SETA program effectiveness (see Figure 3).

4.1 CSFs for SETA program effectiveness (RQ1)

In this section, we present these CSFs in a ranked order (based on the frequency count of coded excerpts) within each SETA program lifecycle phase.

4.1.1 CSF-DS1: conduct an initial assessment of employee security awareness. Based on our analysis, this CSF captures the story behind the "Assessment Needs" category within the design phase of the SETA program lifecycle. This CSF highlights the fact that conducting an initial assessment is an essential factor in designing a SETA program. Primarily, a focus on determining what the employees understand about the organization's security policy is crucial, along with an understanding of their appreciation of the risks associated with current cyber security threats. Within this study, the key informants suggest conducting an initial assessment using tools like surveys or quizzes in an effort to gauge how knowledgeable the employees are about IS security issues. For example, one key informant (KI1) mentions "*completing a test on IS security to realize what the employee understands exactly about information security,*" while another informant (KI8) suggests "*an initial assessment to understand what is working and what is not working.*" It is also noteworthy that employees at various levels within the organization will have different types of assessments to complete. For example, the assessment that an IS security manager completes will be different to the one completed by the end-user. As noted by one of the key informants (KI2), "*each level has a specific security awareness programme regarding cybersecurity.*" Therefore, this CSF emphasizes that identifying the current level of understanding around cybersecurity issues, as part of the design phase of a SETA program lifecycle, will increase the likelihood of successful SETA program outcomes.

4.1.2 CSF-DS2: know your audiences to ensure content suitability. Based on our analysis, this CSF captures the story behind the "Target Audiences" category within the design phase of the SETA program lifecycle. This CSF highlights the importance of allocating the appropriate privileges to employees, using their organizational role to determine their security responsibilities. Identifying "who your audiences are" is critical in designing a SETA program to ensure content suitability. Within this research study, key informants explain how most organizations set up a SETA program based on their audiences' levels. Therefore, materials used must be appropriate for each level to ensure that employees understand the contents of the security training. For example, one key informant (KI7) comments, "*we start to plan to design a SETA programme based on audience classification, it's important to provide the material based on knowing those who we are speaking to understand what we are saying [. . .].*" It is clear that a top management employee has different security training to a new graduate employee. As one key informant (KI14) states, "*so employees working in operation sites, oil production, or HR, etc., they might see some different pieces of training and sometimes different material.*" Thus, each job role in the organization has specific responsibilities such that the requisite IS security training needs are different.

4.1.3 CSF-DS3: make a yearly plan to align goals and objectives. Based on our analysis, this CSF captures the story behind the "Goal/Objective" category within the design phase of the

SETA program lifecycle. This CSF highlights the importance of communicating the SETA program objectives (knowing what is required to be delivered) clearly and consistently to the employees. It is also important to ensure that the SETA program goals meet the specific needs of the organization (as captured in its strategy) and these two aspects are aligned during the design phase. Within this research study, key informants suggest that a yearly plan be devised to determine the objectives and design of the SETA program based on the activities it wants to achieve. For example, one key informant (KI6) states, *"[. . .] every year we make a plan, determine our goals or objectives of the year, then we design activities for the awareness programme to see how to execute the plan [. . ..]."* In addition, each year, most organizations update their objectives regarding the SETA program. Another key informant (KI3) comments, *"[. . .] if it wasn't specifically designed, the organisational SETA programme would not succeed. As well, if its objectives are not associated with the strategies of the institution, it will not work."* This suggests that organizations should create a plan for designing a SETA program and that plan should contain what is necessary to be delivered, such as the types of IS security issues or topics.

4.1.4 CSF-DS4: design for cultural context and employee cultural diversity. Based on our analysis, this CSF captures the story behind the "Culture" category within the design phase of the SETA program lifecycle. This CSF focuses on the criticality of understanding the cultural diversity in the organization when designing a SETA program, simply because the cybersecurity message can be interpreted differently from one culture to another. Employees come from different backgrounds, and it is necessary to understand this diversity. Various aspects of cultural context require focus when designing a SETA program, such as: language, knowledge, level of education, age and gender. All these aspects contribute to a successful SETA program outcome. For example, within this research study, the key informants come from many countries and all these countries have their own culture. Therefore, if our key informants represented a typical organization's employees, then these differentiations would need to be considered when designing a SETA program. For example, the cultures of Saudi Arabia, Egypt and UAE care more about language, and as a result, use artefacts for SETA programs, such as videos and posters in Arabic, to make the message more attractive and easier to understand as stated by one key informant (KI16), *"culture is an important factor to consider when you want to design an awareness program, we design the videos in the Arabic language that contains street language; we noticed the employees interact with these kinds of videos."* However, understanding culture across different geographical locations in terms of knowledge, language and education further contributes to the success of a SETA program. As commented by key informant (KI1), *"[. . .] design the SETA programmes in a way that is close to the culture to make it a success."* Therefore, each culture has specific characteristics that make it unique from other cultures and this must be appreciated to ensure the effectiveness of the SETA program.

4.1.5 CSF-DS5: adhere to organizational security policy and the "law of the land". Based on our analysis, this CSF captures the story behind the "Policy" category within the design phase of the SETA program lifecycle. This CSF focuses on the guidelines and procedures needed to protect the IS assets of the organization. These factors can be regulation or legislation that helps to modify employee IS security behavior. It is critically important that all of the organizational security policies and the "law of the land" are adhered to when designing a SETA program (e.g. General Data Protection Regulation (GDPR) in Ireland and the Saudi Arabian Monetary Authority (SAMA) in Saudi Arabia). Within this research study, key informants stress that the organization should be aware of all regulations and policies. Each country has its own rules and regulations regarding data privacy and data security as mentioned by one key informant (KI1), *"most of the organizations design SETA programmes in-house, and these programmes should align with their security policy. For example, laws in some countries are different."* In addition, all employees in the organization are obliged to be aware of the information security policy within their organization. Each organization has its own policies, for instance, the restriction on the sharing of passwords among employees and other social engineering issues. For example, one key informant (KI2) stated "*all members of the organization, from the board to the technical employee, have a duty to be aware of the information security policy and privacy.*" Thus, understanding the business requirements and their policies are fundamental to designing a SETA program.

4.1.6 CSF-DS6: build security awareness campaigns. Based on our analysis, this CSF captures the story behind the "Communication" category within the design phase of the SETA program lifecycle. This CSF highlights the fact that targeted awareness campaigns can update employees (or end-users) on how to mitigate against the potential risks associated with an IS security threat and keep them informed on what is coming and, most crucially, why they need to care. Within this research study, key informants state the need for discussion at the end of an IS security training session or awareness campaign. It is as part of these conversations that individuals understand the security awareness message. For example, one key informant (KI17) noted, "*what is important in this session is to assess if the people are actually getting your security message [. . .]*". In addition, a security awareness campaign should be rolled out every three months and a follow-up also organized with employees, for consistency and reliability, and to emphasize the importance of the security awareness program to the organization as stated by another informant (KI13), "*to build a security awareness and training program, you need to communicate with all the stakeholders and say this is coming. This is why you care. People need to understand why it is important [. . .].*" Therefore, to build a security awareness campaign that plays an important role in the success of a SETA program is of critical importance.

4.1.7 CSF-DV1: sustained communication of relevant messages. Based on our analysis, this CSF captures the story behind the "Communication" category within the development phase of the SETA program lifecycle. This CSF is based on how to communicate with audiences regularly and how to follow up with updated materials and topics. The security message should be repeated differently because the audience can lose concentration and forget. Thus, continuous communication with employees regarding IS security practices is an effective way to assist them in reducing security incidents and breaches. Within this research study, key informants highlight the importance of sustainable communication with the employees for the development of the SETA program. For example, one key informant (KI1) notes, "*we need to direct and inform the employees that this issue of security awareness is not only crucial in their work environment but also in their life routine.*" Effective communication clarifies why some issues are not permitted. It can show the employees examples of real-life cases of human errors at play while informing them of the enormity of the problems by using pictures and real stories as stated by one key informant (KI5), "*[. . .] when we have a real human error, telling them this is a real problem by proving this with pictures and real stories with consequences, is invaluable [. . .].* In addition, security training and awareness materials must be updated based on current situations. For instance, one key informant (KI11) comments, "*we are facing problems such as Covid-19 and working remotely. It is important to have materials based on this situation, so they can connect both things and will never forget whatever was given.*" Thus, it is necessary to always remind the employees that IS security issues exist all the time, whether in the work environment or in one's personal life.

4.1.8 CSF-IM1: apply diverse methods to deliver security awareness messages. Based on our analysis, this CSF captures the story behind the "Communication Channel" category within the implementation phase of the SETA program lifecycle. This CSF highlights that organizations use various approaches to deliver SETA program messaging. For example, they can deliver security awareness messages via SMS texts, emails, online courses, face-to-face meetings, videos, quizzes and posters. In addition, by placing security awareness messages on internal screens in public areas, such as corridors, employees are reminded frequently of this security issue. Thus, organizations determine the best methods to use to implement their SETA program messaging based on their resources, size and budget. Within this research study, key informants identified the various methods to deliver a successful SETA program as commented by one key informant (KI2), *"the best security awareness programmes include various IS security delivery methods because we have to consider individuals' differences."* The popular method used to implement a SETA program is computer-based training (CBT) that includes all training materials and quizzes. It is a platform that anyone can access anywhere. However, the latest trending method is "gamification" which is a very interactive application like playing a game. The organization engages the user by sending out materials or videos and employees can watch the videos and answer the questions accompanying them. For example, one key informant (KI9) states, *"the new trend in Cybersecurity Awareness is 'gamification' - conducting games for employees [...]."* All organizations have access to this and other methods to promote security awareness to their employees.

4.1.9 CSF-IM2: motivate employees to engage in security awareness. Based on our analysis, this CSF captures the story behind the "Motivation" category within the implementation phase of the SETA program lifecycle. This CSF highlights those employees can be encouraged to adhere to IS security policies by earning a bonus or other recognition (reward) based on their practices. This can have a positive impact on the effectiveness of the organization's SETA program. In this research study, key informants mentioned several methods to motivate employees to embrace IS security training. For example, employees can be invited to complete several tasks such as quizzes or videos that are assigned scores. These scores can waive other requirements such as attending security awareness courses. This method was described by a key informant (KI11) as follows: *"I think it is a really good incentive for employees. If the employee can pass the quiz with 100%. You don't have to watch the video [...]."* This type of motivation encourages the employee to learn necessary materials to pass quizzes. An employee can also be motivated by attending events or celebrations that promote the organization's security policy. One key informant (KI1) from Saudi Arabia mentions, *"some government agencies contributed to arranging activities and are welcoming of the employees' families and their children by giving colouring books to their children [...]."* These events include recommendations about appropriate security practices to promote security awareness. Additionally, focusing on the social side motivates employees to attend the events and understand the IS security issues in a social setting.

4.1.10 CSF-EV1: maintain quarterly evaluation of employee performance. Based on our analysis, this CSF captures the story behind the "Periodic Assessment" category within the evaluation phase of the SETA program lifecycle. This CSF focuses on providing a year-end evaluation summary to measure each employee's performance, level of awareness and number of training sessions completed. This evaluation is a report of the employee's progress and provides guidance on improvements to be made. For example, one of the significant tools for evaluating employees' performance in the annual report is the Key Performance Indicators (KPIs) related to IS security issues, such as cybersecurity attacks, phishing campaigns, sharing password policy breaches, etc. Each quarter, most organizations use KPIs to evaluate employee performance and the percentage that fulfill the training requirements, in order to assess the knowledge retained by employees and thereby review the effectiveness of the SETA program. Within this research study, key informants highlight several techniques to assess the employees' responses to the SETA program. One of the techniques used is a survey/questionnaire to evaluate employee knowledge before and after they have undergone training. This type of evaluation answers important questions such as have we overcome the challenges? Or, did we make the same mistakes? One key informant (KI4) comments, *"[...] conducting a questionnaire before the training and after to know the amount of knowledge the employee is getting from the security context. Then we can measure the effectiveness of these programmes [...]."* Another technique is the use of quizzes.

After completing IS security training, passing a quiz can be an effective tool to evaluate the employee's performance as mentioned by one key informant (KI12), "*passing the quizzes can assess the employee behavior and level of awareness [. . .].*" Lastly, by using the KPIs technique, it is possible to identify the number of training sessions/programs the employees attended and completed. A key informant (KI15) explains this, "*[. . .] we need to convince the management that the programme is doing great, and that employee behaviour is being changed. So, KPIs could be used to evaluate them.*" These tools, therefore, assist in the evaluation of employee performance with regard to SETA programs and this also provides an indication of the program's success.

4.1.11 CSF-EV2: measure employee reporting of security incidents. Based on our analysis, this CSF captures the story behind the "Incident Indication" category within the evaluation phase of the SETA program lifecycle. This CSF highlights the security incidents reported by the employee. Most organizations use phishing campaigns to simulate attacks. They want to know how many of the employees click the suspicious links, to measure the employees' awareness and knowledge regarding IS security issues. Thus, an increase in the number of suspicious links or other incidents reported by the employees is a valuable indication of the SETA program's effectiveness. Within this research study, key informants described the methods to evaluate employee behavior and the level of their awareness regarding the detection and reduction in security incidents. When the employee sends emails to the IS security department to report a suspicious link, that reflects on the success of the SETA program. For example, one key informant (KI3) comments, "*the reporting of a suspicious email indicated they get the awareness message.*" The employees are the strongest link to protect the organization, provided they are aware of the suspicious emails and report them directly. In addition, the KPI tool can also be used to compare the current and previous years to measure the percentage of clicks on suspicious links. If employees recognize a percentage decrease in clicks, then it shows that the SETA program is effective and improving security as mentioned by one key informant (KI10), "*KPIs as a tool will let you know percentages and statistics, e.g. how many people clicked on suspicious links [. . .].*" Lastly, most organizations rely on phishing campaigns as a key informant (KI4) states, "*a simulation phishing campaign is used to identify who clicks and opens suspicious emails, and the percentage of those who report the incident to the security department [. . .].*" The main reason for a phishing simulation is to raise the level of awareness among employees. Therefore, reducing the number of security incidents (e.g. clicks on suspicious links) would show that the level of awareness is increasing (highlighting SETA program effectiveness).

In the next section, we now examine the CSF relationships *within* and *across* the SETA program lifecycle phases.

4.2 The CSF relationships within and across the SETA program lifecycle phases (RQ2)

Based on our analysis, we identify nine relationships between the CSFs for SETA program effectives (four relationships between the CSFs *within* the SETA program lifecycle phases and five relationships between the CSFs *across* the SETA program lifecycle phases). Based on our analysis, these nine relationships *within* and *across* the SETA program lifecycle phases (*design*, *development*, *implementation and evaluation*) are deemed important for SETA program effectiveness. As described in our methodology, these 9 relationships between the 11 CSFs were identified during our *axial* coding of the excerpts emerging from the 20 key informant transcripts. Therefore, if a coded excerpt (from a key informant) was linked to more than one CSF (as part of *open* coding), we viewed this as the existence of a potential relationship between the CSFs (see Figure 2 for a visualization of this process). This pattern spotting afforded the research team the opportunity to see these "cause and effect"-type relationships emerge from the key informant stories. Thereafter, as part of our *selective* coding, we were in a position to craft "*meaningful boxes and arrows*" as part of our "*interim struggles*" (theorizing) (c.f. Weick, 1995, p. 389). This iterative process led to the emergence of the Lifecycle Model of CSFs for SETA program effectiveness (see Figure 3).

Table 3 presents the *within* phase relationships as follows: CSF-DS3 impacting on CSF-DS4 and CSF-DS5 (**planning**); CSF-DS1 and CSF-DS2 impacting on CSF-DS6 (**informing**); CSF-IM1 impacting on CSF-IM2 (**encouraging**) and CSF-EV1 impacting on CSF-EV2 (**assessing**). Table 4 presents the *across* phase relationships as follows: CSF-DS6 impacting on CSF-EV2 (**valuing**); CSF-DS4 impacting on CSF-IM1 (**contextualizing**); CSF-IM1 impacting on CSF-DV1 (**re-emphasizing**); CSF-IM2 impacting on CSF-DS5 (**recognizing**) and CSF-EV1 impacting on CSF-DS3 (**scheduling**).

The **planning** relationship (the direct impact of **CSF-DS3:** "Make a Yearly Plan to Align Goals and Objectives" on both **CSF-DS4:** "Design for Cultural Context and Employee Cultural Diversity" and **CSF-DS5:** "Adhere to Organisational Security Policy and the 'Law of the Land'") illustrates that planning the design of a SETA program around the organizational needs is influenced significantly by the organizational context (e.g. culture and security policy). For example, a setup plan to design a SETA program that takes into consideration (i) the use of Arabic language for Arab countries (cultural context) and (ii) the adherence to GDPR in Ireland (regulation and policy context). Therefore, considering the cultural and security policy context in planning, in the design phase of a SETA program, is critical to delivering an effective program.

The **informing** relationship (**CSF-DS6:** "Build Security Awareness Campaigns" is more effective in the presence of **CSF-DS1:** "Conduct an Initial Assessment of Employee Security Awareness" and **CSF-DS2:** "Know Your Audiences to Ensure Content Suitability") highlights that in order to prepare appropriate materials for the audience, it is important to

Table 3. The relationships between the CSFs within the SETA program lifecycle phases

CSF	Has an impact on	Relationship	Description
CSF-DS3: Make a Yearly Plan to Align Goals and Objectives	**CSF-DS4:** Design for cultural context and employee cultural diversity	**Planning**	Enables the design of a programme plan that aligns with the organizational cultural context
	CSF-DS5: Adhere to organizational security policy and the "Law of the Land"		Enables the design of a programme plan that considers organizational security policy and geographical legislation
CSF-DS1: Conduct an Initial Assessment of Employee Security Awareness **CSF-DS2:** Know Your Audiences to Ensure Content Suitability	**CSF-DS6:** Build security awareness campaigns	**Informing**	Enables the delivery of appropriate campaign materials reflecting the awareness and knowledge levels of the target audiences
CSF-IM1: Apply Diverse Methods to Deliver Security Awareness Messages	**CSF-IM2:** Motivate employees to engage in security awareness	**Encouraging**	Enables the use of different communication methods to motivate employees to engage with IS security training materials
CSF-EV2: Measure Employee Reporting of Security Incidents	**CSF-EV1:** Maintain quarterly evaluation of employee performance	**Assessing**	Enables the performance of an employee to be evaluated using the number of security incidents reported by the employee

Source(s): Authors' own creation/work

CSF	Has an impact on	Relationship	Description
CSF-DS6: Build Security Awareness Campaigns	**CSF-EV2:** Measure employee reporting of security incidents	**Valuing**	Enables the use of a simulation attack to raise employee's knowledge of security incidents and ensures these incidents are reported appropriately
CSF-DS4: Design for Cultural Context and Employee Cultural Diversity	**CSF-IM1:** Apply diverse methods to deliver security awareness messages	**Contextualizing**	Enables the use of different communication channels in order to deliver a culturally contextualized security message
CSF-IM1: Apply Diverse Methods to Deliver Security Awareness Messages	**CSF-DV1:** Sustained communication of relevant messages	**Re-emphasizing**	Enables the use of different communication channels with the aim of repeating important security awareness messages
CSF-IM2: Motivate Employees to Engage in Security Awareness	**CSF-DS5:** Adhere to organizational security policy and the "Law of the Land"	**Recognizing**	Enables the motivation of employees through earning recognitions and rewards for complying with IS security policy and legislation
CSF-EV1: Maintain Quarterly Evaluation of Employee Performance	**CSF-DS3:** Make a yearly plan to align goals and objectives	**Scheduling**	Enables the production of a new security plan based on the outcome of the current organizational performance to plan

Source(s): Authors' own creation/work

Table 4. The relationships between the CSFs across the SETA program lifecycle phases

recognize the level of the audience's IS security awareness and knowledge. For example, the campaign should have a classification to provide appropriate materials to the audiences' level of understanding of the security awareness message (e.g. *introductory*, *intermediate* and *advanced*). The introductory content for new "non-IT" employees or the more advanced content for established IT employees with IS security responsibilities. This "targeted audience materials" approach will improve SETA program effectiveness.

The **encouraging** relationship (the direct impact of **CSF-IM1:** "Apply Diverse Methods to Deliver Security Awareness Messages" on **CSF-IM2:** "Motivate Employees to Engage in Security Awareness") highlights that applying different communication channels in IS security training can contribute to employee motivation. Therefore, an employee selecting the method most suitable for their engagement with the IS security awareness message or training materials has a positive impact on SETA program effectiveness.

The **assessing** relationship (the direct impact of **CSF-EV2:** "Measure Employee Reporting of Security Incidents" on **CSF-EV1:** "Maintain Quarterly Evaluation of Employee Performance") highlights that the quantification of the number of times that an employee reports a security incident is a KPI and can reveal a significant amount about the effectiveness of a SETA program, at both an organizational and individual level. For example, at an individual level, an employee with a high percentage of reported incidents reflects positively on their performance (the know-how they have acquired from the IS security training) and most likely increases the likelihood of the employee passing the IS security training. In effect, assessing an employee's performance (by the number of reported incidents) is a good indicator of the effectiveness of the SETA program.

The **valuing** relationship (**CSF-EV2:** "Measure Employee Reporting of Security Incidents" is more effective in the presence of **CSF-DS6:** "Build Security Awareness

Campaigns") suggests that running a simulation attack during an employee awareness campaign will enable the effectiveness of the campaign to be measured. This is possible when the number of security incidents reported (as a result of the simulation attack) is compared with the number of employees involved in the security awareness campaign (and targeted in the simulation attack). Therefore, the higher the number of reported incidents, the better, and this can be viewed as a simple indicator of SETA program effectiveness.

The **contextualizing** relationship (the direct impact of **CSF-DS4:** "Design for Cultural Context and Employee Cultural Diversity" on **CSF-IM1:** "Apply Diverse Methods to Deliver Security Awareness Messages") highlights that the methods to deliver the security awareness message must be customized from one culture to another. For example, providing materials in the Arabic language will make it easy and attractive for Arab country employees to follow. Therefore, understanding the cultural aspects, such as language, knowledge or level of education, to inform the choice of a suitable method is key to ensure the effectiveness of the SETA program.

The **re-emphasizing** relationship (the direct impact of **CSF-IM1:** "Apply Diverse Methods to Deliver Security Awareness Messages" on **CSF-DV1:** "Sustained Communication of Relevant Messages") highlights the need for the use of various communication channels to ensure that the relevancy of security awareness messages is delivered in a sustained way and is accessible to all employees. The ability to capture the attention of all employees, irrespective of their profile or organizational position, is key to the effectiveness of a SETA program. Therefore, avoiding the assumption that all employees consume content the "same way," using a particular means, ensures that the reach is greatest and the effectiveness of the SETA program is maximized.

The **recognizing** relationship (the direct impact of CSF-**IM2:** "Motivate Employees to Engage in Security Awareness" on **CSF-DS5:** "Adhere to Organisational Security Policy and the 'Law of the Land'") highlights the importance of motivational methods to engage employees in an IS security training program. Motivating employees by allocating rewards/ recognition for good practices around the IS security policy will further enhance the effectiveness of a SETA program.

The **scheduling** relationship (the direct impact of **CSF-DS3:** "Make a Yearly Plan to Align Goals and Objectives" on **CSF-EV1:** "Maintain Quarterly Evaluation of Employee Performance") highlights the need to tailor the plan based on the current evaluation. For example, the results of the current year evaluation aid the setup of the schedule for the forthcoming year. This will contribute to the effectiveness of a SETA program.

In the next section, we now discuss the Lifecycle Model of the CSFs for SETA program effectiveness (which positions the 11 CSFs and the 9 relationships across the 4 lifecycle phases).

5. Discussion: The Lifecycle Model of CSFs for SETA program effectiveness

As presented in Table 5, the 11 CSFs are associated with the design (6 CSFs), development (1 CSF), implementation (2 CSFs) and evaluation (2 CSFs) phases of a SETA program lifecycle. The Lifecycle Model (Figure 3) captures the relationships between the 11 CSFs (highlighting the impact of one CSF on another CSF). Where the relationships connect the CSFs *within* and *across* the phases of the SETA program lifecycle, they also highlight the association of design phase activities with evaluation phase activities, design phase activities with implementation phase activities and development phase activities with implementation phase activities.

5.1 The SETA program lifecycle phases and the lifecycle model uniqueness

In this research that naming of our SETA program lifecycle phases (*design*, *development*, *implementation* and *evaluation*) emerged from an analysis of 59 papers on SETA program

Phase	CSF	Alshaikh *et al.* (2018)	Alshaikh *et al.* (2021)	Kirova and Baumöl (2018)	Silic and Lowry (2020)
Design	**CSF-DS1:** Conduct an Initial Assessment of Employee Security Awareness	X	X		
	CSF-DS2: Know Your Audiences to Ensure Content Suitability		X	X	
	CSF-DS3: Make a Yearly Plan to Align Goals and Objectives	X	X		
	CSF-DS4: Design for Cultural Context and Employee Cultural Diversity			X	
	CSF-DS5: Adhere to Organizational Security Policy and the "Law of the Land"	X			
	CSF-DS6: Build Security Awareness Campaigns	X	X		
Development	**CSF-DV1:** Sustained Communication of Relevant Messages			X	
Implementation	**CSF-IM1:** Apply Diverse Methods to Deliver Security Awareness Messages	X	X		X
	CSF-IM2: Motivate Employees to Engage in Security Awareness	X		X	X
Evaluation	**CSF-EV1:** Maintain Quarterly Evaluation of Employee Performance	X		X	
	CSF-EV2: Measure Employee Reporting of Security Incidents	X			
	Total	*8*	*5*	*5*	*2*

Source(s): Authors' own creation/work

Table 5. Evaluating the CSFs against existing SETA program effectiveness literature

delivery. There papers covered a period from 2000 to 2021 and were returned following a search of Scopus, the AIS (Association for Information Systems) eLibrary and the Senior Scholars' Basket of eight Journals. Based on our analysis, we define the four lifecycle phases as follows:

1. **Design:** identify the target audience (employee) needs in order to plan, prioritize and benchmark activities;
2. **Development:** align organizational employee needs with the program goals, content and resources required;
3. **Implementation:** use a combination of the appropriate delivery methods to disseminate the security message;
4. **Evaluation:** establish if the goals of the SETA program are achieved.

Our analysis revealed that while each of the 59 papers reviewed focused on activities or factors linked to one or many phases of a program lifecycle, no individual paper covered all four phases of a SETA program lifecycle; therefore, 40% covered one phase, 20% covered two phases and 40% covered three phases. As an example, Puhakainen and Siponen (2010) present a method to aid the *design* phase (covering one phase); Tsohou *et al.* (2015) discusses success factors for the *design* and *implementation* phases (covering two phases), while Hansche (2001) presents factors to be considered across the *design* (e.g. identify the program goal), *implementation* (e.g. top management commitment) and *evaluation* (e.g. conduct periodic reviews) phases of the SETA program lifecycle (covering three phases).

Perhaps unsurprisingly the majority of the 59 papers (70%) are offering insights to the conversation around the *implementation* phase, 60% of the papers focused on the *design* phase conversation, with 40% of the papers focused on the *development* phase conversation. However, only 30% of the papers offered insights to the *evaluation* phase conversation. Furthermore, the most commonly occurring multi-phase patterns are the *design* + *implementation* and the *development* + *implementation* instances (40% each), with the *implementation* + *evaluation* multi-phase pattern being poorly represented (20%). Therefore, there is a strong narrative and guidance available around the *implementation* and *design* phases of a SETA program lifecycle; however, the *evaluation* phase is underexplored . This observation is not too dissimilar to that made by Alhassan *et al.* (2018) when examining the focus of attention along a Data Governance program lifecycle.

Several studies discuss various factors impacting on SETA program effectiveness (c.f. Alshaikh *et al.*, 2021; Silic and Lowry, 2020; Alshaikh *et al.*, 2018; Kirova and Baumöl, 2018). For example, Alshaikh *et al.* (2021) propose using a social marketing lens to assess the effectiveness of SETA programs. They leverage the key principles of social marketing in order to improve the effectiveness of SETA programs, through employee behavior change. Furthermore, Silic and Lowry (2020) propose implementing a gamification approach as an effective method for increasing the intrinsic motivation, skills and security policy compliance of individuals. They suggest implementing a gamification strategy with two main goals: (1) focusing on positive interventions through gamified training and (2) improving employees' security knowledge to avoid IS/cyber security threats. Finally, Alshaikh *et al.* (2018) present activities (at the level of the *organization*) across four themes that act as a guide on how to implement a SETA program. These themes include the implementation approach, employee motivation, method of delivery and outcome measurement. While Kirova and Baumöl (2018) use the Knowledge, Attitude, and Behavior (KAB) model as a framework to examine the factors that influence the effectiveness of a SETA program. They identify factors (at the level of the *individual*) that influence *knowledge*, *attitude*, *intention* and *behavior*. Therefore, comparing our findings (11 CSFs for SETA program effectiveness) with those presented in the literature, a number of observations can be made around the criticality of these CSFs for SETA program effectiveness.

As presented in Table 5, there is good support in the literature for our CSFs (our emerging categories). However, these studies discuss some, but not all, of these CSFs associated with SETA program effectiveness. Furthermore, based on our analysis, we can see limited investigation into four specific CSFs (centering around four of our emerging categories) as follows: "Culture" (**CSF-DS4**), "Policy" (**CSF-DS5**) in the *design* phase, "Communication" (**CSF-DV1**) in the *development* phase and "Periodic Assessment" (**CSF-EV1**) in the *evaluation* phase (see Appendix C for a comprehensive digest of the supporting literature for the CSFs). As a result of reflecting on the existing literature, the uniqueness of this study (the 11 CSFs for SETA program effectiveness) still holds and represents the most comprehensive coverage (in a single research study) of the factors critical to the success of a SETA program. Furthermore, the focus of each of the 11 CSFs presented in this study is "employee-centric," therefore, helping to progress the conversation around the necessity for employee behavior change. These CSFs impact on SETA program effectiveness, in a positive or negative way, depending on their presence or absence. This is an important feature of these CSFs where a lack of employee behavior change and engagement is a reported concern impacting negatively on SETA program effectiveness. It reiterates the fact that when designing a SETA program, it is important to appreciate that the purpose of the program is to assist employees to comprehend their IS/cyber security responsibilities (Hansche, 2001).

Current research suggests that effective SETA programs are often impacted by (1) *changing employee attitudes* (c.f. Posey *et al.*, 2015; Yaokumah *et al.*, 2019; Alshaikh *et al.*, 2019), (2) *increasing employee compliance* (c.f. Han *et al.*, 2017; Barlow *et al.*, 2018; Dhillon *et al.*, 2020), (3) *raising employee awareness* (c.f. Heikka, 2008; Lebek *et al.*, 2014; Tsohou *et al.*, 2015) and (4) *improving employee practices* (c.f. Chander *et al.*, 2013; Kumah *et al.*, 2019; Topa *et al.*, 2019). Therefore, leveraging our Lifecycle Model (Figure 3), we can in fact map our CSFs to these four areas of impact. For example, four CSFs (**CSF-DS2**, **CSF-DV1**, **CSF-IM2** and **CSF-EV1**) can be mapped to *changing employee attitudes*; two CSFs (**CSF-DS3** and **CSF-DS5**) can be mapped to *increasing employee compliance*; three CSFs (**CSF-DS1**, **CSF-DS6** and **CSF-IM1**) can be mapped to *raising employee awareness*; and two CSFs (**CSF-DS4** and **CSF-EV2**) can be mapped to *improving employee practices* (related to IS\cyber security risks).

Therefore, *changing employee attitudes* (**CSF-DS2**, **CSF-DV1**, **CSF-IM2** and **CSF-EV1**) demands a focus right across the four phases of the SETA program lifecycle (see Figure 3). However, *increasing employee compliance* (**CSF-DS3** and **CSF-DS5**) is linked more to a concerted effort in the design phase. Furthermore, *raising employee awareness* (**CSF-DS1**, **CSF-DS6** and **CSF-IM1**) highlights the importance of the design phase and building the right campaigns for the right employees, while also ensuring that the right approaches are then used to deliver the awareness messages to the various targeted employee cohorts (as happens in the implementation phase). Finally, *improving employee practices* (**CSF-DS4** and **CSF-EV2**) demands that consideration be given to employee culture in the design phase, but thereafter the expectation is placed on employees (in the evaluation phase) to play their part in ensuring the organizational approach to IS\cyber security works.

6. Conclusions and implications

At the present time, there is growing attention on SETA programs from both the academic and practitioner communities. The importance of a SETA program to reducing IS security risks/incidents and to increasing IS security awareness among employees is well documented. However, a review of the SETA program literature reveals that there is a lack of academic studies on SETA program effectiveness that examine all phases of the SETA program lifecycle (design, development, implementation and evaluation) (c.f. Hu *et al.*, 2021; Kirova and Baumoel, 2018; Puhakainen and Siponen, 2010). Therefore, in this study, we provide a greater insight into the dynamic of the SETA program lifecycle, specifically the CSFs, *within* and *across* the phases. As a result, this study provides a number of contributions to both research and practice (see Table 6).

Contribution to	Contribution
Research	• 11 CSFs for the SETA program lifecycle phases (visualized in a Lifecycle Model) • 9 key relationships between the CSFs (4 *within* the lifecycle phases and 5 *across* the lifecycle phases) (visualized in a Lifecycle Model)
Practice	• Leading an effective SETA program (visualized in a Lifecycle Model)

Source(s): Authors' own creation/work

Table 6. Research contributions

In this paper, we advance the first comprehensive conceptualization of the CSFs for SETA program effectiveness. This is an important first step toward the creation of a coherent body of knowledge (grounded in practice) that can support further study. We have been able to leverage the available evidence and propose a Lifecycle Model (see Figure 3) that positions each of the CSFs for SETA program effectiveness. These CSFs address a gap in the literature, and to the best of our knowledge, no other published study has examined all the four phases of the SETA program lifecycle to date. We view our Lifecycle Model of CSFs for SETA program effectiveness as a process model in that it represents a network-style display as opposed to a parsimonious list of variables. Therefore, our Lifecycle Model visualizes the "*conjunctural*" (Ragin, 1987) nature of the 11 CSFs and their multiplicative effects on the effectiveness of a SETA program. While based on our analyzed observations, such an appreciation further improves our understanding regarding the complexity of SETA program delivery within an organizational context. Therefore, we view moving beyond single factor analysis and away from the embryonic mindset of a simple CSF list as a positive development. Being able to "*chain*" CSFs for SETA program effectiveness "*over time*" provides a "*what led to what*" (c.f. Hubberman and Miles, 1994, p. 146) appreciation across the lifecycle phases (design, development, implementation and evaluation).

Following our analysis of the literature on SETA programs and SETA program effectiveness, we appreciate that our work is unique in that it presents one of the first collections of CSFs for SETA program effectiveness (mapped along a program lifecycle). It is worth acknowledging that historically such a collection of CSFs mapped along a Lifecycle Model has proved extremely useful to both academia and practice. For example, the work of Pinto and Slevin (1988) on the CSFs for project management, Nah *et al.* (2001) on the CSFs for enterprise resource planning (ERP) implementation, Tan *et al.* (2009) on the CSFs for information technology (IT) service management and, even more recently, Santisteban *et al.* (2021) on the CSFs throughout the lifecycle of IT start-ups.

Our work is similar in nature to the work of Nah *et al.* (2001) where they classify their 11 CSFs for ERP implementation, identified in the literature, against 4 phases of an ERP lifecycle (chartering, project, shakedown, onward and upward). They suggest that this process theory approach "*focuses on the sequence of events leading up to implementation completion*" (Nah *et al.*, 2001, p. 287). Therefore, irrespective of organizational size, where "*organisations do not have a full understanding of what they should be doing or how to go about it*" (Furnell *et al.*, 2002, p. 353), our CSFs and Lifecycle Model offer an opportunity to explore where the focus of attention may need to be to introduce and sustain an effective SETA program. For example, it is reported that *importance* is the most critical dimension of relevance for IS practitioners, and similar to (Rosemann and Vessey, 2008 p. 3), we view *importance* as research that "*meets the needs of practice by addressing a real-world problem in a timely manner* [currently significant], *and in such a way that it can act as the starting point for providing an eventual solution.*" Therefore, the work presented in this paper is an effort at addressing current shortfalls.

As suggested by McCarthy *et al.* (2022), it is hoped that this practical advice will help practitioners to avoid the *hidden traps* (c.f. Hammond *et al.*, 1998) in their decision making (*status quo trap*, *sunk-cost trap*, *overconfidence trap*, etc.) while promoting a "*focal awareness versus a subsidiary awareness*" with regard to designing, developing, implementing and evaluating a SETA program within an organizational context. Furthermore, the relevance of this work to practice has been enhanced by adopting the key informant approach, which has limited use to date in IS/cyber security research. This approach has provided access to 20 key informants (both knowledgeable and experienced in SETA programs) from various geographic locations. As a result, the 11 CSFs for SETA program effectiveness and the relationships between the CSFs *within* and *across* the SETA program lifecycle phases (emerging from our analysis) provide a valuable insight into the process of leading an effective SETA program in practice. It is noteworthy that having an effective SETA program is extremely important to organizations aiming to reduce IS security risks, through changing employee behavior.

6.1 Limitations and future research

When using semi-structured interviews as part of the key informant technique, it is not uncommon to have a smaller number of interviewees; this can range from 6 interviewees (c.f. Flores and Ekstedt, 2012) to 32 interviewees (c.f. Benova *et al.*, 2019). In using the key informant technique, it is more important to have appropriately qualified (quality) individuals participating in a study, over a larger quantity of individuals. Therefore, we believe that our use of 20 key informants is appropriate for this exploratory research study. However, we are also conscious that while adding to the number of key informants in this study could be very beneficial and revealing for our "*concept development*" work on the CSFs for SETA program effectiveness, it is perhaps more beneficial to move to a larger population of IS/cyber security professionals as part of a study focused on "*construct elaboration*" (Gioia *et al.*, 2012, p. 16). Therefore, we imagine that the foundations are laid in this study, through proposing the 11 CSFs along the Lifecycle Model, to further progress this line of enquiry by either qualitative, quantitative or a mixed method approach. In fact, there is an opportunity to look more closely at the differences in CSFs by, for e.g. industry sector and organization size.

This Lifecycle Model of the CSFs for SETA program effectiveness also provides a foundation for future research. The opportunity to explore would be a worthwhile advancement in understanding what is important to lead an effective SETA program in practice. Currently, it is unknown if the findings reported in this paper are directly applicable to small and medium-sized enterprises (SMEs). This links to our key informants being connected to larger organizations in their current roles, and therefore, their stories are informed by these "larger organizational" contexts. Extant research tells us that SME experiences are different to those of larger organizations when it comes to IS/cyber security (c.f. Furnell *et al.*, 2002). Indeed, significant differences in the "*attitudes*" to IS/cyber security are reported between organizations of different sizes, where smaller organizations place "*lesser value*" on IS/cyber security (Furnell *et al.*, 2002, p. 353). This pattern is further evidenced where cyber-attacks are increasing in SMEs, while decreasing in larger organizations (Chidukwani *et al.*, 2022; Bada and Nurse, 2019; Alotaibi *et al.*, 2016). Therefore, the situational difference in the operational environment of an SME versus a larger organization needs to be explored further, specifically in the context of SETA program effectiveness.

Finally, we appreciate that our 11 CSFs are not yet established as universal, so while these CSFs provide guidance to all undertaking a SETA program, organizations need to be "*mindful of the influence of their own context*" (Borman and Janssen, 2013, p. 85). Therefore, our next step in this research is to evaluate how well these CSFs translate for practitioners (seeing as their emergence came from an analysis of 20 IS/cyber security professionals "lived experiences"). This evaluation will be conducted though administering a survey questionnaire to a sample population with experience in SETA programs. This approach is similar to Nah *et al.* (2001, p. 295) where they refer to the use of a "*survey questionnaire*" to "*evaluate the degree of criticality and importance of the success factors*" and "*how the perceived importance of these factors may differ*" among various stakeholder types (executives, systems users, project team members, vendors and consultants, etc.). An appreciation of the relevance of these findings (the CSFs and the Lifecycle Model) within other organizational contexts (e.g. SMEs) is also a possibility using such a survey questionnaire. In fact, in May 2022 we conducted a preliminary evaluation of the 11 CSFs using a survey questionnaire that was completed by 65 cyber security professionals. The outcome of the evaluation showed that there was no significant difference in the CSFs between the 20 key informants and the 65 survey respondents.

References

Alhassan, I., Sammon, D. and Daly, M. (2018), "Data governance activities: a comparison between scientific and practice-oriented literature", *Journal of Enterprise Information Management*, Vol. 31 No. 2, pp. 300-316, doi: 10.1108/JEIM-01-2017-0007.

Alhassan, I., Sammon, D. and Daly, M. (2019), "Critical success factors for data governance: a theory building approach", *Information Systems Management*, Vol. 36 No. 2, pp. 98-110, doi: 10.1080/10580530.2019.1589670.

AlMindeel, R. and Martins, J.T. (2020), "Information security awareness in a developing country context: insights from the government sector in Saudi Arabia", *Information Technology and People*, Vol. 34 No. 2, pp. 770-788, available at: doi: 10.1108/ITP-06-2019-0269.

Alotaibi, F., Furnell, S., Stengel, I. and Papadaki, M. (2016), "A review of using gaming technology for cyber-security awareness", *International Journal for Information Security Research*, Vol. 6 No. 2, pp. 660-666, doi: 10.20533/ijisr.2042.4639.2016.0076.

Alshaikh, M., Maynard, S.B., Ahmad, A. and Chang, S. (2018), "An exploratory study of current information security training and awareness practices in organizations", *Proceedings of the 51st Hawaii International Conference on System Sciences*, Vol. 9, 50855094, doi: 10.24251/hicss.2018.635.

Alshaikh, M., Naseer, H., Ahmad, A. and Maynard, S.B. (2019), "Toward sustainable behaviour change: an approach for cyber security education training and awareness", Twenty-Seventh European Conference on Information Systems (ECIS2019), available at: https://aisel.aisnet.org/ecis2019_rp/100

Alshaikh, M., Maynard, S.B. and Ahmad, A. (2021), "Applying social marketing to evaluate current security education training and awareness programs in organisations", *Computers Security*, Vol. 100, 102090, doi: 10.1016/j.cose.2020.102090.

Alyami, A., Sammon, D., Neville, K. and Mahony, C. (2020), "Exploring IS security themes: a literature analysis", *Journal of Decision Systems*, Vol. 29 sup1, pp. 425-437, doi: 10.1080/12460125.2020.1848379.

Alyami, A., Sammon, D., Neville, K. and Mahony, C. (2022), "The critical success factors for security education, training and awareness (SETA) programmes", *2022 Cyber Research Conference - Ireland (Cyber-RCI)*, pp. 1-12, doi: 10.1109/Cyber-RCI55324.2022.10032674.

Bada, M. and Nurse, J.R. (2019), "Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs)", *Information and Computer Security*, Vol. 27 No. 3, pp. 393-410, doi: 10.1108/ICS-07-2018-0080.

Barker, K.K., Bosco, C. and Oandasan, I.F. (2005), "Factors in implementing interprofessional education and collaborative practice initiatives: findings from key informant interviews", *Journal of Interprofessional Care*, Vol. 19 sup1, pp. 166-176.

Barlow, J.B., Warkentin, M., Ormond, D. and Dennis, A.R. (2018), "Don't even think about it! The effects of antineutralization, informational, and normative communication on information security compliance", *Journal of the Association for Information Systems*, Vol. 19 No. 8, pp. 689-715, doi: 10.17705/1jais.00506.

Basit, T. (2003), "Manual or electronic? The role of coding in qualitative data analysis", *Educational Research*, Vol. 45 No. 2, pp. 143-154, doi: 10.1080/0013188032000133548.

Bauer, S., Bernroider, E.W.N. and Chudzikowski, K. (2017), "Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks", *Computers and Security*, Vol. 68, pp. 145-159, doi: 10.1016/j.cose.2017.04.009.

Benova, L., Moller, A.B. and Moran, A.C. (2019), "'What gets measured better gets done better': the landscape of validation of global maternal and newborn health indicators through key informant interviews", *PLoS One*, Vol. 14 No. 11, e0224746.

Bhattacherjee, A. (2012), *Social Science Research: Principles, Methods, and Practices*, 2nd ed., CreateSpace Independent Publishing Platform, Tampa, FL.

Borman, M. and Janssen, M. (2013), "Reconciling two approaches to critical success factors: the case of shared services in the public sector", *International Journal of Information Management*, Vol. 33 No. 2, pp. 390-400.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010), "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness", *MIS Quarterly*, Vol. 34 No. 3, pp. 523-548, doi: 10.2307/25750690.

Bullen, C.V. and Rockart, J.F. (1981), "A primer on critical success factors", *Sloan School of Management Working Paper*, pp. 1-64, available at: http://hdl.handle.net/1721.1/1988

Chander, M., Jain, S.K. and Shankar, R. (2013), "Modeling of information security management parameters in Indian organizations using ISM and MICMAC approach", *Journal of Modelling in Management*, Vol. 8 No. 2, pp. 171-189.

Chen, Y.A.N., Ramamurthy, K.R.A.M. and Wen, K.W. (2015), "Impacts of comprehensive information security programs on information security culture", *Journal of Computer Information Systems*, Vol. 55 No. 3, pp. 11-19, doi: 10.1080/08874417.2015.11645767.

Chidukwani, A., Zander, S. and Koutsakis, P. (2022), "A survey on the cyber security of small-to-medium businesses: challenges, research focus and recommendations", *IEEE Access*, Vol. 10, pp. 85701-85719, available at: https://ieeexplore.ieee.org/document/9853515

De Maeyer, D. (2007), "Setting up an effective information security awareness programme", *ISSE/SECURE 2007 - Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe/SECURE 2007 Conference*, Springer, pp. 49–58, doi: 10.1007/978-3-8348-9418-2_5.

Dezdar, S. and Sulaiman, A. (2009), "Successful enterprise resource planning implementation: taxonomy of critical factors", *Industrial Management and Data Systems*, Vol. 109 No. 8, pp. 1037-1052, doi: 10.1108/02635570910991.

Dhillon, G., Talib, Y.Y.A. and Picoto, W.N. (2020), "The mediating role of psychological empowerment in information security compliance intentions", *Journal of the Association for Information Systems*, Vol. 21 No. 1, pp. 152-174, doi: 10.17705/1jais.00595.

Cram, W.A., D'Arcy, J. and Proudfoot, J.G. (2019), "Seeing the forest and the trees: a meta-analysis of the antecedents to information security policy compliance", *MIS Quarterly*, Vol. 43 No. 2, pp. 525-554, doi: 10.25300/MISQ/2019/15117.

D'Arcy, J., Hovav, A. and Galletta, D. (2009), "User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach", *Information Systems Research*, Vol. 20 No. 1, pp. 79-98, doi: 10.1287/isre.1070.0160.

Flores, W.R. and Ekstedt, M. (2012), "A model for investigating organizational impact on information security behavior", *WISP 2012 Proceedings*, available at: https://aisel.aisnet.org/wisp2012/12

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, doi: 10.1108/09576050210447037.

Gioia, D.A., Corley, K.G. and Hamilton, A.L. (2012), "Seeking qualitative rigor in inductive research: notes on the Gioia methodology", *Organizational Research Methods*, Vol. 16 No. 1, pp. 15-31, doi: 10.1177/1094428112452151.

Global Market Estimates (2022), "Cybersecurity awareness training market report", *Global Market Estimates*, available at: https://www.globalmarketestimates.com/market-report/cybersecurity-awareness-training-market-3669

Hammond, J.S., Keeney, R.L. and Raiffa, H. (1998), "The hidden traps in decision making", *Harvard Business Review*, Vol. 76 No. 5, pp. 47-58.

Han, J., Kim, Y.J. and Kim, H. (2017), "An integrative model of information security policy compliance with psychological contract: examining a bilateral perspective", *Computers and Security*, Vol. 66, pp. 52-65, doi: 10.1016/j.cose.2016.12.016.

Haney, J.M. and Lutters, W.G. (2021), "Cybersecurity advocates: discovering the characteristics and skills of an emergent role", *Information and Computer Security*, Vol. 29 No. 3, pp. 485-499, doi: 10.1108/ICS-08-2020-0131.

Hansche, S. (2001), "Designing a security awareness program: part 1", *Information Systems Security*, Vol. 9 No. 6, pp. 1-9, doi: 10.1201/1086/43298.9.6.20010102/30985.4.

He, W. and Zhang, Z. (2019), "Enterprise cybersecurity training and awareness programs: recommendations for success", *Journal of Organizational Computing and Electronic Commerce*, Vol. 29 No. 4, pp. 249-257, doi: 10.1080/10919392.2019.1611528.

Heikka, J. (2008), "A constructive approach to information systems security training: an action research experience", *AMCIS 2008 Proceedings*, No. 319, available at: https://aisel.aisnet.org/amcis2008/319.

Herath, T. and Rao, H.R. (2009), "Protection motivation and deterrence: a framework for security policy compliance in organisations", *European Journal of Information Systems*, Vol. 18 No. 2, pp. 106-125, doi: 10.1057/ejis.2009.6.

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

Hovav, A. and D'Arcy, J. (2012), "Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the US and South Korea", *Information and Management*, Vol. 49 No. 2, p. 99110, available at: http://europepmc.org/abstract/med/10297607

Hu, S., Hsu, C. and Zhou, Z. (2021), "The impact of SETA event attributes on employees' security-related Intentions: an event system theory perspective", *Computers and Security* Vol. 109, 102404, doi: 10.1016/j.cose.2021.102404.

Hubberman, A.M. and Miles, M.B. (1994), *Qualitative Data Analysis*, Sage, Beverly Hills.

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

Karjalainen, M. and Siponen, M. (2011), "Toward a new meta-theory for designing information systems (IS) security training approaches", *Journal of the Association for Information Systems*, Vol. 12 No. 8, pp. 519-543, doi: 10.17705/1jais.00274.

Karjalainen, M., Siponen, M., Puhakainen, P. and Sarker, S. (2013), "One size does not fit all: different cultures require different information systems security interventions", *PACIS 2013 Proceedings*, Paper 98.

Kawulich, B.B. (2004), "Data analysis techniques in qualitative research", *Journal of Research in Education*, Vol. 14 No. 1, pp. 96-113.

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, 102267, doi: 10.1016/j.cose.2021.102267.

Kirova, D. and Baumöl, U. (2018), "Factors that affect the success of security education, training, and awareness programs: a literature review", *JITTA: Journal of Information Technology Theory and Application*, Vol. 19 No. 4, pp. 56-82.

Koh, H.C. and Tan, G. (2011), "Data mining applications in healthcare", *Journal of Healthcare Information Management*, Vol. 19 No. 2, p. 65.

Kumah, P., Yaokumah, W. and Okai, E.S.A. (2019), "A conceptual model and empirical assessment of HR security risk management", *Information and Computer Security*, Vol. 27, pp. 411-433, doi: 10.1108/ICS-05-2018-0057.

Lake, S. (2022), "Cybersecurity hiring remains red-hot-the industry to surpass $400 billion market size by 2027", Fortune, available at: https://fortune.com/education/articles/cybersecurity-hiring-remains-red-hot-the-industry-to-surpass-400-billion-market-size-by-2027/ (accessed 29 September 2022).

Lebek, B., Uffen, J., Neumann, M., Hohler, B. and Breitner, M.H. (2014), “Information security awareness and behavior: a theory-based literature review”, *Management Research Review*, Vol. 37 No. 12, pp. 1049-1092.

Leech, N.L. and Onwuegbuzie, A.J. (2008), “An array of qualitative data analysis tools: a call for data analysis triangulation”, *School Psychology Quarterly*, Vol. 23 No. 4, pp. 587-604, doi: 10.1037/1045-3830.23.4.587.

Mahmood, M.A., Siponen, M., Straub, D., Rao, H.R. and Raghu, T.S. (2010), “Moving toward black hat research in information systems security: an editorial introduction to the special issue”, *MIS Quarterly*, Vol. 34 No. 3, pp. 431-433, doi: 10.2307/25750685.

Markus, M.L. and Rowe, F. (2021), “Guest Editorial: theories of digital transformation: a progress report”, *Journal of the Association for Information Systems*, Vol. 22 No. 2, p. 11.

Marshall, M.N. (1996), “The key informant technique”, *Family Practice*, Vol. 13 No. 1, pp. 92-97, doi: 10.1093/fampra/13.1.92.

Marshall, C. and Rossman, G. (1989), *Designing Qualitative Research*, Sage Publications, Newbury Park, CA.

McCarthy, P., Sammon, D. and Alhassan, I. (2022), “‘Doing’digital transformation: theorising the practitioner voice”, *Journal of Decision Systems*, Vol. 31 sup1, pp. 341-361, doi: 10.1080/12460125.2022.2074650.

Nah, F.F.H., Lau, J.L.S. and Kuang, J. (2001), “Critical factors for successful implementation of enterprise systems”, *Business Process Management Journal*, Vol. 7 No. 3, pp. 285-296, doi: 10.1108/14637150110392782.

Okenyi, P.O. and Owens, T.J. (2007), “On the anatomy of human hacking”, *Information Systems Security*, Vol. 16 No. 6, pp. 302-314.

Olmos-Vega, F.M., Stalmeijer, R.E., Varpio, L. and Kahlke, R. (2022), “A practical guide to reflexivity in qualitative research: AMEE Guide No. 149”, *Medical Teacher*, Vol. 45 No. 3, pp. 241-251, doi: 10.1080/0142159X.2022.2057287.

Pastor, V., Díaz, G. and Castro, M. (2010), “State-of-the-art simulation systems for information security education, training, and awareness”, *2010 IEEE Education Engineering Conference*, pp. 1907-1916, EDUCON 2010, doi: 10.1109/EDUCON.2010.5492435.

Peltier, T.R. (2005), “Implementing an information security awareness program”, *Information Systems Security*, Vol. 14 No. 2, pp. 37–49, doi: 10.1201/1086/45241.14.2.20050501/88292.6, pp. 1758-1772 Publications, Newbury Park, CA.

Pham, H.C., Brennan, L., Parker, L., Phan-Le, N.T., Ulhaq, I., Nkhoma, M.Z. and Nguyen, M.N. (2019), “Enhancing cyber security behavior: an internal social marketing approach”, *Information and Computer Security*, Vol. 28 No. 2, pp. 133-159, doi: 10.1108/ICS-01-2019-0023.

Pinto, J.K. and Slevin, D.P. (1988), “Critical success factors across the project life cycle: definitions and measurement techniques”, *Project Management Journal*, Vol. 19 No. 3, pp. 67-75, available at: https://www.pmi.org/learning/library/critical-success-factors-project-life-cycle-2131#

Posey, C., Roberts, T.L. and Lowry, P.B. (2015), “The impact of organizational commitment on insiders’ motivation to protect organizational information assets”, *Journal of Management Information Systems*, Vol. 32 No. 4, pp. 179-214, doi: 10.1080/07421222.2015.1138374.

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, doi: 10.2307/25750704.

Ragin, C.C. (1987), *The Comparative Method: Moving beyond Qualitative and Quantitative Strategies*, University of California Press, Berkeley.

Rantos, K., Fysarakis, K. and Manifavas, C. (2012), “How effective is your security awareness program? An evaluation methodology”, *Information Security Journal: A Global Perspective*, Vol. 21 No. 6, pp. 328-345.

Reeves, A., Calic, D. and Delfabbro, P. (2021), "'Get a red-hot poker and open up my eyes, it's so boring' 1: employee perceptions of cybersecurity training", *Computers and Security*, Vol. 106, 102281, doi: 10.1016/j.cose.2021.102281.

Rosemann, M. and Vessey, I. (2008), "Toward improving the relevance of information systems research to practice: the role of applicability checks", *MIS Quarterly*, Vol. 32 No. 1, pp. 1-22, doi: 10.2307/25148826.

Santisteban, J., Inche, J. and Mauricio, D. (2021), "Critical success factors throughout the life cycle of information technology start-ups", *Entrepreneurship and Sustainability Issues*, Vol. 8 No. 4, pp. 446-466, doi: 10.9770/jesi.2021.8.4(27).

Silic, M. and Lowry, P.B. (2020), "Using design-science based gamification to improve organizational security training and compliance", *Journal of Management Information Systems*, Vol. 37 No. 1, pp. 129-161, doi: 10.1080/07421222.2019.1705512.

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

Siponen, M. and Vance, A. (2010), "Neutralization: new insights into the problem of employee information systems security policy violations", *MIS Quarterly*, Vol. 34 No. 3, pp. 487-502, doi: 10.2307/25750688.

Strauss, A. and Corbin, J. (1990), *Basics of Qualitative Research: Grounded Theory Procedures and Techniques*, SAGE Publications, Thousand Oaks, CA.

Talib, S., Clarke, N.L. and Furnell, S.M. (2010), "An analysis of information security awareness within home and work environments", *2010 International Conference on Availability, Reliability and Security*, pp. 196-203, IEEE.

Tan, W.G., Cater-Steel, A. and Toleman, M. (2009), "Implementing IT service management: a case study focussing on critical success factors", *Journal of Computer Information Systems*, Vol. 50 No. 2, pp. 1-12, doi: 10.1080/08874417.2009.11645379.

Topa, I. and Karyda, M. (2019), "From theory to practice: guidelines for enhancing information security management", *Information and Computer Security*, Vol. 27 No. 3, pp. 326-342, doi: 10.1108/ICS-09-2018-0108.

Tsohou, A., Karyda, M., Kokolakis, S. and Kiountouzis, E. (2012), "Analyzing trajectories of information security awareness", *Information Technology and People*, Vol. 25 No. 3, pp. 327-352, doi: 10.1108/09593841211254358.

Tsohou, A., Karyda, M., Kokolakis, S. and Kiountouzis, E. (2015), "Managing the introduction of information security awareness programmes in organisations", *European Journal of Information Systems*, Vol. 24 No. 1, pp. 38-58, doi: 10.1057/ejis.2013.27.

Vial, G. (2019), "Understanding digital transformation: a review and a research agenda", *Managing Digital Transformation*, Vol. 28 No. 2, pp. 118-144, doi: 10.1016/j.jsis.2019.01.003.

von Solms, R. and von Solms, B. (2004), "From policies to culture", *Computers and Security*, Vol. 23 No. 4, pp. 275-279, doi: 10.1016/j.cose.2004.01.013.

Vroom, C. and von Solms, R. (2002), "A practical approach to information security awareness in the organization", *Security in the Information Society*, Springer, Boston, MA, pp. 19-37, doi: 10.1007/978-0-387-35586-3_2.

Walsham, G. (2002), "Cross-cultural software production and use: a structurational analysis", *MIS Quarterly*, Vol. 26 No. 4, pp. 359-380, doi: 10.2307/4132313.

Walsham, G. (2006), "Doing interpretive research", *European Journal of Information Systems*, Vol. 15 No. 3, pp. 320-330, available at: https://link.springer.com/article/10.1057/palgrave.ejis.3000589

Weick, K.E. (1995), "What theory is not, theorizing is", *Administrative Science Quarterly*, Vol. 40 No. 3, pp. 385-390, doi: 10.2307/2393789.

Whitman, M.E. and Mattord, H.J. (2008), *Principles of Information Security*, Stamford, CT, Course Technology.

Whittaker, R. (2012), "Issues in mHealth: findings from key informant interviews", *Journal of Medical Internet Research*, Vol. 14 No. 5, e1989, doi: 10.2196/jmir.1989.

Wilson, M. and Hash, J. (2003), "Building an information technology security awareness and training program", *NIST Special Publication*, Vol. 800 No. 50, pp. 1-39.

Yaokumah, W., Walker, D.O. and Kumah, P. (2019), "SETA and security behavior: mediating role of employee relations, monitoring, and accountability", *Journal of Global Information Management (JGIM)*, Vol. 27 No. 2, pp. 102-121, doi: 10.4018/JGIM.2019040106.

Yoo, C.W., Sanders, G.L. and Cerveny, R.P. (2018), "Exploring the influence of flow and psychological ownership on security education, training, and awareness effectiveness and security compliance", *Decision Support Systems*, Vol. 108 February, pp. 107-118, doi: 10.1016/j.dss.2018.02.009.

Zani, A.A.A, Norman, A.A. and Ghani, N.A. (2018), "A Review of Security Awareness Approach: Ensuring Communal Learning", *PACIS 2018 Proceedings*, p. 278, Retrieved from https://aisel.aisnet.org/pacis2018/278

Appendix A: Interview guide

A: Introduction and welcome

(1) Acknowledge the interviewee for accepting the interview and ensure the interviewee has signed the consent form;

(2) Restate the purpose of the research study;

(3) Restate your commitment to privacy and confidentiality and provide verbal assurances that no direct quotes will be attributed to the interviewee or their organization;

(4) Provide the interviewee with the opportunity to state any concerns or request additional information for clarification purposes.

B: Demographic questions

(1) Domain:

(2) Current role:

(3) Years with current organization:

(4) Qualifications:

(5) Certifications (domain specific):

(6) Years of experience:

C: Open-ended interview questions

(1) What are the factors that are important in the *design* of a SETA program?

(2) Why are these factors important in the *design* of a SETA program?

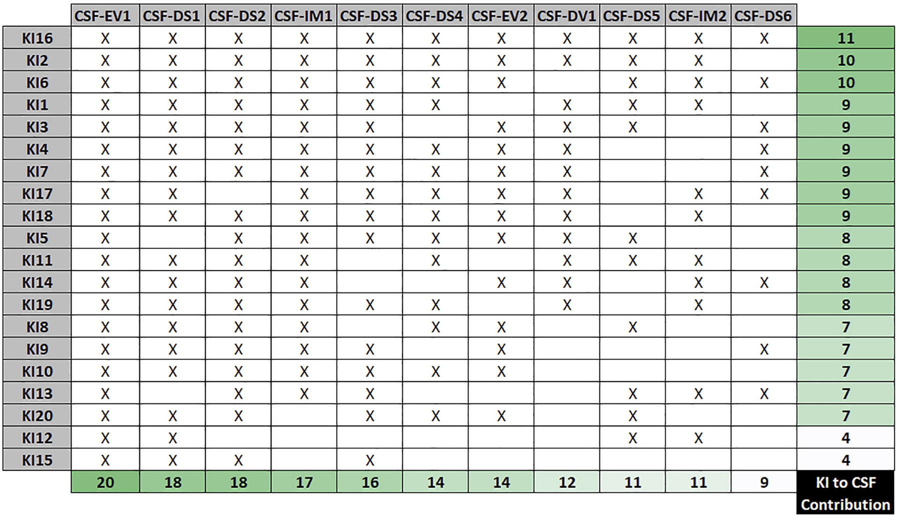
(3) How can organizations ensure that these factors exist in their *design* efforts?

(4) Who should be responsible for the *design* of a SETA program?

(5) What makes a SETA program succeed/fail?

(Questions 1–4 are also asked for the *development*, *implementation* and *evaluation phases*).

Appendix B:
Distribution of contributing key informants to CSFs



	CSF-EV1	CSF-DS1	CSF-DS2	CSF-IM1	CSF-DS3	CSF-DS4	CSF-EV2	CSF-DV1	CSF-DS5	CSF-IM2	CSF-DS6	
KI16	X	X	X	X	X	X	X	X	X	X	X	11
KI2	X	X	X	X	X	X	X	X	X	X		10
KI6	X	X	X	X	X	X	X		X	X	X	10
KI1	X	X	X	X	X	X		X	X	X		9
KI3	X	X	X	X	X		X	X	X		X	9
KI4	X	X	X	X	X	X	X	X			X	9
KI7	X	X	X	X	X	X	X	X			X	9
KI17	X	X		X	X	X	X	X		X	X	9
KI18	X	X	X	X	X	X	X	X		X		9
KI5	X		X	X	X	X	X	X	X			8
KI11	X	X	X	X		X		X	X	X		8
KI14	X	X	X	X			X	X		X	X	8
KI19	X	X	X	X	X	X		X		X		8
KI8	X	X	X	X		X	X		X			7
KI9	X	X	X	X	X		X				X	7
KI10	X	X	X	X	X	X	X					7
KI13	X		X	X	X				X	X	X	7
KI20	X	X	X		X	X	X		X			7
KI12	X	X							X	X		4
KI15	X	X	X		X							4
	20	18	18	17	16	14	14	12	11	11	9	KI to CSF Contribution

Source(s): Author’s own creation/work

Appendix C:
The supporting literature for the CSFs

CSF	Lifecycle phase	Category	Supporting literature
CSF#1 (Conduct an Initial Assessment of Employee Security Awareness)	Design	Assessment Needs	Alshaikh *et al.* (2021), Alshaikh *et al.* (2018), Puhakainen and Siponen (2010), Okenyi and Owens (2007), Peltier (2005) and Vroom and von Solms (2002)
CSF#2 (Build Security Awareness Campaigns)		Communication	Alshaikh *et al.* (2021), Alshaikh *et al.* (2018), Hearth *et al.* (2018), Rantos *et al.* (2012), Puhakainen and Siponen (2010), D'arcy *et al.* 2009 and Vroom and von Solms (2002)
CSF#3 (Design for Cultural Context and Employee Cultural Diversity)		Culture	Kirova and Baumöl (2018), Karjalainen *et al.* (2013), Hovav and D'Arcy (2012), von Solms and von Solms (2004) and Walsham (2002)
CSF#4 (Make a Yearly Plan to Align Goals and Objectives)		Goal/Objective	Alshaikh *et al.* (2021), Alshaikh *et al.* (2018), Rantos and Manifavas (2012), Peltier (2005) and Hansche (2001)
CSF#5 (Adhere to Organizational Security Policy and the "Law of the Land")		Policy	Kirova and Baumöl (2018), D'arcy *et al.* (2009) and Peltier (2005)
CSF#6 (Know Your Audiences to Ensure Content Suitability)		Target Audiences	Alshaikh *et al.* (2021), Kirova and Baumöl *et al.* (2018), De Maeyer (2007), Peltier (2005) and Siponen (2000)
CSF#7 (Sustained Communication of Relevant Messages)	Development	Communication	Barlow *et al.* (2018), Kirova and Baumöl (2018)
CSF#8 (Apply Diverse Methods to Deliver Security Awareness Messages)	Implementation	Communication Channel	Alshaikh *et al.* (2021), Silic and Lowry (2020), Alshaikh *et al.* (2018), Bauer *et al.* (2017), Tsohou *et al.* (2015), Johnson (2006) and Peltier (2005)
CSF#9 (Motivate Employees to Engage in Security Awareness)		Motivation	Silic and Lowry (2020), Alshaikh *et al.* (2018), Kirova and Baumöl (2018), Zani *et al.* (2018), Karjalainen *et al.* (2013), Puhakainen and Siponen (2010) and Herath and Rao (2009)
CSF#10 (Maintain Quarterly Evaluation of Employee Performance)	Evaluation	Periodic Assessment	Alshaikh *et al.* (2018), Kirova and Baumöl (2018), Rantos *et al.* (2012) and Johnson (2006)
CSF#11 (Measure Employee Reporting of Security Incidents)		Incident Indication	Alshaikh *et al.* (2018), Chen *et al.* (2015), D'arcy *et al.*, (2009) and Peltier (2005)

Source(s): Author's own creation/work

Table C1. The supporting literature for the CSFs

Corresponding author
Areej Alyami can be contacted at: a.alyami1988@gmail.com