The current issue and full text archive of this journal is available on Emerald Insight at:
https://www.emerald.com/insight/2056-4961.htm

Received 6 August 2022
Revised 3 October 2022
28 February 2023
29 March 2023
Accepted 1 April 2023

Critical success factors for Security Education, Training and Awareness (SETA) programme effectiveness: an empirical comparison of practitioner perspectives

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

Abstract

Purpose – Cyber security has never been more important than it is today in an ever more connected and pervasive digital world. However, frequently reported shortages of suitably skilled and trained information system (IS)/cyber security professionals elevate the importance of delivering effective Security Education,Training and Awareness (SETA) programmes within organisations. Therefore, the purpose of this study is the questionable effectiveness of SETA programmes at changing employee behaviour and an absence of empirical studies on the critical success factors (CSFs) for SETA programme effectiveness.

Design/methodology/approach – This exploratory study follows a three-stage research design to give voice to practitioners with SETA programme expertise. Data is gathered in Stage 1 using semi-structured interviews with 20 key informants (the emergence of the CSFs), in Stage 2 from 65 respondents to a short online survey (the ranking of the CSFs) and in Stage 3 using semi-structured interviews with nine IS/cyber security practitioners (the emergence of the guiding principles). Using a multi-stage research design allows the authors to propose and evaluate the 11 CSFs for SETA programme effectiveness.

Findings – This study conducted a mean score analysis to evaluate the level of importance of each CSF within two independent groups of IS/cyber security professionals. This multi-stage analysis produces a ranked list of 11 CSFs for SETA programme effectiveness, while the difference in the rankings leads to the emergence of five CSF-specific guiding principles (to increase the likelihood of delivering an effective SETA programme within an organisational context). This analysis also reveals that most of the contradictions/differences in CSF rankings between IS/cyber security practitioners are linked to the design phase of the SETA programme life cycle. While two CSFs, "maintain quarterly evaluation of employee performance" (CSF-DS6) and "build security awareness campaigns" (CSF-EV1), represent the most significant contradiction in this study.

Originality/value – The 11 CSFs for SETA programme effectiveness, along with the five CSF-specific guiding principles, provide a greater depth of knowledge contributing to both theory and practice and lays the

DOI 10.1108/ICS-08-2022-0133

foundation for future studies. Therefore, the outputs of this study provide valuable insights on the areas that practice needs to get right to deliver effective SETA programmes.

Keywords SETA programme, Effectiveness, Security, Cyber, CSFs, Training, Critical success factors, Information security, Education

Paper type Research paper

1. Introduction

Cybersecurity and securing information system (IS) assets have 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 $400bn by 2027 (fortune.com, 2022). Organisations cannot afford the disruption brought by digital attacks and are constantly seeking to protect their critical systems and sensitive data. To mitigate against major cybersecurity incidents, organisations are constantly looking for ways to ensure that their internal (e.g. employee) and external (e.g. supplier) stakeholders are aware of potential IS/cyber security threats and have the "know how" to respond. However, it is argued that "cybercrime actors" are reinventing themselves (developing new capability) at a far quicker pace than organisations are investing in cybersecurity capabilities (fortune.com, 2022). Hence, there is a need for "remarkable changes in how companies prioritise and address their cyber risks" (fortune.com, 2022).

Extant research suggests that organisations use various strategies to safeguard their information assets against IS/cyber security threats, and the Security Education, Training and Awareness (SETA) programme is one of the most prominent strategies used for controlling IS/cyber security threats and protecting information assets (Alshaikh *et al.*, 2018; Kirova and Baumoel, 2018; Tsohou *et al.*, 2015; D'Arcy *et al.*, 2009). In fact, according to Global Market Estimates (2022), the market for IS/cyber security awareness training is anticipated to increase to a value of $12.1bn by 2027, representing a compound annual growth rate of 45.6% from 2022 to 2027. However, SETA programmes often produce questionable results around effectiveness and fail to build an acceptable level of awareness and know-how among employees. In fact, employees having a greater appreciation of "what to do when" is a key outcome for SETA programme effectiveness. Furthermore, frequently reported shortages of suitably skilled and trained IS/cyber security professionals further elevate the importance of delivering effective SETA programmes within organisations.

A SETA programme is viewed as an educational process designed to reduce the number of accidental security breaches that occur due to a lack of individuals' awareness of IS security (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 programmes is widely accepted by academics and practitioners (Alshaikh *et al.*, 2018; Tsohou *et al.*, 2015; D'Arcy *et al.*, 2009; Wilson and Hash, 2003). However, despite the prominence of SETA programmes for organisational IS security, "only a small portion of practitioners" claim that their SETA programmes are "very effective" (Hu *et al.*, 2021, p. 1). It is reported that poor SETA programme effectiveness is linked to the programme's failure to positively impact employee security-related behaviours (Alshaikh *et al.*, 2021; Hu *et al.*, 2021; Alshaikh *et al.*, 2019). Therefore, the key motivation for this study is the questionable effectiveness of SETA programmes at changing employee behaviour and an absence of empirical studies on the critical success factors (CSFs) for SETA programme effectiveness. However, more than focusing on a specific research question, this paper presents the evolution of 11 CSFs for SETA programme effectiveness. Through the execution of a multi-stage research design, we theorise from the SETA programme stories of

IS/cyber security professionals to produce the ranked list of CSFs. Furthermore, given the perceived difference in importance for some of the CSFs, we also present five CSF-specific guiding principles to further clarify the importance of these specific CSFs to achieving SETA programme effectiveness.

The remainder of this paper is organised as follows: Section 2 presents a background to SETA programme effectiveness and CSFs. Section 3 describes the three-stage research approach. Section 4 presents the findings and discussion, organised around the five CSF-specific guiding principles, proposed to increase the likelihood of delivering an effective SETA programme within an organisational context. Section 5 presents the conclusions and implications of the research. Lastly, Section 6 proposes some recommendations for future research.

2. Security Education, Training and Awareness programme effectiveness and critical success factors – why?

The importance of a SETA programme to protect information assets in an organisation has led many researchers to recommend establishing a SETA programme and making it part of any organisation's overall security strategy (D'Arcy *et al.*, 2009; Kirova and Baumoel, 2018). SETA programmes include the following functions:

- provide employees with knowledge regarding organisational information threats and IS security (D'Arcy *et al.*, 2009; Yoo *et al.*, 2018; Dhillon *et al.*, 2020);
- clarify existing technical and procedural countermeasures available to employees (Pastor *et al.*, 2010; Silic and Lowry, 2020);
- determine the possible sanctions for security policy violations in the organisation (Siponen and Vance, 2010; Karjalainen *et al.*, 2013; Herath *et al.*, 2018); and
- improve employees' awareness of their roles and responsibilities in protecting the organisation's information assets (D'Arcy *et al.*, 2009; Lebek *et al.*, 2014).

Where empirical studies investigating the effectiveness of SETA programmes exist, they fail to examine all phases of the SETA programme life cycle (design, development, implementation, evaluation), tending to focus more on one or two of the life cycle 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 organisations to support the introduction of SETA programmes, 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). 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 programmes are "suboptimal" as they "aim to improve employee knowledge acquisition rather than behavior and belief". Therefore, more theorising and conceptual clarity is needed in investigating the effectiveness of SETA programmes (c.f. Alshaikh *et al.*, 2021; Hu *et al.*, 2021; Kirova and Baumoel, 2018; Puhakainen and Siponen, 2010). In particular, guidance in the form of CSFs is seen as particularly useful by helping organisations understand where to focus their efforts (c.f. *reference withheld for review purposes*). In fact, CSFs have been widely investigated and used in IS research and practice over the past three decades to make sense of problems by identifying the factors that could influence business activities and outcomes (c.f. Alhassan *et al.*, 2019). Throughout this period, researchers have identified CSFs, which need more attention from managers, in areas ranging from "project-type" operational initiatives to more "mindset shift" strategic initiatives (c.f. Alhassan *et al.*, 2019).

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). Numerous studies within IS have used the CSFs lens to establish those key areas that demand favourable results to ensure a successful performance (c.f. Rockart, 1979). Several studies have also evaluated the level of importance of CSFs for various phenomena, for example, the implementation of enterprise resource planning (ERP) systems (c.f. Reitsma and Hilletofth, 2018; Ahmad and Cuenca, 2013), the introduction of public-private partnerships (Osei-Kyei and Chan, 2017; Soomro *et al.*, 2016) and delivering shared services (Borman and Janssen, 2013). Within these studies, the research is conducted across multiple stages and uses various techniques to show the similarities and differences in the importance of the CSFs.

To date, little or no research has documented the CSFs for SETA programme effectiveness, especially because the effectiveness of SETA programmes is routinely called into question. In fact, research shows that "failure rates" for the introduction of IS initiatives still remain high. The rate of failure suggests the need to focus the attention of IS professionals and academics on addressing and developing a list of factors that will enable the successful delivery of IS initiatives (c.f. Alhassan *et al.*, 2019). Therefore, we argue that understanding the CSFs for SETA programme effectiveness will lend itself to increasing the effectiveness of a SETA programme within an organisation.

In the next section, we present further details on the research approach.

3. Research approach

To fulfil the research objective, we adopt an exploratory research approach (following a three-stage research design). We use this exploratory approach to give "extraordinary voice to informants, who are treated as knowledgeable agents" (Gioia *et al.*, 2012, p. 18) to investigate a little-understood phenomenon (Marshall and Rossman, 1989). In the context of this research project, this translates as IS/cyber security professionals with SETA programme expertise. 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), we aim to conceptualise the practitioner voice and not "substitute practitioners' understandings for theory" (Markus and Rowe, 2021, p. 273). Therefore, we embrace the Gioia Methodology because it encourages originality in our theorising, where what we already know does not limit "what we can know" (Gioia *et al.*, 2012, p. 16).

In Stage 1, we use an inductive open coding approach to produce 11 CSFs from our analysis of 20 key informant interviews. These CSFs are ranked in a prioritised order (descending) based on the frequency count of coded excerpts across the 20 interview transcripts. 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). In Stage 2, we use mean score ranking to generate a ranked list of the 11 CSFs based on our analysis of 65 responses to a short survey. The answer to each survey question involved ranking the importance of a specific CSF (high/medium/low). In Stage 2, we also compare this ranked list to the ranked list generated in Stage 1. This comparison highlights the position of each CSF in the respective lists and suggests the similarities and differences between the lists. We also use the Mann–Whitney U test to check if there is a difference in the rank sum between the two ranked lists of 11 CSFs (Stage 1 list from 20 key informants and Stage 2 list from 65 survey respondents). The Mann–Whitney U test is a non-parametric test used to study the association of ordinal (rank order) data from two independent groups where the data sets are not assumed to follow any normal distribution pattern (Osei-Kyei and Chan, 2017; Hair *et al.*, 2007). In Stage 3, we present our hermeneutics-inspired analysis of nine follow-up probing interviews with IS/cyber security practitioners involved in Stage 1 (4) and Stage 2 (5) of this research study. All of these practitioners have expertise in organisational SETA programmes. Therefore, our hermeneutics-inspired analysis affords us the opportunity to "understand what people say and do, and why" (Myers, 2009, p. 182). This analysis adds further insights in the five key areas of difference that emerged from our comparative analysis of the ranked lists of 11 CSFs in Stage 2. Thereafter, these differences inform five CSF-specific guiding principles to increase the likelihood of delivering an effective SETA programme within an organisational context.

3.1 Stage 1: 20 key informants (the emergence of the critical success factors)

Stage 1 of this exploratory research follows a systematic inductive approach to concept development. We adopt the "key informant" approach for data gathering and engage with key informants through semi-structured interviews. The main advantage of using the key informant approach is gaining rich data in a short period of time through in-depth interviews. 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 six interviewees (c.f Flores and Ekstedt, 2012) to 32 interviewees (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 stage of the exploratory research study. Therefore, key informants were selected based on their position, experience and professional knowledge about IS/cyber security, particularly SETA programmes. Twenty individual semi-structured interviews were conducted with selected key informants from various geographic locations, including the Gulf nations (Saudi Arabia, United Arab Emirates, Qatar and Kuwait), the Middle East (Egypt and Lebanon), the USA, the UK and Ireland. All of 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 programmes throughout the life cycle phases (design, development, implementation, evaluation) were discussed. The following questions were asked to explore the CSFs for SETA programme effectiveness across these life cycle phases. Questions 1–4 are also asked for the *development*, *implementation* and *evaluation phases*:

Q1. What are the factors that are important in the ***design*** of a SETA programme?

Q2. Why are these factors important in the ***design*** of a SETA programme?

Q3. How can organisations ensure that these factors exist in their ***design*** efforts?

Q4. Who should be responsible for the ***design*** of a SETA programme?

Q5. What makes a SETA programme succeed/fail?

All the interviews were transcribed line-by-line and checked against the voice recordings, where necessary, to ensure the accuracy of the transcription of the interviews. This research adopted an inductive open coding approach as part of our qualitative data analysis (Corbin and Strauss, 1990). When all 20 key informant interviews were transcribed, the data analysis commenced using sentence-by-sentence coding to identify relevant codes. 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 programme. These 212 coded concepts led to the emergence of 15 categories mapped across the four SETA programme life cycle phases (design, development, implementation and evaluation). Specifically, the code/category distribution is as follows:

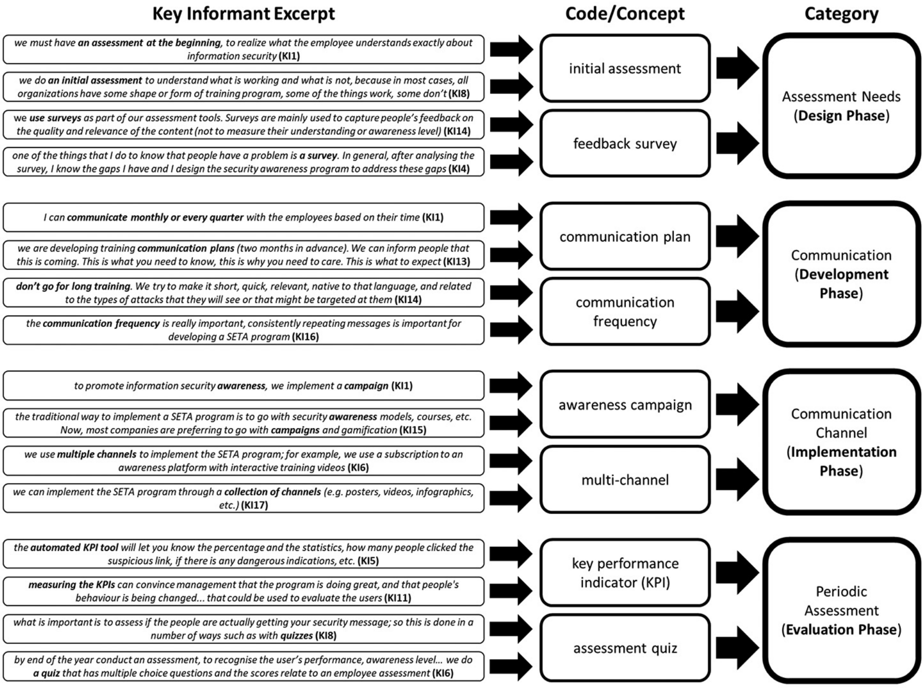
- *design* phase – 95 codes – 8 categories;
- *development* phase – 27 codes – 4 categories;
- *implementation* phase – 50 codes – 5 categories; and
- *evaluation* phase – 40 codes – 3 categories.

The category with the highest coding frequency across each of the SETA programme life cycle phases is as follows:

- *design* phase – 18 coded concepts in the "Assessment Needs" category;
- *development* phase – 12 coded concepts in the "Communication" category;
- *implementation* phase – 17 coded concepts in the "Communication Channel" category; and
- *evaluation* phase – 20 coded concepts in the "Periodic Assessment" category.

See Figure 1 for a sample of our inductive open coding. Thereafter, unpacking the categories with at least five key informant voices (25% coverage) led to the emergence of the 11 CSFs for SETA programme effectiveness.

Table 1 presents these 11 CSFs organised by SETA programme life cycle phase. See *reference withheld for review purposes* for a more detailed discussion on these 11 CSFs.



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)**

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)**

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)**

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)**

Source: Author's own creation/work

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

Table 1. 11 CSFs for SETA programme effectiveness (presented by life cycle phase)

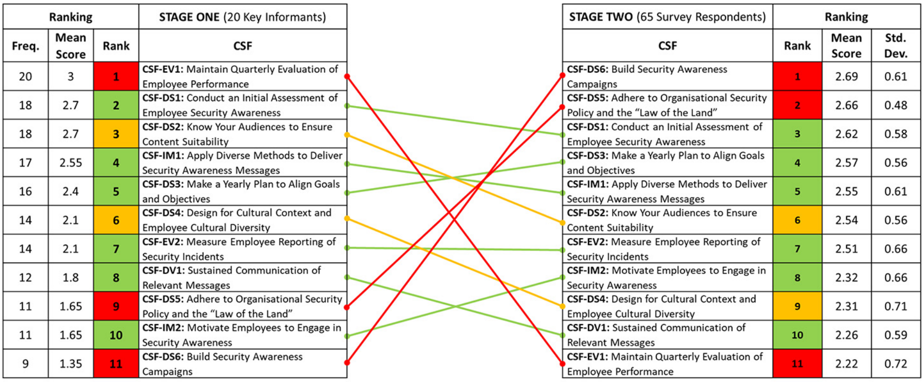
Life cycle phase	CSF	Category	Description
Design	*CSF-DS1*: Conduct an Initial Assessment of Employee Security Awareness	Assessment needs	Determining what the employee understands about the organisation's security policy and their appreciation of the risks associated with current IS/cyber security threats
	CSF-DS2: Know Your Audiences to Ensure Content Suitability	Target audiences	Identifying "who your audiences are" to ensure appropriate content is delivered to the various employee types
	CSF-DS3: Make a Yearly Plan to Align Goals and Objectives	Goal/Objective	Knowing what is required to be delivered to the employee to ensure that the SETA programme goals meet the specific needs of the organisation
	CSF-DS4: Design for Cultural Context and Employee Cultural Diversity	Culture	Understanding the diversity of employee backgrounds (e.g. language, culture, knowledge, level of education, age, gender) so that the IS/cyber security message can be interpreted by all employees
	CSF-DS5: Adhere to Organisational Security Policy and the "Law of the Land"	Policy	Focusing on the guidelines and procedures needed to protect the IS assets of the organisation, to ensure that all of the organisational IS/cyber security policies and the "law of the land" are adhered to when designing a SETA programme
	CSF-DS6: Build Security Awareness Campaigns	Communication	Updating the employee on how to mitigate against the potential risks associated with an IS/cyber security threat, and keeping them informed on what is coming, and most crucially, why they need to care
Development	*CSF-DV1*: Sustained Communication of Relevant Messages	Communication	Repeating the IS/cyber security message in various ways to avoid a lapse in employee concentration
Implementation	*CSF-IM1*: Apply Diverse Methods to Deliver Security Awareness Messages	Communication channel	Using various approaches to deliver IS/cyber security awareness messaging (e.g. SMS, emails, online courses, face-to-face meetings, videos, quizzes, posters, screens in public corridors, etc.) so that the employee is reminded frequently of the IS/cyber security issue
	CSF-IM2: Motivate Employees to Engage in Security Awareness	Motivation	Encouraging the employee to adhere to IS/cyber security policies by earning a bonus, or other recognition (rewards), based on their practices
Evaluation	*CSF-EV1*: Maintain Quarterly Evaluation of Employee Performance	Periodic assessment	Providing a year-end evaluation summary to measure each employee's performance (e.g. level of awareness, number of training sessions completed, etc.) and to provide guidance on necessary improvements
	CSF-EV2: Measure Employee Reporting of Security Incidents	Incident indication	Using phishing campaigns to simulate attacks (knowing how many employees click the suspicious links) to measure the employee awareness and knowledge regarding IS/cyber security issues

Source: Authors' own creation/work

Furthermore, Figure 2 (the left-hand side of the visual) presents these CSFs in a ranked prioritised order (descending) based on the frequency count of coded excerpts across the 20 interview transcripts. The mean score is also presented for each CSF based on the following formula ([coded concepts* numerical value of a CSF importance of "high"]/total number of key informants). For example, the mean score of CSF-DV1 (ranked eighth in Figure 2) is 1.8, calculated as ([12*3]/20). Therefore, having generated a ranked order list of CSFs for SETA programme effectiveness (in Stage 1), we now needed to evaluate if this ranked order list is appropriate for others in the IS/cyber security practitioner community. This evaluation is presented in the next section.

3.2 Stage 2: 65 survey respondents (the ranking of the critical success factors)

In Stage 2 of this exploratory research study, we adopted a *Request-For-Comment* (RFC) approach (c.f. Chen *et al.*, 2013) to evaluate the ranked importance of the 11 CSFs. Online surveys are an effective way "to elicit feedback from a wide range of participants in a scalable way" (Lo *et al.*, 2015, p. 416). Surveying practitioners (using short simply surveys) to determine (i) their confidence in academic outputs or (ii) their perception of research relevance is a common practice (c.f. Kitchenham and Pfleeger, 2008). However, it is important to design these surveys such that participants require "as little effort as possible to complete it" (Lo *et al.*, 2015, p. 416). To achieve this, we designed a short 11-question survey (one question per CSF using an ordinal scale of high/medium/low) to gather practitioner perspectives on the ranked importance of each of the CSFs for SETA programme effectiveness (see Appendix 1 for a sample of the survey questions). Therefore, we limited our response type to numerical (ordinal scale) but subjective data, capturing the respondent's preferences (Kitchenham and Pfleeger, 2008, p. 67). Therefore, we viewed the short survey as a data gathering instrument that would provide numerical descriptions of the importance of each CSF (based on the perception of the sample population). Overall, our approach is similar in style to that taken by Nah *et al.* (2001, p. 295) where they refer to the use of a "survey questionnaire" to evaluate the importance of their 11 CSFs for ERP implementation and "how the perceived importance of these factors may differ" among respondents. In our survey, a respondent was required to answer all 11 questions to submit a valid survey response. This RFC approach ensured that each respondent evaluated each one of the 11 CSFs. The facility also existed for respondents to provide additional



Ranking			STAGE ONE (20 Key Informants)
Freq.	Mean Score	Rank	CSF
20	3	1	CSF-EV1: Maintain Quarterly Evaluation of Employee Performance
18	2.7	2	CSF-DS1: Conduct an Initial Assessment of Employee Security Awareness
18	2.7	3	CSF-DS2: Know Your Audiences to Ensure Content Suitability
17	2.55	4	CSF-IM1: Apply Diverse Methods to Deliver Security Awareness Messages
16	2.4	5	CSF-DS3: Make a Yearly Plan to Align Goals and Objectives
14	2.1	6	CSF-DS4: Design for Cultural Context and Employee Cultural Diversity
14	2.1	7	CSF-EV2: Measure Employee Reporting of Security Incidents
12	1.8	8	CSF-DV1: Sustained Communication of Relevant Messages
11	1.65	9	CSF-DS5: Adhere to Organisational Security Policy and the "Law of the Land"
11	1.65	10	CSF-IM2: Motivate Employees to Engage in Security Awareness
9	1.35	11	CSF-DS6: Build Security Awareness Campaigns

STAGE TWO (65 Survey Respondents)	Ranking		
CSF	Rank	Mean Score	Std. Dev.
CSF-DS6: Build Security Awareness Campaigns	1	2.69	0.61
CSF-DS5: Adhere to Organisational Security Policy and the "Law of the Land"	2	2.66	0.48
CSF-DS1: Conduct an Initial Assessment of Employee Security Awareness	3	2.62	0.58
CSF-DS3: Make a Yearly Plan to Align Goals and Objectives	4	2.57	0.56
CSF-IM1: Apply Diverse Methods to Deliver Security Awareness Messages	5	2.55	0.61
CSF-DS2: Know Your Audiences to Ensure Content Suitability	6	2.54	0.56
CSF-EV2: Measure Employee Reporting of Security Incidents	7	2.51	0.66
CSF-IM2: Motivate Employees to Engage in Security Awareness	8	2.32	0.66
CSF-DS4: Design for Cultural Context and Employee Cultural Diversity	9	2.31	0.71
CSF-DV1: Sustained Communication of Relevant Messages	10	2.26	0.59
CSF-EV1: Maintain Quarterly Evaluation of Employee Performance	11	2.22	0.72

Figure 2. CSF ranked list comparison (Stage 1 and Stage 2)

Source: Author's own creation/work

comments following completion of the survey. These comments were also factored into the follow-up probing interviews conducted in Stage 3.

The survey was designed on Google Forms and was distributed electronically to practitioners in the IS/cyber security professional community (SETA programme specialists). These practitioners were initially invited by email, and if they agreed to participate were then sent the link to the survey. For example, we invited participants from the Cyber Research Conference Ireland 2022, along with members of several cyber security groups, including Women in Cyber Security Middle East, Hemaya Cyber Ladies and Information Security Association – Hemaya. Some of the cyber security group members also shared the invite with professionals within their networks. None of the 20 key informants from Stage 1 was invited to participate in Stage 2.

The survey went live on 5 May 2022 and remained open for five days (until 9 May). A total of 65 responses were gathered during this time (25 responses on Day 1, 26 on Day 2, 7 on Day 3, 5 on Day 4 and 2 on Day 5), with responses coming mainly from Ireland, the UK and the Middle East. Once the survey was closed, the data were downloaded to MS Excel. A data analysis table was generated containing the min/max, the mean, median and standard deviation for all 11 CSFs. Figure 2 (the right-hand side of the visual) presents these CSFs in a ranked, prioritised order (descending) based on the mean score of each CSF. Figure 2 is inspired by similar comparative type visual displays used in other studies [e.g. Table 3 from Wong (1998) and Figure 4 from Ahmad and Cuenca (2013)].

In this stage, we also compare both ranked lists of the 11 CSFs emerging from the two independent groups (Stage 1 list from 20 key informants and Stage 2 list from 65 survey respondents). Figure 2 presents a visual of this comparison (similarities and differences) and highlights the position of each CSF in the respective lists. We also use the Mann–Whitney *U* test to check if there is a difference in the rank sum between the two ranked lists. In this research, the statistical test was performed by hand, following the steps outlined in the following video (www.youtube.com/watch?v=BT1FKd1Qzjw). The workings of the *Ustat* for Stage 1 (n^1) and Stage 2 (n^2) are available in Appendix 2. We use the mean value for each of the 11 CSFs across both groups, rank each of the CSFs and calculate the rank sum for Stage 1 (109.5 with a $Ustat = 43.5$) and Stage 2 (143.5 with a $Ustat = 77.5$). The null hypothesis is stated as follows: *in the population, the rank sum (sum of the rankings) in the two groups does not differ*, whereas the alternative hypothesis suggests that the sum of the rankings does differ. The critical values of the Mann–Whitney *U* (two-tailed testing) are available at this links (https://ocw.umb.edu/psychology/psych-270/other-materials/RelativeResourceManager.pdf). The value of the *Ucrit* at $\alpha = 0.05$ (95% confidence interval) is 30 (where n^1 and n^2 are both 11). Based on our calculations, the null hypothesis was accepted ($Ustat > Ucrit$), suggesting that there is no significant difference in the CSFs between the two groups (Stage 1: 20 key informants and Stage 2: 65 survey respondents). For example, in our analysis, $Ucrit = 30$ and the lowest $Ustat = 43.5$.

However, as seen in Figure 2, there is a somewhat contradictory element to the CSF rankings between Stage 1 and Stage 2. For example, CSF-EV1 is the 1st ranked CSF from Stage 1 but is the 11th ranked CSF from Stage 2. Furthermore, the inverse is also true, where CSF-DS6 is the 11th ranked CSF from Stage 1 but is the 1st ranked CSF from Stage 2. In total, five critical areas of difference emerge from our comparative analysis of the ranked lists of 11 CSFs. In Figure 2, the three red lines represent a significant difference in the ranking (between both practitioner groups) of three specific CSFs (*CSF-EV1*, *CSF-DS5* and *CSF-DS6*). The two orange lines represent a modest, but of interest, difference in two specific CSFs (*CSF-DS2* and *CSF-DS4*). Finally, the six green lines represent insignificant differences in the ranking (between both practitioner groups) of six specific CSFs (*CSF-DS1*, *CSF-IM1*, *CSF-DS3*, *CSF-EV2*, *CSF-DV1* and *CSF-IM2*). Therefore, we progress our understanding of the differences (captured by the red and orange lines) in the next section.

3.3 Stage 3: 9 follow-up probing interviews (the emergence of the guiding principles)

In Stage 3 of this exploratory research study, we use a hermeneutics-inspired approach to analyse and interpret the answers provided by nine IS/cyber security practitioners (four from Stage 1 and five from Stage 2) to the questions emerging from the differences in the ranking of the CSFs between Stage 1 (20 key informants) and Stage 2 (65 survey respondents) (see Figure 2). In this stage, we are trying to make sense of the "seemingly contradictory" (Myers, 2009, p. 170) text that has emerged around five specific CSFs (difference in their ranked importance). Furthermore, we take these differences as a sign of "confused, incomplete, cloudy, and contradictory views" (Myers, 2009, p. 171) among the IS/cyber security community (specifically those with expertise in SETA programmes). Therefore, our interpretative work aims to bring to light an underlying sense of clarity, and the following questions were asked to qualify the importance of the five specific CSFs:

(1) Is building a security awareness campaign important (*CSF-DS6*)? Why?

(2) Is maintaining a quarterly evaluation of employee performance important (*CSF-EV1*)? Why?

(3) How can adherence to policy (organisational and legislative) be improved (*CSF-DS5*)?

(4) Is tailored content for employees important (*CSF-DS2*)? Why?

(5) Is the cultural context and the employee background important (*CSF-DS4*)? Why?

Ultimately in this stage, we discovered reasons for the importance of *CSF-DS6*, *CSF-EV1*, *CSF-DS5*, *CSF-DS2* and *CSF-DS4*. Four of these contradictions (CSF-DS2, CSF-DS4, CSF-DS5, CSF-DS6) are linked to the design phase of the SETA programme life cycle, while one contradiction (CSF-EV1) highlights the challenging nature of SETA programme evaluation. Therefore, these contradictions afford us the opportunity to present five guiding principles (four in design and one in evaluation) to complement the ranked list of 11 CSFs for SETA programme effectiveness within an organisational context (see Table 2). These guiding principles are ordered by the degree of difference (contradiction) between the Stage 1 and Stage 2 rankings (see Figure 2).

In the next section, we present a discussion of our research findings (the five CSF-specific guiding principles emerging from Stage 3).

4. Discussion of findings

The outcome of this research suggests that there is no significant difference between the 20 key informants (Stage 1) and 65 survey respondents (Stage 2) in terms of their perception of the ranked importance of the 11 CSFs for SETA programme effectiveness. However, this research also highlights that there are five specific CSFs for SETA programme effectiveness that need to be examined, given the differences that emerged from our comparative analysis. These five guiding principles are now discussed to further improve the likelihood of delivering an effective SETA programme. We also reflect these findings against existing literature.

4.1 Principle 1: raise employee IS/cyber security awareness and knowledge to enhance organisational maturity

CSF-DS6: Build Security Awar*eness Campaigns* focuses on updating the employee on how to mitigate against the potential risks associated with an IS/cyber security threat, keeping them

CSF	Ranking (Stage) One	Two	Guiding principle
CSF-DS6: Build Security Awareness Campaigns	11	1	Raise employee IS/cyber security awareness and knowledge to enhance organisational maturity
CSF-EV1: Maintain Quarterly Evaluation of Employee Performance	1	11	Evaluate employee performance at a frequency that aligns with the organisational IS/cyber security strategy
CSF-DS5: Adhere to Organisational Security Policy and the "Law of the Land"	9	2	Secure top management support to encourage all employees to comply with IS/cyber security policy
CSF-DS2: Know Your Audiences to Ensure Content Suitability	3	6	Avoid a one size fits all approach to programme content to promote employee engagement
CSF-DS4: Design for Cultural Context and Employee Cultural Diversity	6	9	Appreciate employee cultural differences to shape programme content

Source: Authors' own creation/work

Table 2. Guiding principles for five CSFs with difference/ contradiction

informed on what is coming, and, most crucially, why they need to care. Figure 2 visualises the contradictory rankings between Stage 1 and Stage 2 for this CSF. We believe that this difference exists because the perspectives of the experts (involved in delivering SETA programmes) differ regarding where to position awareness building along the SETA programme lifecycle. For example, in the early stage of the design phase of the SETA programme (to clarify all security issues for their employees to achieve the SETA programme goals) or in the final stage of the evaluation phase (to assess employee knowledge of IS security and to determine whether or not the programme is effective at changing employee behaviour).

Based on our review of the story of the importance of this CSF (*CSF-DS6*), the IS/cyber security practitioners highlighted that security awareness campaigns simply keep employees updated about what is going on (e.g. new cyberattack methods) and how to protect themselves and the organisation. For example, one practitioner states, "[. . .] as technology develops, fraud and security incidents are constantly updated, and new attack techniques are developed". The campaign also aims to enhance organisational IS/cyber security maturity, and this is especially challenging where employees have varying levels of IS/cyber security knowledge and experience (e.g. new hires vs senior leaders) and may fail to recognise an IS/cyber security issue. As one practitioner states, "the campaign can provide detailed information about phishing, social engineering, and other technical attacks". As a result, the main goal of an IS/cyber security awareness campaign is to raise employee awareness and knowledge.

In comparing these findings with those presented in the literature, several observations can be made around the criticality of building an IS/cyber security awareness campaign as part of a SETA programme. For example, Rantos *et al.* (2012) discuss launching an awareness campaign across the company to cover all IS security topics as a vital element of measuring the effectiveness of the SETA programme. Several studies highlight the need to design an awareness campaign as a periodic short communication to clarify the importance of the SETA programme in terms of protecting the IS assets, personal data, enhancing IS/cyber security awareness, complying with IS/cyber security policy and reducing IS/cyber security risks (Vroom and Solms, 2002; Puhakainen and Siponen, 2010). Therefore, formal awareness campaigns are communications with employees with the specific aim of increasing the understanding of, and reducing the likelihood of, harmful IS practices within the organisation (D'Arcy *et al.*, 2009; Hearth *et al.*, 2018).

4.2 Principle 2: evaluate employee performance at a frequency that aligns with the organisational IS/cyber security strategy

CSF-EV1: Maintain Quarterly Evaluation of Employee Performance focuses on providing a year-end evaluation summary (e.g. metrics) to measure each employee's performance (e.g. level of awareness, number of training sessions completed, etc.) and to provide guidance on necessary improvements. Figure 2 visualises the contradictory rankings between Stage 1 and Stage 2 for this CSF. We believe that this difference exists because the perspectives of the experts differ on whether an assessment should be conducted at the start or at the end of the year. Some experts believe in assessing employee knowledge, to determine their level of awareness and then building the SETA programme around that, while others believe that the assessment should be done at the end of the year to evaluate the effectiveness of the current programme (while also informing the design of the forthcoming year).

Based on our review of the story of the importance of this CSF (*CSF-EV1*) to SETA programme effectiveness, the IS/cyber security practitioners highlight the criticality of conducting employee assessments to assess security awareness and knowledge levels and motivate employees to participate in the SETA programme. However, IS/cyber security practitioners have differing views on whether the time frame for evaluating employee performance should be quarterly or annually. A significant number of practitioners prefer to conduct annual assessments. For example, one practitioner states, "if you ask employees to do evaluations every quarter, some organisations will simply fail because employees will get tired and fatigued". However, there is a strong preference for quarterly assessment also. For example, one practitioner states, "while it is very important to evaluate the employee at least once a year, I prefer to conduct employee assessments every three months to track their progress". Therefore, it appears as if the time frame for conducting employee assessments can be determined based on the organisational IS/cyber security strategy. Furthermore, while organisations use various tools to assess employee performance, one practitioner calls out the importance of defining the correct KPIs, for example, "we must ensure that 90% of employees, preferably 98%, have successfully completed the training courses". In contrast, another practitioner states, "we can evaluate employee performance by using phishing simulation (e.g. did they get the security awareness message, did they report suspicious links)". Ultimately, the evaluation results also inform the next cycle of designing an effective SETA programme within the organisation.

In comparing these findings with those presented in the literature, several studies discuss approaches to evaluate SETA programmes. For example, Rantos *et al.* (2012) illustrate several methods for evaluating a SETA programme. One of those methods is using a survey/questionnaire to evaluate the success of the programme overall. Other methods evaluate security awareness campaigns by highlighting some IS security issues and measuring the effectiveness of the SETA programme in addressing the existing gaps (Alshaikh *et al.*, 2018; Johnson, 2006). However, this is an area that still requires further research.

4.3 Principle 3: secure top management support to encourage all employees to comply with IS/cyber security policy

CSF-DS5: Adhere to Organisational Security Policy and the "Law of the Land" is concerned with focusing on the guidelines and procedures needed to protect the IS assets of the organisation, to ensure that all of the organisational security policies and the "law of the land" are adhered to when designing a SETA programme. Figure 2 visualises the contradictory rankings between Stage 1 and Stage 2 for this CSF. We believe that this difference is linked to the fact that some organisations design their SETA programmes in-house and ensure that their security policies comply with localised legal requirements. In contrast, other organisations use a more generic CBT (computer-based training) design that simply informs employees of the country's regulations (but does not link back to the organisational security policy).

Based on our review of the story of the importance of this CSF (*CSF-DS5*), the IS/cyber security practitioners highlight the need to obtain top management support to ensure that all organisational employees adhere to the IS/cyber security policy. The practitioners express the view that top management can improve employee security awareness and practices because their acts of policy compliance encourage other employees to follow their lead. For example, one practitioner states, "in order to get employees to commit to security policies and regulations, we need top management support". Therefore, improving SETA programme effectiveness begins with top management demonstrating the importance of implementing security regulations and policies and then training employees on these security regulations and policies. It also appears that for some IS/cyber security professionals enforcing severe penalties for IS/cyber security policy violations can help improve SETA programme effectiveness. For example, one practitioner states, "we have a security policy, and if you fail to follow the policy three times in a row, you will be fired". The view exists that this enhances employee commitment and adherence to the fundamentals of IS/cyber security awareness. Furthermore, implementing the appropriate IS/cyber security standards is identified as a key to reducing IS security risks and is critical to delivering an effective SETA programme (assisting organisational employees to manage cyberattacks and IS/cyber security threats). For example, one practitioner states, "once ISO 27000 certified, you will have regular audits, and the system will be audited. The audits will ensure continuous improvement [. . .]". Typically, organisations conduct internal or external audits every six months to motivate employees to follow their IS security policies.

In comparing these findings with those presented in the literature, several observations can be made around the criticality of top management support to IS/cyber security policy adherence as part of a SETA programme. For example, Puhakainen and Siponen (2010) conducted an empirical investigation into the significance of the role of top management in ensuring employee compliance with IS policy. Hu *et al.* (2012) also provided a detailed explanation of the significance of top management support to IS policy compliance and the changes to organisational culture. Active participation by top management in the development, implementation and enforcement of security policy can enhance employees' perceptions that IS policy and procedures are legitimate and fair (Hu *et al.*, 2012). Therefore, top management plays an important role in encouraging employees to adhere to IS/cyber security policy to deliver an effective SETA programme.

4.4 Principle 4: avoid a one size fits all approach to programme content to promote employee engagement

CSF-DS2: Know Your Audiences to Ensure Content Suitability focuses on identifying "who your audiences are" to ensure appropriate content is delivered to the various employee types. Figure 2 visualises the contradictory rankings between Stage 1 and Stage 2 for this CSF. We believe that the slightly different stories highlight how organisational size and resources play an important role in delivering appropriate security awareness materials to employees at various levels. Employee differences (e.g. culture, knowledge, age, etc.) should be considered when preparing resources, and content customisation should align with the organisation's own strategies and IS/cyber security plans. Therefore, IS/cyber security awareness content should be designed in such a way as it is neither too technical nor too general for the target audiences.

Based on our review of the story of the importance of this CSF (*CSF-DS2*) to SETA programme effectiveness, the IS/cyber security practitioners highlight the criticality of tailoring the content of the IS/cyber security message to the audience level (e.g. level of education, age, role, etc.) to provide them with the appropriate training materials. The aim of this is to increase IS/cyber security policy compliance and achieve the organisational goals. For example, one practitioner states, "we will tailor the content, based on the audience targets, in order to get people to engage with it". Therefore, customising content is essential to ensure SETA programme effectiveness. As one practitioner states, "it is absolutely essential to tailor the content of the cyber security awareness message and make it simple, direct, and attractive [. . .]". As a result, it is impossible to apply the concept of "one-size-fits-all", and the same IS/cyber security awareness message cannot be delivered to everyone in the organisation.

In comparing these findings with those presented in the literature, several observations can be made. For example, Peltier (2005) discusses establishing an IS/cyber security awareness programme by classifying the audience to ensure the IS/cyber security message is communicated effectively. Accordingly, a SETA programme must comprise a plan to transmit the IS/cyber security message to the target audience (De Maeyer, 2007; Siponen, 2000). Therefore, it can be argued that identifying the target audiences in designing a SETA programme is the main step towards its success; thereby, delivering thorough IS/cyber security training to each employee with appropriately suitable material.

4.5 Principle 5: appreciate employee cultural differences to shape programme content

CSF-DS4: Design for Cultural Context and Employee Cultural Diversity focuses on understanding the diversity of employee backgrounds (e.g. language, culture, knowledge, level of education, age, gender) so that the IS/cyber security message can be interpreted by all employees. Figure 2 visualises the contradictory rankings between Stage 1 and Stage 2 for this CSF. We believe this is linked to the fact that the IS/cyber security practitioners involved in this research study come from different cultures (e.g. Saudi Arabia, Kuwait, Ireland, the US, the UK, etc.). As a result, given their differing backgrounds and experiences, what works in one cultural context might not work in another.

Based on our review of the story of the importance of this CSF (*CSF-DS4*) to SETA programme effectiveness, the IS/cyber security practitioners highlight that each culture has its own sense of privacy, which should be considered when designing a SETA programme. For example, one practitioner states, "it is critical to understand the culture from which they come. To build security awareness content in simple language that adheres to the security policy". Thus, culture is an essential factor that can influence how individuals act, with differences and similarities between individualist and collectivist cultures (Parks and Vu, 1994). For example, one practitioner reveals, "in the context of country culture, Saudi Arabia is collectivist while Ireland is individualist". Therefore, employees from collectivist cultures tend to collaborate in a more trusting fashion and will share their passwords, whereas employees from individualist cultures tend to be more conscious and will not share their passwords (Moorman and Blakely, 1995). Essentially, navigating these cultural realities within an organisational context is extremely important for SETA programme effectiveness.

In comparing these findings with those presented in the literature, a number of observations can be made. Previous studies address "culture" in the context of IS/cyber security practice. For example, Hovav and D'Arcy (2012) examine the influence of culture on IS/cyber security policies, training and monitoring. To understand culture in terms of IS/cyber security practice is to understand individual differences within each cultural context (c.f. Walsham, 2002). These cultural differences can be beliefs, norms and values in a social setting, known collectively as a country. Thus, different cultures require different IS/cyber security interventions (Kirova and Baumoel, 2018; Karjalainen *et al.*, 2013; von Solms and von Solms, 2004). Thus, understanding the cultural context is an essential factor when designing an effective SETA programme.

5. Conclusions and implications

It is reported that *importance* is the most critical dimension of relevance for IS practitioners. 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, while IS/cyber security is a current hot topic and a top concern for many practitioners (both business and IT), the ability to lead an effective SETA programme, and identify the CSFs for doing so, is an area of IS research not yet well established. Therefore, this study is unique in its approach and contributes to the IS/cyber security conversation in the following three ways:

1. one of the first studies to produce a ranked list of CSFs for SETA programme effectiveness; thereby, conceptualising SETA programme effectiveness in a digestible, easy to understand, way (see Figure 2);
2. one of the first studies to provide a set of guiding principles for the CSFs that could be the most challenging to "get right" in practice (see Table 2); and
3. one of the first studies to highlight that the "design" phase of a SETA programme life cycle will be the most contentious in terms of building a shared understanding (among all organisational stakeholders) of what is critical to delivering an effective SETA programme within the organisation.

In this research, we capture the essence of the practitioners' views on the importance of the CSFs for SETA programme effectiveness. By comparing Stage 1 and Stage 2 outputs, we are provided with a context against which a more accurate interpretation of the realities of SETA programme effectiveness can be achieved. Therefore, the outcome of Stage 3 of this research showcases that practice matters and the topic of SETA programme effectiveness (and the CSFs to achieve it) matters to practice. In conclusion, we believe that we have taken practice into consideration and delivered something of practical value in this research. For example, the difference (as to the importance of each CSF) between the two groups of IS/cyber security professionals showcases variation based on past experiences. This variation further advances our theorising and brings further clarity to the SETA programme effectiveness story (through the emergence of the five guiding principles). Furthermore, we are also aware that the research team's effort at qualitative data analysis (in Stage 1 of this research) sets the agenda for the remaining stages. However, the similarity in perceived importance (for the majority) of the CSFs (between Stage 1 and Stage 2) also highlights the shared theoretical sensitivities of both the researchers and the practitioners in this research study.

Beyond the value of the 11 CSFs for SETA programme effectiveness, this paper also presents an approach to evaluate the outputs of a multi-stage grounded (data-to-theory) study. For example, we use an *RFC* approach to take the outputs from Stage 1 (*the emergence of the CSFs*) and generate a comparative ranked order list to generate a new output in Stage 2 (*the ranking of the CSFs*). Finally, the differences between the ranked order lists in Stage 1 and Stage 2 produce the output for Stage 3 (*the emergence of the guiding principles*). This movement through the stages showcases an innovative approach to evaluating outputs, emerging from iterative data gathering and analysis, where the views of participants are used to fuel our theorising and theory development efforts. Therefore, this evaluation approach further increases the relevance of the work (around *accessibility* and *applicability*). To note, as per Rosemann and Vessey (2008, p. 3), *accessibility* is understood as "the research is understandable, readable, and focuses on results", and *applicability* is understood to be "whether it provides guidance and/or direction, and whether it provides concrete recommendations" that are easy to apply in practice.

Finally, prefacing the five guiding principles (presented in Table 2) with "Do We" allows each principle to serve as a pre-commencement readiness check to guide SETA programme endeavours; and/or as an in-progress reflective aid for practitioners to assess the efficacy of their existing SETA programme activities. We believe that asking and answering these five questions will help to start conversations and build a shared understanding among organisational IS/cyber security practitioners, with the aim of delivering an effective SETA programme within an organisational context. For example, the "design" phase is the preliminary phase in a SETA programme life cycle. The design phase activities are most often concerned with identifying the target audiences and their needs, outlining and budgeting for a training and awareness plan, setting up priorities and benchmarks, along with risk management and business contingency planning (Alshaikh *et al.*, 2018; Tsohou *et al.*, 2015; Puhakainen and Siponen, 2010; Wilson and Hash, 2003). Therefore, having meaningful conversations around these design phase activities is of the utmost importance.

6. Recommendations for future research

Using a three-stage research approach to capture IS/cyber security practitioner voices allowed their SETA programme stories to be interrogated, the outcome of which leads to the emergence of the 11 CSFs for SETA programme effectiveness (across the life cycle phases) and the five CSF-specific guiding principles to further improve the likelihood of delivering an effective SETA programme within an organisational context. However, these CSFs and guiding principles are not yet established as universal, so while these CSFs and guiding principles provide guidance to all undertaking a SETA programme, organisations need to be "mindful of the influence of their own context" (Borman and Janssen, 2013, p. 85). Furthermore, 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 and five CSF-specific guiding principles for SETA programme effectiveness, it is perhaps more beneficial to move to a larger population of IS/cyber security practitioners as part of a study focused on "construct elaboration" (Gioia *et al.*, 2012, p. 16).

Finally, providing a list of CSFs is only a partial aid to success; more is needed on the implementation actions required around any list of CSFs stated (c.f. Alhassan *et al.*, 2019). Therefore, now that we have identified a ranked list of 11 CSFs for SETA programme effectiveness, along with the five CSF-specific guiding principles, there is a need to examine the "conjunctural" (Ragin, 1987) nature of these CSFs. Such an appreciation would further improve our understanding regarding the complexity of SETA programmes. This would lend itself to the development of a process model for SETA programme effectiveness, embracing the life cycle phases (*design*, *development*, *implementation*, *evaluation*) and chaining (c.f. Hubberman and Miles, 1994) the CSFs within and across these phases.

References

Ahmad, M.M. and Cuenca, R.P. (2013), "Critical success factors for ERP implementation in SMEs", *Robotics and Computer-Integrated Manufacturing*, Vol. 29 No. 3, pp. 104-111, doi: 10.1016/j.rcim.2012.04.019.

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.

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 HI International Conference on System Sciences*, 9, pp. 5085-5094, doi: 10.24251/hicss.2018.635

Alshaikh, M., Naseer, H., Ahmad, A., Maynard, S.B., Paper Alshaikh, R. and Sean, M. (2019), "Toward sustainable behaviour change: an approach for cyber security education training and awareness", *Twenty-Seventh European Conference on Information Systems (ECIS2019)*, pp. 0-14, 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 and Security*, Vol. 100, doi: 10.1016/j.cose.2020.102090.

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.

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*, Vol. 14 No. 11, p. e0224746, doi: 10.1371/journal.pone.0224746.

Borman, M. and Janssen, M. (2013), "Similarities and differences in critical success factors across context and time: an examination in the setting of shared services", *A Journal of Electronic Services in the Public and Privat Sectors*, Vol. 9 No. 1, pp. 85-105, available at: www. jstor.org/stable/10.2979/eservicej.9.1.85

Chen, R., Sharman, R., Rao, H.R. and Upadhyaya, S.J. (2013), "Data model development for fire related extreme events: an activity theory approach", *MIS Quarterly*, Vol. 37 No. 1, pp. 125-147, available at: www. jstor.org/stable/43825940

Corbin, J.M. and Strauss, A. (1990), "Grounded theory research: procedures, canons, and evaluative criteria", *Qualitative Sociology*, Vol. 13 No. 1, pp. 3-21.

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.

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.

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

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.

Global Market Estimates (2022), "2022 Cybersecurity awareness training market report".

Hair, J.F., Money, A.H., Samouel, P. and Page, M. (2007), "Research methods for business", *Education + Training*, Vol. 49 No. 4, pp. 336-337, doi: 10.1108/et.2007.49.4.336.2.

Han, J.Y., 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.

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, doi: 10.1108/ITP-10-2017-0322.

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, pp. 99-110.

Hu, Q., Dinev, T., Hart, P. and Cooke, D. (2012), "Managing employee compliance with information security policies: the critical role of top management and organizational culture", *Decision Sciences*, Vol. 43 No. 4, pp. 615-660.

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, p. 102404, doi: 10.1016/j.cose.2021.102404.

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

Johnson, E.C. (2006), "Security awareness: switch to a better programme", *Network Security*, Vol. 2006 No. 2, pp. 15-18, doi: 10.1016/S1353-4858(06)70337-3.

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

Khando, K., Gao, S., Islam, S.M. and Salman, A. (2021), "Enhancing employees information security awareness in private and public organisations: a systematic literature review", *Computers and Security*, Vol. 106, p. 102267, doi: 10.1016/j.cose.2021.102267.

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

Kitchenham, B.A. and Pfleeger, S.L. (2008), "Personal opinion surveys", in Shull, F., Singer, J. and Sjøberg, D.I.K. (Eds), *Guide to Advanced Empirical Software Engineering*, Springer, London, doi: 10.1007/978-1-84800-044-5_3.

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.

Lo, D., Nagappan, N. and Zimmermann, T. (2015), "How practitioners perceive the relevance of software engineering research", *ESEC/FSE 2015: Proceedings of the 10th Joint Meeting on Foundations of Software Engineering: Bergamo, Italy, August 30–September 4*, pp. 415-425, available at: https://ink.library.smu.edu.sg/sis_research/3083

Maeyer, D.D. (2007), "Setting up an effective information security awareness programme", ISSE/SECURE 2007 Securing Electronic Business Processes, pp. 49-58.

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

Moorman, R.H. and Blakely, G.L. (1995), "Individualism-collectivism as an individual difference predictor of organizational citizenship behavior", *Journal of Organizational Behavior*, Vol. 16 No. 2, pp. 127-142.

Myers, M.D. (2009), "Qualitative research in business and management", *Qualitative research in business and management*, pp. 1-364.

Nah, F., Lau, J. 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, doi: 10.1080/10658980701747237.

Osei-Kyei, R. and Chan, A.P.C. (2017), "Empirical comparison of critical success factors for public-private partnerships in developing and developed countries: a case of Ghana and Hong Kong", *Engineering, Construction and Architectural Management*, Vol. 24 No. 6, pp. 1222-1245, doi: 10.1108/ECAM-06-2016-0144.

Parks, C.D. and Vu, A.D. (1994), "Social dilemma behavior of individuals from highly individualist and collectivist cultures", *Journal of Conflict Resolution*, Vol. 38 No. 4, pp. 708-718.

Pastor, V., Díaz, G. and Castro, M. (2010), "State-of-the-art simulation systems for information security education, training and awareness", *IEEE EDUCON 2010 Conference*, *IEEE*, pp. 1907-1916.

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

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 CA Press, Berkeley.

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

Reitsma, E. and Hilletofth, P. (2018), "Critical success factors for ERP system implementation: a user perspective", *European Business Review*, Vol. 30 No. 3, pp. 285-310, doi: 10.1108/EBR-04-2017-0075.

Rockart, J.F. (1979), "Chief executives define their own data needs", *Harvard Business Review*, Vol. 57 No. 2, pp. 81-93, available at: http://europepmc.org/abstract/med/10297607

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.

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.

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

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.

Soomro, M.A., Soomro, S.A. and Memon, A.H. (2016), "Barriers and motivations for developing transportation public private partnerships in Pakistan".

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.

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 Solms, R.V. (2002), "A practical approach to information security awareness in the organization", *Security in the Information Society*, Springer, Boston, MA, pp. 19-37.

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

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

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.

Wong, C. (1998), "Determining factors for local economic development: the perception of practitioners in the North West and Eastern regions of the UK", *Regional Studies*, Vol. 32 No. 8, pp. 707-720, doi: 10.1080/00343409850119409.

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, pp. 107-118, doi: 10.1016/j.dss.2018.02.009.

Further reading

Alyami, A., Sammon, D., Neville, K. and Mahony, C. (2023), "The critical success factors for security education, training and awareness (SETA) program effectiveness: a lifecycle model", *Information Technology & People*, Vol. 36 No. 8, pp. 94-125.

Bhattacherjee, A. (2012), "Social science research: principles, methods, and practices".

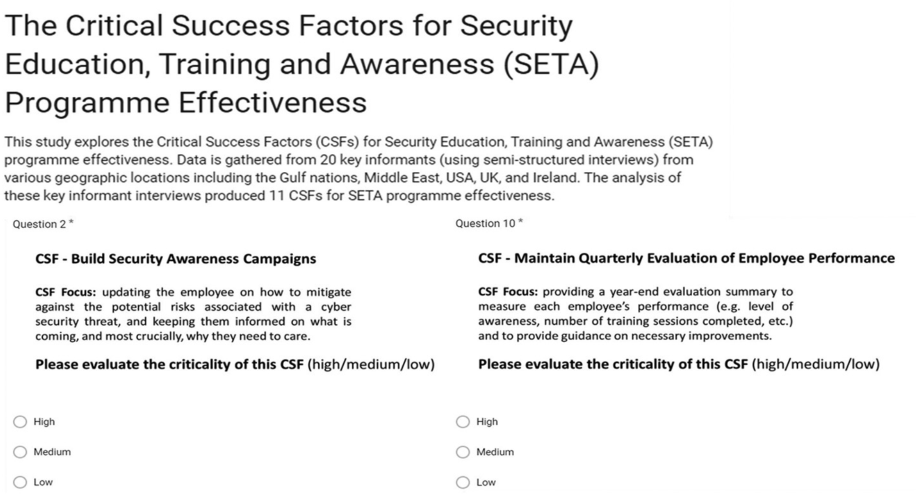
How To ... Perform the Mann-Whitney U Test (By Hand). (2016). *How to ... Perform the Mann-Whitney U Test (By Hand)*, YouTube, available at: www.youtube.com/watch?v=BT1FKd1Qzjw

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/business/articles/2022/07/22/cybersecurity-hiring-remains-red-hot-the-industry-to-surpass-400-billion-market-size-by-2027 (accessed 29 September 2022).

Corresponding author

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

Appendix 1



The Critical Success Factors for Security Education, Training and Awareness (SETA) Programme Effectiveness

This study explores the Critical Success Factors (CSFs) for Security Education, Training and Awareness (SETA) programme effectiveness. Data is gathered from 20 key informants (using semi-structured interviews) from various geographic locations including the Gulf nations, Middle East, USA, UK, and Ireland. The analysis of these key informant interviews produced 11 CSFs for SETA programme effectiveness.

Question 2 *

CSF - Build Security Awareness Campaigns

CSF Focus: updating the employee on how to mitigate against the potential risks associated with a cyber security threat, and keeping them informed on what is coming, and most crucially, why they need to care.

Please evaluate the criticality of this CSF (high/medium/low)

○ High

○ Medium

○ Low

Question 10 *

CSF - Maintain Quarterly Evaluation of Employee Performance

CSF Focus: providing a year-end evaluation summary to measure each employee's performance (e.g. level of awareness, number of training sessions completed, etc.) and to provide guidance on necessary improvements.

Please evaluate the criticality of this CSF (high/medium/low)

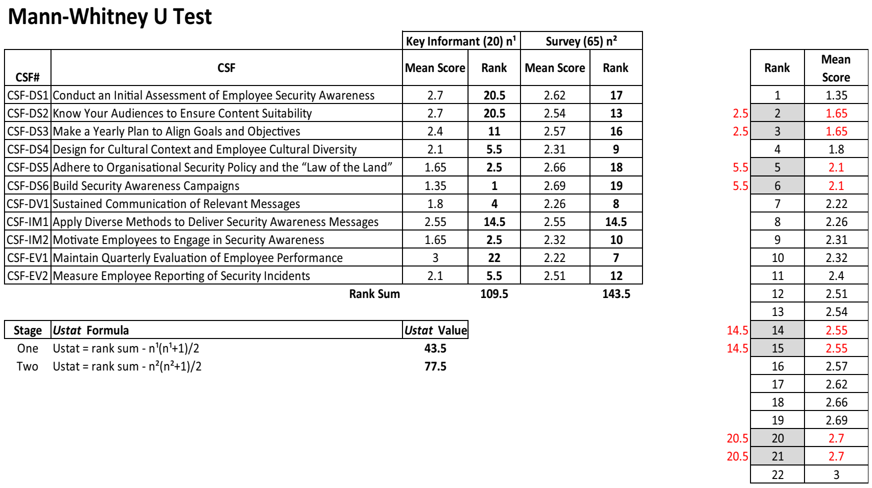
○ High

○ Medium

○ Low

Source: Author's own creation/work

Appendix 2



Mann-Whitney U Test

		Key Informant (20) n^1		Survey (65) n^2	
CSF#	**CSF**	**Mean Score**	**Rank**	**Mean Score**	**Rank**
CSF-DS1	Conduct an Initial Assessment of Employee Security Awareness	2.7	**20.5**	2.62	**17**
CSF-DS2	Know Your Audiences to Ensure Content Suitability	2.7	**20.5**	2.54	**13**
CSF-DS3	Make a Yearly Plan to Align Goals and Objectives	2.4	**11**	2.57	**16**
CSF-DS4	Design for Cultural Context and Employee Cultural Diversity	2.1	**5.5**	2.31	**9**
CSF-DS5	Adhere to Organisational Security Policy and the "Law of the Land"	1.65	**2.5**	2.66	**18**
CSF-DS6	Build Security Awareness Campaigns	1.35	**1**	2.69	**19**
CSF-DV1	Sustained Communication of Relevant Messages	1.8	**4**	2.26	**8**
CSF-IM1	Apply Diverse Methods to Deliver Security Awareness Messages	2.55	**14.5**	2.55	**14.5**
CSF-IM2	Motivate Employees to Engage in Security Awareness	1.65	**2.5**	2.32	**10**
CSF-EV1	Maintain Quarterly Evaluation of Employee Performance	3	**22**	2.22	**7**
CSF-EV2	Measure Employee Reporting of Security Incidents	2.1	**5.5**	2.51	**12**
	Rank Sum		**109.5**		**143.5**

Stage	*Ustat* Formula	*Ustat* Value
One	Ustat = rank sum - $n^1(n^1+1)/2$	**43.5**
Two	Ustat = rank sum - $n^2(n^2+1)/2$	**77.5**

	Rank	Mean Score
	1	1.35
2.5	2	1.65
2.5	3	1.65
	4	1.8
5.5	5	2.1
5.5	6	2.1
	7	2.22
	8	2.26
	9	2.31
	10	2.32
	11	2.4
	12	2.51
	13	2.54
14.5	14	2.55
14.5	15	2.55
	16	2.57
	17	2.62
	18	2.66
	19	2.69
20.5	20	2.7
20.5	21	2.7
	22	3

Source: Author's own creation/work