Ollscoil na hÉireann, Corcaigh
National University of Ireland, Cork

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

Thesis presented by
Areej Alyami
117228132

Thesis submitted for the degree of Doctor of Philosophy in Business Information Systems
University College Cork
Cork University Business School

Head of School/Department: Prof. Frederic Adam
Supervisors: Prof. David Sammon, Dr. Karen Neville, and Dr. Carolanne Mahony
[January 2023]

Table of Contents

List of Tables

List of Figures

The Author hereby declares that, except where duly acknowledged, this thesis is entirely his own work and has not been submitted for any degree in the National University of Ireland, or any other University.

Acknowledgements

During the PhD journey, I have faced many ups and downs. I remembered how many times I was upset, lost, feeling down, crying, thrilled and optimistic. I believe this journey has changed my whole life and makes me more mature and conscious. Many individuals supported me to complete the thesis under various circumstances.

First of all, I would like to thank my sponsor (Saudi Arabia Government) for the scholarship and their financial support during the years of my study in Ireland.

Foremost, I would like to express my deepest appreciation to my supervisors Prof. David Sammon, Dr. Karen Neville, and Dr. Carolanne Mahony. I could not have undertaken this journey without your patience, guidance, support, and constructive criticism. Special thanks to Prof. Dave for many times I was feeling down, you encouraged me to continue and move on. I have learned a lot from their knowledge and experience of the research. Dr. Karen, I appreciate your help during the first year of the research when you shared with me many papers to understand the IS security field. Dr. Carolanne, I appreciated you encouraging me to participate in various workshops to improve my research knowledge.

Also, I can't forget Prof. Ciara Heavin, Prof. Fred Adam (Head of BIS), and Prof. Joseph Feller during the first year of the structured BIS PhD programme (including all BIS staff who taught me and shared their tremendous knowledge and support throughout the PhD journey).

Special thanks to my colleagues in the BIS lab for sharing knowledge and long productive conversations. To Dr. Reem Alshammari, a Leader in Cyber Security and Technology in the Energy Sector in Kuwait, for her time and effort to connect me with professionals in the IS security field in Golf countries. Also, the Hemaya cyber security non-profit organisation in Saudi Arabia

for giving me the chance to be a participant in this valuable organisation (and for providing me with massive help in collecting my data).

To my friends in Cork, I will keep all our memories in my mind and my heart forever. Thank you for everything: time, kindness, friendship and ultimately encouragement.

Last, I would be remiss in not mentioning my family. Words cannot express my gratitude to my parents. May God's mercy be upon them. To my father's soul Engineer. Nasser thank you from the bottom of my heart for believing in me. The lessons I have learned from you. When I was feeling down and you said take it easy and life goes on. To my mother Wadha the kind heart in my life. You have always been beside me, supporting, helping, and encouraging me to be who I am today. Thank you for your prayers and caring.

My brothers and my lovely sisters give me positive vibes in my life and tremendous encouragement.

Abstract

Security Education, Training, and Awareness (SETA) programmes are one of the most important cybersecurity strategies to protect the valuable assets of any organisation, raise awareness, change behaviour, comply with Information Systems (IS) security policy, and minimises IS security threats. The significance of SETA programmes is widely accepted by both academics and practitioners. However, more research is needed to improve SETA programme effectiveness in organisations. A review of the relevant IS/cyber security literature reveals a lack of research into the Critical Success Factors (CSFs) for SETA programme effectiveness. Therefore, this research study explores the CSFs for SETA programme effectiveness.

A multi-stage research design is adopted for this research study. Stage One involves the gathering and analysis of lived experiences (using semi-structured interviews) from 20 key expert informants. Emerging from this stage are 11 CSFs for SETA programme effectiveness. These CSFs are mapped along the phases of the SETA programme lifecycle (*design*, *development*, *implementation*, *evaluation*). Furthermore, 9 relationships between these CFSs are identified (both *within* and *across* the lifecycle phases). This research output is a Lifecycle Model of CSFs for SETA programme effectiveness.

Stage Two of this research involves an evaluation of the importance of the 11 CSFs for SETA programme effectiveness (emerging from stage one). This evaluation is achieved through administering a short online survey questionnaire (completed by 65 respondents - IS/cyber security professionals) and a series of follow-up probing interviews (with 9 IS/cyber security professionals – 4 key informants for stage one, and 5 survey respondents for stage two). Emerging from this stage is a ranked list of CSFs and 5 guiding principles to overcome the challenges of delivering an effective SETA programme. This research output is an *evaluated* Lifecycle Model of CSFs for SETA programme effectiveness.

Overall, this research provides a depth of insight contributing to both theory and practice and lays the foundation for further research.

Chapter One: Introduction

1. Introduction to the Study

This thesis is organised as a series of papers, with an introduction and conclusion chapter. This chapter provides an overview of the research conducted and presented in this thesis. This chapter: (i) embeds the research problem (section 1.1) and identifies the research objective and research questions (section 1.2); (ii) highlights the main contributions of the research (section 1.3); (iii) identifies the plan of this research, and the research approach (section 1.4), (iv) outlines the thesis structure, including a summary of each chapter (section 1.5), and lastly, (v) section 1.6 concludes the chapter.

1.1 Research Problem

Rising IS Security attacks and insider threats are a tremendous challenge for businesses and organisations to survive. According to a global report by The Ponemon Institute (2020), insider threat incidents have increased 44% in the last two years, with costs per incident increasing by more than a third to $15.38 million. The insider threats include employees, temporary workers, and external consultants who have been given authorised access to organisational information (Li and Kettinger, 2021; Posey et al., 2015). Thus, organisations use various methods to protect organisational information assets from security threats. A SETA programme is one of the most vital and prominent approaches to managing IS security risks, safeguarding IS and information assets in an organisation (Hu et al., 2021).

However, a review of the SETA programme literature reveals that current SETA programmes are ‘ineffective’ due to the high number of data breaches and IS security risks which still occur (Alshaikh et al., 2021; Hu et al., 2021, Alshaikh et al., 2021; He and Zhang, 2019). In addition, 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., 2021a, p.1). It is argued that more theorising and conceptual clarity are needed in investigating the effectiveness of SETA programmes (c.f. Alshaikh et al., 2021; Hu et al., 2021b; Kirova and

Baumöl, 2018; Puhakainen and Siponen, 2010). In fact, Alshaikh et al. (2021, p.1) posit that existing SETA programmes are *"suboptimal"* as they *"aim to improve employee knowledge acquisition rather than behaviour and belief"*. Therefore, more theorising and conceptual clarity is required to examine the efficacy of SETA programs (cf. Alshaikh et al., 2021; Hu et al., 2021). The researcher argues that the effectiveness of a SETA programme inside an organisation can be achieved through a better knowledge of the Critical Success Factors (CSFs) for SETA programme effectiveness.

1.2 Research Objective and Research Questions

An analysis of the SETA programme literature finds that present SETA programmes are unsuccessful due to the high number of data breaches and IS security threats. Therefore, conceptual clarity is required to examine the effectiveness of SETA programmes. In fact, the shortage of previous studies addressing the CSFs explicitly for SETA programme effectiveness across the life cycle phases (design, development, implementation, and evaluations) is the primary impetus for this work.

The objective of this research is ***"to explore the Critical Success Factors (CSFs) for Security Education, Training and Awareness (SETA) programme effectiveness"***.

To achieve this objective, the following three research questions are explored::

- **RQ1:** What are the CSFs for SETA programme effectiveness?
- **RQ2:** How are these CSFs for SETA programme effectiveness mapped along the SETA programme lifecycle (design, development, implementation, evaluation)?
- **RQ3:** What is the ranked order of these CSFs for SETA programme effectiveness?

Figure 1 presents a visual of the role played by each of the research questions in fulfilling our research objective of this study. The researcher now provides a brief description of the role of each research question and the relevant chapters /papers.

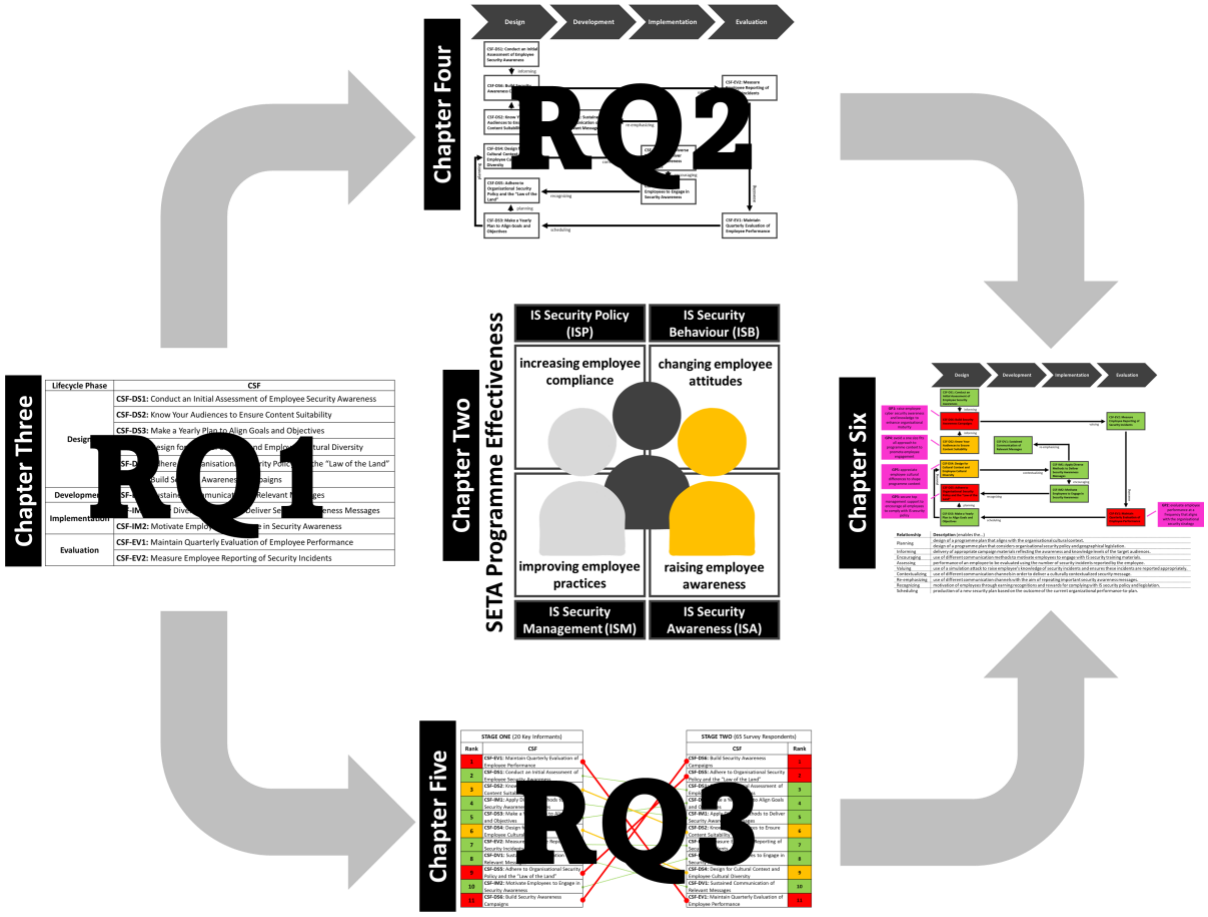


Figure 1. The Relationship between each Research Question

1.2.1 RQ1: What are the CSFs for SETA programme effectiveness?

This research question explores the CSFs for SETA programme effectiveness. Identifying the CSFs for each phase of the SETA programme lifecycle leads to building a foundation for the organisation to deliver an effective SETA programme. Thus, this question aims to establish *'what'* things an organisation needs to get right in order to have a chance of delivering an effective SETA programme. This research question is asked and answered in Chapter 3 (paper 2).

1.2.2 RQ2: How are these CSFs for SETA programme effectiveness mapped along the SETA programme lifecycle (design, development, implementation, evaluation)?

This research question aims to associate the CSFs with the phases of a SETA programme lifecycle (design, development, implementation, evaluation) and proposes a Lifecycle Model of the CSFs for SETA programme effectiveness. This demonstrates the relationships between the CSFs (highlighting the impact of one CSF on another CSF). Thus, these CSFs are mapped against the phases of the SETA programme lifecycle (design, development, implementation, evaluation), and the relationships identified between the CSFs are vital for a deep understanding of SETA programme effectiveness. Therefore, to enable the effective delivery of a SETA programme, this question aims to establish *'how'* and *'when'* the things that are important to get right within an organisation should be implemented along the SETA programme lifecycle. This research question is asked and answered in Chapter 4 (paper 3).

1.2.3 RQ3: What is the ranked order of these CSFs for SETA programme effectiveness?

This research question produces a ranked list (in order of importance) of the CSFs for SETA programme effectiveness (based on a practitioner evaluation). Thus, evaluating the CSFs in order of importance helps to conceptualise SETA programme effectiveness and gain a deeper understanding. Therefore, this question aims to evaluate the *'what'* and *'why'* components (steps, initiatives, and processes, etc.) that can be difficult to get right within an organisation, in order to deliver an effective SETA programme. This research question is asked and answered in Chapter 5 (paper 4).

1.3 An Overview of the Main Research Contributions

This thesis contributes to both the academic and practitioner communities. The main contribution is the *evaluated* Lifecycle Model of CSFs for SETA programme effectiveness. This Lifecycle Model contributes to the IS Security community by addressing the theoretical and practical challenges around SETA programme effectiveness. A summary of the main contributions is represented in Table 1.

Contribution	**Artefact**	**Location**
A conceptualisation of the key messages across four IS/cyber "security themes" that highlight the importance of SETA programme effectiveness. The four IS "security themes" are IS Security Policy (ISP), IS Security Behaviour (ISB), IS Security Management (ISM), and IS Security Awareness (ISA).	Figure 2	Paper 1 (Chapter 2)
The CSFs for SETA programme effectiveness. The 11 CSFs are associated with a SETA programme lifecycle.	Table 2	Paper 2 (Chapter 3)
A Lifecycle Model of CSFs for SETA programmes effectiveness. These CSFs are explicitly mapped along the phases of a SETA programme lifecycle (*design*, *development*, *implementation*, *evaluation*), and the relationships between the CSFs are also highlighted, showing the multiplicative nature of the CSFs.	Figure 3	Paper 3 (Chapter 4)
A ranked list of CSFs for SETA programme effectiveness, along with a set of 5 guiding principles to support getting the most challenging CSFs "right" in practice, along the phases of a SETA programme lifecycle (*design*, *development*, *implementation*, *evaluation*). An *evaluated* Lifecycle Model.	Figure 4 & Figure 5	Paper 4 (Chapter 5)

Table 1 An Overview of the Main Research Contributions

The conceptualisation visual (Figure 2) represents a SETA programme and its effectiveness have associated with four key messages that include increasing employee compliance (ISP key message), changing employee attitudes (ISB key message), improving employee practices (ISM key message), and raising employee awareness (ISA key message). These key messages provide the motivation for the research study. This is discussed in detail in Chapter 2 (paper 1). The 11 CSFs for SETA programme effectiveness that emerge from this research (see Table 2) provide a greater depth of insight into the *design* (6 CSFs), *development* (1 CSF), *implementation* (2 CSFs), and *evaluation* (2 CSFs) of a SETA programme. This is discussed in detail in Chapter 3 (paper 2). Furthermore, the connection between the CSFs *within* and *across* the SETA programme lifecycle phases (see Figure 3) also provides valuable insight and understanding of the process of leading an effective SETA programme in practice. This is discussed in detail in Chapter 4 (paper 3).

The majority of contradictions/differences in CSF rankings between IS/cyber security practitioners (see Figure 4) are associated with the *design* phase of the SETA programme lifecycle. The two CSFs that differ the most, from most to least significant and vice versa, are "maintain quarterly evaluation of employee performance" (**CSF-EV1**) and "build security awareness campaigns" (**CSF-DS6**). Exploring these contradictions/differences enabled us to present five guiding principles (four in the *design* phase and one in the *evaluation* phase) to complement the ranked list of 11 CSFs (by lifecycle phase) and increase the likelihood of delivering an effective SETA programme within an organisational context (see Figure 5). This is discussed in detail in Chapter 5 (paper 4).

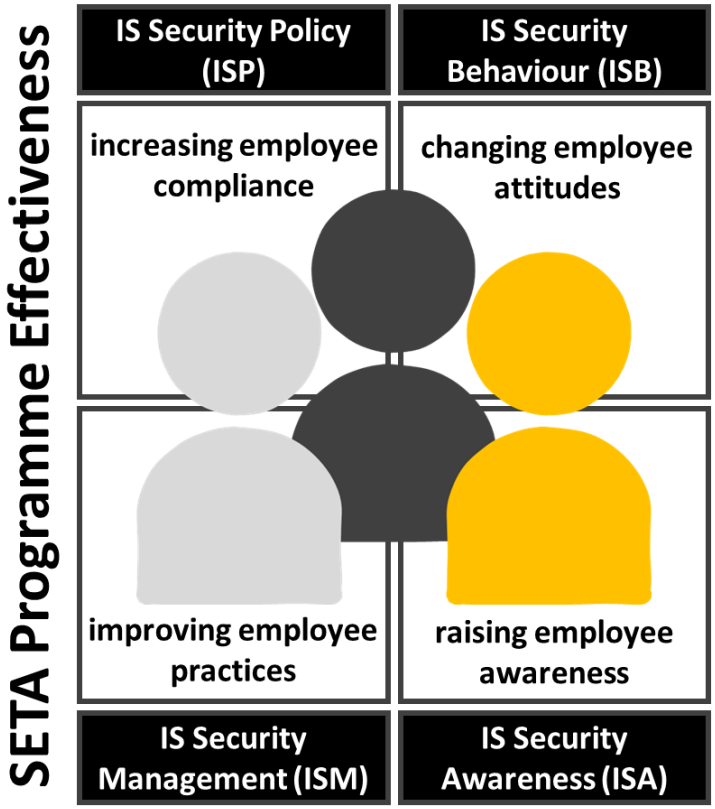


Figure 2.Conceptualising the Key Messages for SETA Programme Effectiveness .

Lifecycle Phase	Category	CSF	Description
Design	Assessment Needs	**CSF-DS1:** Conduct an Initial Assessment of Employee Security Awareness	determining what the employee understands about the organisation's security policy and their appreciation of the risks associated with current cyber security threats.
	Target Audiences	**CSF-DS2:** Know Your Audiences to Ensure Content Suitability	identifying "who your audiences are" to ensure appropriate content is delivered to the various employee types.
	Goal/Objective	**CSF-DS3:** Make a Yearly Plan to Align Goals and Objectives	knowing what is required to be delivered to the employee to ensure that the SETA programme goals meet the specific needs of the organisation.
	Culture	**CSF-DS4:** Design for Cultural Context and Employee Cultural Diversity	understanding the diversity of employee backgrounds (e.g. language, culture, knowledge, level of education, age, gender) so that the cyber security message can be interpreted by all employees.
	Policy	**CSF-DS5:** Adhere to Organisational Security Policy and the "Law of the Land"	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.
	Communication	**CSF-DS6:** Build Security Awareness Campaigns	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.
Development	Communication	**CSF-DV1:** Sustained Communication of Relevant Messages	repeating the cyber security message in various ways to avoid a lapse in employee concentration.
Implementation	Communication Channel	**CSF-IM1:** Apply Diverse Methods to Deliver Security Awareness Messages	using various approaches to deliver 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 cyber security issue.
	Motivation	**CSF-IM2:** Motivate Employees to Engage in Security Awareness	encouraging the employee to adhere to IS security policies by earning a bonus, or other recognition (rewards), based on their practices.
Evaluation	Periodic Assessment	**CSF-EV1:** Maintain Quarterly Evaluation of Employee Performance	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.
	Incident Indication	**CSF-EV2:** Measure Employee Reporting of Security Incidents	using phishing campaigns to simulate attacks (knowing how many employees click the suspicious links), in order to measure the employee awareness and knowledge regarding cyber security issues.

Table 2.The CSFs for SETA Programme Effectiveness.

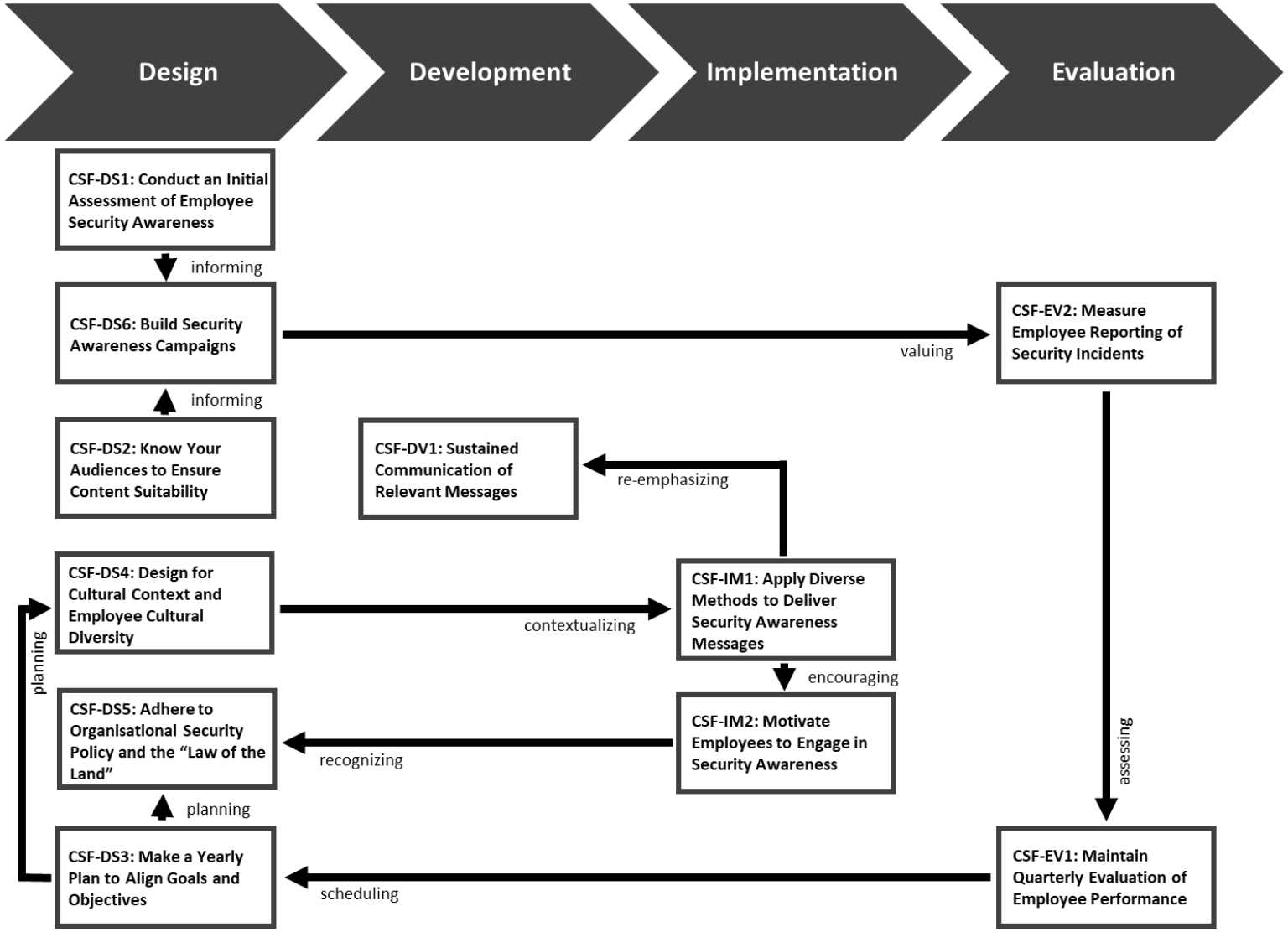


Figure 3.The Lifecycle Model of CSFs for SETA Programme Effectiveness.

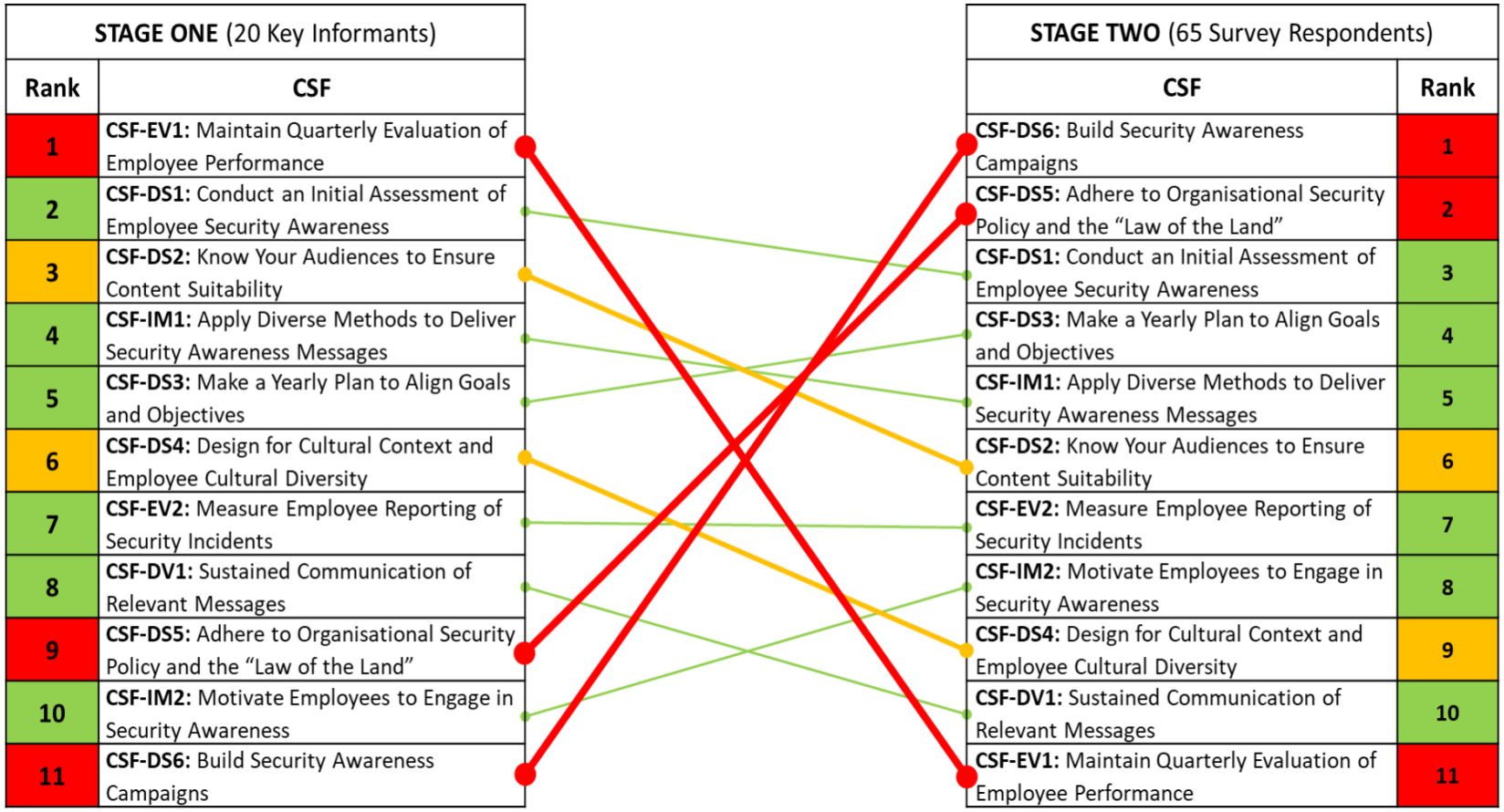
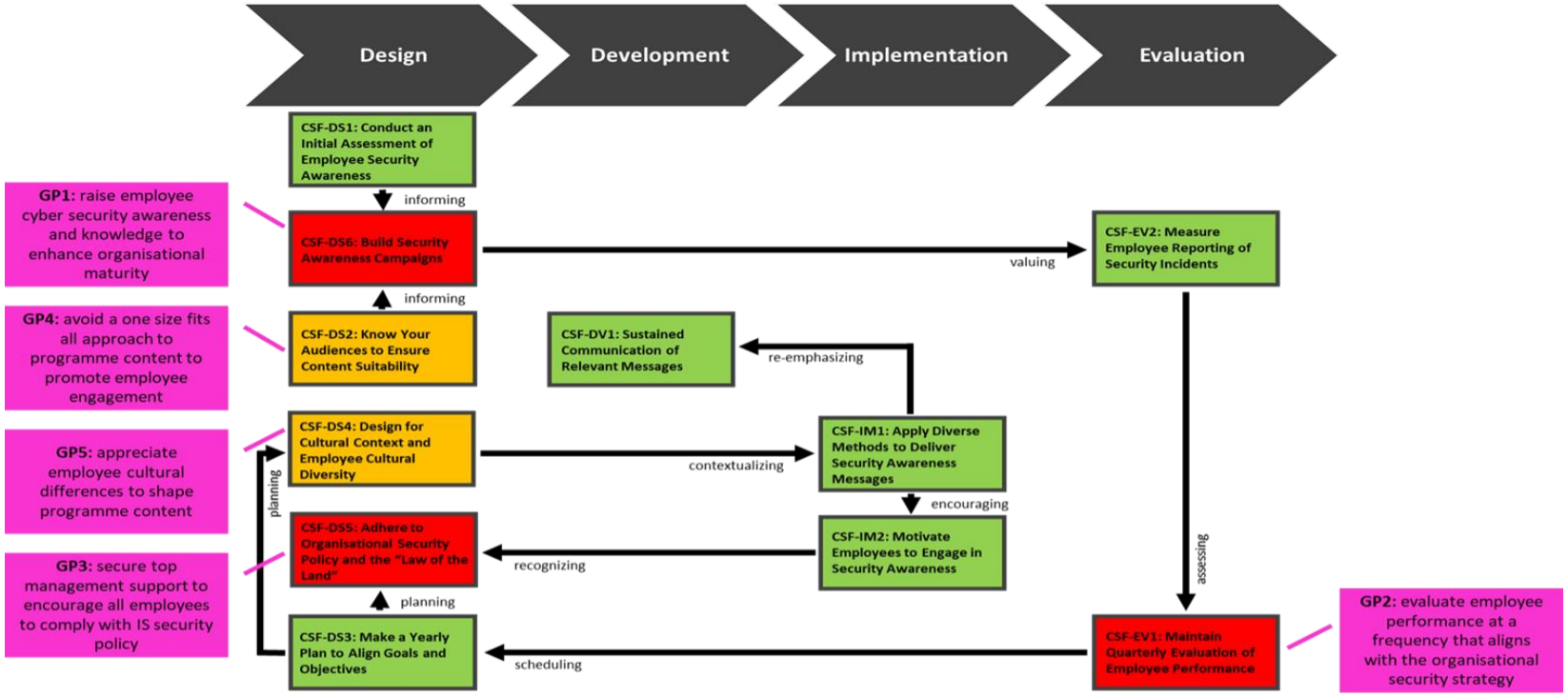


Figure 4. CSF Ranked List Comparison (Stage One and Stage Two).



Relationship	**Description** (enables the...)
Planning	design of a programme plan that aligns with the organisational cultural context.
	design of a programme plan that considers organisational security policy and geographical legislation.
Informing	delivery of appropriate campaign materials reflecting the awareness and knowledge levels of the target audiences.
Encouraging	use of different communication methods to motivate employees to engage with IS security training materials.
Assessing	performance of an employee to be evaluated using the number of security incidents reported by the employee.
Valuing	use of a simulation attack to raise employee's knowledge of security incidents and ensures these incidents are reported appropriately.
Contextualizing	use of different communication channels in order to deliver a culturally contextualized security message.
Re-emphasizing	use of different communication channels with the aim of repeating important security awareness messages.
Recognizing	motivation of employees through earning recognitions and rewards for complying with IS security policy and legislation.
Scheduling	production of a new security plan based on the outcome of the current organizational performance-to-plan.

Figure 5. The "evaluated" Lifecycle Model of CSFs for SETA Programme Effectiveness.

1.4 Research Approach

Researchers must define their personal philosophical position because it provides a starting point for the research process and guides the selection of appropriate research methods (Mayer, 2015). Weber (2004) defines the need for the researcher to select the appropriate research method based on their research goals, regardless of which approach is deemed the most popular, as well as their merits and limitations. As a result, the researcher needs to investigate the various types of knowledge obtained by employing different research methods. Each research method could provide knowledge based on the phenomena being studied.

This section will discuss the various research paradigms and justify the adoption of an interpretivist paradigm in this study. Information Systems (IS) researchers adopt two main paradigms positivism or interpretivism (Walsham, 2006). First, positivism research has typically been the dominant approach in information systems (IS) research (Orlikowski and Baroudi,1991; Klein and Myers, 1999; Siponen and Tsohou, 2018). Siponen and Tsohou (2018) proposed that the beliefs of positivism have impacted the IS field more than any other philosophical research.

Positivist research usually follows deductive methods to test a theory or hypothesis that can be confirmed through observations (O'Leary, 2004). Myers and Avison (2002) define positivist research as "*assum[ing] that reality is objectively given and can be described by measurable properties which are independent of the observer (researcher) and his or her instruments*" (p.242). It is referred to as realist or practical epistemology, the assumption that something already exists in the world and the researcher can observe or test it (Tracy, 2013). In this philosophy, research depends primarily on mathematical and statistical techniques to generate context- and time-free generalisations (Bogdan and Taylor, 2007). Therefore, positivist research is commonly associated with deduction and quantitative research methods such as surveys, experiments, and field studies, whereas interpretive research philosophy is commonly associated with qualitative research (Orlikowski and Baroudi, 1991).

In contrast, the interpretivist paradigm aims to recognise phenomena from the perspective of the people experiencing them (Orlikowski and Baroudi, 1991). Interpretivist research tends to use qualitative data and implement methods such as observations and unstructured interviews (Livesey, 2006). The IS research community is becoming more interested in interpretivism as it addresses the complicated issues surrounding the connection between IS and management, organisations, and individual behaviour (Pather and Remenyi, 2005; Chowdhury, 2014). Additionally, IS researchers will undoubtedly be impacted by the growing popularity of interpretivism among social scientists in general (Walsham, 2006; Averweg and Kroeze, 2012). Hermeneutics and phenomenology are the philosophical foundations of interpretive research (Boland, 1985). Klein and Myers (1999) debated that interpretive research advocates for IS researchers to understand human behaviour and action in social and organisational contexts. Some researchers have criticised the interpretive approach for its 'focuses on particularities and neglect the general' (Hackley, 2007, p. 104). Another criticism is that the research outcomes can be subjective, and the researcher may interpret participant information in a biased manner and manipulate it in a particular direction (Orlikowski and Baroudi, 1991). Bhardwaj (1996) discusses that the interpretivist approach is appropriate to the IS researcher for the following reasons: (i) it recognises the connection between the human element and the technological aspect of the IS research, and (ii) it advocates for the use of a variety of research methodologies for IS study.

1.4.1 Research Design

In this section, the researcher highlights the research design implemented for this study. The interpretivist perspective was deemed the most appropriate for this research due to the exploratory nature of this study, *exploring* the CSFs for SETA programme effectiveness. This paradigm allows the researcher to investigate individuals' perceptions based on various experiences and learn from them (Creswell, 2009). Further, the interpretivist approach allows for in-depth qualitative data analysis (Guthrie, 2010).

Given the objective and exploratory nature of this research, qualitative research methods are deemed appropriate to answer our three research questions because they allow us to explore new

ideas, capture new phenomena, and identify the rich contextualised detail of complex concepts (Bhattacharjee, 2012; Cassell and Symon, 2004). Furthermore, an exploratory research approach supports the development of research questions reflecting what is happening in current phenomena. For example, what are the patterns, categories, and themes emerging in the structure? How are these patterns linked with one another? An exploratory approach most often uses qualitative research methods, such as case studies and field studies, while using qualitative data gathering through interviewing, participant observation, and document analysis (Bhattacherjee, 2012). Previous scholars have investigated and explored CSFs in IS by applying qualitative methods, demonstrating the appropriateness of interpretive qualitative research when exploring CSFs (c.f. Alhassan et al., 2019). Therefore, the researcher decided to follow the Gioia methodology to advocate a Grounded Theory approach. The methodology emphasises the development of theory grounded in the data, rather than the use of pre-existing theories to interpret the data (Gioia et al., 2012). There, the research aims to generate new ideas around delivering an effective SETA programme. It is also worth mentioning that Design Science Research (DSR) is another possible approach that could have been used to develop and validate something new (an artefact) for SETA programme effectiveness. However, DSR typically involves multiple iterations of designing, building, and evaluating *"artefacts"* in order to improve their functionality and usefulness. (Peffers et al., 2007). Therefore, the most important aspect of DSR is the use of rigorous evaluation methods to assess the effectiveness and impact of the artefact(s) produced. This evaluation can involve testing the artefact with users, comparing it to existing solutions, or conducting other types of experiments or surveys (Peffers et al., 2007). To conclude, while Grounded Theory (the Gioia methodology) and DSR are both used in research to develop and validate new theories, DSR is more focused on building and evaluating new IT artefacts (and this was not the primary focus of this research study).

Building theory is often executed from the bottom up, with the researcher collecting data, identifying patterns, and then constructing a theory based on those patterns (Gregor,2006). This method is especially beneficial when examining new phenomena or when existing theories are insufficient to explain the observed behaviour (Walsham,1995). Following a review of the literature, it became clear that studies addressing SETA programme effectiveness were not taking a process-oriented view (across all the lifecycle phases). This further supported the motivation to

explore the CSFs (the things an organisation needs to get right) across the SETA programme lifecycle. Therefore, the researcher used a data-first approach to build a process model, where the goal of a process model is to understand the causal links between variables and how they interact. Therefore, in identifying the CSFs for SETA programme effectiveness and their interrelatedness (across the lifecycle phases), a process model (the Lifecycle Model of CSFs for SETA programme effectiveness) is proposed in this research study.

Overall, this research presents a much-needed interpretation of the realities of SETA programme effectiveness. In order to achieve this a *process theory* perspective is adopted. This perspective allows a time-ordering sequence of events (to reveal underlying causal logic about a phenomenon) based on narratives (Burton-Jones, et al., 2015; Markus & Robey, 1988). It shows how *outcomes of interest* (e.g. CSFs) evolve (through a sequence of events) and is an excellent perspective to understand *how* and *why* outcomes of interest emerge, which is a core element for *theorising* (Niederman et al., 2018). In fact, Sutton & Staw (1995) suggest that this *underlying causal logic* is necessary to produce good theory. The advantage of using a process theory perspective is the fact that a process theory tends to be contextually rich and able to capture high complexities. Finally, the logic of a process theory can help researchers communicate with practitioners, showcasing both the rigors and relevance of their theoretical endeavours, where practitioners can frame their experiences and researchers can examine these same experiences through the process theory-in-use. Notwithstanding this, a process theory may be viewed as less accurate in capturing a phenomenon (Langley, 1999) because it models the phenomenon at a higher level of abstraction. Therefore, a process theory may suffer from a lack of predictive power (Langley, 1999). Furthermore, a process theory can be particular to individual organisations and can be challenging for generalisation to other contexts (Crowston, 2000).

In this research we capture the essence of the practitioners' views on the importance of the CSFs for SETA programme effectiveness. By comparing stage one and stage two 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 two 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 different 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, the researcher is aware that their efforts at qualitative data analysis (in stage one of this research) sets the agenda for the remaining stages. However, the similarity in perceived importance (for the majority) of the CSFs (between stage one and stage two) 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 research also presents an approach to evaluate the outputs of a multi-stage grounded (data-to-theory) study. For example, we use a *Request-For-Comment* approach to take the outputs from stage one and generate a comparative ranked order list to generate a new output in stage two. Finally, the 5 guiding principles emerge from the differences between the ranked order lists (in stage one and stage two). 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.

In the next section, the researcher provides a detailed description of the approach to data gathering and data analysis.

1.4.2 Data Gathering and Data Analysis

The data gathering procedures followed in this research project are approved by the Social Research and Ethics Committee (SREC) of University College Cork (see Appendix A).

Selecting appropriate data collection methods is fundamental to the success of a research study (Kothari, 2004). This research adopts the “key informant” approach for data gathering and engages with the key informants through semi-structured interviews. A key informant is an expert in a particular field who is highly experienced and knowledgeable (Kumar et al., 1993; Wengler et al.,

2006). Therefore, in this research study, key informants were selected based on their position, experience, and knowledge of IS/cyber security, particularly SETA programmes. The advantage of the key informant method is the ability to gain quality data in a short period through in-depth interviews (Barker et al., 2005).This helps the researcher to get a preliminary understanding of the research phenomena (Marshall, 1996; Cossham and Johanson, 2019).

Moreover, interviews are one of the most suitable techniques for gathering valuable data from experts (Marshall and Rossman, 1989). The semi-structured interview is suited to exploring new ideas, capturing new phenomena, and identifying the rich contextualised detail of complex concepts (Myers and Newman, 2007). There are two rounds applied to gathering the data. In round one, twenty 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), the USA, the UK, and Ireland. See Table 3 for an overview of the key informants. In round two, nine follow-up interviews were conducted with experts from the Middle East and Ireland to ask probing questions about some of the CSFs for SETA programme effectiveness.

Data analysis is a crucial step in qualitative research (Leech and Onwuegbuzie, 2008). The primary purpose of data analysis is to understand what is going on (c.f. Kawulich, 2004). Data analysis occurs during three phases: i) data are organised, ii) data are reduced through summarisation and categorising, and iii) themes in the data are identified and linked (c.f. Patton, 1990). This research adopts an inductive open, axial, and selective coding approach as part of our qualitative data analysis. See Figure 6 for a sample of our open coding and Figure 7 for a sample of our axial coding.

KI #	Country	Role	Sector	Experience (years)	Qualification (education / professional accreditation)
1	Saudi Arabia	IS security consultant	Education	> 12 years	PhD (Security Software Design)
2	Saudi Arabia	CISO (chief information officer)	Fintech	~ 8 years	BSc (Computing) CEH, CISSP
3	Saudi Arabia	Supervisor in the cybersecurity department	Education	10 years	PhD (Cyber Security Management) ISO27001
4	Kuwait	Cyber security leader	Oil & Gas	~ 22 years	PhD (Management & Operations) Cybersecurity Influencer
5	Lebanon	Governance and risk management compliance manager	Banking	10 years	BSc (Computer Information Systems) CISA, CISM, CRISC, CIPM
6	Qatar	Senior manager for governance risk and compliance	Telecommunications	12 years	MSc (Cyber Security) CISM, ISO27001
7	UAE	InfoSec training lead	IT Services (SME)	10 years	BSc (Computer Software Engineering)
8	UAE	Consultant in IS security	IT Services (SME)	> 17 years	MBA CISSP, ISO27001, CRISC
9	Saudi Arabia	CISO (chief information officer)	Petrochemicals & Chemicals	15 years	MSc (Information Security) ISOC
10	Kuwait	CISO (chief information officer	Oil & Energy	8 years	MSc (Computer Engineering)
11	USA	Consultant in IS security	Financial Services & Education	20 years	BSc (Computer Information Systems) Certified SANS Instructor
12	UK	CISO (chief information officer)	IT Services	~ 20 years	MSc (Information Security) CISSP, CISM, ISO27001
13	USA	Director for cyber leadership and strategy solutions	IT Services	25 years	MBA (Information Security Management) CISM
14	Kuwait	Head of information security governance	IT Services	20 years	MSc (Information Security) CISM, ISO270001
15	Saudi Arabia	Cyber security consultant	Computer & Network Security	10 years	PHD (Cyber Security) CISM
16	Egypt	Head of cyber security	Banking	20 years	MSc (Business Information Technology) C|CISO, CISM, CRISC, ISO27001
17	UK	Security Awareness Manager	Banking	15 years	MSc (Information Security & Privacy)
18	USA	Director of Security Awareness	Computer & Network Security	> 20 years	MBA Certified SANS Instructor
19	Ireland	Senior lecture in IS security	Education	17 years	PhD (IS Security Management)
20	Ireland	IT security officer	Education	21 years	MBA (Technology & Management)

Table 3.The key informants' current role, years of experience, country, industry sector, qualifications, and interview duration

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

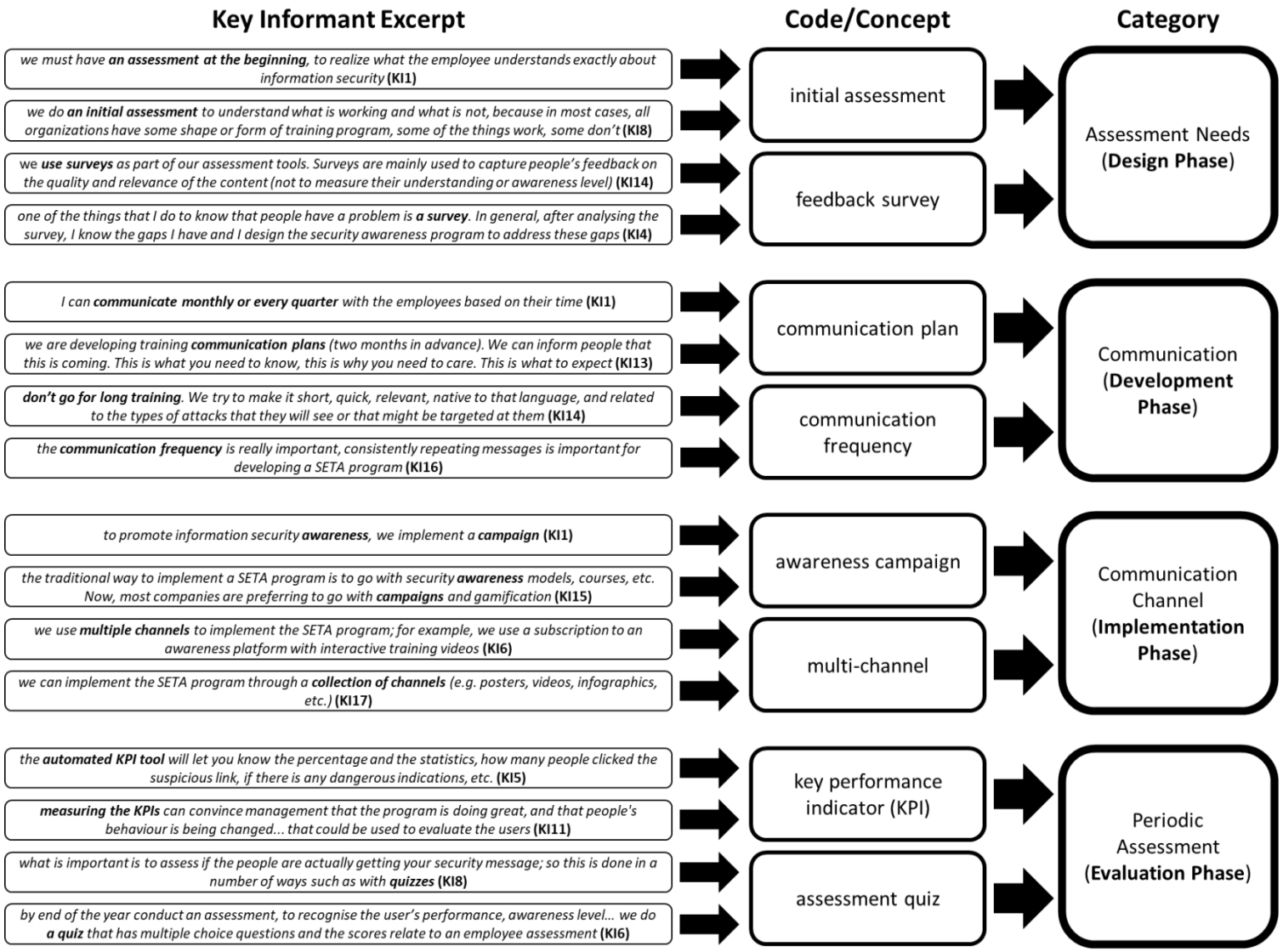


Figure 6. A Sample of Coding (a snapshot of the highest frequency categories across the four lifecycle phases)

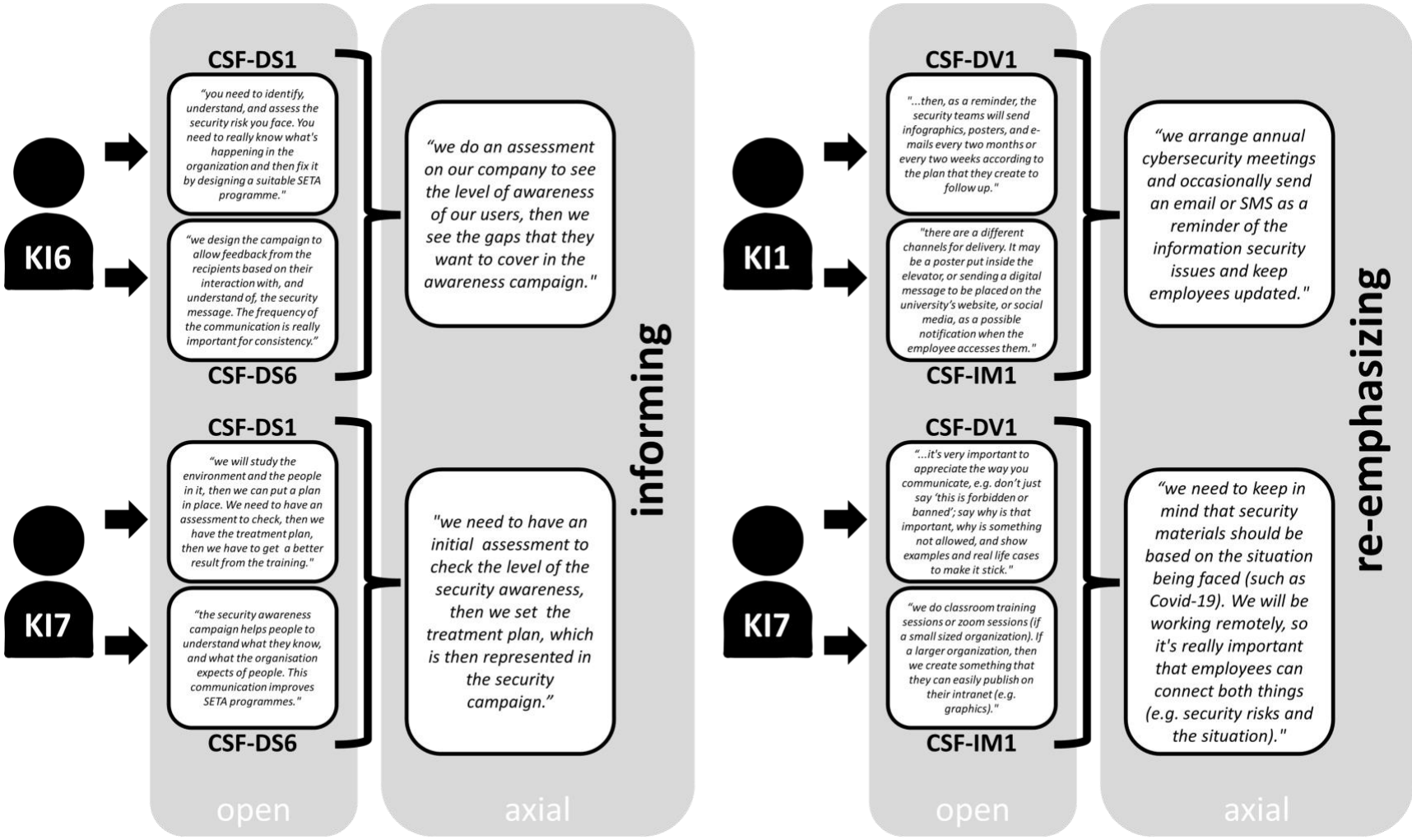


Figure 7. A Sample of our Axial Coding (a snapshot of the within phase and across phase CSF relationships.

1.5 Thesis Structure: Overview of the Chapters

This section presents an overview of the chapters that make up the main body of the thesis. The current chapter (Chapter One) and Chapter Six relate to the introduction and conclusion of the thesis, respectively. Chapter One introduces the research objective and questions, along with the research contributions. The thesis structure, along with a brief description of each paper, are also provided in this chapter. In Chapter Six, the research objective and research questions are revisited. The research conclusions, contributions, implications, limitations, and future research directions are also discussed. The remaining four chapters (Chapter Two to Chapter Five) each refer to a research paper drafted as part of the research study. The researcher now covers these four specific chapters within the following subsections.

1.5.1 Chapter Two

In the first paper, the researcher highlights the need for an *employee-centric* focus on SETA programmes. However, while the researcher does not provide any specific advice on how to achieve SETA programme effectiveness, a model which captures four key messages emerging from the IS/cyber security literature is presented. These messages point to the need for a focus on *awareness* and *behaviour* (at the individual/employee level) and *policy* and *management* (at the organisational level). Therefore, this paper provides the motivation for undertaking our empirical work and exploring the critical success factors (CSFs) for SETA programme effectiveness.

The paper that makes up this chapter is titled *"Placing SETA Programmes in IS Security Research: A Literature Analysis"*. This paper is currently under review (revision 1) in the CABS1 ranked journal: *Journal of Decision Systems*. Initial feedback on the paper from the four reviewers suggested that:

- *This paper is very well written* (R1).
- *The four themes are relevant and well-described* (R2).
- *The contribution and value of the work need to be stated much more clearly* (R3).
- *This is a well-written paper on a topic that is extremely relevant right now* (R4).

1.5.2 Chapter Three

In the second paper, the researcher reports on the first part of our empirical study. This involves presenting an analysis of the 20 key informant stories (based on their lived experiences). These key informants are IS/cyber security professionals with a range of experiences in SETA programme delivery. The output from this part of the empirical study leads to the emergence of 11 CSFs for SETA programme effectiveness. While a list of CSFs is presented in this paper, there is no detailed presentation of the CSFs against the phases of a SETA programme lifecycle. Therefore, this paper produces the inputs for the next paper, which looks at mapping these 11 CSFs to the phases of a SETA programme lifecycle.

The paper that makes up this chapter is titled *"The Critical Success Factors for Security Education, Training and Awareness (SETA) Programmes"*. This paper will soon be published by IEEE as part of the proceedings of the 1st Cyber Research Conference Ireland (CRCI) held in April 2022 in Galway, Ireland. This paper was awarded the **BEST PAPER AWARD** at the conference. This award (judged by an awards committee comprising of academics and practitioners) can be viewed as a peer-evaluation of the *relevance* and *utility* of the 11 CSFs for SETA programme effectiveness.

1.5.3 Chapter Four

In the third paper, the researcher presents a process model of the 11 CSFs across the SETA programme lifecycle (referred to as the Lifecycle Model). This model positions each CSF in one of the four phases (*design* (6 CSFs), *development* (1 CSF), *implementation* (2 CSFs), and *evaluation* (2 CSFs)). Furthermore, 9 relationships between these CSFs are also presented, with 4 being *within*-phase relationships and 5 being *across*-phase relationships. This Lifecycle Model highlights the nature of the CSFs and the need for a focused attention on all 11 CSFs. However, in this paper, the researcher does not present any evaluation of the *relevance* of the CSFs to a wider group of IS/cyber security professionals (beyond the 20 key informants).

The paper that makes up this chapter is titled *"The Critical Success Factors for Security Education, Training and Awareness (SETA) Programme Effectiveness: A Lifecycle Model".* This paper is

currently under review (revision 1) in the CABS3 ranked journal: *Information Technology & People*. Initial feedback on the paper from the three reviewers suggested that:

- *This paper presents an interesting approach to a topic worthy of further research* (R1).
- *The paper is generally well-written but lacking details in various places* (R2).
- *The paper is well-written and logically structured, and the quality of communication is very good. I enjoyed the discussion of this topic area and believe the results from this work can be of benefit to other researchers. The findings are presented well, and I found Figure 1 (Lifecycle Model) particularly useful and clear to present the CSFs* (R3).

1.5.4 Chapter Five

In the fourth paper, the researcher reports on the second part of our empirical study. This involves evaluating the *importance* of each CSF (based on the ranked list of mean scores). To progress this evaluation, 65 IS/cyber security professionals (independent of the 20 key informants) complete a short survey questionnaire, where they are asked to rank the importance of each CSF (*high-medium-low*) based on their experiences. Thereafter, the researcher compares the results (mean score rankings) between the two groups (20 key informants and 65 survey respondents). Our results show no significance difference in the ranked order between the two groups. However, based on *contradictions* in the perceived importance of 5 specific CSFs, the researcher conducted a series of follow-up probing interviews with 9 IS/cyber security professionals (4 key informants and 5 survey respondents). The outcome of this follow-up led to 5 guiding principles also being proposed to address potential challenges in delivering on these 5 CFSs and achieving SETA programme effectiveness.

The paper that makes up this chapter is titled *"Critical Success Factors for Security Education, Training and Awareness (SETA) Programme Effectiveness: An Empirical Comparison of Practitioner Perspectives".* This paper is currently under review (revision 1) in the CABS1 ranked journal: *Information and Computer Security*. Initial feedback on the paper from the two reviewers suggested that:

- *Readability (quality of communication) is at a good level* (R1).
- *This paper looks into CSFs for SETA programme effectiveness, which is something not previously widely researched* (R2).

1.6 Conclusions

This chapter presents the research motivation and establishes the main elements of the research by outlining the research objective and the three research questions while also summarising the main contributions of the study. It describes the research approach and summarises each chapter (as part of the thesis structure).

The remainder of this thesis includes a collection of papers that outline the research story, starting with a review of the literature (Chapter Two), Identifying the 11 CSFs for SETA programme effectiveness (Chapter Three), and providing a Lifecycle Model for SETA programme effectiveness and the relationships among them (Chapter 4), Evaluating the importance of the 11 CSFs for SETA programme effectiveness (Chapter Five). Finally, the thesis ends with a concluding chapter that presents a discussion and conclusion of the thesis (Chapter Six).

Chapter Two: Placing A SETA Programme in IS security Research: A Literature Analysis - (Paper 1)

Abstract

The objective of this paper is to identify the key message from each of four IS "security themes" (emerging from a review of 87 IS security research papers) and highlight their importance to an organisational SETA (Security Education, Training and Awareness) programme. The four IS "security themes" are IS Security Policy (ISP), IS Security Behaviour (ISB), IS Security Management (ISM), and IS Security Awareness (ISA). Based on our analysis, these four IS "security themes" represent a significantly large portion of all IS/cyber security research conversations taking place between 1992 and 2019. In concluding this paper, the researcher argues that for SETA programme effectiveness you need to be focused on 'increasing employee compliance' (ISP key message), 'changing employee attitudes' (ISB key message), 'improving employee practices' (ISM key message), and 'raising employee awareness' (ISA key message). The researcher *presents a simple conceptual model that captures these four key messages, as a decision aid for SETA programme effectiveness.*

Keywords: cybersecurity, SETA programme effectiveness, literature, open coding

2.1 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 $400 billion by 2027 (fortune.com, 2022). The devasting 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"* (fortune.com, 2022). Organisations use various strategies to safeguard their information assets against security threats. However, a Security Education, Training and Awareness (SETA) programme is one of the most prominent strategies used for controlling IS security threats and

protecting information assets. 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).

A previous review of 87 IS security research papers, published in top IS and IS Security journals (between 1992 and 2019), conducted by (***ref withheld for review purposes***), led to the emergence of 12 IS "security themes". These IS "security themes" capture the focus of the research activity throughout this 27-year period. Close on 70% of all the papers reviewed are published in five journals, namely: *Management Information Systems Quarterly* (20%), *Information Systems Journal* (13%), *Computers and Security* (13%), *Information and Management* (11%), and *Communications of the AIS* (10%). Furthermore, four IS "security themes" dominate the areas of research focus, namely: *IS Security Policy - ISP* (27%), *IS Security Behaviour - ISB* (17%), *IS Security Management - ISM* (17%), and *IS Security Awareness - ISA* (11%). As a result of this literature review work, these four IS "security themes" are viewed as being central to the IS/cyber security conversations taking place in organisations (accounting for 72% of all security research conversations analysed). There are synergies between these IS "security themes" with an aim of reducing IS security risks. For example, through raising employee awareness (ISA), increasing employee compliance (ISP), changing employee attitudes (ISB), and improving employee practices (ISM). Therefore, it can be argued that employees (*'who'*) are often presented with the *'what'*, *'when'*, *'where'*, *'why'*, and *'how'* of IS security, and this presentation is delivered through the rollout of a SETA programme. In fact, (***ref withheld for review purposes***) suggest that the IS "security themes" emerging from their literature analysis are linked to the purpose of a SETA programme, specifically mentioned alongside IS Security Awareness (ISA), as a means of raising employee awareness of IS security risks. Therefore, the researcher extends this further and argue that the four IS "security themes" (ISP, ISB, ISM, and ISA) are central to the design, development, implementation, and evaluation of an organisational SETA programme.

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). Therefore, SETA programme effectiveness is an organisational 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 organisations manage their approach to IS security on a continuous basis in an effort to cultivate a compliant culture amongst employees. Therefore, motivated by the questionable effectiveness of SETA programmes, the objective of this research is *to identify the key message from each of the four IS "security themes" and highlight their importance to an organisational SETA programme.* The researcher believes this work will benefit organisational decision makers in their efforts to deliver effective SETA programmes.

The remainder of this paper is organised as follows: Section 2 presents a background to SETA programmes; Section 3 presents the findings and discussion, organised around the four IS "security themes"; lastly, Section 4 presents the conclusions and contributions of the research, in the form of a decision aid for SETA programme effectiveness.

2.2 SETA Programmes

Cybersecurity 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 organisations 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, this aligns with the proposal of Haney and Lutters (2021, p.486), who argue the need for *"cybersecurity advocates"*, a resource *"which has a behaviour change focus and impact"*. They see this proposal as a concerted effort to change this *"status quo"* where *"people routinely fail to protect their digital assets"* (Haney and Lutters, 2021, p.485). Haney and Lutters (2021) describe these cybersecurity advocates *"as catalysts for cybersecurity adoption"* (p.485), and a *"people-*

oriented service profession" (p.486). Ultimately, cybersecurity advocates are *"security professionals for whom promoting, educating, and encouraging adoption of security are major components of their jobs"* (Haney and Lutters, 2021, p.485). Therefore, building a balance of technical and non-technical competencies in cybersecurity within organisations can be seen as critical to progressing the effectiveness of an organisational SETA programme.

Cybersecurity researchers *"consistently argue"* that organisations need SETA programmes *"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 security literature that *"the effectiveness of a security program requires ongoing voluntary compliance from employees"* (Pham et al, 2020, p.134). Therefore, the organisational challenge is to develop engaging SETA programmes *"to promote and maintain the requisite user behaviors to increase cybersecurity"* (Pham et al, 2020, 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 programmes. Furthermore, this sense of employee "security fatigue" comes at a significant organisational cost, where, despite significant investment in SETA programmes, 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 $12.1 billion by 2027, representing a compound annual growth rate (CAGR) of 45.6% from 2022 to 2027 (Global Market Estimates, 2022).

Several SETA programme definitions can be found in the literature (see Table 4). Despite their variability, they all hold the employee central in their focus. Notwithstanding this, existing research on SETA programmes 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 organisational SETA programmes to improve cybersecurity behaviour *"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 programmes *"succeed in producing positive outcomes remains unclear"* (Reeves, et al., 2021, p.1). Whether this is because of organisational security policy, security management frameworks, employee behaviour or employee awareness, or a multiplicative effect of all these areas, it is something that still needs to be unpacked.

SETA Programme Definition	**Reference**
"as an educational program that aims to reduce the number of accidental security breaches in the organisation by people who come into contact with information assets" (p.140).	Whitman and Mattord (2008)
"as the degree to which an organisation formally provides its employees with an awareness of what threats exist in the work environment, why these threats exist and how they can more securely engage in work activities" (p.204).	Lowry et al. (2015)
"the mechanisms by which organisations foster awareness, educate users as to the importance of security, and train insiders to effectively take on security roles" (p.3930).	Burns et al. (2015)
"an educational process by which employees fulfil the necessary conditions for information security at the organisation" (p.55).	Han et al. (2017)
"as an educational program that is designed to reduce security breaches that occur through a lack of employee security" (p.107).	Yoo et al. (2018)
"refer to organised information security training activities that are related to security training, and awareness raising of an organisation's employees" (p.3).	Alshaikh et al. (2019)
"as the ongoing effort to provide employees with security knowledge and skills, enable their deep understanding of why security protection is needed, and increase their awareness of security issues" (p.1).	Hu et al. (2021)

Table 4:SETA Programme Definitions

Therefore, based on our analysis of the literature, in the next section the researcher now explores the four IS "security themes" (ISP, ISB, ISM, and ISA) in order to identify the key message for each.

2.3 Findings and Discussion

In this section the researcher highlights the key message from each of the four IS "security themes" (ISP, ISB, ISM, and ISA) and discuss their importance to an organisational SETA programme.

2.3.1 IS Security Policy (ISP)

IS Security Policy (ISP) is a set of structured procedures, guidelines, roles, and responsibilities that employees must adhere to in order to protect the use of their organisation's information systems assets from external and internal threats (Lowry and Moody, 2015). Implementing ISP in

the organisation is important to protect the integrity and confidentiality of information, availability of services, and uninterrupted operation of business processes (Goel and Chengalur 2010). Also, ISP aims to secure organisational information systems assets by guiding employees on how to properly treat information resources and preventing data misuse and abuse (Ifinedo et al., 2014; Koohang etal.,2020). Table 5 presents a sample of our open coding from the ISP literature reviewed.

References	Excerpts	Category	Theme
Boss et al., 2015	"Also showed what could be considered mid-range relative importance in terms of predicting **security policy compliance**" (p.543).	Policy Compliance	IS Security Policy
Sikolia et al., 2018	"The severity of the penalty will positively affect the intention to **comply** with organisational information **security policies**" (p.3).		
Johnston et al., 2015	"Is based on the notion that computer abuse and IS misuse behaviors are directly related to a **failure of compliance** and thus constitute **security policy violations**" (p.118).	Non-Policy Compliance	
Warkentin and Willison, 2009	"They may introduce risk via passive **non-compliance** with **security policies**, laziness, sloppiness, poor training, or lack of motivation" (p.102).		

Table 5: Sample Open Coding for the ISP Security Theme

As stated earlier in the paper, research suggests that the majority of IS security breaches happen because the employee violates IS security policy (Hearth and Rao, 2009; Kolkowska et al., 2017; Siponen et al., 2014). Therefore, in the literature, numerous studies focus on two sides of the same policy coin, namely: *compliance* and n*on-compliance*. In fact, one of the key issues in IS security is organisational employees not complying with IS security policy. Non-compliance, where employees fail to follow the security policy of their organisation, causes serious security problems (Puhakainen and Siponen, 2010; Herath et al., 2018; Li et al., 2019) and numerous studies have used various approaches to analyse employee non-compliance with IS security policy (c.f. Barlow et al., 2018; Guo and Yuan, 2012; Kolkowska et al., 2017; Vance et al., 2015; Siponen and Vance, 2010). For example, Siponen and Vance (2010) studied neutralisation and deterrence theory as a model to overcome the issues of policy compliance; they found the influence of organisational

sanction was minimised when the employees used neutralisation techniques to justify their behaviour. Guo and Yuan (2012) investigated the indirect influence of organisational sanctions through personal self- and workgroup- sanctions, which help to prevent employee violation of IS security policy. Another approach has used the accountability theory to decrease access-policy violations (Vance et al., 2015).

Several researchers recommend a SETA programme approach as a deterrence method to reduce IS security violations caused by employee non-compliance with the organisation's IS security policy (c.f. Posey et al., 2014; Herath et al., 2018). For example, Posey et al. (2014) state that one of the primary functions of the SETA programme is to detail potential sanctions imposed by the organisation for security policy violations. Thus, when the employee recognises the possible penalties, it minimises the violations of IS security policy. The SETA programme plays an effective role in reducing employee non-compliance with the organisation's IS security policy.

While there is limited research investigating the role of SETA programmes in minimising employee non-compliance with ISP (Li et al., 2019), there is a wide range of studies focusing on theoretical perspectives around developing employee compliance with ISP (Herath and Rao, 2009; Bulgurcu et al., 2010; Chen et al., 2018; D'Arcy & Lowry, 2017; Ifinedo, 2014; Puhakainen & Siponen, 2010; Siponen & Vance, 2010). For example, Herath and Rao (2009) developed a model that integrated protection motivation theory and deterrence theory to understand the factors that influence employees to comply with security policy. While Bulgurcu et al. (2010) proposed an ISP compliance model that included variables such as self-efficacy to consider the vulnerability of resources and awareness. Furthermore, the literature addresses various approaches that advocate compliance with IS security policy through using a rewards system (Siponen et al., 2014; Cram et al., 2019) or a formal sanction (penalties for IS security violations) (Pahnila et al., 2007; Chen et al., 2018) to address employee adherence to ISP.

There is support in the literature that a SETA programme can increase employee compliance and minimise ISP violations (Barlow et al., 2018; Peltier, 2005; Lowry and Moody, 2015). For example, a SETA programme is a key mechanism to improve ISP compliance through reminding employees of their security policy responsibilities (Herath et al., 2018). However, it is also

suggested that more research is needed regarding the role of specific SETA programme techniques to increase employee compliance with IS security policy (Barlow et al., 2018; Cram et al., 2019; Puhakainen & Siponen, 2010).

To conclude this section, following a review of the literature categorised as the ISP "security theme", it is clearer that SETA programme effectiveness can be achieved by the programmes ability to increase employee compliance, thereby meeting the ISP key message.

2.3.2 IS Security Behaviour (ISB)

IS Security Behavior (ISB) focuses on individuals' behaviour, relating to protecting information systems assets (Crossler et al., 2013). ISB aims at improving employee attitudes, intentions and beliefs to reduce IS security risks due to the fact that the majority of IS security breaches are caused by employees (Warkentin and Willison, 2009; Mahmood et al., 2010; Wang et al., 2019). Table 6 presents a sample of our open coding from the ISB literature reviewed.

References	Excerpts	Category	Theme
Padayachee, 2012	"Information **security behavior** refers to a set of core information security activities that have to be adhered to by end-users to maintain information security" (p.1).	Security Behaviour	IS Security Behaviour
Johnson, 2006	"Establishment of a security education training and awareness programme that fulfils this task and monitors employees' **security behaviour**" (p.354).		
Alshaikh et al., 2018	"Discusses the security awareness programme that leads to security **positive behaviour** as a key factor" (p.68).	Compliance Behaviour	
Bulgurcu et al., 2010	"Provides guidance to information security practitioners about what outcomes can be manipulated to influence employees' **compliance behavior**" (p.530).		

Table 6. Sample Open Coding for the ISB Security Theme

A number of studies have used various theoretical perspectives to better understand how to improve employee behaviour in order to reduce IS security risks (Bulgurcu et al., 2010; D'Arcy

and Herath, 2011; Boss et al., 2015). For example, General Deterrence Theory (GDT), one of the most widely applied theories in IS security research, is particularly used within behavioural IS security research to investigate human behaviour as related to the concept of 'computer criminal intent' (Bulgurcu et al., 2010; D'Arcy & Herath, 2011; Willison and Warkentin, 2013; Warkentin and Siponen, 2015). Adapted Protection Motivation Theory (PMT), another leading theoretical foundation, has been used in IS security research, motivating individuals to adopt behavioural security. In addition, to protect the Information Systems assets of the organisation; a multitude of approaches can be applied from PMT theory. For example, 'fear appeals' research has frequently focused on PMT (Boss et al., 2015), where *"persuasive messages designed to scare people by describing the terrible things that will happen to them if they do not do what the message recommends"* (Witte, 1992, p.329).

Beyond these studies that investigate behavioural factors, they can also influence IS security compliance (Barlow et al., 2018; Crossler et al., 2013; Li et al., 2019; Padayachee, 2012; Willison and Warkentin, 2013). Compliant IS security behaviour refers to *"a set of core information security activities that have to be adhered to by end-users to maintain information security"* (Padayachee, 2012, p.1). The major variables used to identify compliant IS security behaviour include social norms, self-efficacy, response efficacy, response cost, perceived severity of sanctions and perceived certainty of sanctions (Li et al., 2019). Furthermore, there is yet another IS security research stream that concentrates on behavioural non-compliance (Bulgurcu et al., 2010; Djajadikerta et al., 2015; Willison & Warkentin, 2013).

Based on our analysis the researcher observed that several studies have been published regarding managing employee security behaviour in order to reduce insider risks, such as establishing a SETA programme (Karjalainen and Siponen, 2011; Pham et al., 2019; Dupuis et al., 2019). For example, the adoption of educational games (e.g. gamification principles) in SETA programmes enhances the employee IS security knowledge, motivations, and behaviours (Silic and Lowry, 2020; Hwang and Helser, 2021). Additionally, other studies examine how SETA programmes affect employee behaviour (Jansen and Van Schaik, 2018; Yaokumah et al., 2019). Despite this, a number of studies also show that further investigation is critical for understanding human behaviour, particularly the factors that influence security-compliant or noncompliant behaviour,

in order to have an effective SETA programme (Lebek et al., 2014; Pham et al., 2019). Therefore, ISB presents many opportunities to explore issues at the intersection of individuals, information systems, and organisations toward an effective SETA programme (Boss et al., 2015).

To conclude this section, following a review of the literature categorised as the ISB "security theme", it is clearer that SETA programme effectiveness can be achieved by the programmes ability to change employee attitudes, thereby meeting the ISB key message.

2.3.3 IS Security Management (ISM)

Information Security Management (ISM) is referred to as a series of processes through which organisational data is systematically collected, evaluated, and classified with an aim of identifying the optimal strategy, tactical and operational, to protect the organisation's information systems assets (Choobineh et al., 2007; Keller et al., 2005). The goal of ISM is to reduce damage to organisational information systems assets by preventing and controlling security problems caused by unexpected interruptions and cyber-attacks (Kim et al., 2015). However, several researchers argue that there is still a shortage of theoretical conceptualisations in ISM research, for example, threats and vulnerabilities, and the factors that influence security management (Siponen and Baskerville, 2018; Topa and Karyda, 2019).

Many organisations focus on protecting their information systems assets by applying a security standard framework for security best practice and control (Flores et al., 2014; Topa and Karyda, 2019). Two such security standards include those published by the National Institute of Standards and Technology (NIST) and the International Organisation for Standardisation (ISO). For example, the **NIST** 800-30 framework provides security managers with risk management perspective, describing the steps they should take to identify risks, apply controls, and improve security. While **ISO** information security standards guide security managers on how to design and implement practices towards establishing and proposing security controls (Stoneburner et al., 2002; Lambrinoudakis, 2013). Indeed, the ISO27K series comprises of information security standards that provide best practice recommendations on ISM (e.g. security risks managed through security controls). For example, the international standard for ISM is ISO/IEC 27001 and is

recognised as providing the *"de facto guidelines"* for best practice ISM (Almeida and Respício, 2018, p.174). This ISM standard demands that controls and processes (systematic approach) are in place, to mitigate against organisational security risks, by helping to safeguard both the information systems assets and employees. In fact, achieving certification under ISO/IEC 27001 demands that the organisation's Information Security Management System (ISMS) can be audited (Almeida and Respício, 2018, p.174). Table 7 presents a sample of our open coding from the ISM literature reviewed.

References	Excerpts	Category	Theme
Siponen and Baskerville, 2018	"One of the more notable **standards** for **ISS management** is… an ISO standard for ISS management known as… ISO/IEC 27002" (p.245).	Security Management Standards	IS Security Management
Backhouse et al., 2006	"The BOC Group intended to use this document as the internal mechanism for **standardising security management**" (p.420).		
Hu et al., 2012	"The effectiveness of balanced and comprehensive information **security management** programs" (p.650).	Security Management	
	"Information **security management** initiatives, such as training programs that are designed based on such theoretical understanding" (p.648).		
D'Arcy et al., 2009	"Effective IS **security management** should aim to maximise the number of deterred and prevented abusive acts" (p.81).		

Table 7. Sample Open Coding for the ISM Security Theme

Moreover, in the literature, studies focus on two thematic areas of ISM: employee (*micro* level) and organisational (*macro* level). Studies in ISM approaches at the *micro* level aim to establish why end-users get involved in risky behaviour (Bulgurcu et al., 2010; Babatunde and Selamat, 2012; Flores et al., 2014). For example, Flores et al. (2014) state that ISM has been over reliant on technical control measures, while most IS security failures occur due to the violation of controls by individuals. Therefore, understanding how to manage employee attitudes will help to reduce the incidents of Information Systems assets misuse. Another study by Babatunde and Selamat (2012) examined how factors such as standards, policies, awareness, training programmes, cultures, employee motivation, and top management commitment effect ISM development and

performance. Understanding these various aspects of ISM contribute to the control of IS security risks and cyber-attacks. Other studies in ISM approaches focus on the *macro* level to establish which organisational factors contribute to effective holistic information systems security management (Choobineh et al., 2007; Kritzinger and Smith, 2008; Siponen and Willison, 2009; Puhakainen and Siponen, 2010). For example, Kritzinger and Smith (2008) argue that ISM should ensure the security of information through proactive management of information security risk. While Siponen and Baskerville (2018) argue that ISM security standards (e.g. ISO/IEC 27002) intend to capture best practice in problem solving.

However, several studies highlight the role of SETA programmes in effective ISM. For example, Whitman (2004) proposes three aspects for effective ISM: a comprehensive policy; existence of security control mechanisms; and an awareness and training programme. Therefore, this highlights the responsibility of those in management responsible for establishing a SETA programme, one which can deliver a holistic approach to IS security to make the organisation more secure. Additionally, the adoption of a security standards frameworks also improves practices around the SETA programme itself (D'Arcy et al, 2009; Topa and Karyda, 2019). For example, Topa and Karyda (2019) investigate the effect of IS security standards (e.g. ISO27K) on a SETA programme, where the standards offer guidance for security management practice that is integrated into the SETA programme to promote security knowledge.

To conclude this section, following a review of the literature categorised as the ISM "security theme", it is clearer that SETA programme effectiveness can be achieved by the programmes ability to improve employee practices, thereby meeting the ISM key message.

2.3.4 IS Security Awareness (ISA)

The most cited definition of IS Security Awareness (ISA) in the literature is by Hu et al. (2007), where they define ISA as an employee's overall knowledge and understanding of potential issues related to information security risks and their ramifications. However, others (D'Arcy et al., 2009; Tsohou et al., 2008) suggest that there is no clear definition of ISA in the literature. ISA aims to reduce human error, theft, accidents, carelessness, and misuse of Information Systems assets by

individuals (Tsohou et al. 2008; Lebek et al., 2014). Table 8 presents a sample of our open coding from the ISA literature reviewed.

Reference	Excerpt	Concept	Category
Kritzinger and Smith, 2008	"Information **security awareness** is about ensuring that all employees in an organisation are aware of their role and responsibility" (p.225).	Security Awareness	IS Security Awareness
Barlow et al., 2018	"Despite the widespread use of SETA programs that are designed to increase **awareness of security** policies and often emphasise the sanctions for violations" (p.690).		
Li et al., 2019	"Train and assist them in creating a shared vision and goals through dedicated information security **awareness campaigns**" (p.351).	Awareness Campaigns	
Tsohou et al., 2008	"A general **awareness campaign** has little effect alone on user behaviour and awareness" (p.19).		

Table 8. Sample Open Coding for the ISA Security Theme

It is worth mentioning, that there is a shortage of empirical studies that support the benefit of SETA programmes in reducing IS risks (D'Arcy et al., 2009; Karjalainen & Siponen, 2011; Tsohou et al., 2015). Notwithstanding this, the literature emphasises the importance of focusing on ISA in organisations, in order to make employees conscious of the risks related to IS security and educate them on the roles and responsibilities surrounding the misuse of Information Systems assets (Bulgurcu et al., 2010; Lebek et al., 2014; Tsohou et al., 2015; Koohang et al., 2020). For example, Bulgurcu et al. (2010) studied the impact of ISA on beliefs and attitudes toward compliance with IS security policy (ISP). They found that ISA plays a key role in employee compliance behaviour. Thus, increasing the focus on ISA encourages favourable attitudes and behaviours regarding IS security, which helps to change individual behaviour (Tsohou et al., 2008).

D'Arcy et al. (2009) proposed that the organisation can use three security countermeasures (to reduce IS asset misuse): (i) user awareness of security policies; (ii) security education, training, and awareness (SETA) programmes; and (iii) computer monitoring. Thus, the security countermeasures influence the organisation's sanctions, leading to reduced IS misuse intention.

Moreover, several studies discuss the effect of SETA programmes on ISA to reduce IS security threats. For example, Barlow et al. (2018) studied three theory-based (informational-normative-anti-neutralisation) communication approaches, that integrate into SETA programmes, aiming to increase compliance behaviour in order to reduce IS security threats.

Other studies argue that SETA programmes play a significant role in raising employee awareness of IS security issues (Heikka, 2008; Siponen et al., 2009; Lebek et al., 2014; Tsohou et al., 2015). For example, Siponen et al. (2009) state that a SETA programme helps employees to be more aware and improve their knowledge of IS security issues. They are also, raising the employee's awareness of their organisation's vulnerability because of IS security threats. Tsohou et al. (2015) developed a theoretical framework to address how SETA programmes improve security concerns among individuals. They contend the SETA programme has a positive influence on employee ISA levels. Furthermore, several researchers recommend implementing security awareness campaigns to promote IS security awareness in the organisation. Therefore, the significance of awareness campaigns is growing in a cybersecurity culture and is a widely recognised part of a SETA programme (Siponen, 2000; Reid and Van Niekerk, 2016).

To conclude this section, following a review of the literature categorised as the ISA "security theme", it is clearer that SETA programme effectiveness can be achieved by the programmes ability to raise employee awareness, thereby meeting the ISA key message.

2.4 Conclusions

Despite the fact that there is a growing volume of research around SETA programmes, there is still limited research of *"practical value"* available on *"organisational strategies to improve"* SETA programmes, with recommendations to guide the development of SETA programmes being *"fragmented and dispersed"* and not cumulative in nature (Alshaikh *et al.*, 2021, p. 3). Furthermore, based on our analysis of the literature, there is still a shortage of evidence supporting the fact that launching a SETA programme will:

1. promote security policy compliance (e.g. through motivation and rewards systems),
2. improve employee security behaviour (e.g., through penalties for violations),
3. influence the management of security risks (e.g., through security standards), and

4. raise the level of security awareness (e.g., through awareness campaign communications).

This suggests that the key message from each of the four IS "security themes" (ISP, ISB, ISM, and ISA) are not being adequately addressed by organisational SETA programmes. Therefore, more needs to be done to address the effectiveness of SETA programmes. For example, understanding the Critical Success Factors (CSFs) for SETA programme effectiveness along the SETA programme lifecycle phases (design, development, implementation, evaluation) would be very beneficial for organisational decision makers in support of their delivery efforts. 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). However, to date, little or no research has documented the CSFs for SETA programme effectiveness, especially since the effectiveness of SETA programmes is routinely called into question (***ref withheld for review purposes***).

In this paper the researcher has presented our process (theorising) in order to avoid *"'black boxing' the process of discovery"* (Hammond, 2018, p.3). In this work, theorising is about focusing on what is important and *"abstracting something from the data in order to explain what is happening"* (Hammond, 2018, p.4). Through identifying the key message across the four IS "security themes", the researcher presents a conceptual model (see Figure 8) for SETA programme effectiveness. This model is the *"product of a long engagement with data"* (Hammond, 2018, p.5). Therefore, theorising on the patterns the researcher has observed in this literature analysis, it could be argued across the four IS "security themes" (ISP, ISB, ISM, and ISA) that:

- without an explicit focus on organisational sanctions (c.f. Guo and Yuan, 2012; Johnston et al., 2015), employee motivation (c.f. Li et al., 2014; Sikolia et al., 2018), and employee rewards (c.f. Boss et al., 2015; Kirova and Baumöl, 2018), it is unlikely that a SETA programme will be effective when it comes to IS Security Policy (**ISP**).
- without applying a penalty (c.f. Siponen et al., 2014; Chen et al., 2018) it is unlikely that a SETA programme will be effective when it comes to IS Security Behaviour (**ISB**) as the employee may not be concerned with the impact of not following proper practices.
- without top management responsibility for budget and standards (Tsohou et al., 2008) it is unlikely that a SETA programme will be effective when it comes to IS Security Management (**ISM**).

- without up-to-date communication of IS security issues (security awareness campaign) to raise employee awareness (Barlow, et al., 2018) it is unlikely that a SETA programme will be effective when it comes to IS Security Awareness (**ISA**).

In terms of practical advice emerging from this literature analysis, to deliver an effective SETA programme, the following can be argued: the SETA programme must be aligned with the key message from each of the four IS "security themes" (ISP, ISB, ISM, and ISA). See Figure 1 for a visual of this alignment. In fact, SETA programmes and their effectiveness typically links to addressing each one of the four IS "security themes". For example, compliance with IS policy (Han et al.,2017; Barlow et al.,2018; Dhillon et al.,2020), changing behaviours (Posey et al.,2013; Yaokumah et al.,2019; Alshaikh et al.,2019), increasing the level of awareness (Heikka ,2008; Lebek et al., 2014; Tsohou et al., 2015), and managing IS security risks (Chander et al., 2013; Kumah et al., 2019; Topa and Karyda 2019). Therefore, the researcher argues that for SETA programme effectiveness you need to be focused on increasing employee compliance (ISP key message), changing employee attitudes (ISB key message), improving employee practices (ISM key message), and raising employee awareness (ISA key message). Ultimately, organisations need employees to buy-in to these 4 key messages. Therefore, articulating IS "security themes" can assist in making effective decisions and reducing cybersecurity risks faced by organisations.

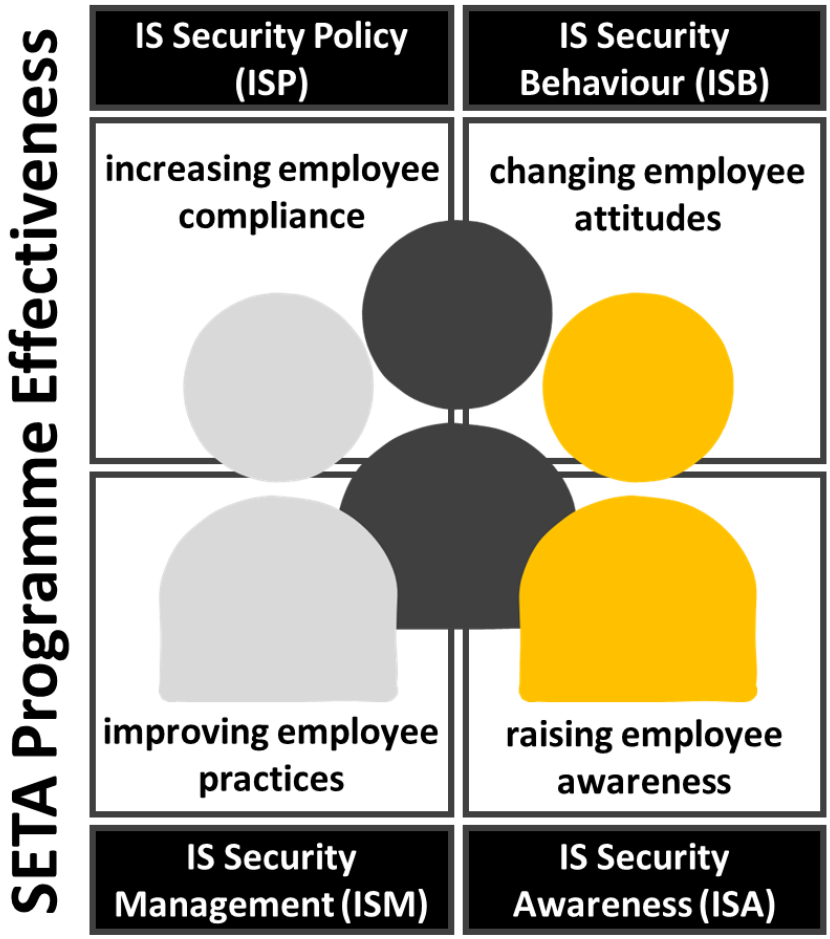


Figure 8. IS "Security Themes" Key Messages for SETA Programme Effectiveness

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 (e.g. *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 programme within an organisational context.

Chapter Three: The Critical Success Factors for Security Education, Training and Awareness (SETA) Programme Effectiveness - (Paper 2)

Abstract

This study explores the Critical Success Factors (CSFs) for Security Education, Training and Awareness (SETA) programmes. 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 produces eleven CSFs for SETA programmes. These CSFs are mapped along the phases of a SETA programme lifecycle (design, development, implementation, evaluation).

Keywords

SETA; Security; CSFs; Key Informant

3.1 Introduction

One of the most vital and prominent approaches to managing IS security risks and safeguarding IS and information assets in an organisation is its Security Education, Training, and Awareness (SETA) programme. Many researchers recommend establishing a SETA programme as part of the organisation's overall security strategy (Alshaikh et al, 2018; Kirova and Baumöl, 2018; Tsohou et al., 2015; D'Arcy et al., 2009). In the literature, the SETA programme is also referred to as IS security training (Parrish and San Nicolas, 2012; Karjalainen and Siponen; Heikka, 2008), and an IS awareness programme (Bauer et al., 2017; Tsohou et al., 2015). Peltier, 2005). The importance of SETA programmes has received significant academic attention: various studies discuss the use of a SETA programme to improve employees' behaviour (Alshaikh et al., 2019; Bulgurcu et al., 2010; Mahmood et al., 2010), to comply with IS policy (Cram et al., 2019; Barlow et al., 2018; Puhakainen and Siponen, 2010), and to increase the level of awareness and reduce IS security risks (Tsohou et al., 2015; Karjalainen and Siponen, 2011; D'Arcy et al., 2009).

Despite the prominence of SETA programmes for organisational IS/cyber security governance *"only a small portion of practitioners"* claim that their SETA programmes are *"very effective"* (Hu *et al.*, 2021a, p.1). It is reported that poor SETA programme effectiveness is linked to the

programmes failure to achieve its goal of impacting positively on employee security-related behaviours (Alshaikh *et al.*, 2021; Hu *et al.*, 2021a; 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.*, 2021a, 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.*, 2021b; Kirova and Baumöl, 2018; Puhakainen and Siponen, 2010). This paper sets out to address this research need ***"to explore the Critical Success Factors (CSFs) for Security Education, Training and Awareness (SETA) programme effectiveness"***.

The paper is organised as follows: Section 2 presents a background to SETA programmes. Section 3 describes the methodology: the data gathering and the data analysis techniques. Section 4 presents the findings: the CSFs for SETA programmes. Lastly, section 5 presents the conclusion and the plan for future research.

3.2 A SETA Programme Background

The Security Education, Training and Awareness (SETA) programme is an educational process designed to reduce the number of accidental security breaches that occur due to a lack of employee 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 existing literature distinguishes between education, training, and awareness terminologies based on their specific aim and target. For example, Whitman and Mattord (2008) propose that the aim of 'education' is for security experts to gain a deep knowledge regarding the design and implementation of a SETA programme; 'training' helps employees to acquire a level of skill that enables them to perform their job securely; and 'awareness' encompasses the delivery of information and informal training to employees to increase their awareness of potential risks and IS security issues. Therefore, the significance of SETA programmes is widely accepted by both academics and practitioners (Wilson and Hash, 2003; D'Arcy *et al.*, 2009; Tsohou *et al*., 2015; Alshaikh *et al*., 2018). Based on a review of the literature, SETA programmes typically address the following:

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

In fact, there is a stream of research that examines SETA programmes by focusing on an individual employee (micro-level) analysis and explores the factors that affect security behaviour directly or indirectly. This then allows exploration of the factors that influence security-compliant behaviour (Burns *et al*., 2015; Alshaikh *et al*., 2019). Another research stream focuses on the individual but also identifies organisational-level factors that influence information security compliance policies (Chen *et al*., 2015; Lowry *et al*., 2015; Burns *et al*., 2018). A third stream focuses on an organisational level (macro-level) analysis, providing directions for the design and implementation of awareness programmes, change of information security strategy, power relations, and allocation of responsibilities (Straub and Willke, 1998; Peltier, 2005; Puhakainen and Siponen, 2010; Karjalainen and Siponen, 2011; Tsohou *et al*.,2015).

However, research is still required on the design, development, implementation, and evaluation phases of SETA programmes (Alyami *et al.,* 2020; Alshaikh *et al.,* 2018). For example, where empirical studies investigating the effectiveness of SETA programmes exist, they fail to examine all phases of the SETA programme lifecycle (design, development, implementation, evaluation), tending to focus more on one or two of the lifecycle phases. For example, Puhakainen and Siponen (2010) propose a method to **design** an information security awareness programme, while Okenyi and Owens (2007) identify four factors that contribute to the **development** of a successful SETA programme. Furthermore, Silic and Lowry (2020) report on the use of an IT artefact (a gamified security training system) enabling a SETA programme **implementation**, while Rantos *et al.* (2012) provide a methodology to assist organisations in the **evaluation** of their awareness programme efforts.

Leveraging the SETA programme lifecycle phases (design, development, implementation, evaluation), the researcher now explores the CSFs for SETA programmes. Each one of these CSFs

is mapped to the relevant lifecycle phase. This mapping produces 11 CSFs for SETA programmes. In the next section, the researcher presents further details on our research methodology.

3.3 Research Methodology

To fulfil the research objective, 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. The CSFs for SETA programmes are the outcome of this exploratory research approach.

3.3.1 Data Gathering

In this research, the researcher adopts 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); (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 programmes.

Interviews are one of the most suitable techniques for gathering valuable data from experts (Marshall and Rossman, 1989). The semi-structured interview is suited to exploring new ideas, capturing new phenomena, and identifying the rich contextualised detail of complex concepts. Twenty 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 9 provides a list of the key informants' positions, years of experience and interview duration.

KI #	Country	Role	Experience (years)	Interview duration (minutes)
1	Saudi Arabia	IS security consultant	> 12 years	60
2	Saudi Arabia	CISO (chief information officer)	~ 8 years	45
3	Saudi Arabia	Supervisor in the cybersecurity department	10 years	55
4	Kuwait	Cyber security leader	~ 22 years	60
5	Lebanon	Governance and risk management compliance manager	10 years	40
6	Qatar	Senior manager for governance risk and compliance	12 years	45
7	UAE	InfoSec training lead	10 years	40
8	UAE	Consultant in IS security	> 17 years	50
9	Saudi Arabia	CISO (chief information officer)	15 years	55
10	Kuwait	CISO (chief information officer	8 years	40
11	USA	Consultant in IS security	20 years	60
12	UK	CISO (chief information officer)	~ 20 years	55
13	USA	Director for cyber leadership and strategy solutions	25 years	45
14	Kuwait	Head of information security governance	20 years	50
15	Saudi Arabia	Cyber security consultant	10 years	60
16	Egypt	Head of cyber security	20 years	55
17	UK	Security Awareness Manager	15 years	50
18	USA	Director of Security Awareness	> 20 years	45
19	Ireland	Senior lecture in IS security	17 years	45
20	Ireland	IT security officer	21 years	50

Table 9. The key informants' positions, years of experience, and interview duration

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 CSFs for SETA programmes, throughout the lifecycle phases (design, development, implementation, evaluation), were discussed. The interviews were conducted in two languages, some in Arabic and some in English, and the Arabic interviews were translated into English also. 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.

3.3.2 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 the researcher adopted an inductive open coding approach as part of our qualitative data analysis. This coding technique is aimed at generating concepts from field data (Walsham, 2006) and according to Strauss and Corbin (1990, p.61) open coding is defined as *"the process of breaking down, examining, comparing, conceptualising, and categorising data"*. Moving through the open coding process afforded us the opportunity to identify the concepts or key ideas hidden within the key informant interview data and related to the phenomenon of interest (c.f. Bhattacherjee, 2012). As part of our open coding, the researcher also grouped similar concepts into higher-order, more abstract concepts, called categories.

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 4 SETA programme lifecycle phases. 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; **evaluation** phase – 40 codes – 3 categories. Thereafter, unpacking the categories with at least five key informant voices (25% coverage) led to the emergence of the 11 CSFs for SETA programmes. The next section discusses the research findings.

3.4 Findings: The CSFs For SETA Programme

Critical Success Factors (CSFs) are defined as *"key areas where things must go right in order to successfully achieve objectives and goal"* (Bullen and Rockart, 1981, p.9). CSFs have been widely researched, debated, and cited across a wide range of information systems (IS) topics, which accounts for their continuing popularity. In essence, their simplicity, as a statement of focus and

action, is their most valued characteristic. Given the purpose of this study, the remaining sections present the CSFs for SETA programmes.

3.4.1 CSF-DS1: Conduct an Initial Assessment of Employee Security Awareness

This CSF highlights the fact that conducting an initial assessment is an essential factor in designing a SETA programme. 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, 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 mentions *"completing a test on IS security to realise what the employee understands exactly about information security"* while another informant 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 organisation 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: *"each level has a specific security awareness programme regarding cybersecurity".* Therefore, this CSF emphasises that identifying the current level of understanding around cybersecurity issues, as part of the design phase of a SETA programme lifecycle, will increase the likelihood of successful SETA programme outcomes.

In comparing these findings with those presented in the literature, a number of observations can be made. Several studies have called out the importance of understanding the need to establish a SETA programme and identify the security awareness plan that addresses employee needs (Alshaikh et al., 2018; Puhakainen and Siponen, 2010; Vroom and von Solms, 2002). In fact, Peltier (2005) suggests that when organisations use assessments to determine what the expected threats are and what the associated risk level of these threats is, then the information needed to protect the organisation is provided. The outcome of the assessments helps to determine the needs that must be covered. This kind of assessment assists in designing an appropriate SETA programme and makes it easier to prioritise the design to meet a specific need (Okenyi and Owens, 2007). As a result, this step is crucial to show the current position of the organisation with regard to security reports, previous incident attacks and previous threat responses.

3.4.2 CSF-DS2: Know Your Audiences to Ensure Content Suitability

This CSF highlights the importance of allocating the appropriate privileges to employees, using their organisational role to determine their security responsibilities. Identifying "who your audiences are" is critical in designing a SETA programme to ensure content suitability. Within this research study, key informants explain how most organisations set up a SETA programme 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 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 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 organisation has specific responsibilities such that the requisite IS security training needs are different.

In comparing these findings with those presented in the literature, Pelter (2005) discusses establishing a security awareness programme by classifying the audience to ensure the security message is communicated effectively. Accordingly, a SETA programme must comprise a plan to transmit the IS security message to the target audience (De Maeyer, 2007; Siponen, 2000). It can be argued that identifying the target audiences in designing a SETA programme is the main step toward its success; thereby delivering particular security training, with appropriately suitable material, to each employee.

3.4.3 CSF-DS3: Make a Yearly Plan to Align Goals and Objectives

This CSF highlights the importance of communicating the SETA programme objectives (knowing what is required to be delivered) clearly and consistently to the employees. It is also important to ensure that the SETA programme goals meet the specific needs of the organisation (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 programme based on the activities it wants to achieve. For example, one key informant

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 organisations update their objectives regarding the SETA programme. Another key informant commented: *"…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 organisations should create a plan for designing a SETA programme and that plan should contain what is necessary to be delivered, such as the types of IS security issues or topics.

In comparing these findings with those presented in the literature, several observations can be made around tailoring SETA programmes to meet specific organisational needs. For example, Rantos and Manifavas (2012) discuss methods to create an effective awareness programme. One of those methods is based on planning around the specific needs (e.g., materials to cover on the security awareness programme) to meet the organisation's goals. Other studies mentioned that identifying the objectives is the initial step when establishing a SETA programme (Peltier, 2005; Hansche, 2001). Most organisations initiate the design of the SETA programme with specific goals in mind. For example, a plan and new security policies to address any ongoing challenges (from years previous) and to ensure the delivery of a successful SETA programme. Therefore, to establish the SETA programme, one must have a clear goal that supports the organisation's overall mission.

3.4.4 CSF-DS4: Design for Cultural Context and Employee Cultural Diversity

This CSF focuses on the criticality of understanding the cultural diversity in the organisation when designing a SETA programme, 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 programme, such as: language, knowledge, level of education, age, and gender. All these aspects contribute to a successful SETA programme 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

organisation's employees, then these differentiations would need to be considered when designing a SETA programme. For example, the cultures of Saudi Arabia, Egypt, and UAE care more about language, and as a result use artefacts for SETA programmes, such as videos and posters in Arabic, to make the message more attractive and easier to understand. As stated by one key informant: *"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 programme. As commented by key informant: *"...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 programme.

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 security practice. For example, Hovav and D'Arcy (2012) examine the influence of the culture on the IS security policies, training, and monitoring. In fact, to understand culture in terms of IS 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 security interventions (Kirova and Baumöl et al., 2018; Karjalainen et al., 2013; Von Solms and Von Solms, 2004). Thus, understanding the cultural context is an essential factor when designing a successful SETA programme.

3.4.5 CSF-DS5: Adhere to Organisational Security Policy and the "Law of the Land"

This CSF focuses on the guidelines and procedures needed to protect the IS assets of the organisation. These factors can be regulation or legislation that help to modify employee IS security behaviour. It is critically important that all of the organisational security policies and the "law of the land" are adhered to when designing a SETA programme (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 organisation 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: *"most of the organisations 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 organisation are obliged to be aware of the information security policy within their organisation. Each organisation 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 stated: *"all members of the organisation, 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 programme.

In comparing these findings with current literature, a number of observations can be made. Some studies focus on the security policy and regulations in building a SETA programme (D'Arcy et al, 2009; Peltier, 2005). The security policies are presented to the employees to show what is expected from them. Therefore, to make a SETA programme successful, the employee should follow the policies and regulations in order to deal with issues such as: how to deal with suspicious sites; how to keep company data confidential; and which information can be shared on social media.

3.4.6 CSF-DS6: Build Security Awareness Campaigns

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 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 organised with employees, for consistency and reliability, and to emphasise the importance of the security awareness programme to the organisation. As stated by another informant: *"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 programme is of critical importance.

In comparing these findings with those presented in the literature, a number of observations can be made around the criticality of building a security awareness campaign as part of a SETA programme. For example, Rantos et al., (2012) discuss launching the 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 security awareness, complying with IS security policy, and reducing IS security risks (Vroom and von Solms, 2002; Puhakainen and Siponen, 2010). Therefore, formal awareness campaigns are communications with employees with the specific aim of: [1] increasing the understanding of, and [2] reducing the likelihood of, harmful information security practices within the organisation (D'arcy et al., 2009; Hearth et al., 2018).

3.4.7 CSF-DV1: Sustained Communication of Relevant Messages

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 programme. For example, one key informant 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: *"…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 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.

In comparing these findings with existing literature, the researcher finds a limited number of studies that examine the impact of communication on the effectiveness of a SETA programme. This presents an opportunity for further research. For example, Barlow et al. (2018) state that more research on the role of communication in delivering a SETA programme is required. Therefore, from a practical point of view, sustained communication plays an important role in the success of a SETA programme.

3.4.8 CSF-IM1: Apply Diverse Methods to Deliver Security Awareness Messages

This CSF highlights that organisations use various approaches to deliver SETA programme messaging. For example, they can deliver security awareness messages via SMS, 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, organisations determine the best methods to use to implement their SETA programme messaging based on their resources, size, and budget. Within this research study, key informants identified the various methods to deliver a successful SETA programme. As commented by one key informant: *"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 programme 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 organisation 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 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.

In comparing these findings with those presented in the literature, several studies discuss different methods to implement a SETA programme (Silic and Lowry, 2020; Bauer et al., 2017; Tsohou et al., 2015; Johnson, 2006; Peltier, 2005). For example, Silic and Lowry (2020) present a study that aims to improve security training in organizations by applying a gamification approach. While other studies discuss different communication channels such as posters, videos, emails etc. to deliver a SETA programme (Johnson, 2006; Peltier, 2005). It can be argued that the successful implementation of a SETA programme can be determined by a diversity of delivery methods aligned with individual differences.

3.4.9 CSF-IM2: Motivate Employees to Engage in Security Awareness

This CSF highlights that 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 programme. 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 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 from Saudi Arabia mentions that *"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.

For this study the researcher uses the definition of 'motivation' proposed by Rogers (1975), where motivation can be either intrinsic (doing something since one finds it interesting) or extrinsic (doing something since one is obliged to, or to be rewarded). Several studies examine the influence of motivation to sustain compliance with IS security policy (Puhakainen and Siponen,

2010; Herath and Rao, 2009), change employee behaviour (Alshaikh et al., 2018; Kirova and Baumöl, 2018; Karjalainen et al., 2013) and reduce IS security risk (Zani et al., 2018). Although the researcher did not find studies that examine the impact of motivational aspects on the effectiveness of SETA programmes, it is an area that requires further research.

3.4.10 CSF-EV1: Maintain Quarterly Evaluation of Employee Performance

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 fulfil the training requirements, in order to assess the knowledge retained by employees and thereby review the effectiveness of the SETA programme. Within this research study, key informants highlight several techniques to assess the employees' responses to the SETA programme. 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? As one key informant 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*: "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/programmes the employees attended and completed. As a key informant explains: *"… 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 programmes and this also provides an indication of the programme's success.

In comparing these findings with those presented in the literature, it was noted that there are several studies which discuss the use of evaluations for the SETA programme. 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 that gaps exist and measuring the effectiveness of the SETA programme (Alshaikh et al., 2018; Johnson, 2006). However, this is an area that requires further research.

3.4.11 CSF-EV2: Measure Employee Reporting of Security Incidents

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 programme's effectiveness. Within this research study, key informants described the methods to evaluate employee behaviour 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 programme. For example, one key informant 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 programme is effective and improving security. As mentioned by one key informant: "*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 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 programme effectiveness).

In comparing these findings with those presented in the literature, a number of observations can be made. Several studies recommend various countermeasures that can be used to reduce IS security incidents (c.f. Chen et al., 2015; D'Arcy et al., 2009; Peltier, 2005). For example, D'Arcy et al., (2009) proposes that a SETA programme aims to mitigate IS risks and security incidents. Understanding the IS security policies through the delivery of SETA reduces IS security misuse (Peltier, 2005). It can be argued that a decreasing number of security incidents and security attacks provides an organization with a significant indication that the practice improvements are due to a successful SETA programme.

3.5 Conclusions And Future Research

This paper presents an exploratory study identifying the CSFs for SETA programmes. The CSFs emerge from the analysis of 20 key informant accounts of SETA programme effectiveness. The 11 CSFs are associated with the design, development, implementation, and evaluation phases of a SETA programme lifecycle. The researcher found six CSFs relating to the **design** phase (CSF#1,2,3,4,5,6), one CSF relating to the **development** phase (CSF#7), two CSFs relating to the **implementation** phase (CSF#8,9), and two CSFs relating to the **evaluation** phase (CSF#10,11). The next step in this research is to conduct a focus group with additional key informants (experts) who have valuable experience in SETA programmes. The purpose of this next step is to validate our findings and to rank the 11 CSFs in order of importance. These findings will further contribute to building a lifecycle model of CSFs for SETA programmes.

Chapter Four: The Critical Success Factors for Security Education, Training and Awareness (SETA) Programme Effectiveness: A Lifecycle Model - (Paper 3)

Abstract

Purpose- This study explores the Critical Success Factors (CSFs) for Security Education, Training and Awareness (SETA) programme effectiveness. The questionable effectiveness of SETA programmes at changing employee behaviour and an absence of empirical studies on the CSFs for SETA programme effectiveness is the key motivation for this study.

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 programme expertise. Data is 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 programme effectiveness. These CSFs are mapped along the phases of a SETA programme lifecycle (design, development, implementation, evaluation) and 9 relationships identified between the CSFs (*within* and *across* the lifecycle phases) are highlighted. The CSFs and their relationships are visualised in a Lifecycle Model of CSFs for SETA programme effectiveness.

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

Keywords- SETA Programme; Effectiveness; Security; CSFs; Key Informant; Lifecycle Model

Paper type- Research paper.

4.1 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 $400 billion by 2027 (fortune.com, 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"* (fortune.com, 2022). Organisations use various strategies to safeguard their information systems and information assets against security threats. However, a Security Education, Training and Awareness (SETA) programme is one of the most prominent strategies used for controlling IS security threats and protecting information assets, and many researchers recommend establishing a SETA programme 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 programme definitions can be found in the literature, despite their variability, they all hold the employee central in their focus. Therefore, a SETA programme is most often viewed as an educational process 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 programmes 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 programmes 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 organisational 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 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). Furthermore, Talib et al. (2010) have observed that while some organisations claim to measure the effectiveness of their SETA programmes, no actuals are provided as to the level of effectiveness. It is reported that poor SETA programme effectiveness is linked to the programmes failure to achieve its goal of impacting positively on employee security-related behaviours (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 programmes 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 programmes (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 amongst employees.

Further leveraging this need for conceptual clarity, research is still required on the design, development, implementation, and evaluation phases of the SETA programme lifecycle (Alyami *et al.*, 2020; Alshaikh *et al.*, 2018). For example, where empirical studies investigating the effectiveness of SETA programmes exist, they fail to examine all phases of the SETA programme lifecycle (design, development, implementation, 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 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). In effect, despite the fact that there is a growing volume of research around SETA programmes, there is still limited research of *"practical value"* available on *"organisational strategies to improve"* SETA programmes, with recommendations to guide

the development of SETA programmes being *"fragmented and dispersed"* and not cumulative in nature (Alshaikh *et al.*, 2021, p. 3). Therefore, through leveraging the SETA programme lifecycle phases, this paper sets out to address this research need by exploring the following **research questions**: (i) *What are the Critical Success Factors (CSFs) for SETA programme effectiveness?* and, (ii) *How are these CSFs related to each other?* These CSFs are mapped against the phases of the SETA programme lifecycle and the relationships identified between the CSFs are highlighted. The CSFs and their relationships are visualised in a Lifecycle Model of the CSFs for SETA programme 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 programme effectiveness (RQ1) and the relationships between these CSFs (both *within* and *across* the SETA programme lifecycle phases) (RQ2). Section 5 presents an evaluation of our findings (visualised as a Lifecycle Model) against the existing literature. Lastly, section 6 presents the conclusions and contributions of the research.

4.2 Background

Existing research on SETA programmes 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 organisational SETA programmes to improve cybersecurity behaviour *"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 programmes *"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 behaviour or employee awareness, or a multiplicative effect of all these areas, it is something that still needs to be unpacked (***reference withheld for review purposes***).

IS/cyber security researchers *"consistently argue"* that organisations need SETA programmes *"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 programme *"requires ongoing voluntary compliance from employees"* (Pham et al, 2019, p.134). Therefore, the organisational challenge is to develop engaging SETA programmes *"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 programmes. Furthermore, this sense of employee "security fatigue" comes at a significant organisational cost, where, despite significant investment in SETA programmes, 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 $12.1 billion 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 organisations 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 behavioural change. In fact, it is this absence of behavioural change that leads to a questioning of SETA programme 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 programmes. 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 organisations can be seen as critical to progressing the effectiveness of an organisational SETA programme.

4.3 Research Methodology

To fulfil the research objective and answer the research questions, this research follows an exploratory design. As agreed by Marshall & 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), The researcher aims to conceptualise 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 1st order (informant-centric) terms"* during initial data coding, and further *"organise 1st-order codes into 2nd-order (theory-centric) themes"* (Gioia et al., 2012, p.18). The researcher embraces 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 the researcher is looking to develop new concepts linked to how organisations organise themselves to deliver more effective SETA programmes.

The CSFs for SETA programme 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 (***reference withheld for review purposes***). 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).

4.3.1 Data Gathering

In this research, the researcher adopts 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); (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 programme 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 exploring new ideas, capturing new phenomena, and identifying the rich contextualized detail of complex concepts. Twenty 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 10 provides a list of

the key informants' current role, years of experience, industry sector, qualifications, and interview duration. The key informants were recruited through (i) prior knowledge of, and working relationships with, practitioners currently active in IS/cyber security, (ii) speakers at practitioner conferences and webinars, and (iii) LinkedIn connections.

In this study, the researcher conducts a series of semi-structured interviews where each key informant reveals their experiences (positive and negative) with delivering SETA programmes. In particular, the researcher is most interested in exploring two sides of a key informant's SETA programme experience, namely the *"what"* and the *"how"* across the SETA programme lifecycle phases (*design, development, implementation, evaluation*). This simply translates as "what" action they need to take and "how" they enable that action, in their role (leading a SETA programme). These actions are also in the context of the key informant striving for the best possible outcome (an effective SETA programme). 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 programmes throughout the lifecycle phases (*design, development, implementation, evaluation*) were discussed. See Appendix A for the Interview Guide used.

nterviews took place over seven months (between April 2021 and October 2021) and ranged in duration from 40 to 60 minutes with an average interview duration of 50 minutes. Due to 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 (***ethical approval number withheld for review purposes***). 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 sixteen 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.

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, 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 & Gas	~ 22 years	PhD (Management & Operations) Cybersecurity Influencer	60
5	Lebanon	Governance and risk management compliance manager	Banking	10 years	BSc (Computer Information Systems) CISA, CISM, CRISC, 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, CRISC	50
9	Saudi Arabia	CISO (chief information officer)	Petrochemicals & Chemicals	15 years	MSc (Information Security) ISOC	55
10	Kuwait	CISO (chief information officer	Oil & Energy	8 years	MSc (Computer Engineering)	40
11	USA	Consultant in IS security	Financial Services & 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, 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 & Network Security	10 years	PHD (Cyber Security) CISM	60
16	Egypt	Head of cyber security	Banking	20 years	MSc (Business Information Technology) C|CISO, CISM, CRISC, ISO27001	55
17	UK	Security Awareness Manager	Banking	15 years	MSc (Information Security & Privacy)	50
18	USA	Director of Security Awareness	Computer & 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 & Management)	50

Table 10.The key informants' current role, years of experience, country, industry sector, qualifications, and interview duration.

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

4.3.2 Data Analysis

Data analysis is a crucial step in qualitative research (Leech & Onwuegbuzie, 2008). Its main purpose is to develop an understanding of the phenomenon of interest (Kawulich, 2004). In this research the researcher adopts 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* the researcher aims 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), the researcher is thinking systematically about the data in order to link the emergent categories and form relationships (c.f. Alhassan et al., 2019; Bhattacherjee et al., 2012; Dezdar and Sulaiman, 2009; Strauss and Corbin, 1990). Finally, during *selective coding* the researcher tells 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 data progressed. There was also a constant reflection back to the literature (e.g. SETA programme effectiveness and SETA programme 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 programme. These 212 coded excerpts led to the emergence of 15 categories mapped across the 4 SETA programme 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; **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 4 categories (reducing the number of coded excerpts to 187) and [ii] the emergence of the CSFs (11 remaining categories) for SETA programme effectiveness. The category with the highest coding frequency and key informant voices across each of the SETA programme 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); **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 F for the distribution of contributing key informants to CSFs (ranked in descending order).

From November 2021 to January 2022, the analysis of the open coding outputs produced the initial list of 11 CSFs for SETA programme 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, the researchers 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. The researchers deemed this relationship as relevant if it suggested a "cause and effect" type relationship was present in their story of achieving SETA programme effectiveness. Again, the researchers 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 4-month period. See Figure 2 for a sample of our axial coding.

Finally, our effort at *selective coding* allows us to tell a compelling theorising story around the outputs (the 11 CSFs for SETA programme effectiveness and the 9 relationships between these CSFs). See Figure 11 for our Lifecycle Model of CSFs for SETA programme 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 *"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 the researcher discusses the research findings which are then presented as a Lifecycle Model of CSFs for SETA programme effectiveness.

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 Organisational 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%)	

Table 11.Key Informant Frequency and Coded Excerpt Distribution for each CSF.

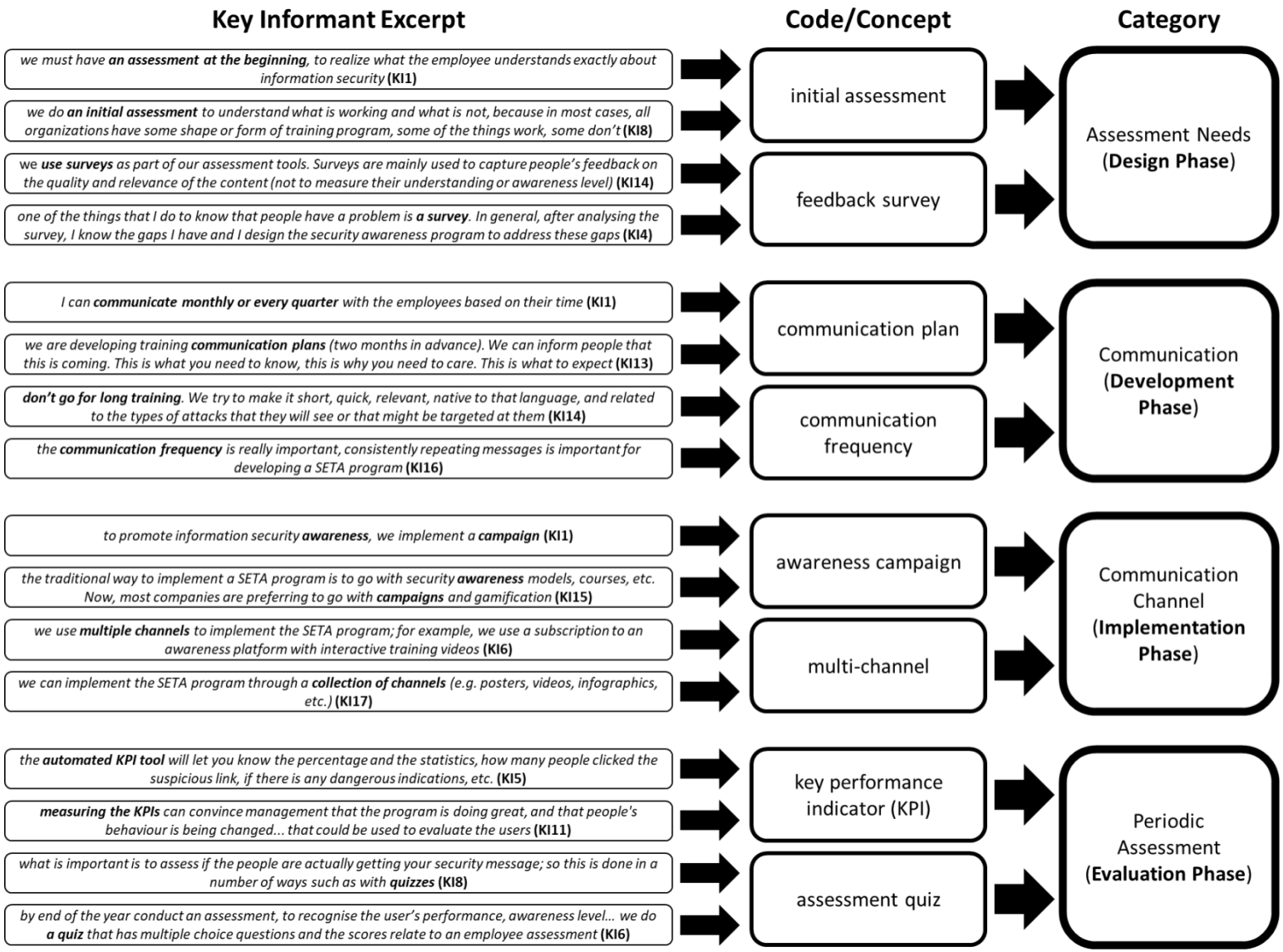


Figure 9.A Sample of our Open Coding (a snapshot of the highest frequency categories across the four lifecycle phases)

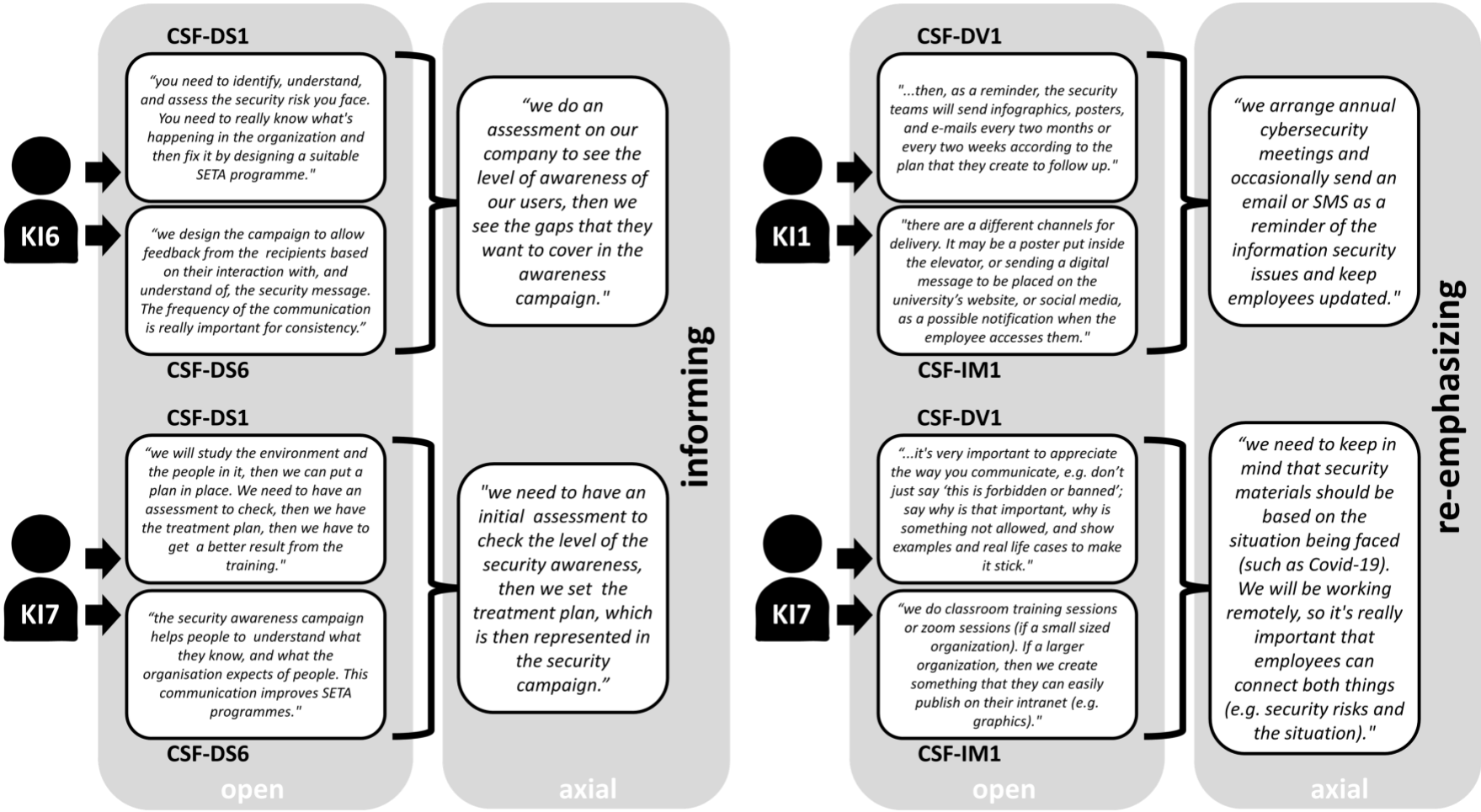


Figure 10.A Sample of our Axial Coding (a snapshot of the within phase and across phase CSF relationships)

4.4 Findings: The CSFs and the CSF Relationships

In this section the researcher sets about answering our research questions (based on our analysis of the 20 key informant interviews). In section 4.1 the researcher presents the 11 CSFs for SETA programme effectiveness (RQ1). In section 4.2 the researcher presents 9 relationships between the CSFs *within* (4) and *across* (5) the SETA programme lifecycle phases (*design*, *development*, *implementation*, *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 visualised in the Lifecycle Model of CSFs for SETA programme effectiveness (see Figure 3).

4.4.1 CSFs for SETA Programme Effectiveness (RQ1)

In this section the researcher presents these CSFs in a ranked order (based on the frequency count of coded excerpts) within each SETA programme lifecycle phase.

4.4.1.1 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 programme lifecycle. This CSF highlights the fact that conducting an initial assessment is an essential factor in designing a SETA programme. 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, 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 organisation 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 programme lifecycle, will increase the likelihood of successful SETA programme outcomes.

4.4.1.2 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 programme 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 programme to ensure content suitability. Within this research study, key informants explain how most organizations set up a SETA programme 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.

4.4.1.3 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 programme lifecycle. This CSF highlights the importance of communicating the SETA programme objectives (knowing what is required to be delivered) clearly and consistently to the employees. It is also important to ensure that the SETA programme 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 programme 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 programme. 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 organisations should create a plan for designing a SETA programme and that plan should contain what is necessary to be delivered, such as the types of IS security issues or topics.

4.4.1.4 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 programme lifecycle. This CSF focuses on the criticality of understanding the cultural diversity in the organization when designing a SETA programme, 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 programme, such as: language, knowledge, level of education, age, and gender. All these aspects contribute to a successful SETA programme 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 organisation's employees, then these differentiations would need to be considered when designing a SETA programme. For example, the cultures of Saudi Arabia, Egypt, and UAE care more about language, and as a result, use artefacts for SETA programmes, 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 programme. 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 programme.

4.4.1.5 CSF-DS5: Adhere to Organisational 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 programme 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 help to modify employee IS security behaviour. It is critically important that all of the organizational security policies and the "law of the land" are adhered to when designing a SETA programme (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 programme.

4.4.1.6 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 programme 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 programme 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 programme is of critical importance.

4.4.1.7 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 programme 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 programme. 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.

4.4.1.8 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 programme lifecycle. This CSF highlights that organizations use various approaches to deliver SETA programme messaging. For example, they

can deliver security awareness messages via SMS, 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 programme messaging based on their resources, size, and budget. Within this research study, key informants identified the various methods to deliver a successful SETA programme. 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 programme 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.

4.4.1.9 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 programme 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 programme. 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 that *"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.

4.4.1.10 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 programme 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 fulfil the training requirements, in order to assess the knowledge retained by employees and thereby review the effectiveness of the SETA programme. Within this research study, key informants highlight several techniques to assess the employees' responses to the SETA programme. 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? As 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/programmes the employees attended and completed. As a key informant (KI15) explains: *"… 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 programmes and this also provides an indication of the programme's success.

4.4.1.11 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 programme 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 programme's effectiveness. Within this research study, key informants described the methods to evaluate employee behaviour 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 programme. 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 programme 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 programme effectiveness).

In the next section the researcher now examines the CSF relationships *within* and *across* the SETA programme lifecycle phases.

4.4.2 The CSF relationships within & across the SETA programme lifecycle phases (RQ2)

Based on our analysis the researcher identifies 9 relationships between the CSFs for SETA programme effectives (four relationships between the CSFs *within* the SETA programme lifecycle phases and five relationships between the CSFs *across* the SETA programme lifecycle phases). Based on our analysis, these 9 relationships *within* and *across* the SETA programme lifecycle phases (*design*, *development*, *implementation*, *evaluation*) are deemed important for SETA programme 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), the researcher viewed this as the existence of a potential relationship between the CSFs (see Figure 2 for a visualisation 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, the researcher was in a position to craft *"meaningful boxes and arrows"* as part of our *"interim struggles"* (theorising) (c.f. Weick, 1995, p.389). This iterative process led to the emergence of the Lifecycle Model of CSFs for SETA programme 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 programme 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 programme 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 programme, is critical to delivering an effective programme.

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 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, 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 programme effectiveness.

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 organisational cultural context.
	CSF-DS5: Adhere to Organisational Security Policy and the "Law of the Land"		Enables the design of a programme plan that considers organisational 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.

Table 12.The relationships between the CSFs within the SETA programme lifecycle phases.

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 programme 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 (key performance indicator) and can reveal a significant amount about the effectiveness of a SETA programme, 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 programme.

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, where this can be viewed as a simple indicator of SETA programme 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 suitable method, is key to ensure the effectiveness of the SETA programme.

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	**CSF-IM1:** Apply Diverse Methods to Deliver Security Awareness Messages	**Contextualizing**	Enables the use of different communication channels in order to deliver a culturally

Employee Cultural Diversity			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 Organisational 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.

Table 13. The relationships between the CSFs across the SETA programme lifecycle phases

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 organisational position, is key to the effectiveness of a SETA programme. 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 programme is maximised.

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 programme. To motivate employees by allocating rewards/recognition for good practice around the IS security policy will further enhance the effectiveness of a SETA programme.

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 programme.

In the next section the researcher now discusses the Lifecycle Model of the CSFs for SETA programme effectiveness (which positions the 11 CSFs and the 9 relationships across the four lifecycle phases).

4.5 Discussion: The Lifecycle Model of CSFs for SETA Programme Effectiveness

As presented in Table 14, the 11 CSFs are associated with the design (six CSFs), development (one CSF), implementation (two CSFs), and evaluation (two CSFs) phases of a SETA programme 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 programme 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.

4.5.1 The SETA Programme Lifecycle Phases and the Lifecycle Model Uniqueness

In this research that naming of our SETA programme lifecycle phases (*design, development, implementation*, *evaluation*) emerged from an analysis of 59 papers on SETA programme delivery. There papers covered a period from 2000-2021 and were returned following a search of Scopus, the AIS eLibrary, and the Senior Scholars' Basket of 8 Journals. Based on our analysis the researcher defines the four lifecycle phases as follows:

- **Design:** identify the target audience (employee) needs in order to plan, prioritise, and benchmark activities.
- **Development:** align organisational employee needs with the programme goals, content and resources required.
- **Implementation:** use a combination of the appropriate delivery methods to disseminate the security message.
- **Evaluation:** establish if the goals of the SETA programme 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 programme lifecycle, no individual paper covered all four phases of a SETA programme lifecycle; therefore, 40% covered one phase, 20% covered two phases, and 40% covered three phases (***reference withheld for review purposes***). 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 programme goal), *implementation* (e.g. top management commitment), and *evaluation* (e.g. conduct periodic reviews) phases of the SETA programme 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 programme lifecycle, however, the *evaluation* phase is underexplored (***reference withheld for review purposes***). This observation is not too dissimilar to that made by Alhassan et al. (2018) when examining the focus of attention along a Data Governance programme lifecycle.

Several studies discuss various factors impacting on SETA programme 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 programmes. They leverage the key principles of social marketing in order to improve the effectiveness of SETA programmes, through employee behaviour 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: (i) focusing on positive interventions through gamified training, and (ii) 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 programme. 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 programme. They identify factors (at the level of the *individual*) that influence *knowledge*, *attitude*, *intention*, and *behaviour*. Therefore, comparing our findings (11 CSFs for SETA programme effectiveness) with those presented in the literature, a number of observations can be made around the criticality of these CSFs for SETA programme 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 programme effectiveness. Furthermore, based on our analysis the researcher 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 programme effectiveness) still holds and represents the most comprehensive coverage (in a single research study) of the factors critical to the success of a SETA programme. 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 behaviour change. These CSFs impact on SETA programme 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 behaviour changes and engagement is a reported concern impacting negatively on SETA programme effectiveness. It reiterates the fact that when designing a SETA programme, it is important to appreciate that the purpose of the programme is to assist employees to comprehend their IS/cyber security responsibilities (Hansche, 2001).

Current research (***reference withheld for review purposes***) suggests that effective SETA programmes are often impacted by: (i) *changing employee attitudes* (c.f. Posey et al., 2015;

Yaokumah et al., 2019; Alshaikh et al., 2019), (ii) *increasing employee compliance* (c.f. Han et al., 2017; Barlow et al., 2018; Dhillon et al., 2020), (iii) *raising employee awareness* (c.f. Heikka, 2008; Lebek et al., 2014; Tsohou et al., 2015), and (iv) *improving employee practices* (c.f. Chander et al., 2013; Kumah et al., 2019; Topa et al., 2019). Therefore, leveraging our Lifecycle Model (Figure 3), the researcher can map the CSFs to these four areas of impact. For example, four CSFs (**CSF-DS2**, **CSF-DV1**, **CSF-IM2**, **CSF-EV1**) can be mapped to *changing employee attitudes*; two CSFs (**CSF-DS3**, **CSF-DS5**) can be mapped to *increasing employee compliance*; three CSFs (**CSF-DS1**, **CSF-DS6**, **CSF-IM1**) can be mapped to *raising employee awareness*; and two CSFs (**CSF-DS4**, **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**, **CSF-EV1**) demands a focus right across the four phases of the SETA programme lifecycle (see Figure 3). However, *increasing employee compliance* (**CSF-DS3**, **CSF-DS5**) is linked more to a concerted effort in the design phase. Furthermore, *raising employee awareness* (**CSF-DS1**, **CSF-DS6**, **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**, **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 organisational approach to IS\cyber security works.

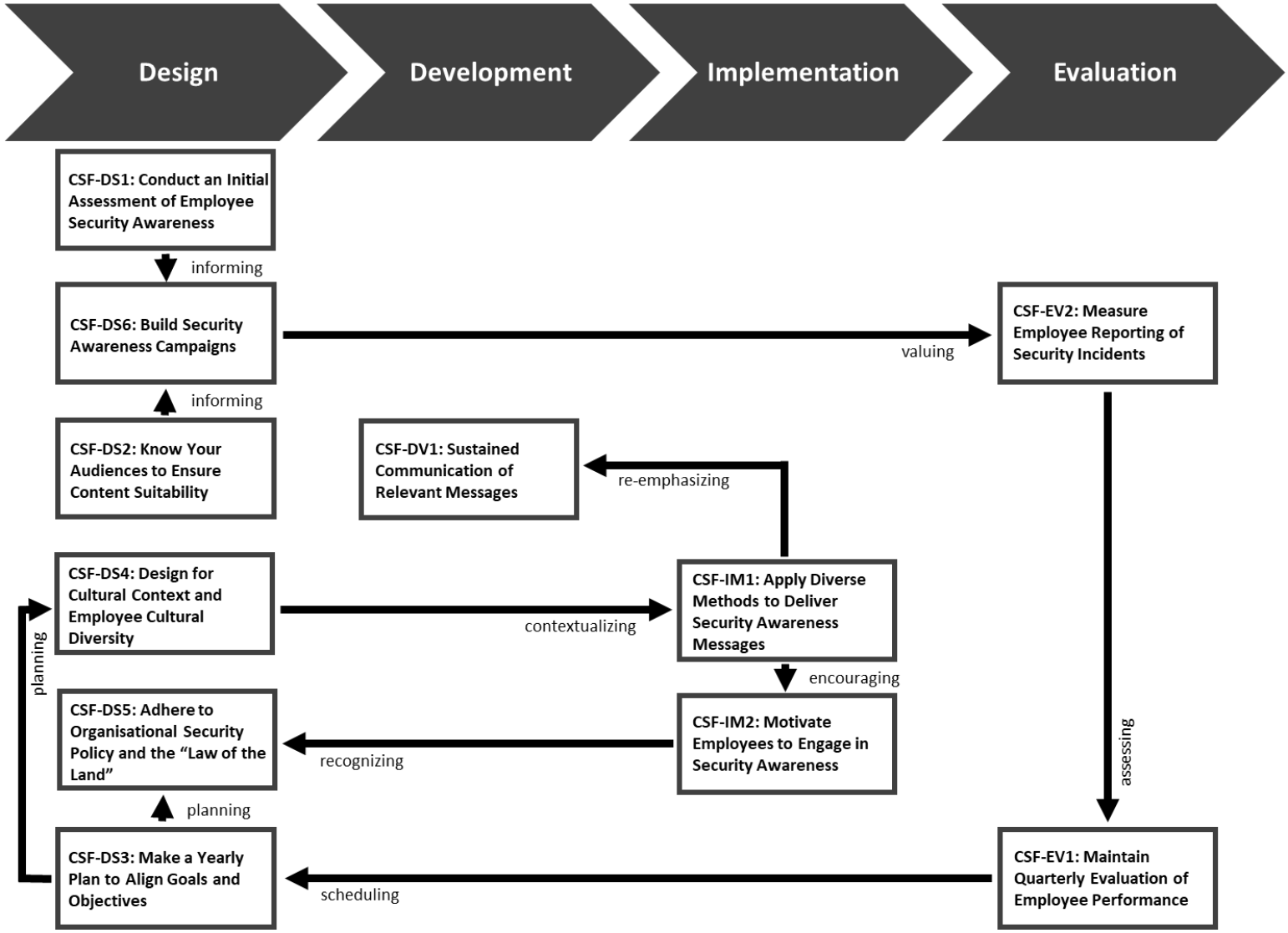


Figure 11.The Lifecycle Model of CSFs for SETA Programme Effectiveness.

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 Organisational 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**

Table 14.Evaluating the CSFs against Existing SETA Programme Effectiveness Literature

4.6 Conclusions and Implications

At the present time, there is growing attention on SETA programmes from both the academic and practitioner communities. The importance of a SETA programme to reducing IS security risks/incidents and to increasing IS security awareness among employees is well documented. However, a review of the SETA programme literature reveals that there is a lack of academic studies on SETA programme effectiveness that examine all phases of the SETA programme lifecycle (design, development, implementation, evaluation) (c.f. Hu et al., 2021; Kirova and Baumoel, 2018; Puhakainen & Siponen, 2010). Therefore, in this study, the researcher provides a greater insight into the dynamic of the SETA programme 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 15).

Contribution to	**Contribution**
Research	• 11 CSFs for the SETA programme 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 programme (visualized in a Lifecycle Model)

Table 15.Research Contributions

In this paper the researcher advances the first comprehensive conceptualisation of the CSFs for SETA programme effectiveness. This is an important first step towards the creation of a coherent body of knowledge (grounded in practice) that can support further study. The researcher has been able to leverage the available evidence and propose a Lifecycle Model (see Figure 11) that positions each of the CSFs for SETA programme 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 programme lifecycle, to date. The researcher views our Lifecycle Model of CSFs for SETA programme 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 visualises the *"conjunctural"* (Ragin, 1987) nature of the 11 CSFs and their multiplicative effects on the effectiveness of a SETA programme. While based on our analysed observations, such an appreciation further improves our understanding regarding the complexity of SETA programme delivery within an organizational context. Therefore, the researcher views 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 programme 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, evaluation).

Following our analysis of the literature on SETA programmes and SETA programme effectiveness, the researcher appreciates that this work is unique in that it presents one of the first collections of CSFs for SETA programme effectiveness (mapped along a programme lifecycle). It is worth acknowledging that historically, such a collection of CSFs mapped along a Lifecycle Model have 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 ERP (enterprise resource planning) implementation, Tan et al. (2009) on the CSFs for 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 four phases of an ERP lifecycle (chartering, project, shakedown, onward & 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 programme. For example, it is reported that *importance* is the most critical dimension of relevance for IS practitioners, and similar to (Rosemann & Vessey, 2008 p.3) The researcher views *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 (e.g. *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 programme 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 programmes) from various geographic locations. As a result, the 11 CSFs for SETA programme effectiveness and the relationships between the CSFs *within* and *across* the SETA programme lifecycle phases (emerging from our analysis), provide a valuable insight into the process of leading an effective SETA programme in practice. It is noteworthy that having an effective SETA programme is extremely important to organisations aiming to reduce IS security risks, through changing employee behaviour.

4.6.1 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 & 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, the researcher believes that our use of 20 key informants is appropriate for this exploratory research study. However, the researcher is 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 programme 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, the researcher imagines 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 example, industry sector and organisation size.

This Lifecycle Model of the CSFs for SETA programme 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 programme in practice. Currently, it is unknown if the findings reported in this paper are directly applicable to SMEs. This links to our key informants being connected to larger organisations 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 organisations 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 organisations of different sizes, where smaller organisations 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 organisations (Chidukwani et al., 2022; Bada & Nurse, 2019; Alotaibi et al., 2016). Therefore, the situational difference in the operational environment of an SME versus a larger organisation needs to be explored further, specifically in the context of SETA programme effectiveness.

Finally, the researcher appreciates that the 11 CSFs are not yet established as universal, so while these CSFs 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). 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 programmes. 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"* amongst various stakeholder types (e.g. executives, systems users, project team members, vendors & 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 the researcher 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 (***reference withheld for review purposes***).

Chapter Five: Critical Success Factors for SETA Programme Effectiveness: An Empirical Comparison of Practitioner Perspectives – (Paper 4)

Abstract

Purpose- Cybersecurity 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 cybersecurity professionals elevate the importance of delivering effective SETA programmes within organisations. 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 CSFs for SETA programme effectiveness.

Study 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 one using semi-structured interviews with 20 key informants (the emergence of 11 CSFs), in stage two from 65 respondents to a short online survey (the ranking of the CSFs), and in stage three using semi-structured interviews with 9 cyber security practitioners (the importance of the CSFs). Using a multi-stage research design allows us to propose and evaluate the 11 CSFs for SETA programme effectiveness.

Findings- In this study, our multi-stage analysis produces a ranked list of 11 CSFs for SETA programme effectiveness, along with the emergence of five principles to increase the likelihood of delivering an effective SETA programme within an organisational context. Our analysis also reveals that most of the contradictions/differences in CSF rankings between cyber security practitioners are linked to the design phase of the SETA programme lifecycle. While two CSFs, "maintain quarterly evaluation of employee performance" (CSF-DS6) and "build security awareness campaigns" (CSF-EV1), represent the most significant contradiction in our study.

Originality/value- The 11 CSFs for SETA programme effectiveness, along with the 5 principles to increase the likelihood of SETA programme effectiveness, provide a greater depth of knowledge contributing to both theory and practice and lays the foundation for future studies.

Keywords- SETA Programme; Effectiveness; Security; Cyber; CSFs.

Paper type- Research paper.

5.1 Introduction

Cybersecurity has never been more important than it is today in an ever more connected and pervasive digital world. In fact, the cybersecurity market size is expected to surpass $400 billion by 2027 (fortune.com, 2022). Furthermore, according to Global Market Estimates (2022), the market for cybersecurity awareness training is anticipated to increase to a value of $12.1 billion by 2027, representing a compound annual growth rate (CAGR) of 45.6% from 2022 to 2027. According to the Ponemon Institute (2020), insider threat occurrences have increased by 44% over the past two years, while the cost per incident has increased by more than a third to just over $15 million. The insider risks can include employees, temporary workers, or external consultants who have been provided authorised access to organisational knowledge (Posey et al., 2015). Therefore, with the number of cyber-attacks increasing each year, *"adequate cybersecurity measures are becoming a necessary venture for companies of all shapes and sizes"* (fortune.com, 2022). Therefore, organisations use various strategies to safeguard their information assets against security threats. A Security Education, Training and Awareness (SETA) programme is one of the most prominent strategies used for controlling IS security threats and protecting information assets.

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 cyber 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). However, frequently reported shortages of suitably skilled and trained cybersecurity professionals elevate the importance of delivering effective Security Education, Training and Awareness (SETA) programmes within organisations. This is true where SETA programmes are viewed as an effective way to build awareness and know-how amongst employees, to an acceptable level. However, these SETA programmes often produce questionable results around effectiveness. Therefore, having a greater appreciation of *'what to do when'* is very important in improving the effectiveness of a SETA programme.

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 CSFs for 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 11 CSFs for SETA programme effectiveness and the five principles to increase the likelihood of delivering an effective SETA programme within an organisational context. Lastly, section 5 presents the conclusions and contributions of the research.

5.2 SETA Programme Effectiveness and CSFs - 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 Baumöl, 2018). SETA programmes include the following functions: (1) provide employees with knowledge regarding organisational information threats and IS security (D'Arcy *et al*., 2009; Yoo *et al*., 2018; Dhillon *et al*., 2020) ;(2) clarify existing technical and procedural countermeasures available to employees (Pastor *et al*., 2010; Silic and Lowry, 2020); (3) determine the possible sanctions for security policy violations in the organisation (Siponen and Vance, 2010; Karjalainen *et al.,* 2013; Herath, *et al*., 2018), and (4) 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 lifecycle (design, development, implementation, 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 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 Baumöl, 2018; Puhakainen and Siponen, 2010). In particular, guidance in the form of Critical Success Factors (CSFs) is seen as particularly useful by helping organisations understand where to focus their efforts (c.f. ***ref withheld for review purposes***). In fact, CSFs have been widely investigated and used in IS research and practice over the last three decades in order 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, that 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 Information Systems (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 (PPP) (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 since 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, the researcher argues that understanding the CSFs for SETA programme effectiveness will lend itself to increasing the effectiveness of a SETA programme within an organisation. However, 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, this research not only presents 11 CSFs for SETA programme effectiveness (mapped against the four phases of the SETA programme lifecycle – design, development, implementation, and evaluation) but also seeks to present a ranked list of CSFs (in order of their importance), along with five principles to increase the likelihood of delivering an effective SETA programme within an organisational context.

In the next section, the researcher presents further details on the research approach.

5.3 Research Approach

In this paper, the researcher presents a three-stage research design. In stage one, the researcher uses 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 two, the researcher uses 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 two, the researcher also compares this ranked list to the ranked list generated in stage one. This comparison highlights the position of each CSF in the respective lists and suggests the similarities and differences between the lists. The researcher also uses 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 one list from 20 key informants and stage two 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 datasets are not assumed to follow any normal distribution pattern (Osei-kyei and Chan, 2017; Hair et al., 2007). In stage three, the researcher presents our hermeneutics-inspired analysis of 9 follow-up probing interviews with cyber security practitioners involved in stage one (4) and stage two (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 two. Thereafter, these differences inform five principles to increase the likelihood of delivering an effective SETA programme within an organisational context.

5.3.1 *Stage 1: 20 Key Informants (The Emergence of the CSFs)*

Stage one of this exploratory research follows a systematic inductive approach to concept development. The researcher adopts 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 6 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, the researcher believes 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 lifecycle phases (design, development, implementation, evaluation) were discussed. The following questions were asked in order to

explore the CSFs for SETA programme effectiveness across these lifecycle phases. Questions 1-4 are also asked for the *development*, *implementation*, and *evaluation phases*.

1. What are the factors that are important in the ***design*** of a SETA programme?
2. Why are these factors important in the ***design*** of a SETA programme?
3. How can organisations ensure that these factors exist in their ***design*** efforts?
4. Who should be responsible for the ***design*** of a SETA programme?
5. 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 4 SETA programme lifecycle phases (design, development, implementation, 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; *evaluation* phase – 40 codes – 3 categories. The category with the highest coding frequency across each of the SETA programme lifecycle 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; *evaluation* phase – 20 coded concepts in the "Periodic Assessment" category. See Figure 5 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 16 presents these 11 CSFs organised by SETA programme lifecycle phase. See (***ref withheld for review purposes***) for a more detailed discussion on these 11 CSFs. Furthermore, Table 17 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 8th in Table 18) is 1.8, calculated as ((12*3)/20).

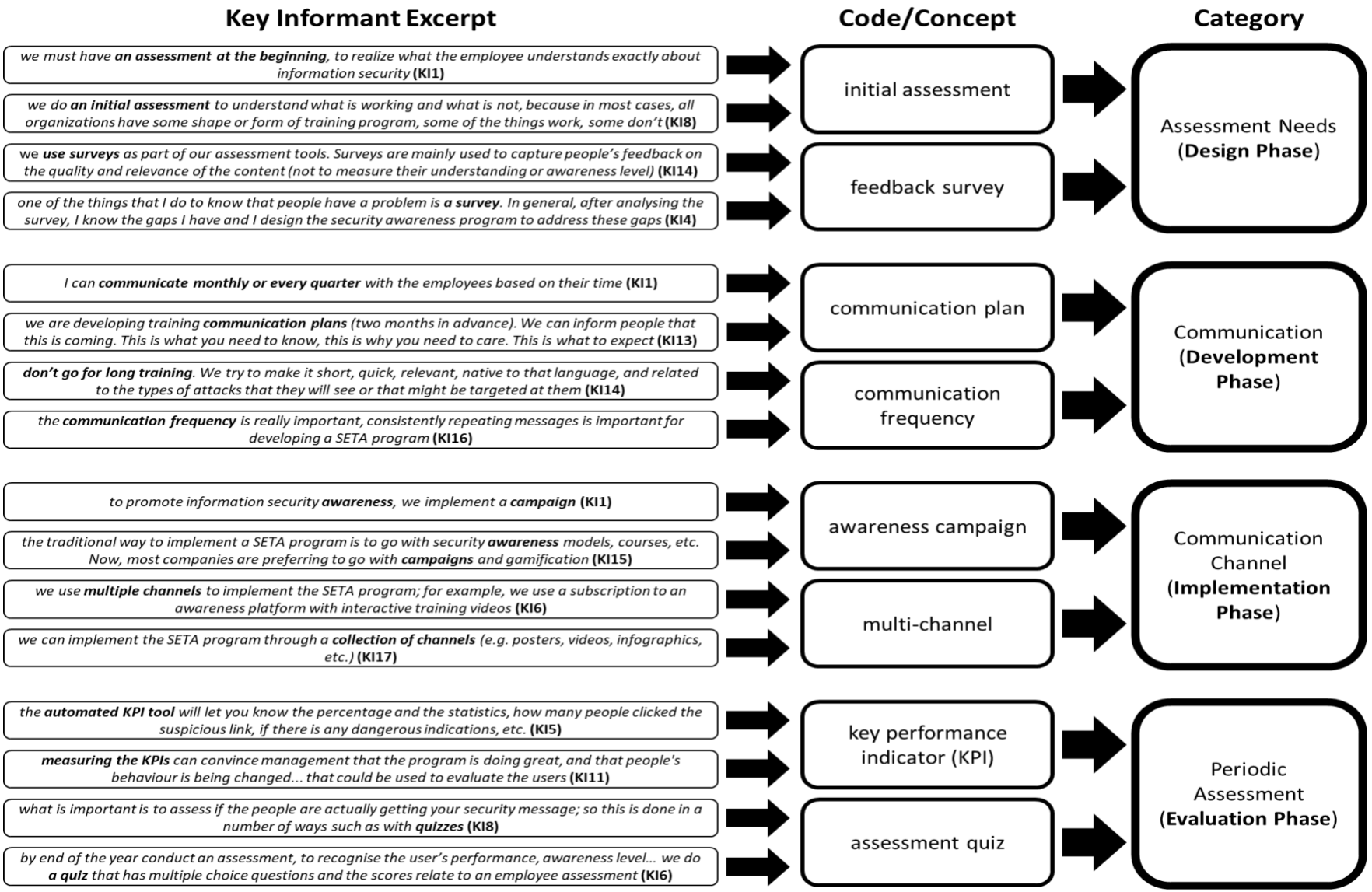

Key Informant Excerpt
Code/Concept
Category
we must have an assessment at the beginning, to realize what the employee understands exactly about information security (KI1)
we do an initial assessment to understand what is working and what is not, because in most cases, all organizations have some shape 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)

Figure 12. A Sample of our Inductive Open Coding (a snapshot of the highest frequency categories across the four lifecycle phases)

Lifecycle 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 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 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 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 a 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 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 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 cyber security issue.
	CSF-IM2: Motivate Employees to Engage in Security Awareness	Motivation	encouraging the employee to adhere to IS 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 cyber security issues.

Table 16. 11 CSFs for SETA Programme Effectiveness (presented by lifecycle phase)

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

Table 17.CSFs Ranking (Stage One - ranked by frequency count of codes).

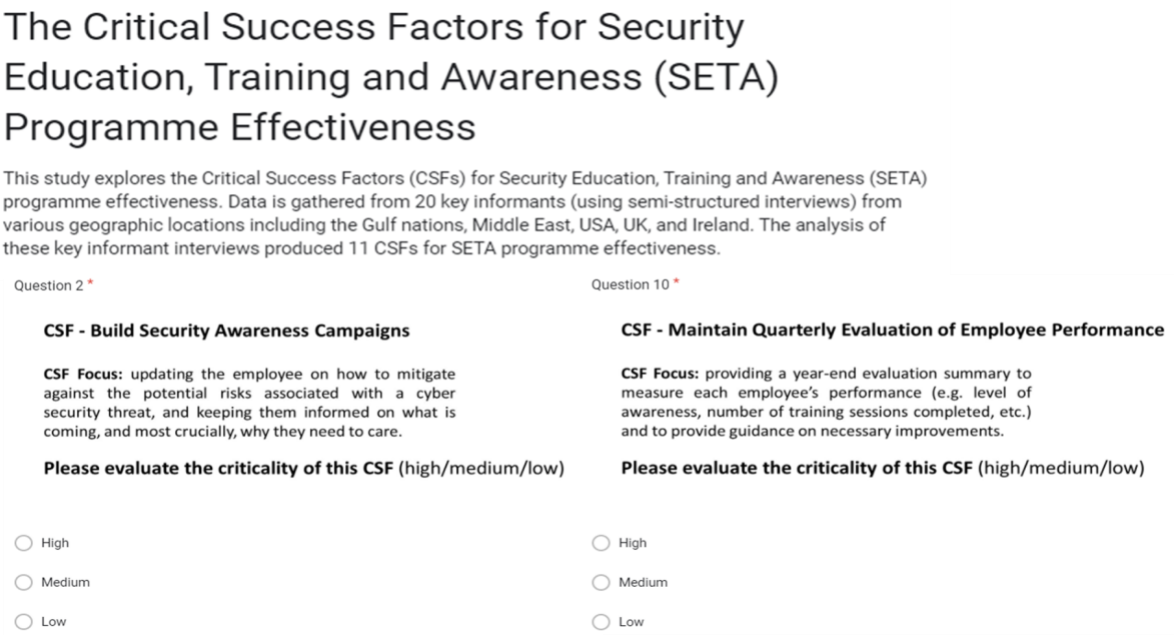


Figure 13. Sample Survey Questions

5. 3.2 Stage 2: 65 Survey Respondents (The Ranking of the CSFs)

In stage two of this exploratory research study, the researcher designed a short 11-question survey (1 question per CSF) to gather practitioner perspectives on the importance of each of the CSFs for SETA programme effectiveness. The researcher used an ordinal scale (high/medium/low) to allow respondents to rank the importance of each CSF. See Figure 13 for a sample survey question. A respondent was required to answer all questions to submit a valid survey response.

The survey was designed on Google Forms and was distributed electronically to practitioners in the 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, the researcher invited participants from the Cyber Research Conference Ireland (CRCI) 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 one was invited to participate in stage two.

The survey went live on May 5th (2022) and remained open for 5 days (until May 9th). 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. Table 18 presents these CSFs in a ranked, prioritised order (descending) based on the mean score of each CSF.

In this stage, the researcher also compares both ranked lists of 11 CSFs emerging from the two independent groups (stage one list from 20 key informants and stage two list from 65 survey respondents). Figure 3 presents a visual of this comparison (similarities and differences) and highlights the position of each CSF in the respective lists. The researcher also uses 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 one (n^1) and stage two (n^2) are available in Appendix A. The researcher uses the mean value for each of the 11 CSFs across both groups, rank each of the CSFs, and calculate the rank sum for stage one (109.5 with a *Ustat* = 43.5) and stage two (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 also available at this link (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 one: 20 key informants and stage two: 65 survey respondents). For example, in our analysis, *Ucrit* = 30 and the lowest *Ustat* = 43.5.

However, as seen in Figure 14, there is a somewhat contradictory element to the CSF rankings between stage one and stage two. For example, CSF-EV1 is the 1st ranked CSF from stage one but is the 11th ranked CSF from stage two. Furthermore, the inverse is also true, where CSF-DS6 is the 11th ranked CSF from stage one but is the 1st ranked CSF from stage two. In total, five critical areas of difference emerge from our comparative analysis of the ranked lists of 11 CSFs.

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

Table 18. CSFs for SETA Programme Effectiveness (Stage Two - ranked by mean score)

5.3.3 Stage 3: 9 Follow-Up Probing Interviews (The Insights into the CSF Importance)

In stage three of this exploratory research study, the researcher uses a hermeneutics-inspired approach to analyses and interpret the answers provided by 9 practitioners (4 from stage one and 5 from stage two) to questions emerging from the differences in the ranking of the CSFs between stage one (20 key informants) and stage two (65 survey respondents) (see Figure 3). In this stage, the researcher is trying to make sense of the *"seemingly contradictory"* (Myers, 2009, p.170) text that has emerged in this research around the five CSFs (difference in their ranked importance). Furthermore, the researcher takes these differences as a sign of *"confused, incomplete, cloudy, and contradictory views"* (Myers, 2009, p.171) amongst the cyber security community (specifically those with expertise in SETA programmes). For example, the following questions were asked to establish the significance of the CSFs:

- Is building a security awareness campaign important (CSF-DS6)? Why?
- Is maintaining a quarterly evaluation of employee performance important (CSF-EV1)? Why?
- How can adherence to policy (organisational and legislative) be improved (CSF-DS5)?

- Is tailored content for employees important (CSF-DS2)? Why?
- Is the cultural context and the employee background important (CSF-DS4)? Why

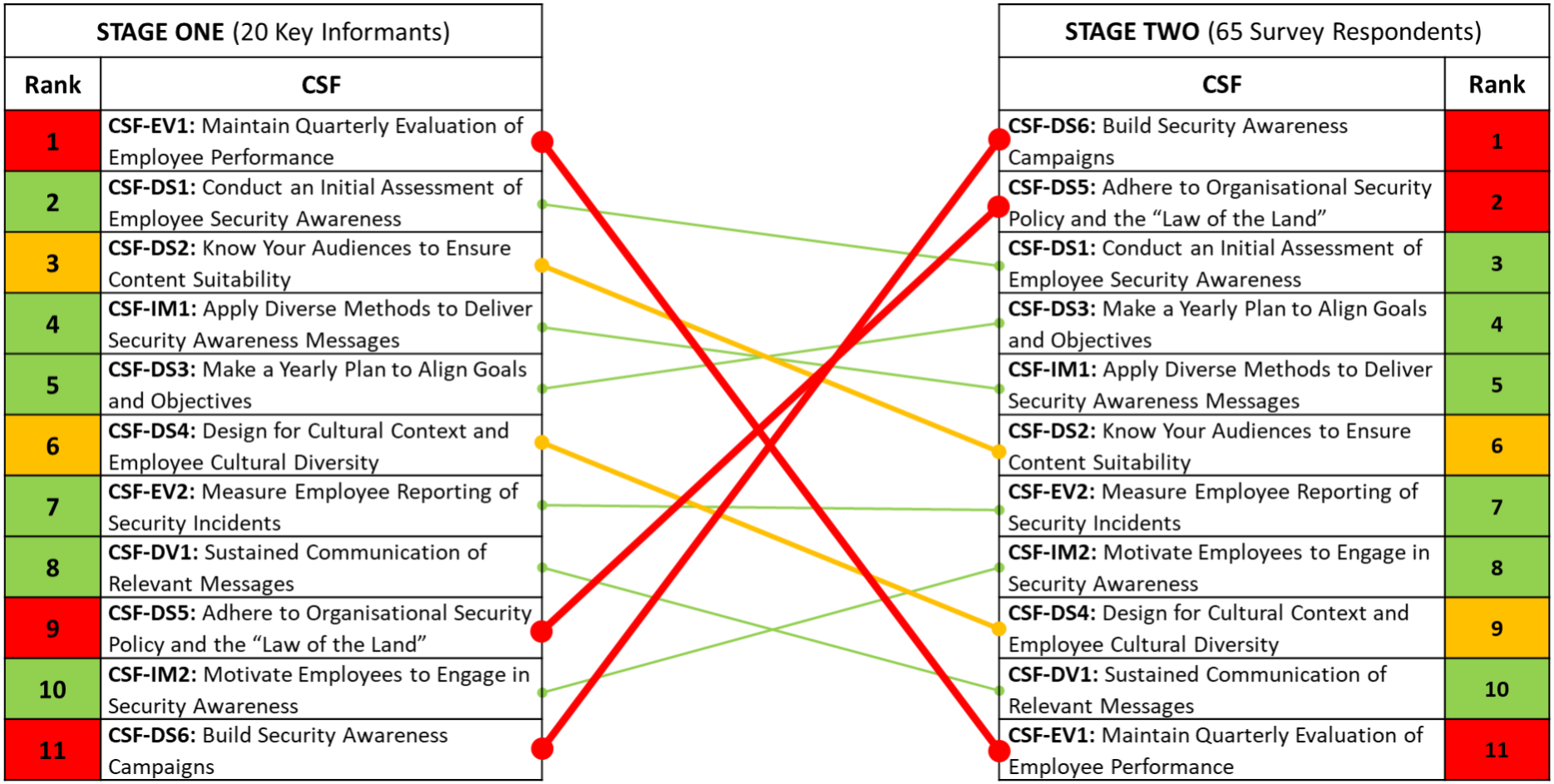


Figure 14. CSF Ranked List Comparison (Stage One and Stage Two)

Therefore, our interpretative work aims to bring to light an underlying sense of clarity. Ultimately in this stage, the researcher 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 lifecycle, while one contradiction (CSF-EV1) highlights the challenging nature of SETA programme evaluation. Therefore, these contradictions afford us the opportunity to present five principles (four in design and one in evaluation) to complement the ranked list of 11 CSFs and increase the likelihood of delivering an effective SETA programme within an organisational context (see Table 19). These principles are ordered by the degree of difference (contradiction) between the stage one and stage two rankings (based on the outcome of our comparative work).

CSF	**Ranking (Stage)**		**Principle**
	One	**Two**	
CSF-DS6: Build Security Awareness Campaigns	11	1	Raise employee 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 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 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

Table 19.Principles for Five CSFs with Difference/Contradiction

In the next section, the researcher presents a discussion of our research findings.

5.4 Discussion of Findings

The outcome of this research suggests that there is no significant difference between the 20 key informants (stage one) and 65 survey respondents (stage two) 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 key areas (the differences that emerged from our comparative analysis) that need to be examined, within the context of an organisational SETA programme, to improve effectiveness. These five areas (each linked to a CSF) are presented as principles to complement the CSFs. In this section the researcher now discusses these five principles to further improve the likelihood of delivering an effective SETA programme. The researcher also reflect these findings against existing literature.

5.4.1 Principle 1: raise employee cyber security awareness and knowledge to enhance organisational maturity

CSF-DS6: Build Security Awareness Campaigns focuses on updating the employee on how to mitigate against the potential risks associated with a cyber-security threat, keeping them informed on what is coming, and, most crucially, why they need to care. Figure 14 shows the contradictory views between stage one and stage two. The researcher believes that this is 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 in order 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 cyber-security practitioners highlighted that security awareness campaigns simply keep employees updated about what is going on (e.g. new cyber-attack 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 cybersecurity maturity, this is especially challenging where employees have varying levels of cybersecurity knowledge and experience (e.g. new hires vs senior leaders) and may fail to recognise an IS 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 a 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 a 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 security awareness, complying with IS security policy, and reducing IS security risks (Vroom and von Solms, 2002; Puhakainen and Siponen, 2010). Therefore, formal awareness campaigns are communications with employees with the specific aim of: [1] increasing the understanding of, and [2] reducing the likelihood of harmful information security practices within the organisation (D'arcy et al., 2009; Hearth et al., 2018).

5.4.2 Principle 2: evaluate employee performance at a frequency that aligns with the organisational 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 14 shows the contradictory views between stage one and stage two. The researcher believes that this is because the perspectives of the experts differ on whether an assessment should be conducted at the start or 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 cyber-security practitioners highlight the criticality of conducting employee

assessments to [1] assess security awareness and knowledge levels and [2] motivate employees to participate in the SETA programme. However, cyber security practitioners have differing views on whether the timeframe 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 timeframe for conducting employee assessments can be determined based on the organisational 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 the use of evaluations for the SETA programme. 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 requires further research.

5.4.3 Principle 3: secure top management support to encourage all employees to comply with IS 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 14 shows the contradictory views between stage one and stage two. The researcher believes that this is linked to the fact that some organisations design their SETA programmes in-house and ensure that their security policies are compliant 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 cyber-security practitioners highlight the need to obtain top management support to ensure that all organisational employees adhere to the IS 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 cyber security professionals enforcing severe penalties for 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 cyber security awareness. Furthermore, implementing the appropriate 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 cyber-attacks and 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 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 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 information security policy. Hu et al., (2012) also provided a detailed explanation of the significance of top management support to information security policy compliance and the change of organisational culture. Active participation by top management in the development, implementation, and enforcement of security policy can enhance employees' perceptions that information security policy and procedures are legitimate and fair (Hu et al., 2012). Therefore, top management play an important role in encouraging employees to adhere to security policy in order to deliver an effective SETA programme.

5.4.4 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 3 shows the contradictory views between stage one and stage two. The researcher believes 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 cyber security plans. Therefore, 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 cyber-security practitioners highlight the criticality of tailoring the content of the cybersecurity message to the audience level (e.g. level of education, age, role, etc.) in order to provide them with the appropriate training materials. The aim of this is to increase IS 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 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, Pelter (2005) discusses establishing a security awareness programme by classifying the audience to ensure the security message is communicated effectively. Accordingly, a SETA programme must comprise a plan to transmit the IS 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 toward its success, thereby delivering thorough security training, with appropriately suitable material, to each employee.

5.4.5 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 cyber security message can be interpreted by all employees. Figure 14 shows the contradictory views between stage one and stage two. The researcher believes this is linked to the fact that the cyber security practitioners involved in this research study come from different cultures (e.g. Saudi Arabia, Kuwait, Ireland, US, 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 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 security practice. For example, Hovav and D'Arcy (2012) examine the influence of culture on IS security policies, training, and monitoring. To understand culture in terms of IS 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 security interventions (Kirova and Baumöl et al., 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.

5.5 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), the researcher views *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 cybersecurity 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 cybersecurity 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 14.
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 19.

3. One of the first studies to highlight that the 'Design' phase of a SETA programme lifecycle will be the most contentious in terms of building a shared understanding (amongst all organisational stakeholders) of what is critical to delivering an effective SETA programme within the organisation.

Finally, to further increase the relevance of this work (around *accessibility* and *applicability*), the researcher suggests that IS practitioners use the five principles in pre-commencement readiness checks and/or in-progress reflective aids. 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. Prefacing the 5 principles (presented in Table 19) with *"Do We"* allows each principle to serve [1] as a pre-commencement readiness check to guide SETA programme endeavours along the design, development, implementation, and evaluation phases of the lifecycle; and/or [2] as an in-progress reflective aid for practitioners to assess the efficacy of their existing lifecycle phase activities. The researcher believes that asking and answering these five questions will help to start conversations and build a shared understanding amongst organisational cybersecurity 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 lifecycle. 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.

5.6 Recommendations for Future Research

Using a three-stage research approach to capture cybersecurity 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 lifecycle phases) and the 5 principles to further improve the likelihood of delivering an effective SETA programme within an

organisational context. However, these CSFs and principles are not yet established as universal, so while these CSFs and 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, the researcher is 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 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). The researcher imagines that has laid the foundations by proposing the 11 CSFs and 5 principles in this study. Therefore, further progress in this line of enquiry could be made through either qualitative, quantitative or mixed-method approaches. In fact, there is an opportunity to look more closely at the differences in the CSFs by industry, sector (public v private), organisation type (SME v MNC), and organisation size (# of employees), to further examine the difference in CSFs across organisational contexts.

Finally, the researcher has identified 11 CSFs for SETA programme effectiveness, there is a need to examine the *"conjunctural"* (Ragin, 1987) nature of these CSFs and their effects on the effectiveness of a SETA programme. Such an appreciation would further improve our understanding regarding the complexity of SETA programmes. Moving beyond single factor analysis and away from the embryonic mindset of simple lists and classifications of CSFs would be a positive development. Being able to *"chain"* CSFs for SETA programme effectiveness *"over time"* would provide a *"what led to what"* (c.f. Hubberman and Miles, 1994, p.146) appreciation, which would lend itself to the development of a process model for SETA programmes across the lifecycle phases (design, development, implementation, evaluation). This process theory would be presented as a causal map (network style display) as opposed to a parsimonious list of variables or a matrix.

Chapter Six: Discussion and Conclusion

6. Discussion and Conclusion

6.1 Introduction

This chapter builds on the previous chapters to (i) discuss the research findings (how the CSFs positively impact the effectiveness of the SETA programme), (ii) highlight research contributions, and (iii) draw conclusions. It begins by answering the research questions of this study. The research objective is "***to explore the Critical Success Factors (CSFs) for Security Education, Training and Awareness (SETA) programme effectiveness"***. This is accomplished by answering the following research questions:

- **RQ1:** What are the CSFs for SETA programme effectiveness?
- **RQ2:** How are these CSFs for SETA programme effectiveness mapped along the SETA programme lifecycle (design, development, implementation, evaluation)?
- **RQ3:** What is the ranked order of these CSFs for SETA programme effectiveness?

The remainder of this chapter is organised as follows: Section 6.2 presents a summary of the eleven CSFs for SETA programme effectiveness (RQ1). Section 6.3 illustrates the possible relationships between the CSFs for SETA programme effectiveness (RQ2). Section 6.4 provides a comparison between the CSFs (RQ3). Section 6.5 compares the findings with the literature. Finally, Section 6.6 presents the conclusion and research implications, including research contributions, implications for theory and practice, limitations, and future work.

6.2 CSFs for the SETA programme effectiveness

The CSFs were identified based on an analysis of twenty key informant accounts of the SETA programme's effectiveness. The eleven CSFs are associated with the phases of a SETA programme lifecycle: design, development, implementation, and evaluation. Accordingly, the researcher identified six CSFs associated with the design phase (CSF-DS1, CSF-DS2, CSF-DS3, CSF-DS4, CSF-DS5, CSF-DS6), one CSF associated with the development phase (CSF-DV1), two CSFs associated with the implementation phase (CSF-IM1, CSF-IM2), and two CSFs associated with the evaluation phase (CSF-EV1, CSF#10,11). These CSFs are presented in Table 20 below.

Lifecycle Phase	Category	CSF	Description
Design	Assessment Needs	**CSF-DS1:** Conduct an Initial Assessment of Employee Security Awareness	determining what the employee understands about the organisation's security policy and their appreciation of the risks associated with current cyber security threats.
	Target Audiences	**CSF-DS2:** Know Your Audiences to Ensure Content Suitability	identifying "who your audiences are" to ensure appropriate content is delivered to the various employee types.
	Goal/Objective	**CSF-DS3:** Make a Yearly Plan to Align Goals and Objectives	knowing what is required to be delivered to the employee to ensure that the SETA programme goals meet the specific needs of the organisation.
	Culture	**CSF-DS4:** Design for Cultural Context and Employee Cultural Diversity	understanding the diversity of employee backgrounds (e.g. language, culture, knowledge, level of education, age, gender) so that the cyber security message can be interpreted by all employees.
	Policy	**CSF-DS5:** Adhere to Organisational Security Policy and the "Law of the Land"	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.
	Communication	**CSF-DS6:** Build Security Awareness Campaigns	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.
Development	Communication	**CSF-DV1:** Sustained Communication of Relevant Messages	repeating the cyber security message in various ways to avoid a lapse in employee concentration.
Implementation	Communication Channel	**CSF-IM1:** Apply Diverse Methods to Deliver Security Awareness Messages	using various approaches to deliver 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 cyber security issue.
	Motivation	**CSF-IM2:** Motivate Employees to Engage in Security Awareness	encouraging the employee to adhere to IS security policies by earning a bonus, or other recognition (rewards), based on their practices.
Evaluation	Periodic Assessment	**CSF-EV1:** Maintain Quarterly Evaluation of Employee Performance	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.
	Incident Indication	**CSF-EV2:** Measure Employee Reporting of Security Incidents	using phishing campaigns to simulate attacks (knowing how many employees click the suspicious links), in order to measure the employee awareness and knowledge regarding cyber security issues.

Table 20.The CSFs for SETA Programme Effectiveness

6.3 Possible CSFs relationships

Further analysis of the eleven CSFs for the SETA programme's effectiveness reveals a series of relationships between some of the CSFs. As previously discussed, the researcher found nine relationships between the CSFs (four *within* the SETA programme lifecycle phases (design, development, implementation, evaluation) and five *across* the lifecycle phases). These relationships are considered significant for SETA programme effectiveness. The analysis of the data showed that a CSF can impact on one or more of the other CSFs, as discussed in Chapter 4 (paper 3). The CSFs and the relationships are visualised in the *lifecycle model of CSFs for SETA programme effectiveness* (see Figure 15).

Our analysis identified and described four relationships *within* the SETA programme lifecycle phases (design, development, implementation, evaluation) (see Table 21). These relationships are as follows: CSF-DS3 impacting CSF-DS4 and CSF-DS5 (**planning**); CSF-DS1 and CSF-DS2 impacting CSF-DS6 (**informing**); CSF-IM1 impacting CSF-IM2 (**encouraging**); and CSF-EV1 impacting CSF-EV2 (**assessing**).

The researcher identified and described five relationships between the CSFs *across* the SETA programme lifecycle phases (see Table 22). These relationships are as follows: CSF-DS6 impacting CSF-EV2 (**valuing**); CSF-DS4 impacting CSF-IM1 (**contextualising**); CSF-IM1 impacting CSF-DV1 (**re-emphasizing**); CSF-IM2 impacting CSF-DS5 (**recognising**); and CSF-EV1 impacting CSF-DS3 (**scheduling**). These nine relationships are deemed important for SETA programme effectiveness across the SETA programme lifecycle phases (design, development, implementation, and evaluation) as they deliver valuable insight and understanding of the process of leading an effective SETA programme in practice.

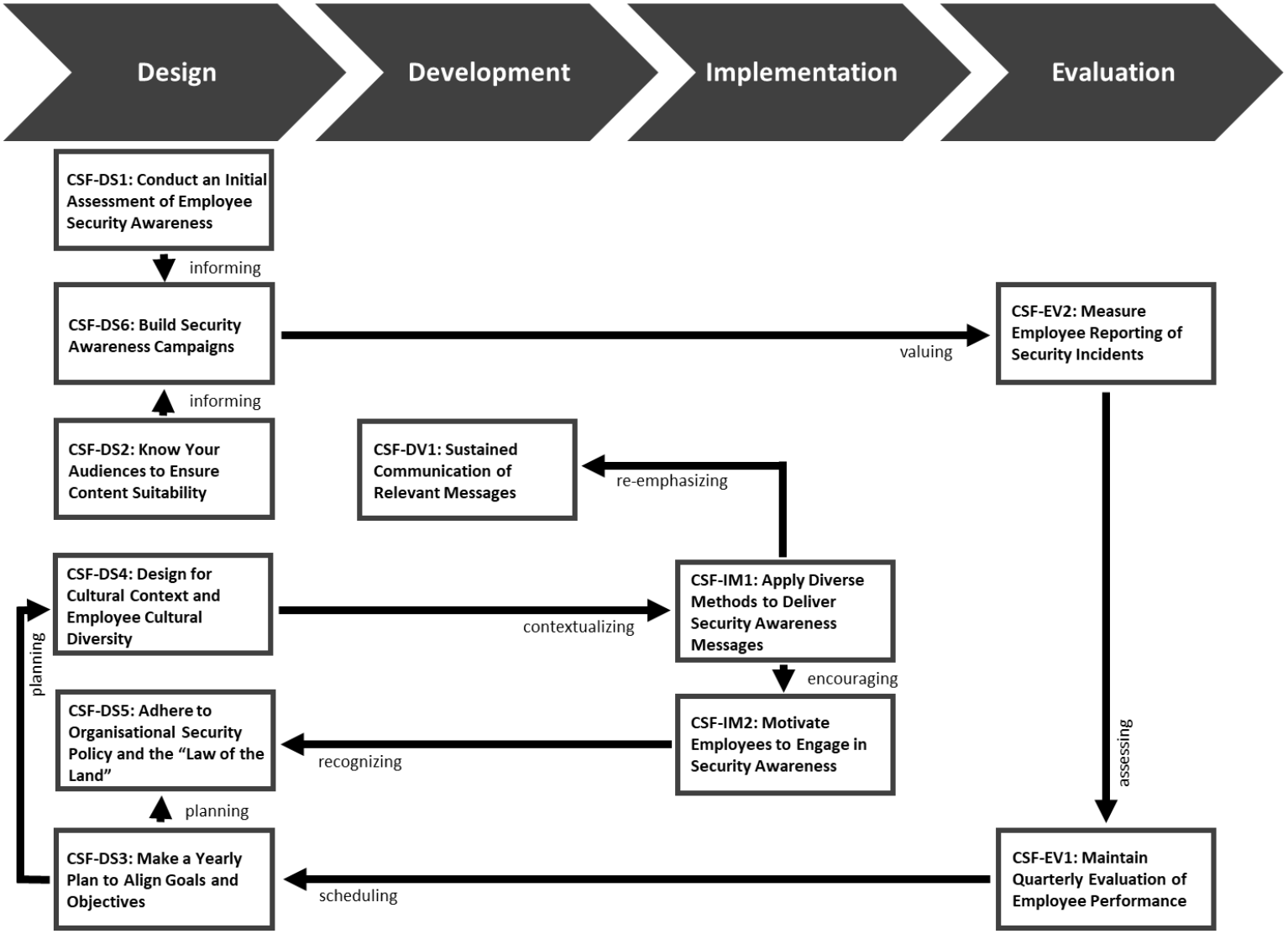


Figure 15. The Lifecycle Model of CSFs for SETA Programme Effectiveness

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 organisational cultural context.
	CSF-DS5: Adhere to Organisational Security Policy and the "Law of the Land"		Enables the design of a programme plan that considers organisational security policy and geographical legislation.
CSF-DS1: Conduct an Initial Assessment of Employee Security Awareness	**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-DS2: Know Your Audiences to Ensure Content Suitability			
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.

Table 21. The relationships between the CSFs within the SETA programme lifecycle phases.

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 employees' 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	**Contextualising**	Enables the use of different communication channels in order to deliver a culturally contextualised security message.
CSF-IM1: Apply Diverse Methods to Deliver Security Awareness Messages	**CSF-DV1:** Sustained Communication of Relevant Messages	**Re-emphasising**	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 Organisational Security Policy and the "Law of the Land"	**Recognising**	Enables the motivation of employees through earning recognition 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 organisational performance-to-plan.

Table 22.The relationships between the CSFs across the SETA programme lifecycle phases.

6.4 Comparison between the CSFs

This section aims to evaluate the eleven CSFs for the SETA programme effectiveness reported in Chapter 5 (paper 4). It reports on stage two of the multi-stage research design to evaluate the importance of the CSFs for SETA programme effectiveness. In stage one, an analysis of 20 key informant interviews produced the eleven CSFs, ranked in a prioritised order (descending) based on the frequency count of coded excerpts across the 20 interview transcripts (see Table 23) which ranks the CSFs from 1 to 11.

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

Table 23.CSFs Ranking (Stage One - ranked by frequency count of codes).

As represented in Table 23, the researcher is ranking the CSFs 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 8th in Table 22) is 1.8, calculated as ((12*3)/20). Also, as shown in Table 23, the number one ranked CSF is in the evaluation phase: **CSF-EV1** (*Maintain Quarterly Evaluation of Employee Performance*), while the lowest ranked CSF is in the design phase: **CSF-DS6** (*Build Security Awareness Campaigns*).

In stage two, the researcher analysed 65 survey responses (IS/cyber security practitioners with SETA programme experience) to generate an independently ranked list of the CSFs, based on the mean score ranking. The result of the short survey involved respondents ranking the importance of a specific CSF (high/medium/low). Then, the researcher compared this ranked list to the ranked list generated in stage one. This comparison highlights the position of each CSF in the respective lists and suggests the similarities and differences between the lists (see Figure 16).

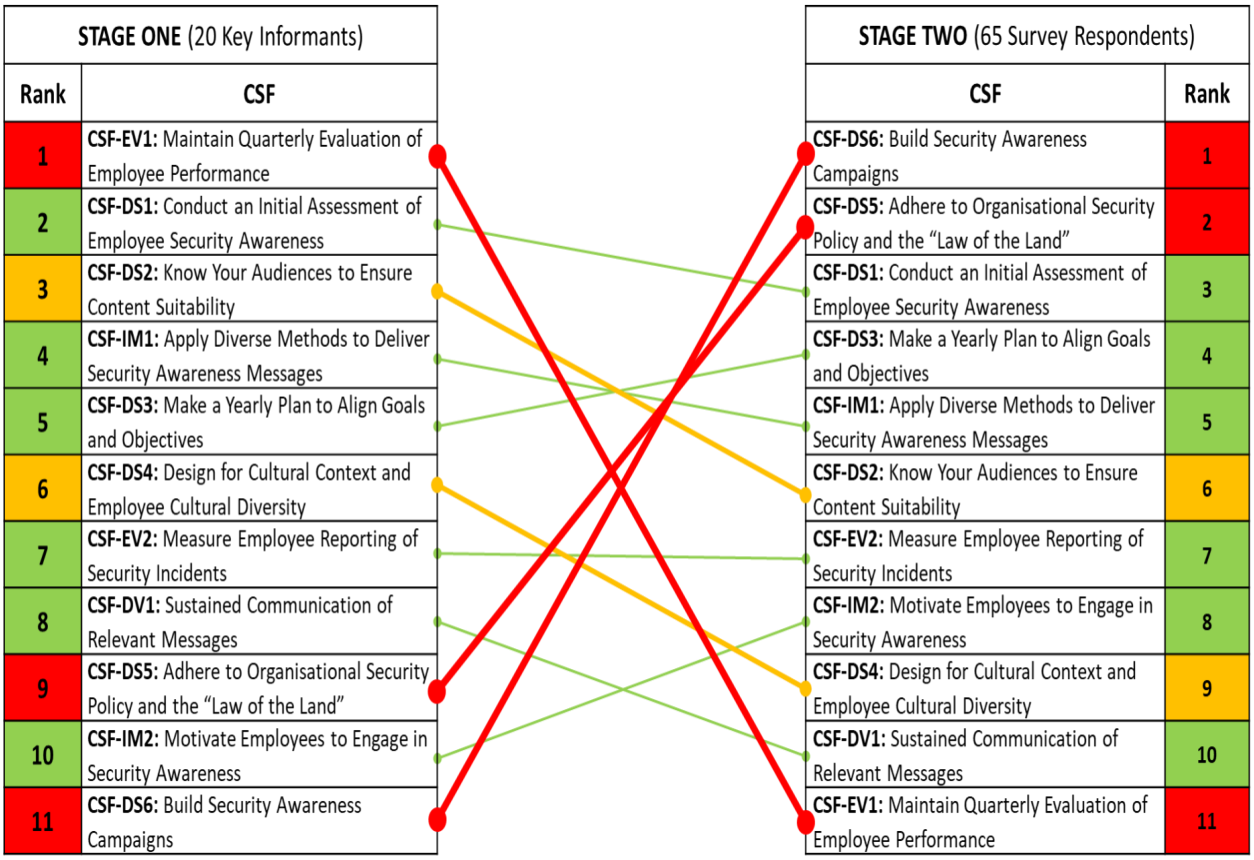


Figure 16. CSF Ranked List Comparison (Stage One and Stage Two).

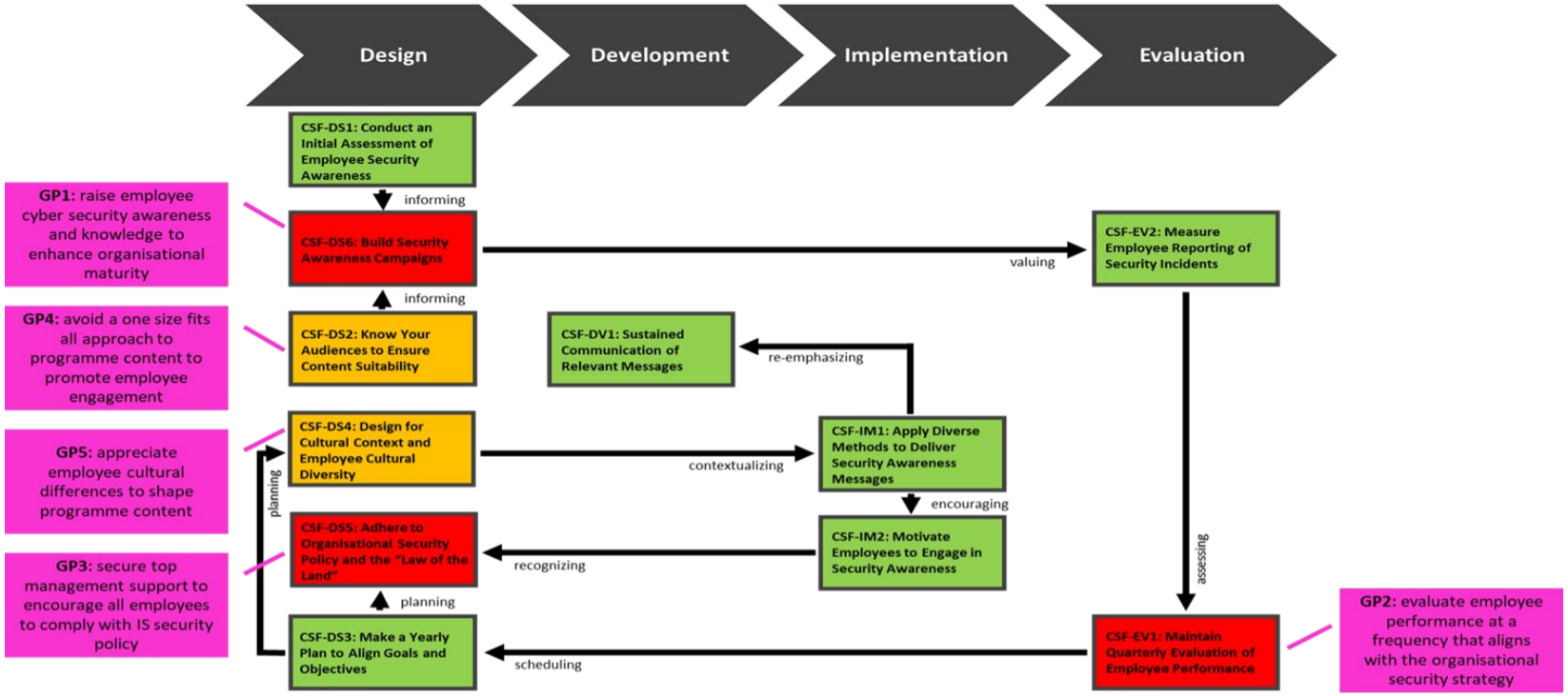
Figure 16 shows a somewhat contradictory element to the CSF rankings between stages one and two. In total, five critical areas of difference emerged from our comparative analysis of the ranked lists of 11 CSFs, which are (CSF-DS2, CSF-DS4, CSF-DS5, CSF-DS6, and CSF-EV1). Therefore, to understand more about these differences in the CSFs ranking, and why these differences materialised, the researcher conducted follow-up probing interviews with nine practitioners (four participants from stage one five from stage two). The aim was to get a deeper insight into the CSFs.

Furthermore, the researcher used a hermeneutics-inspired approach to analyse and interpret the follow- up interviews. Therefore, the researcher discovered reasons for the importance of CSF-DS6, CSF-EV1, CSF-DS5, CSF-DS2, and CSF-DS4 which led to the identification of five principles (to complement the CSFs). Four principles linked to the design phase, with one linked

to the evaluation phase. This result aims to further improve the likelihood of delivering an effective SETA programme. These five principles are presented in Table 24 and overlaid on an *evaluated* Lifecycle Model (see Figure 17).

CSF	Principle	Description
CSF-DS6: Build Security Awareness Campaigns	Raise employee cyber security awareness and knowledge to enhance organisational maturity	Raising the level of cyber security awareness by keeping the employee up-to-date on potential IS Security risks.
CSF-EV1: Maintain Quarterly Evaluation of Employee Performance	Evaluate employee performance at a frequency that aligns with the organisational security strategy	The annual number of employee performance evaluations varies from organisation to organisation. Aims to provide their employee with a vital enhancement.
CSF-DS5: Adhere to Organisational Security Policy and the "Law of the Land"	Secure top management support to encourage all employees to comply with IS security policy	Obtaining the support of top management to implement and adhere to the IS security policy.
CSF-DS2: Know Your Audiences to Ensure Content Suitability	Avoid a one size fits all approach to programme content to promote employee engagement	To ensure employee engagement with the security awareness message, the message must be tailored to employee differences.
CSF-DS4: Design for Cultural Context and Employee Cultural Diversity	Appreciate employee cultural differences to shape programme content	Understanding cultural differences is crucial in designing an effective SETA programme.

Table 24.Principles for Five CSFs with Difference/Contradiction.



Relationship	**Description** (enables the...)
Planning	design of a programme plan that aligns with the organisational cultural context.
	design of a programme plan that considers organisational security policy and geographical legislation.
Informing	delivery of appropriate campaign materials reflecting the awareness and knowledge levels of the target audiences.
Encouraging	use of different communication methods to motivate employees to engage with IS security training materials.
Assessing	performance of an employee to be evaluated using the number of security incidents reported by the employee.
Valuing	use of a simulation attack to raise employee's knowledge of security incidents and ensures these incidents are reported appropriately.
Contextualizing	use of different communication channels in order to deliver a culturally contextualized security message.
Re-emphasizing	use of different communication channels with the aim of repeating important security awareness messages.
Recognizing	motivation of employees through earning recognitions and rewards for complying with IS security policy and legislation.
Scheduling	production of a new security plan based on the outcome of the current organizational performance-to-plan.

Figure 17. The "evaluated" Lifecycle Model of CSFs for SETA Programme Effectiveness.

6.5 Comparison with the IS Security literature

As mentioned in the introduction (Chapter 1), there are no comprehensive studies focusing on the Critical Success Factors (CSFs) for Security, Education, Training and Awareness (SETA) programme effectiveness. Reviewing the current literature provides several observations that can be made around the criticality of these CSFs for SETA programme effectiveness. There is good support in the literature for the majority of the CSFs (or, more specifically, the emerging category associated with each CSF) across the lifecycle phases. However, these studies discuss some, but not all, of these CSFs associated with SETA programme effectiveness. Furthermore, based on our empirical analysis, the researcher can see limited investigations into four specific CSFs (centring 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 Chapter 4 – paper 3).

6.5.1 Mapping CSFs to the IS "security themes"

Based on our review of the literature, this section discusses the impact of the CSFs for SETA programme effectiveness on the four IS "security themes" identified in Chapter 2 (paper 1), as follows: *IS Security Awareness (ISA)*, *IS Security Policy (ISP)*, *IS Security Management (ISM)* and *IS Security Behaviour (ISB)*. For example, effective SETA programmes are linked to: (i) changing individuals' behaviours (Posey et al.,2013; Yaokumah et al.,2019; Alshaikh et al.,2019), (ii) compliance with IS policy (Han et al.,2017; Barlow et al.,2018; Dhillon et al.,2020), (iii) increasing the level of individual awareness (Heikka, 2008; Lebek et al., 2014; Tsohou et al., 2015), and (iv) managing IS security risks (Chander et al., 2013; Kumah et al., 2019; Topa et al.,2019). Figure 18 presents a mapping of the CSFs (emerging from our empirical work (see Chapter 3 – paper 2)) to the key messages for SETA programme effectiveness across the four IS "security themes" (emerging from our review of the literature) visualised in Chapter 2 (paper 1).

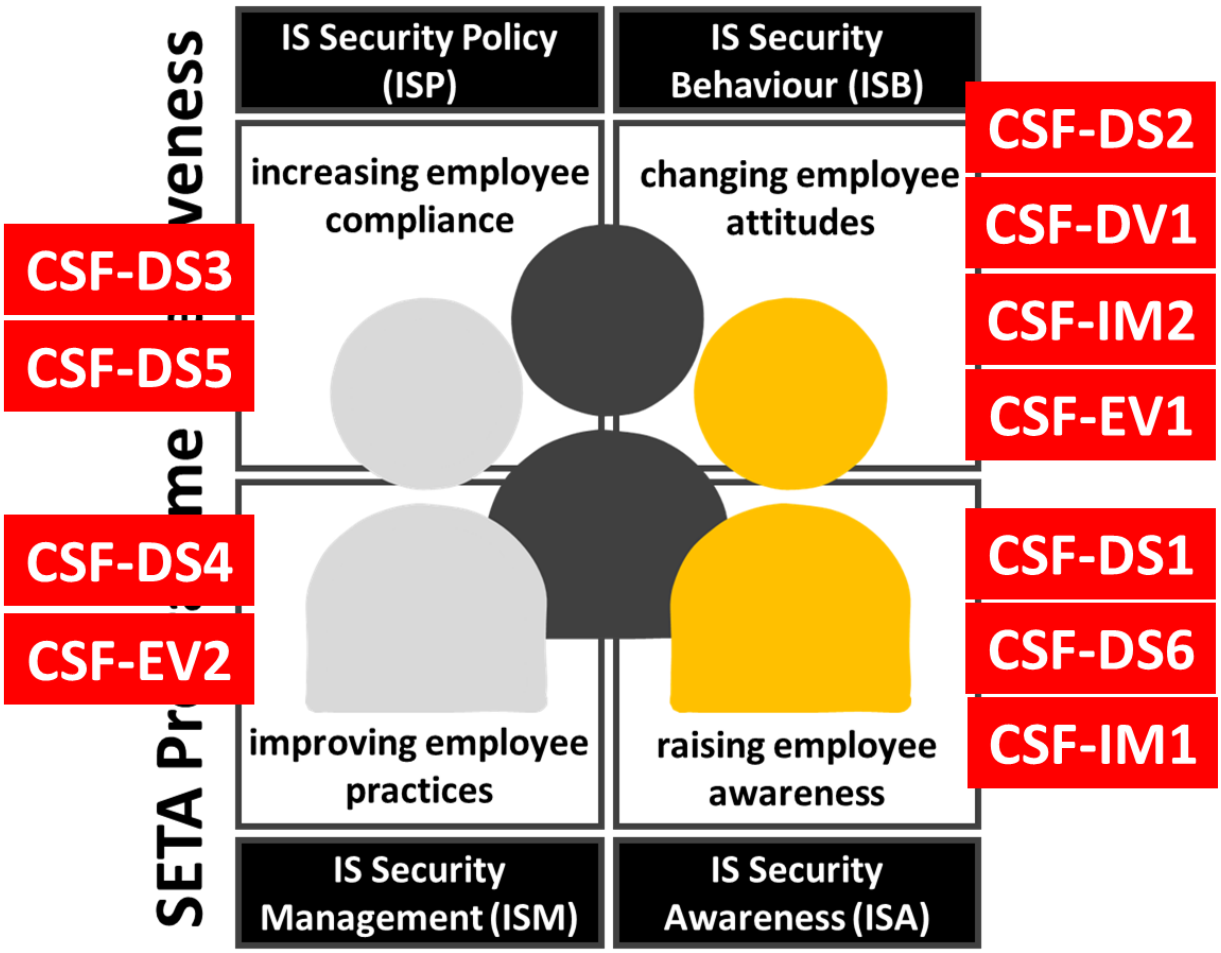


Figure 18.Mapping the CSFs to the Key Messages for SETA Programme Effectiveness

However, based on our analysis, the researcher has identified that a limited number of studies examine the impact of three CSFs (**CSF-DS1**, **CSF-DS6**, **CSF-IM1**) (or more specifically, the emerging category associated with each CSF) on raising employee awareness (ISA). For example, Peltier (2005) suggests that when organisations use assessments to determine the expected threats and the associated risk level of these threats, then the information needed to protect the organisation is provided. The outcome of the assessments helps to determine the needs that must be covered. Thus, understanding the results of the assessment assist in creating security awareness plan to raise the level of IS security awareness. Siponen (2000) argued for raising the consciousness of security through designing security awareness campaigns. The importance of awareness campaigns or programmes is growing in a cybersecurity culture and is widely recognised within the SETA programme (Reid and Van Niekerk, 2016). They are also raising the

employee's awareness of their organisation's vulnerability as a result of IS security threats. Tsohou et al., (2015) developed a theoretical framework to address how SETA programmes raise security concerns among individuals. They contend that the SETA programme has a positive influence on the employee's ISA level.

While other studies examine the impact of two CSFs (**CSF-DS3**, **CSF-DS5**) (or more specifically, the emerging category associated with each CSF) on increasing employee compliance (ISP). For example, a plan and new security policies to address any ongoing challenges (from previous years) and to ensure the delivery of a successful SETA programme (Alshaikh et al., 2021). Therefore, to establish the SETA programme, one must have a clear goal that supports the organisation's overall mission. The security policies are presented to the employees to show what is expected from them. A SETA programme assists employees to eliminate obstacles at work and support achieving ISP's compliance. (D'Arcy et al., 2009; Hearth et al., 2018). Thus, the employee should follow the policies and regulations to deal with issues such as: how to deal with suspicious sites, how to keep company data confidential, and which information can be shared on social media.

Moreover, a limited number of studies examine the impact of two CSFs (**CSF-DS4**, **CSF-EV2**) (or more specifically, the emerging category associated with each CSF) on improving employee practices (ISM) related to IS security risks. For example, a study by Babatunde and Selamat (2012) examined how factors such as standards, policies, training programmes, cultures, employee motivation, and top management commitment affect ISM development and performance. Understanding the various aspects of the culture assists in controlling IS security risks and attacks. Additionally, measuring the security standards management improves practice security management (D'Arcy et al., 2009; Topa and Karyda, 2019). For example, Topa and Karyda (2019) investigate the effect of security standards to control and reduce IS security attacks.

Lastly, other studies examine the impact of four CSFs (**CSF-DS2**, **CSF-DV1**, **CSF-IM2**, **CSF-EV1**) (or more specifically, the emerging category associated with each CSF) on changing employee attitudes (ISB). For example, Kirova and Baumöl (2018) identify factors (e.g. standards and regulations, communication, fear, security policy) that affect positively on individual behaviour. Furthermore, according to Barlow et al. (2018), continuous communication plays an

important role in reminding the employee of the current IS security issues and enhancing their attitude toward dealing with IS security risks. Researchers have also suggested using a rewards system integrated with the SETA programme, to help to improve employee behaviour (Cram et al.,2019). Therefore, an important feature of these CSFs is where a lack of employee behaviour changes and engagement is a reported concern impacting negatively on SETA programme effectiveness.

6.6 Conclusions and Research Implications

IS security threats are currently regarded as one of the top concerns in organisations/businesses. In fact, one of the important countermeasure mechanisms to reduce IS security risks is the Security Education Training and Awareness (SETA) programme (D'Arcy et al., 2009; Bulgurcu et al., 2010; Haeussinger and Kranz,2013; Koohang et al.,2020). The impact of SETA programmes is widely accepted by both academics and practitioners (Wilson and Hash, 2003; D'Arcy *et al.*, 2009; Tsohou *et al*., 2015; Alshaikh *et al*., 2018). A review of the literature on the effectiveness of the SETA programme reveals that a lack of comprehension of the nature of the SETA programme is seen as the primary reason for its ineffectiveness (Hu et al., 2021). It is arguing more theorising and conceptual clarity are needed in investigating the effectiveness of SETA programmes (c.f. Alshaikh et al., 2021; Hu et al., 2021b; Kirova and Baumöl, 2018; Puhakainen and Siponen, 2010). Current studies fail to examine all of the phases of the SETA programme lifecycle (design, development, implementation, evaluation), and focus just 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). This research study aimed to leverage the conceptual need by exploring the Critical Success Factors (CSFs) for SETA programme effectiveness that are mapped along the phases of a lifecycle (design, development, implementation, evaluation). Thus, doing this exploratory study led to the identification of the CSFs for SETA programme effectiveness which is not well-explored area of IS research.

This PhD research study is based on a collection of papers (see Chapters 2, 3, 4 and 5). This collection of papers provides an insight into the evolution of the research around the CSFs for SETA programme effectiveness. Figure 19 provides a diagrammatic view of the structure of the thesis.

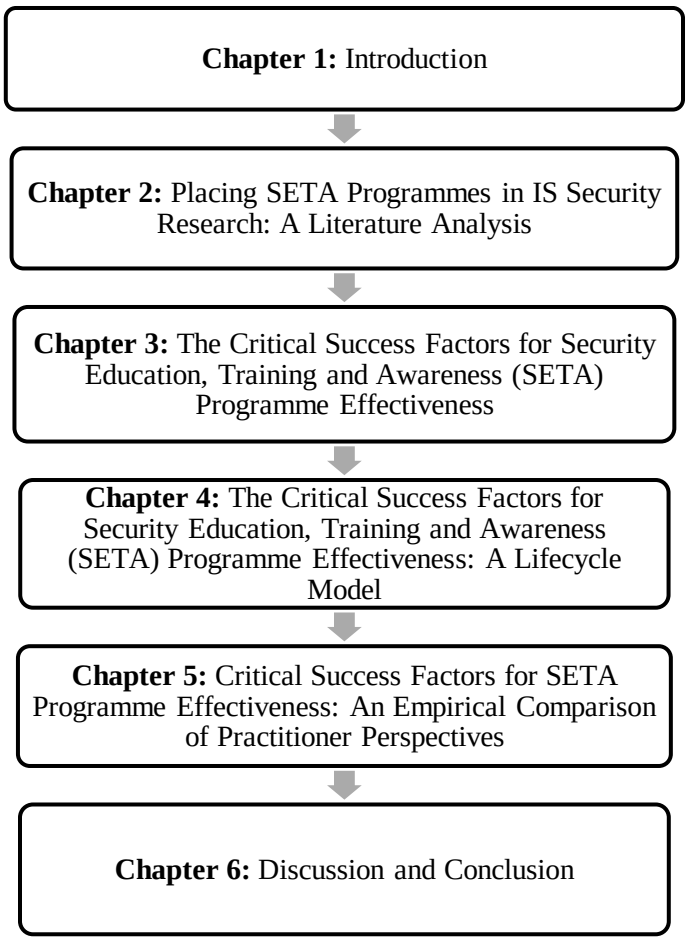


Figure 19. Structure of the Thesis.

Paper 1 (Chapter 2) is the literature review chapter that introduces the IS "security themes" and the role of SETA programmes within each theme. Paper 2 (Chapter 3) presents eleven CSFs for SETA programme effectiveness. These are based on the analysis of 20 key informant interviews. This paper provides a full description of the CSFs for the SETA programme effectiveness. Paper 3 (Chapter 4) presents nine relationships between the CSFs for SETA programme effectiveness (visualised as a lifecycle model). Paper 4 (Chapter 5) evaluates the importance of the eleven CSFs for SETA programme effectiveness. This paper compares stage one (semi-structured interviews with 20 key informants) and stage two (65 respondents to an online survey questionnaire and semi-structured interviews with 9 cyber security practitioners) outputs; the result being five principles to complement the eleven CSFs in the delivery of an effective SETA programme.

6.6.1 Research Contributions and Implications

This research study offers a number of contributions to academics and practice, both in terms of what was accomplished and how it was done. These main contributions have been presented across the collection of papers and as a digest in Chapter 1 (Section 1.3).

The eleven CSFs identified for SETA programme effectiveness provides future researchers and practitioners with guidelines in how to conduct an effective SETA programme. Thus, there is an opportunity for researchers to extend the CSFs list in the future. They can apply a range of different research methods to collect and analysis research data. Furthermore, addressing the relationships between the CSFs for SETA programme effectiveness led to the Lifecycle Model of CSFs for SETA programme effectiveness. This lifecycle model is a foundation for further studies. The researcher suggests that researchers can examine these relationships further, providing a good opportunity to test and evaluate the existing relationships and identify new relationships between the CSFs. Furthermore, the emergence of the five principles to complement the CSFs can also be examined within the context of an organisational SETA programme (e.g. within SME and MNC contexts) in an effort to compare and contrast perspectives on SETA programme effectiveness.

Lastly, in terms of practice implications, in this study, the researcher evaluated the identified CSFs in order of importance. The researcher presented a ranked list of CSFs for SETA programme effectiveness, mapped against the four phases of the SETA programme lifecycle (design, development, implementation, and evaluation) to provide a full picture to establish an effective SETA programme. Thus, practitioners can use our findings as guidance to establish an effective SETA programme.

6.6.2 Limitations and Future Research

During this PhD study, the researcher strove to achieve the highest level of objectivity, accuracy and validity. However, all research studies are commonly constrained by a number of factors and this research study is not without limitations. Thus, future research can overcome the several limitations of this study which are addressed as follows.

Due to the time frame allocated for a PhD thesis, the researcher missed the opportunity to examine the differences in CSFs by industry sector (public v private), organisation type (SME v MNC), and organisation size (# of employees). Thus, for future work, it is recommended that researchers further examine the identified CSFs across organisational contexts to learn more about SETA programme effectiveness. In addition, the existing relationships between the CSFs for the SETA programme effectiveness require further investigation and study in order to establish any additional connections between the CSFs. This will further enhance our understanding of the CSFs and improve the utility of the lifecycle model. Such an appreciation would further advance our knowledge of the complexity of SETA programmes. This would facilitate a further (i) evaluation and (ii) enhancement of the process model for SETA programme effectiveness presented in this thesis.

References:

Alhassan, I., Sammon, D., and Daly, M. (2019). Critical Success Factors for Data Governance: A Theory Building Approach. *Information Systems Management*, 36(2), pp.98-110, https://doi.org/10.1080/10580530.2019.1589670

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

Almeida, L., & Respício, A. (2018). Decision support for selecting information security controls. *Journal of Decision Systems*, *27*(sup1), 173-180. https://doi.org/10.1080/12460125.2018.1468177

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*, *34*(2), 770-788. DOI: https://doi-org.ucc.idm.oclc.org/10.1108/ITP-06-2019-0269

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

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*, *9*, 5085 5094.https://doi.org/10.24251/hicss.2018.635

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*, *100*, 102090. https://doi.org/10.1016/j.cose.2020.102090

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)*, 0–14. Retrieved from https://aisel.aisnet.org/ecis2019_rp/100

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

Averweg, U. R., and Kroeze, J. H. (2012). Practitioner-based research in Information Systems. *TD: The Journal for Transdisciplinary Research in Southern Africa*, *8*(2), 252-267.

Babatunde, D. A., & Selamat, M. H. (2012). Investigating information security management and its influencing factors in the Nigerian banking industry: a conceptual model. *International Journal on Social Science & Art*, *2*(2), 55-59.

Backhouse, J., Hsu, C. W., & Silva, L. (2006). Circuits of power in creating de jure standards: Shaping an international information systems security standard. *MIS quarterly*, 413-438.

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, 19(8), 689–715. https://doi.org/ 10.17705/1jais.00506

BASIT, T. 2003. Manual or electronic? The role of coding in qualitative data analysis. *Educational research,* 45**,** pp.143-154.

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*, *68*, 145–159. https://doi.org/10.1016/j.cose.2017.04.009

Bharadwaj, A.S. (1996). Integrating Positivist and Interpretive Approaches to Information Systems Research: A Lakatosian Model. Second Americas Conference on Information Systems, Phoenix, Arizona, August 16-18.

Bhattacherjee, A. (2012). Social science research: Principles, methods, and practices (2nd ed.). Tampa, FL: CreateSpace Independent Publishing Platform.

Borman, M., & Janssen, M. (2013). Reconciling two approaches to critical success factors: The case of shared services in the public sector. *International Journal of Information Management*, *33*(2), 390-400.

Boss, S., Galletta, D., Lowry, P.B., Moody, G.D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. MIS Quarterly (MISQ), 39(4), 837–864. https://doi.org/10.25300/MISQ/2015/39.4.5

Brehmer, M., Abbas, A. E., and Vaidyanathan, N. (2021). Towards Designing a Method to Create Sticky Information Security Training for SMEs: Identifying Design Factors. In 29th European

Conference on Information Systems (ECIS 2021): Human Values Crisis in a Digitizing World (pp. 1-13). Association of the Information Systems (AIS). https://aisel.aisnet.org/ecis2021_rip/28/

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, 34(3), 523–548. https://doi.org/10.2307/25750690

Bullen, C. V., and Rockart, J. F. (1981). A primer on critical success factors.

Burns, A. J., Roberts, T. L., Posey, C., Bennett, R. J., and Courtney, J. F. (2018). Intentions to Comply Versus Intentions to Protect: A VIE Theory Approach to Understanding the Influence of Insiders 'Awareness of Organizational SETA Efforts. *Decision Sciences*, *49*(6), 1187–1228. https://doi.org/10.1111/deci.12304

Burton-Jones, A., McLean, E. R., & Monod, E. (2015). Theoretical perspectives in IS research: from variance and process to conceptual latitude and conceptual fit. *European journal of information systems*, *24*, 664-679.

Chander, M., Jain, S. K., & Shankar, R. (2013). Modeling of information security management parameters in Indian organizations using ISM and MICMAC approach. *Journal of Modelling in Management*.

Chen, X., Wu, D., Chen, L., & Teng, J.K. (2018). Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables. Information & Management, 55(8), 1049–1060. https://doi.org/10.1016/j.im.2018.05.011

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*, *55*(3), 11-19. http:10.1080/08874417.2015.11645767

Choobineh, J., Dhillon, G., Grimaila, M. R., & Rees, J. (2007). Management of information security: Challenges and research directions. *Communications of the Association for Information Systems*, *20*(1), 57.

Chowdhury, M. F. (2014). Interpretivism in aiding our understanding of the contemporary social world. *Open Journal of Philosophy*, *2014*.

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, 43(2), 525–554. https://doi. org/10.25300/MISQ/2019/15117

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. Computers & Security, 32(3), 90–101. https://doi.org/10.1016/j.cose.2012.09.010

Crowston, K. (2000). Process as theory in information systems research. In *Organizational and Social Perspectives on Information Technology: IFIP TC8 WG8. 2 International Working Conference on the Social and Organizational Perspective on Research and Practice in Information Technology* June 9–11, 2000, Aalborg, Denmark (pp. 149-164) Springer US.

D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. European Journal of Information Systems, 20(6), 643–658. https://doi.org/10.1057/ejis.2011.23

D'Arcy, J., Herath, T., Yim, M.-S., Nam, K., and Rao, H. R. (2018). Employee Moral Disengagement in Response to Stressful Information Security Requirements: A Methodological Replication of a Coping-Based Model. *AIS Transactions on Replication Research*, *4*(June), 1–18. https://doi.org/10.17705/1atrr.00028

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*, *20*(1), 79 98.https://doi.org/10.1287/isre.1070.0160

D'Arcy, J., & Lowry, P. B. (2017). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*, *29*(1), 43-69. DOI: 10.1111/isj.12173

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*, (2007), 49–58. https://doi.org/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, 109(8), pp.1037–1052. doi:10.1108/0263557091099

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*, *21*(1), 152–174. https://doi.org/10.17705/1jais.00595

Djajadikerta, H.G., Roni, S.M., & Trireksani, T. (2015). Dysfunctional information system behaviors are not all created the same: Challenges to the generalizability of security-based research. Information &Management, 52(8), 1012–1024. https://doi.org/10.1016/j.im.2015.07.008

Dupuis, M., Geiger, T., Slayton, M., & Dewing, F. (2019, September). The use and non-use of cybersecurity tools among consumers: Do they want help?. In *Proceedings of the 20th Annual SIG Conference on Information Technology Education* (pp. 81-86)

Flores, W.R., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. Computers & Security, 43(6), 90–110. https://doi.org/10.1016/j.cose.2014.03.004

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*, *16*(1), pp.15-31.

Global Market Estimates. (2022). 2022 Cybersecurity Awareness Training Market report.

Goel, S., & Chengalur-Smith, I. N. (2010). Metrics for characterizing the form of security policies. Journal of Strategic Information Systems, 19(4), 281–295. https://doi.org/10.1016/j.jsis.2010.10.002

Gregor, S. (2006). The nature of theory in information systems. MIS Quarterly, 30(3), 611-642.

Guo, K. H., & Yuan, Y. (2012). The effects of multilevel sanctions on information security violations: A mediating model. Information & Management, 49(6), 320–326. https://doi.org/10.1016/j.im.2012. 08.001

Hammond, J.S., Keeney, R.L., & Raiffa, H. (1998). The hidden traps in decision making. *Harvard Business Review*, 76(5), 47–58.

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, 66, 52–65. https://doi.org/10.1016/j.cose.2016.12.016

Haney, J. M., & Lutters, W. G. (2021). Cybersecurity advocates: discovering the characteristics and skills of an emergent role. *Information & Computer Security*. https://doi.org/10.1108/ICS-08-2020-0131

Hansche, S. (2001). Designing a security awareness program: Part 1. *Information systems security*, *9*(6), 1-9. http:10.1201/1086/43298.9.6.20010102/30985.4

Harris, S. (2002). *All-in-one CISSP certification exam guide*. McGraw-Hill/Osborne.

He, W., & Zhang, Z. (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. *Journal of Organizational Computing and Electronic Commerce*, *29*(4), 249-257. https://doi.org/10.1080/10919392.2019.1611528

Heikka, J. (2008). A constructive approach to information systems security training: An action research experience. *14th Americas Conference on Information Systems, AMCIS 2008*,*1*,15–22. https: https://aisel.aisnet.org/amcis2008/319/

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

Herath, T., and Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures, and perceived effectiveness. *Decision Support Systems*, *47*(2), 154–165. https://doi.org/10.1016/j.dss.2009.02.005

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*, *31*(6), 1135–1162. https://doi.org/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*, *49*(2), 99110.http://europepmc.org/abstract/med/10297607

Hu, Q., Hart, P., & Cooke, D. (2007). The role of external and internal influences on information systems security - a neo-institutional perspective. Journal of Strategic Information Systems, 16(2), 153–172. https://doi.org/10.1016/j

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

Hwang, M. I., & Helser, S. (2021). Cybersecurity educational games: a theoretical framework. *Information & Computer Security*.

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. Information & Management, 51(1), 69–79. https://doi. org/10.1016/j.im.2013.10.001 .*Practice*, *13*(5), 66-80.

Jansen, J., & Van Schaik, P. (2018). Testing a model of precautionary online behaviour: The case of online banking. *Computers in Human Behavior*, *87*, 371-383.

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework. *MIS quarterly*, *39*(1), 113-134.

Karjalainen, M., & Siponen, M. (2011). Toward a new meta-theory for designing information systems (IS) security training approaches. Journal of the Association for Information Systems, 12(8), 519–543. https://doi.org/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*, *14*(1), 96-113.

Keller, S., Powell, A., Horstmann, B., Predmore, C., & Crawford, M. (2005). Information security threats and practices in small businesses. *Information systems management*, *22*(2), 7.

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

Kim, S., Kim, G., & French, A. M. (2015). Relationships between need-pull/technology-push and information security management and the moderating role of regulatory pressure. *Information Technology and Management*, *16*(3), 173-192.

Kirova, D., & Bauмöl, 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*, *19*(4), 56-82.

Klein, H. K., and Myers M. D. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. In special issue: Intensive Research. MIS Quarterly, 23(1), 67- 93.

Kolkowska, E., Karlsson, F., & Hedström, K. (2017). Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method. The Journal of Strategic Information Systems, 26(1), 39–57.https://doi.org/10.1016/j.jsis.2016.08.005

Koohang, A., Anderson, J., Nord, J. H., & Paliszkiewicz, J. (2020). Building an awareness-cantered information security policy compliance model. *Industrial Management & Data Systems*. Kritzinger, E., & Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. *Computers & security*, *27*(5-6), 224-231.

Kumah, P., Yaokumah, W., & Okai, E. S. A. (2019). A conceptual model and empirical assessment of HR security risk management. *Information & Computer Security*.

Lake, S. (2022, July 22). "*Cybersecurity hiring remains red-hot-the industry to surpass $400 billion market size by 2027"*. Fortune. Retrieved September 29, 2022, from https://fortune.com/education/business/articles/2022/07/22/cybersecurity-hiring-remains-red hot-the-industry-to-surpass-400-billion-market-size-by-2027/

Lambrinoudakis, C. (2013). Evaluating and enriching information and communication technologies compliance frameworks with regard to privacy. *Information Management & Computer Security*. https://doi.org/10.1108/IMCS-09-2012-0051

Langley, A. (1999). Strategies for Theorizing from Process Data. *The Academy of Management Review*, *24*(4), 691–710. http://www.jstor.org/stable/259349

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*, *37*(12), 1049–1092. https://doi.org/10.1108/MRR-04-2013-0085

Leech, N. L., and Onwuegbuzie, A. J. (2007). An array of qualitative data analysis tools: A call for data analysis triangulation. *School psychology quarterly*, *22*(4), 557.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. International Journal of Information Management, 45, 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Li, H., Yoo, S., & Kettinger, W. J. (2021). The roles of IT strategies and security investments in reducing organizational security breaches. *Journal of Management Information Systems*, *38*(1), 222-245. DOI: 10.1080/07421222.2021.1870390

Lowry, P. B., & Moody, G. D. (2015). Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. *Information Systems Journal*, *25*(5), 433-463.

Mahmood, M.A., Siponen, M., Straub, D., Rao, H.R., & Raghu, T.S. (2010). Moving toward black hat research in information systems security: An editorial introduction to the special issue. MIS Quarterly, 34(3), 431–433. https://doi.org/10.2307/25750685

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

Marshall, M. N. (1996). The key informant technique. *Family Practice*, *13*(1), 92–97. https://doi.org/10.1093/fampra/13.1.92

Markus, M. L., & Robey, D. (1988). Information technology and organizational change: Causal structure in theory and research. *Management science*, *34*(5), 583-598.

McCarthy, P., Sammon, D. and Alhassan, I. (2022) "Doing Digital Transformation: Theorising the Practitioner Voice", in Proceedings of the 2022 Open Conference of the IFIP WG 8.3 Decision Support, Budapest, Hungary,15th-17th June 2022.

Myers, M. D., and Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and organization*, *17*(1), 2-26.

Niederman, F., Müller, B., & March, S. T. (2018). Using process theory for accumulating project management knowledge: A seven-category model. *Project Management Journal*, *49*(1), 6-24.

Okenyi, P. O., and Owens, T. J. (2007). On the anatomy of human hacking. *Information Systems Security*, *16*(6),302-314. https:10.1080/10658980701747237

Orlikowski, W. J., and Baroudi, J. J. (1991). Studying information technology in organizations: Research approaches and assumptions, Information Systems Research, 2(1), 1-28.

Padayachee, K. (2012). Taxonomy of compliant information security behavior. Computers & Security, 31(5), 673–680. https://doi.org/10.1016/j.cose.2012.04.004

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Which factors explain employees' adherence to information security policies? An empirical study.

Parrish, J. L., and San Nicolas-Rocca, T. (2012). Toward Better Decisions with Respect to Is Security: Integrating Mindfulness Into IS Security Training. *Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)*, 1–16. Retrieved from http://aisel.aisnet.org/wisp2012/17

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, EDUCON 2010*, 1907–1916. https://doi.org/10.1109/EDUCON.2010.5492435

Pather, S., and Remenyi, D. (2005). Some of the philosophical issues underpinning research in information systems-from positivism to critical realism: reviewed article. *South African Computer Journal*, *2005*(35), 76-83.

Patton, M. Q. (1990). *Qualitative evaluation and research methods*. SAGE Publications, inc.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. Journal of management information systems, 24(3), 45-77

Peltier, T. R. (2005). Implementing an information security awareness program. *Information Systems Security*, *14*(2), 37–49. https://doi.org/10.1201/1086/45241.14.2.20050501/88292.6pp. 1758-1772 Publications, Newbury Park, CA.

Pham, H. C., Brennan, L., Parker, L., Phan-Le, N. T., Ulhaq, I., Nkhoma, M. Z., & Nguyen, M. N. (2019). Enhancing cyber security behavior: an internal social marketing approach. *Information & Computer Security*.

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

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

Rantos, K., Fysarakis, K., and Manifavas, C. (2012). How effective is your security awareness program? An evaluation methodology. *Information Security Journal: A Global Perspective*, *21*(6), 328-345 research: developing taxonomy, themes.

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

Reid, R., & Van Niekerk, J. (2016). Decoding audience interpretations of awareness campaign messages. *Information & Computer Security*.

Rogers, R. (1975). A Protection Motivation Theory Of Fear Appeals And Attitude Change. *Journal of Psychology: Interdisciplinary and Applied*. https://doi.org/10.1080/00223980.1975.9915803

Sikolia, D., Twitchell, D., & Sagers, G. (2018). Protection motivation and deterrence: Evidence from a fortune 100 company. *AIS Transactions on Replication Research*, *4*(1), 7

Silic, M., and Lowry, P. B. (2020). Using design-science based gamification to improve organizational security training and compliance. *Journal of Management Information Systems*, *37*(1), 129-161. https://doi.org/10.1080/07421222.2019.1705512

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. Information Management & Computer Security, 8(1), 31–41. https://doi.org/10.1108/09685220010371394

Siponen, M., & Baskerville, R.L. (2018). Intervention effect rates as a path to research relevance: Information systems security example. Journal of the Association for Information Systems, 19(4), 247–264. https://doi.org/10.17705/1jais.00491

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. MIS Quarterly, 34(3), 487–502. https://doi.org/10.2307/25750688

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & management*, *46*(5), 267-270.

Siponen, M., and Tsohou, A. (2018). Demystifying the influential IS legends of positivism. *Journal of the Association for Information Systems*, *19*(7).

Siponen, M., and Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. MIS Quarterly, 34(3), 487–502. https://doi.org/10.2307/25750688

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

Siqi Hu, Carol Hsu and Zhongyun Zhou (2021a) Security Education, Training, and Awareness Programs: Literature Review, Journal of Computer Information Systems, DOI: 10.1080/08874417.2021.1913671

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems. *Nist special publication*, *800*(30), 800-30.

Straub, D. W., and Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly: Management Information Systems*, *22*(4), 441–464. https://doi.org/10.2307/249551

Strauss, A., and Corbin, J. (1990). Basics of qualitative research: Grounded theory procedures and techniques. Thousand Oaks, CA: SAGE Publications, Inc.

Sutton, R. I., & Staw, B. M. (1995). What theory is not. *Administrative science quarterly*, 371-384.

Topa, I., & Karyda, M. (2019). From theory to practice: guidelines for enhancing information security management. *Information & Computer Security*.

Tsohou, A., Karyda, M., Kokolakis, S., and Kiountouzis, E. (2012). Analyzing trajectories of information security awareness. *Information Technology and People*, *25*(3), 327-352. DOI: https://doi-org.ucc.idm.oclc.org/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*, *24*(1), 38–58. https://doi.org/10.1057/ejis.2013.27

Tsohou, A., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2008). Investigating information security awareness: Research and practice gaps. Information Security Journal: A Global Perspective,17(5–- 6),207–227.https://doi-org.ucc.idm.oclc.org/10.1080/19393550802492487

Vance, A., Lowry, P.B., & Eggett, D.L. (2015). Increasing accountability through the user interface design artifacts: A new approach to addressing the problem of access-policy violations. Mis Quarterly, 39(2), 345–366. https://doi.org/10.25300/MISQ/2015/39.2.04

Von Solms, R., and Von Solms, B. (2004). From policies to culture. *Computers and security*, *23*(4), 275-279 https://doi.org/10.1016/j.cose.2004.01.013

Vroom, C., and Solms, R. V. (2002). A practical approach to information security awareness in the organization. In *Security in the Information Society* (pp. 19-37). Springer, Boston, MA. https: 10.1007/978-0-387-35586-3_46

Walsham, G. (2002). Cross-cultural software production and use: a structurational analysis. *MIS quarterly*, 359-380.

Walsham, G. (2006). Doing Interpretive Research. European Journal of Information Systems, 15(3),320–330. Retrieved from https://link.springer.com/article/10.1057/palgrave.ejis.3000589

Walsham, G. (1995). Interpretive case studies in IS research: nature and method. European Journal of Information Systems, 4(2), 74-81.

Wang, J., Shan, Z., Gupta, M., & Rao, H.R. (2019). A longitudinal study of unauthorized access attempts on information systems: The role of opportunity contexts. MIS Quarterly, 43(2), 601 622. https://doi.org/10.25300/MISQ/2019/14751

Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. MIS Quarterly, 39(1), 113–134. https:// doi.org/10.25300/MISQ/2015/39.1.06

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems*, *18*(2), 101-105.
Whitman, M. E. (2004). In defence of the realm: understanding the threats to information security. *International Journal of Information Management*, *24*(1), 43-57.

Whitman, M.E., and Mattord, H.J. 2008. Principles of Information Security. Stamford, Connecticut: Course Technology.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. MIS Quarterly, 37(1), 1–20. https://doi.org/10.25300/MISQ/2013/37.1.01

Wilson, M., and Hash, J. (2003). Building an information technology security awareness and training program. *NIST Special publication*, *800*(50), 1-39.

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. Communications Monographs, 59(4), 329–349. https://doi.org/10.1080/03637759209376276

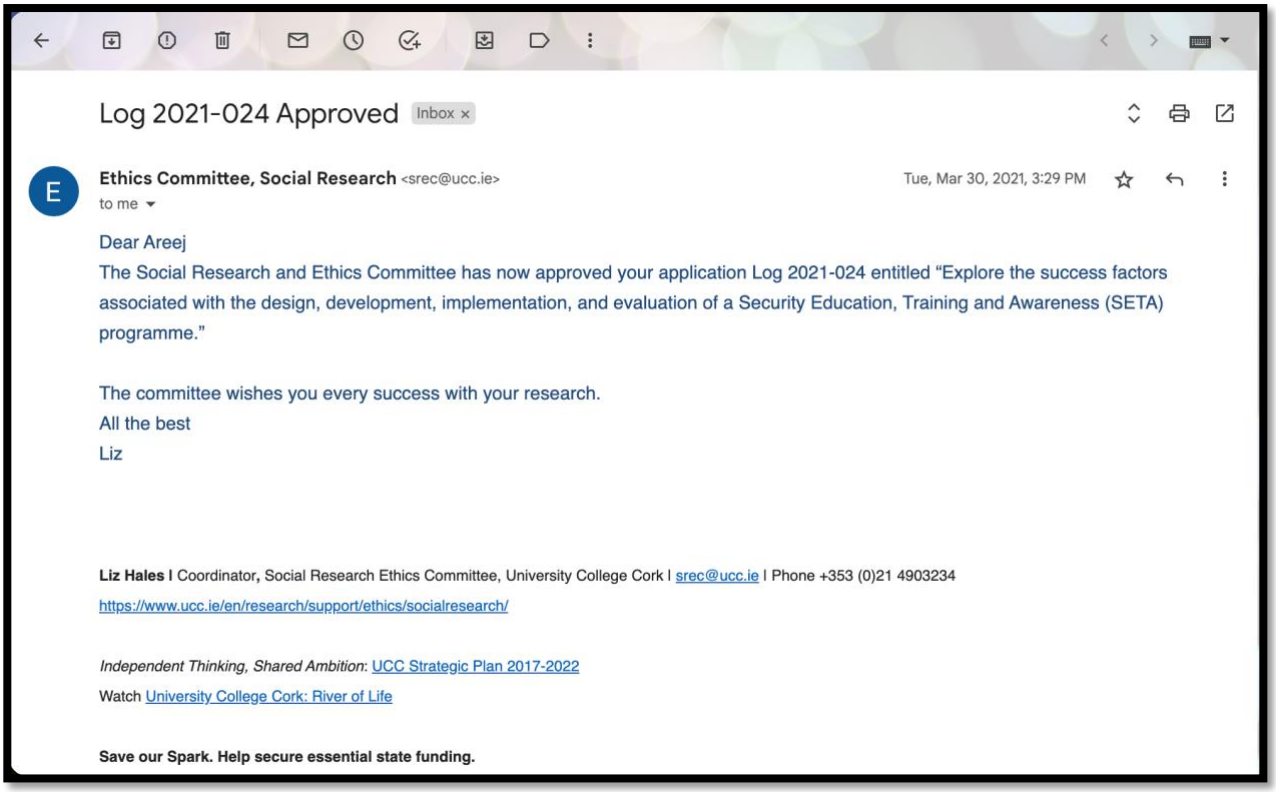
Wu He and Zuopeng (Justin) Zhang (2019) Enterprise cybersecurity training and awareness programs: Recommendations for success, Journal of Organizational Computing and Electronic Commerce, 29:4, 249-257, DOI: 10.1080/10919392.2019.1611528

Yaokumah, W., Walker, D. O., & Kumah, P. (2019). SETA and security behavior: Mediating role of employee relations, monitoring, and accountability. *Journal of Global Information Management (JGIM)*, *27*(2), 102-121

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*, *108*(February), 107–118. https://doi.org/10.1016/j.dss.2018.02.009

Appendix

Appendix A: Ethical Approval Email



Log 2021-024 Approved Inbox ×

Ethics Committee, Social Research <srec@ucc.ie> Tue, Mar 30, 2021, 3:29 PM

to me

Dear Areej

The Social Research and Ethics Committee has now approved your application Log 2021-024 entitled "Explore the success factors associated with the design, development, implementation, and evaluation of a Security Education, Training and Awareness (SETA) programme."

The committee wishes you every success with your research.

All the best

Liz

Liz Hales I Coordinator, Social Research Ethics Committee, University College Cork I srec@ucc.ie I Phone +353 (0)21 4903234

https://www.ucc.ie/en/research/support/ethics/socialresearch/

Independent Thinking, Shared Ambition: UCC Strategic Plan 2017-2022

Watch University College Cork: River of Life

Save our Spark. Help secure essential state funding.

Appendix B: An Invitation Letter

Areej Alyami

Business Information Systems.

Cork University Business School.

To Whom It May Concern,

I am a PhD researcher in Business Information Systems at University College Cork (UCC). My research topic is *to explore the critical success factors associated with the design, development, implementation, and evaluation of a Security Education, Training and Awareness (SETA) programme effectiveness.* As part of this research, I am conducting interviews with IS Security practitioners who have knowledge of, and experience in, Security Education, Training and Awareness (SETA) programmes. These interviews will take up to 60 minutes. Having reviewed your profile on LinkedIn I would like to invite you to participate (as a key informant) in my PhD research study. Your professional experiences would be greatly appreciated and hugely beneficial to the outcome of this study overall.

While a SETA programme is an organisational intervention introduced to reduce the number of IS security breaches linked to the concept of employee behaviour, amongst others, existing research studies do not examine all aspects of the programme lifecycle (design, development, implementation, evaluation). This research gap is the key motivation for this research study. The outcome of this exploratory research study is to build a conceptual model of the *Critical Success Factors for a SETA Programme effectiveness lifecycle*. As a "thank you" for your participation I will also share the findings of the study with you.

I would be delighted if you could agree to an interview using MS Teams, phone, or another VOIP application that might be more convenient for you.

I have attached an Information Sheet which explains the detail of the research. To enroll and assist me in this research please sign the enclosed consent form and email to me as a pdf file at a.alyami1988@gmail.com

I look forward to hearing from you.

Please contact me if you have any queries.

Best Regards,

Areej Alyami e-mail: a.alyami1988@gmail.com

Appendix C: Information Sheet

Thank you for considering participating in this research project. The purpose of this document is to explain to you what the work is about and what your participation would involve, so as to enable you to make an informed choice.

The purpose of this study is *to explore the critical success factors associated with the design, development, implementation, and evaluation of a Security Education, Training and Awareness (SETA) programme effectiveness.* The data being gathered for this study is through interviews with IS Security practitioners who have knowledge of, and experience in, Security Education, Training and Awareness (SETA) programmes. These interviews will take up to 60 minutes, depending on interviewee availability.

Participation in this study is completely voluntary. There is no obligation to participate, and should you choose to do so you can refuse to answer specific questions or decide to withdraw from the interview. Once the interview has been concluded, you can choose to withdraw your details at any time in the subsequent two weeks.

All of the information you provide will be kept confidential and anonymous and will be available only to me (the researcher) and to my supervisors. The only exception is where information is disclosed which indicates that there is a serious risk to you or to others. Once the interview is completed, the recording will immediately be transferred to the University College Cork OneDrive system and wiped from the recording device. The data will be retained for a minimum of ten years on the UCC OneDrive system, after which time the data will be disposed of. The information you provide may contribute to research publications. Also, the analysis of the data will be part of my thesis.

The researcher does not anticipate any negative outcomes from participating in this study. However, at the end of the interview, I will discuss with you how you found the experience and how you are feeling.

This study has obtained ethical approval from the UCC Social Research Ethics Committee.

If you have any queries about this research, you can contact me: E-mail. **a.alyami1988@gmail.com** and you can contact my research supervisors at UCC:

- Professor David Sammon (dsammon@ucc.ie)
- Dr. Karen Neville (KarenNeville@ucc.ie)
- Dr. Carolanne Mahony (carolanne.mahony@ucc.ie)

If you agree to take part in this study, please sign the consent form overleaf.

Appendix D : Consent Form

I……agree to participate in **Areej Alyami**'s research study.

The purpose and nature of the study has been explained to me in writing.

I am participating voluntarily.

I give permission for my interview with Areej Alyami to be audio-recorded.

I understand that I can withdraw from the study, without repercussions, at any time, whether before it starts or while I am participating.

I understand that I can withdraw permission to use the data within two weeks of the interview, in which case the material will be deleted.

I understand that anonymity will be ensured in the write-up by disguising my identity.

I understand that disguised extracts from my interview may be quoted in the thesis and any subsequent publications if I give permission below:

(Please tick one box:)

I agree to quotation/publication of extracts from my interview ☐

I do not agree to quotation/publication of extracts from my interview ☐

Signed: ……. Date: …….

PRINT NAME: …….

Appendix E: 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 programme?
2. Why are these factors important in the ***design*** of a SETA programme?
3. How can organisations ensure that these factors exist in their ***design*** efforts?
4. Who should be responsible for the ***design*** of a SETA programme?
5. What makes a SETA programme succeed/fail?

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

Appendix F: 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