

## Journal Pre-proof

Applying Social Marketing to Evaluate Current Security Education Training and Awareness Programs in Organisations

Moneer Alshaikh , Sean B Maynard , Atif Ahmad

PII: S0167-4048(20)30363-1  
DOI: <https://doi.org/10.1016/j.cose.2020.102090>  
Reference: COSE 102090



To appear in: *Computers & Security*

Received date: 15 April 2020  
Revised date: 16 October 2020  
Accepted date: 18 October 2020

Please cite this article as: Moneer Alshaikh , Sean B Maynard , Atif Ahmad , Applying Social Marketing to Evaluate Current Security Education Training and Awareness Programs in Organisations, *Computers & Security* (2020), doi: <https://doi.org/10.1016/j.cose.2020.102090>

This is a PDF file of an article that has undergone enhancements after acceptance, such as the addition of a cover page and metadata, and formatting for readability, but it is not yet the definitive version of record. This version will undergo additional copyediting, typesetting and review before it is published in its final form, but we are providing this version to give early visibility of the article. Please note that, during the production process, errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

© 2020 Published by Elsevier Ltd.

# Applying Social Marketing to Evaluate Current Security Education Training and Awareness Programs in Organisations

Moneer Alshaikh<sup>a b\*</sup>

<sup>a</sup>Department of Cybersecurity, College of Computer Science and Engineering, University of Jeddah, Saudi Arabia, [malshaikh@uj.edu.sa](mailto:malshaikh@uj.edu.sa)

<sup>b</sup>School of Computing and Information Systems, Melbourne School of Engineering, The University of Melbourne, Victoria, 3010. [alshaikhm@unimelb.edu.au](mailto:alshaikhm@unimelb.edu.au)

Sean B Maynard<sup>b</sup>

School of Computing and Information Systems, Melbourne School of Engineering, The University of Melbourne, Victoria, 3010. [sean.maynard@unimelb.edu.au](mailto:sean.maynard@unimelb.edu.au)

Atif Ahmad<sup>b</sup>

School of Computing and Information Systems, Melbourne School of Engineering, The University of Melbourne, Victoria, 3010. [Atif@unimelb.edu.au](mailto:Atif@unimelb.edu.au)

\* Corresponding author: E-mail address: [malshaikh@uj.edu.sa](mailto:malshaikh@uj.edu.sa)

(M. Alshaikh)

University of Jeddah, Jeddah, Saudi Arabia, 6420 University of Jeddah Road, P.O. Box 13151 Jeddah 21493

## Abstract

*The effectiveness of cybersecurity management programs is contingent on improving employee security behaviour. Security education, training, and awareness (SETA) programs aim to drive positive behaviour change in support of cybersecurity objectives. In this paper, we argue that existing SETA programs are suboptimal as they aim to improve employee knowledge acquisition rather than behaviour and belief. We apply social marketing principles to examine SETA practices across six organisations. We find that SETA programs fail to implement the key principles and concepts of social marketing that are essential for positive behaviour change. We therefore propose a novel development process for SETA based on a social marketing approach. We explain how the new approach can be used to develop SETA programs that are focused on behaviour change.*

**Keywords:** *Information Security Education Training and Awareness, Behavioural Information Security, Behaviour Change, Social Marketing, Security Interventions.*

## 1 Introduction

Security researchers consistently argue that organisations need information security education, training, and awareness (SETA) programs to raise employees' awareness of security risk, and to provide them with the required skills and knowledge to comply with security policy ([Alshaikh 2020](#); [Cram et al. 2019](#); [Karjalainen et al. 2019](#)). Despite the widespread implementation of such programs in many organisations, the rate of unintended breaches of security directives is still increasing. A recent report shows that 70% of security incidents are caused by employee noncompliance with organisational information

security directives ([NTT Security 2019](#)). This trend is consistent with previous security reports (e.g., [Accenture & HfS Research 2016](#); [SANS 2017](#)) and academic literature (e.g., [Almestahiri et al. 2017](#); [Chatterjee et al. 2015](#); [Crossler et al. 2013](#); [Guo et al. 2011](#); [Warkentin and Willison 2009](#)).

When developing SETA programs, organisations turn to “best practice” and industry standards. However, it remains unclear as to which SETA strategies are effective in specific contexts ([Almestahiri et al. 2017](#); [Beyer et al. 2015](#); [Ki-Aries and Faily 2017](#); [Warkentin and Willison 2009](#)). As the literature points out, an underlying reason is that the standards and guidelines are neither grounded in theory nor on empirical evidence ([Alshaikh et al. 2019](#); [Jampen et al. 2020](#); [Ng et al. 2009](#); [Park and Chai 2018](#); [Siponen and Willison 2009](#)). Further, existing SETA programs aim to improve employee knowledge acquisition rather than behaviour and belief. Therefore, for organisations there is little clarity on how to increase the effectiveness of SETA programs to alter employee behaviour.

While there is considerable research on SETA conducted in the information systems security behaviour field ([Guo et al. 2011](#); [Puhakainen and Siponen 2010](#); [Sharma and Warkentin 2019](#); [Siponen and Vance 2010](#); [Willison and Warkentin 2013](#); [Willison et al. 2018](#)), these studies approach the problem from an individual behaviour perspective instead of focusing at an organisational level. Within these studies, several theories (e.g., deterrence theory, neutralisation theory and protection motivation theory) have been applied to explain noncompliance with security policies ([D'Arcy and Herath 2011](#); [Hanus and Wu 2016](#); [Siponen and Vance 2010](#)). However, the literature does not provide strategies and approaches to assist organisations in developing an effective SETA program to change employee behaviour ([Alshaikh et al. 2019](#)).

In this paper, we explore social marketing as an approach for developing more effective SETA programs. Our justification is that social marketing has been successfully used in the past to improve the effectiveness of behaviour change programs in other domains ([Almestahiri et al. 2017](#); [Tapp and Rundle-Thiele 2016](#)). Therefore, the aim of this paper is to use social marketing approaches to: (1) assess the effectiveness of the development process of existing SETA programs; and (2) propose a novel SETA development process. The study addresses the following research question:

*How can organisations develop effective SETA programs to achieve behaviour change?*

The paper is organized as follows. In our background section, we present best-practice industry guidelines on SETA; followed by introducing the social marketing approach to behaviour change. Subsequently, we explain the research methodology employed in this research. We then report the findings of the exploratory study where we map key social marketing principles to SETA practices in the six organisations under investigation. Next, we propose a new approach for the SETA development process based on social marketing. Finally, we conclude with implications of the research and direction for future work.

## 2 Background

In this section, we introduce background research on SETA and Social Marketing.

### 2.1 Security Education, Training and Awareness (SETA)

There is a broad consensus in the literature on the need for organisations to develop SETA programs to protect their information assets ([Ahmad et al. 2020](#); [Khan et al. 2011](#)). The significant role of SETA programs is evident from the fact that existing information security management frameworks integrate SETA with other key security functions (such as: security policy, risk management and incident management) ([Alshaikh et al. 2014](#); [Chaudhry et al. 2012](#); [Kritzinger and Smith 2008](#); [Shedden et al. 2011](#); [Shedden et al. 2009](#)).

The literature clearly distinguishes the different roles of education, training and awareness. [Whitman and Mattord \(2017\)](#) suggest: *Education* is where security professionals integrate security skills and

competencies into a common body of knowledge for the design and implementation of information security; *Training* is where relevant employees gain needed security skills and competency around security so that they can perform their job; *Awareness* involves focussing all other employees' attention on security, giving them the ability to avoid behaviours that would compromise information security. Most organisations when implementing SETA programs only implement *awareness* for employees and *education* and *training* are conducted by external providers for individual personnel where required. Subsequently, in this research, our focus will be only on *awareness* when we discuss SETA.

The importance of SETA programs for safeguarding information assets has led many authors to recommend their establishment within organisations as part of their overall security strategy ([D'Arcy et al. 2009](#); [Öğütçü et al. 2016](#)). There are several guidelines for organisations developing SETA programs ([De Maeyer 2007](#); [Herold 2010](#); [Karjalainen and Siponen 2011](#); [Whitman and Mattord 2017](#)). These approaches can be broken down into three fundamental phases: (1) *development*, (2) *implementation* and (3) *evaluation*. The following discussion uses these three to discuss existing approaches and models for developing SETA programs.

The development phase includes activities used to understand the current organisational situation, obtain management support and acquire resources to develop an effective program ([Bowen et al. 2006](#); [Power and Forte 2006](#)). These activities include conducting a needs assessment for a SETA program (which may include legislated requirements), defining goals and objectives, establishing the SETA development team, and identifying the target audience for a SETA program. The literature discusses the importance of understanding the needs of an organisation and the design SETA programs that meet these specific needs. For instance, [Bada et al. \(2019\)](#) suggests that security awareness should be professionally prepared and organised for it to work and needs to be targeted and actionable. Development phase activities also include developing materials for SETA consisting of tasks around topic selection and material creation ([Johnston and Warkentin 2010](#)).

The implementation phase focuses on the conduct of the SETA program using a variety of delivery methods. The literature on the implementation of SETA programs discusses methods of effectively delivering SETA messages. These include the use of a combination of methods for delivery, such as newsletters, emails, note-taking tools to aid memory (e.g. pens and notepads), and posters that expose those within the organisation to convey the security messages on consistent and ongoing bases ([Abawajy 2014](#); [Peltier 2005](#)).

The final SETA phase is evaluation, where the organisation reviews and evaluates its SETA initiatives to measure their effectiveness. Effectiveness is usually measured through identifying changes in employee behaviour that impact information security ([Öğütçü et al. 2016](#)). Existing approaches focus on evaluating the knowledge obtained for the program ([Fertig et al. 2020](#); [PCI 2014](#)). This is a very limited view of evaluation. Evaluation should also focus on the effect of SETA on the overall security of the organisation because of the change in employee behaviour ([Tsohou et al. 2015](#)). One way to measure the effectiveness of SETA is to compare the incidence of noncompliance-related security events before and after implementation of the SETA program. Further, the discussion of the evaluation of SETA programs has been always focused on the outcome of program (raising employees' awareness) overlooking the important aspect of evaluating the practices and overall approach to the development of SETA in organisations.

Best-practice standards such as ISO/IEC 27002 stress the need for SETA programs, recommending that “*all employees of the organisation should receive appropriate awareness, education and training and regular update in organisational policies and procedures, as relevant for their job function*” ([ISO/IEC 2013](#)). However, the standards do not provide clear and practical guidance on how SETA programs should be implemented. Instead they provide guidance that is conceptual, lacks support from empirical data, is generic in nature, and pays little consideration to organisational context ([Beyer et al. 2015](#); [Fertig et al. 2020](#); [Siponen and Willison 2009](#)). Although there are practical guidelines specifically developed

for SETA, these are not grounded in theory and do not have the status of industry standards, so organisations are not required to comply with the directives.

In a recent seminal paper published in MISQ, [Cram et al. \(2019\)](#) conducts a meta-analysis of security behaviour studies. Among the practical implications of their study was the need to address the lack of a systematic approach for developing SETA programs and for more theory-informed approaches. Calls for more theory-informed approaches is consistently made in several publications since 2010 ([Karjalainen and Siponen 2011](#); [Lebek et al. 2013](#); [Puhakainen and Siponen 2010](#)). Consequently, considerable Information Systems research has been conducted into security behaviour in organisations. A number of theories (e.g., deterrence theory, rational choice theory, planned behaviour theory, protection motivation theory) have been applied to study: (1) why employees do not comply with policy, and (2) the role of SETA programs in protecting organisations and changing employees' behaviour. However, drawing from the meta-analysis of [Cram et al. \(2019\)](#), these contributions are not reflected in the practice of SETA in organisations. We provide two possible explanations for this. First, that IS studies are primarily driven by the need to contribute to knowledge rather than to provide practical guidance to organisations. Second, the studies address SETA in terms of individual security behaviours of employees rather than on organisational strategies to improve SETA.

Although individual studies have provided many useful recommendations to develop effective SETA programs, taken collectively these studies present a large and sometimes overlapping array of theoretical constructs or components that has led to mixed results and limited practical value. Specifically, recommendations are fragmented and dispersed and do not build cumulatively to guide the development of SETA programs in organisations.

To address the need for systematic development of SETA programs and a more theory-informed approach, this study draws on the social marketing approach and proposes a new approach to design theory-informed SETA programs. The next section will discuss the social marketing approach.

## 2.2 Social Marketing

Social marketing is defined as *“the systematic application of marketing alongside other concepts and techniques to achieve specific behavioural goals for social good”* ([French et al. 2011, p.11](#)). Social marketing has been a recognized discipline since the early 1970s that mainly focuses on influencing behaviours ([Lee and Kotler 2015](#); [McKenzie-Mohr 2011](#)). Social marketing techniques has been utilized and proven to be effective in areas such as public health (smoking, vaccination), and environmental sustainability (recycling, reduce waste).

Unlike commercial marketing where the objective is to sell products and services, social marketing is focused on influencing behaviour. Social marketing draws on behaviour theories and methodologies to address social issues. As shown in Figure 1, the social marketing triangle presents key principles of social marketing and links between these principles to influence human behaviour ([French and Blair-Stevens 2005](#); [French et al. 2011](#)).





**Figure 1 Social Marketing Triangle** ([French and Blair-Stevens 2005](#))

As shown in Table 1, there are eight key social marketing principles ([French and Blair-Stevens 2005](#)). Understanding these principles is important to ensure greater consistency of approach to the development and evaluation of social marketing campaigns ([French and Blair-Stevens 2005](#); [French et al. 2010](#); [French et al. 2011](#)). In this paper, we will use these principles as a lens to assess the effectiveness of existing SETA programs in the organisations under investigation.

**Table 1: A List of Key Social Marketing Principles**

<p><b>Customer Orientation:</b> The customer, located at the centre of the social marketing triangle, is the central focus of a social marketing campaign. An understanding of what motivates or moves their behaviour is important as this directly impacts the types of interventions that take place to change behaviour.</p>
<p><b>Focus on Behaviour:</b> The social marketing approach aims to influence specific behaviours not just knowledge and attitude. Understanding current behaviour is extremely important as this will help to determine how to influence that behaviour. An evidence-based approach should be used to understand the behaviour. This is done by first analysing the target audiences' behaviour (problem behaviour and desired behaviour) and then setting actionable and measurable behavioural goals and key indicators in relation to the specific social issue being addressed.</p>
<p><b>Theory Based:</b> Social marketing uses behavioural theories to understand behaviour and to inform and guide the selection of appropriate intervention strategies. Theory informed interventions are more successful, leading to longer lasting changes to behaviour (<a href="#">French and Blair-Stevens 2005</a>; <a href="#">Michie et al. 2014</a>). Several behavioural theories, models and frameworks (e.g., diffusion of innovation theory, self-control theory, health belief model and stage of change model) are frequently used by social marketers (<a href="#">Lee and Kotler 2015</a>). Theories explain what influences behaviour and models describe processes of behaviour change (<a href="#">French and Blair-Stevens 2005</a>; <a href="#">Glanz and Rimer 1997</a>). This principle is particularly useful to address the lack of theory informed SETA programs.</p>
<p><b>Develop 'Insight':</b> Social marketing is driven by 'actionable insights' that provide practical guidance for the selection and development of interventions (<a href="#">French and Blair-Stevens 2005</a>; <a href="#">French et al. 2010</a>). After initially developing a general understanding of the audience, key factors and issues relevant to positively influencing specific behaviour are identified. This may identify emotional and physical barriers to behaviour change.</p>
<p><b>Exchange:</b> A social marketing campaign must include a compelling 'exchange' offer based on thorough analysis of the perceived / actual costs versus perceived / actual benefits from adopting the new behaviour (<a href="#">McKenzie-Mohr 2011</a>). Exchange theory postulates that for exchange to take place the target audience to must perceive benefits equal to or greater than perceived cost (<a href="#">French and Blair-Stevens 2005</a>). The target audience in social marketing tends to change their behaviour if they perceive that the benefits from adopting the desired behaviour are equal to or greater than the effort involved in performing the new behaviour or giving up unwanted behaviour (<a href="#">Lee and Kotler 2015</a>). An effective social marketing campaign should maximise benefits and</p>

minimise costs.
<b>Competition:</b> Social marketing uses the concept of ‘competition’ to examine the internal and external factors that compete for people’s time and attention to adopt a desired behaviour ( <a href="#">French and Blair-Stevens 2005</a> ; <a href="#">French et al. 2010</a> ). Strategies would be developed to minimise the impact of competition linked to the <i>exchange</i> offered.
<b>Audience Segmentation:</b> Audience segmentation is important to develop tailored intervention strategies to effectively influence behaviour ( <a href="#">McKenzie-Mohr 2011</a> ). This avoids the use of a generalized ‘a one size fits all’ approach by dividing the target audience into smaller groups ‘segments’ that share common beliefs, attitudes and behaviours ( <a href="#">French et al. 2010</a> ). Segments are prioritised and selected based on clear criteria, such as size and readiness to change ( <a href="#">Lee and Kotler 2015</a> ) and interventions are applied directly to the specific audience segment.
<b>Method Mix:</b> Social marketing applies an appropriate mix of methods to achieve the goals of the campaign. While it is important to use mix methods to avoid reliance on single approach, it is also important integrate the methods to achieve synergy and enhance overall impact ( <a href="#">Sowers et al. 2007</a> ). There are five intervention strategies that can be implemented Design (to alter the environment), Inform (to communicate facts and attitudes) Control (to regulate and enforce), Educate (to enable and empower) and Service (to provide support services) ( <a href="#">French et al. 2011</a> ).

The social marketing triangle, including the eight key principles, is vital for the development of successful social marketing campaigns to influence behaviour. Social Marketing is used to assess and review a range of existing initiatives ([French et al. 2010](#); [Grier and Bryant 2004](#); [Sowers et al. 2007](#)). For instance, [Almestahiri et al. \(2017\)](#) study tobacco cessation programs to identify the extent to which social marketing key principles are used in change behaviour. They concluded that use of segmentation, exchange, and competition was rarely reported and that there is limited use of theory to develop an understanding of their target markets, to explain relationships. [Andreasen \(2002\)](#) report on the use of a social marketing approach to increase responses to the population census. The aim of the social marketing campaign was to achieve a high rate of response to the census questionnaire. Research has identified target groups that had low response rate as the main target audience for the campaign. Then several intervention methods used to raise the awareness of the benefit of Census in providing *vital information that will mean more and better resources for them and their community*. Higher response rate of 67% was achieved more than it was predicted based on the previous year data.

### 2.3 Using Social Marketing in SETA programs

In the cyber security context, [Ashenden and Lawrence \(2013\)](#), argue that social marketing could be useful to address current challenges in the domain. The authors apply a social marketing framework to assess a public fraud campaign called the “Devil’s in Your Details”. They discuss several aspects of the public fraud campaign such as setting clear behavioural goals, developing insights of the target audience, identifying target audience, using mixed methods to change behaviour. [Ashenden and Lawrence \(2013\)](#) conclude by stating that rather than focusing on awareness of issues, organisations should focus on the behaviour they wish to change, using a social marketing framework. Further, reviewing this type of campaign through a social marketing lens assists organisations to identify gaps in their SETA programs related to key social marketing principles.

Our review of the literature revealed that social marketing principles have not been used to design, assess or evaluate SETA programs in organisations. Therefore, we investigate a number of organisations to determine whether SETA programs have used the social marketing key principles to change and influence employees’ security behaviour.

## 3 Research Methodology

To answer the research question we use a qualitative, exploratory research approach to gain a rich picture of the research phenomenon ([Stebbins 2001](#)). Qualitative methods allow us to develop a rich picture of

the relevant phenomena and allows us to investigate aspects of the phenomena that may not be obvious at the outset of the research project (Boudreau and Robey 2005; Eisenhardt 1989; Klein and Myers 1999; Yin 2018). The empirical data in the paper comes from six semi-structured interviews with SETA experts across six organisations (see Table 2). We selected participants based on their experience in SETA development. As this research is exploratory in nature, we wanted a good mix of different types of organisations and a variety of management levels to be represented across the organisations.

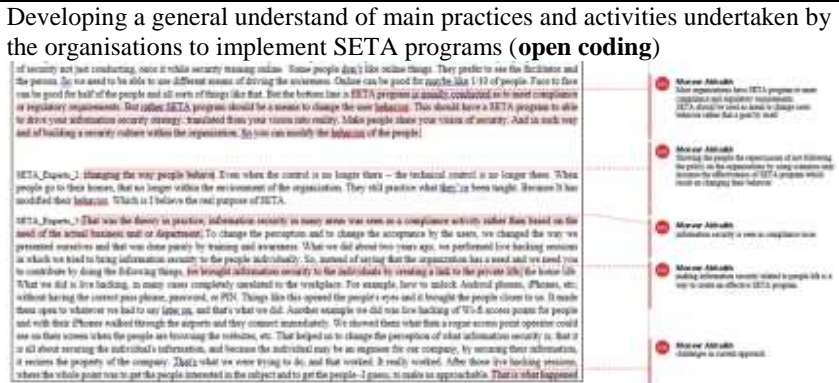
**Table 2. Study participant details**

ID	Role	Industry	Years of Experience
CISO1	Chief Information Security Officer	Government	15+
CISO2	Chief Information Security Officer	Automotive	10+
MGR1	Security Manager	IT Services	5+
MGR2	Senior Security Manager	Insurance	20+
MGR3	Security Awareness Manager	Banking	10+
MGR4	Security Awareness Manager	Banking	9+

The semi-structured interview questions (see Appendix A) investigated how SETA programs were implemented within the participants' organisation. Interviews lasted 60 minutes on average and were audio recorded. Participants were asked open questions to encourage them to describe in their own words the activities they undertake to manage the organisation's SETA program. Follow-up questions directed the participants to address the specific practices and activities in the SETA program. Participants reported on their current organisations, but also mentioned their experience from past organisations, which further enriches the empirical data with reflections drawn from even more organisations. The interviews were transcribed from audio recording and multiple passes were performed through the data to cluster the quotes and identify recurring themes that addressed the research question to gain an understanding of the development process of SETA programs. This resulted in approximately 80 pages of transcribed text.

As shown in Table 3, to interpret the empirical data, we used the three-step analysis process of open, axial and selective coding for qualitative data analysis as per the tradition of Information Systems research (see Neuman (2014); Corbin and Strauss (2015)).

**Table 3 Data analysis process**

Analysis Process	Input	Output
1) Read transcripts to identify themes, making notes and highlighting concepts related to SETA programs in organisations	6 Interviews transcripts approx. 80 pages combined.	Developing a general understand of main practices and activities undertaken by the organisations to implement SETA programs ( <b>open coding</b> ) 
2) group related concepts to determine practices and activities	Using the output from the first analysis to develop coding based on social marketing	Develop themes related to practices and activities undertaken by organisations to implement SETA programs (e.g., aim of SETA, planning for SETA, SETA activities & types, measuring and evaluating impact of SETA programs)



related to SETA programs in organisations	principles (axial coding)	<table border="1"> <thead> <tr> <th data-bbox="517 271 943 297">The development stage</th> <th data-bbox="948 271 1350 297">Comments and reflections</th> </tr> </thead> <tbody> <tr> <td data-bbox="517 304 943 450"> <ul style="list-style-type: none"> <li>Conduct a Needs Assessment for SETA program</li> </ul> <p>SETA_Experts_1: we identify the needs of the department and then we identify the level of the awareness in the department. Then we identify the priority for the upcoming year and that's what we prioritize. We try to identify a theme for the entire year, or at least half a year and don't mix those themes. Because, then again, it is a waste of our efforts if there is just too much information thrown at the people.</p> </td> <td data-bbox="948 304 1350 450"> <p>A gap analysis or an assessment is done to identify what areas/topics that employees need to be aware of. In addition, to the topic the assessment should identify the people who should be given awareness, type of education.</p> <p>"Topic and people"</p> <p>The focus of the data is on training and awareness.</p> </td> </tr> <tr> <td data-bbox="517 456 943 483"> <ul style="list-style-type: none"> <li>Identify the needs for SETA from Policy, Risk assessment reports and incident response reports.</li> </ul> </td> <td data-bbox="948 456 1350 483"> <p>There are several inputs to the development process of SETA such as policy, incident report, risk assessment, threat intelligence, users' feedback</p> </td> </tr> </tbody> </table>	The development stage	Comments and reflections	<ul style="list-style-type: none"> <li>Conduct a Needs Assessment for SETA program</li> </ul> <p>SETA_Experts_1: we identify the needs of the department and then we identify the level of the awareness in the department. Then we identify the priority for the upcoming year and that's what we prioritize. We try to identify a theme for the entire year, or at least half a year and don't mix those themes. Because, then again, it is a waste of our efforts if there is just too much information thrown at the people.</p>	<p>A gap analysis or an assessment is done to identify what areas/topics that employees need to be aware of. In addition, to the topic the assessment should identify the people who should be given awareness, type of education.</p> <p>"Topic and people"</p> <p>The focus of the data is on training and awareness.</p>	<ul style="list-style-type: none"> <li>Identify the needs for SETA from Policy, Risk assessment reports and incident response reports.</li> </ul>	<p>There are several inputs to the development process of SETA such as policy, incident report, risk assessment, threat intelligence, users' feedback</p>
The development stage	Comments and reflections							
<ul style="list-style-type: none"> <li>Conduct a Needs Assessment for SETA program</li> </ul> <p>SETA_Experts_1: we identify the needs of the department and then we identify the level of the awareness in the department. Then we identify the priority for the upcoming year and that's what we prioritize. We try to identify a theme for the entire year, or at least half a year and don't mix those themes. Because, then again, it is a waste of our efforts if there is just too much information thrown at the people.</p>	<p>A gap analysis or an assessment is done to identify what areas/topics that employees need to be aware of. In addition, to the topic the assessment should identify the people who should be given awareness, type of education.</p> <p>"Topic and people"</p> <p>The focus of the data is on training and awareness.</p>							
<ul style="list-style-type: none"> <li>Identify the needs for SETA from Policy, Risk assessment reports and incident response reports.</li> </ul>	<p>There are several inputs to the development process of SETA such as policy, incident report, risk assessment, threat intelligence, users' feedback</p>							
3) use social marketing principles as a lens to assess SETA programs in organisations	Using themes and subthemes identifies in the second analysis and key social marketing principles (Selective coding)	Group related concepts to determine whether the social market principles are considered in SETA programs (see Appendix B).						

The first analysis step involved reading the interview transcripts, making notes, and highlighting concepts related to SETA programs in organisations. These were subsequently clustered to higher-level more abstracted categories, leading to the development of a general understanding of the main practices and activities undertaken by the organisations to implement SETA programs (**open coding**). In the second analysis step, related concepts were grouped to identify relationships among the codes (**axial coding**), i.e. the key themes in the data related to the implementation of SETA programs in organisations. Finally, in the third analysis step, we used social marketing principles as a lens to assess SETA programs in organisations. **Selective coding** was applied to develop our understanding of the themes from the empirical data grouping related concepts to determine whether the social market principles are considered in SETA programs. This was done by mapping the respondents' description of SETA in their organisations to the key social marketing principles. From this, we built a narrative of how to improve the effectiveness of SETA programs.

## 4 Findings and Discussion

The following sections present our findings and discussion using the social marketing lens.

### 4.1 Employee Orientation

From social marketing, understanding what motivates or moves the behaviour of employees is the first step in developing interventions (SETA) to change that behaviour. We found that although the six organisations had different levels of maturity, the main driver for developing SETA programs was compliance. Also, the central focus of these programs was not on employees, but rather on the requirements of internal (e.g. legal team) and/or external parties (e.g. government) to enforce the implementation of information security standards and regulations. Thus, subsequent requirements included the need to prove that the organisation had indeed implemented these standards and regulations within the organisation.

Most respondents stated that their main SETA activity is to conduct mandatory security training for all employees using computer-based training (CBT). CISO1 reports: "*we have mandatory online training that everyone must complete*". Respondents reported that they must provide statistics of the number of employees who completed the training and how many times they have undertaken this type of training as part of their reporting to show compliance and their contribution to raise the awareness of the employees.

However, in some organisations, although the SETA program started with a compliance focus (mandatory CBT), further SETA activities were implemented as the program matured. These SETA activities may include ongoing awareness campaigns, training for specific groups/teams and an intensive awareness

campaign over a day or a week. These activities tend to be motivated by observed behaviour within the organisation. CISO2 reports: *“every month we have awareness messages which comes in the form of email or poster”*. Mgr3 also comments: *“we have a focused security awareness program for specific employees. For example, in my job at the Banking sector, we have specific SETA programs for call centre people”*. MGR4 also states: *“we have an annual security awareness week. That's run right across the group”*. However, there was limited evidence that employee motivation for behaviour was observed and investigated in these organisations.

A SETA program that is not ‘employee oriented’ has several disadvantages. Primarily, the lack of understanding around what motivates employees to abide by security directions may inhibit the effectiveness of any SETA activities that take place. Also, failure to understand the needs of employees around their learning style, job requirements and processes also presents challenges when developing an effective SETA program. We argue that understanding employees’ behaviour, and motivations for that behaviour, is critical when developing SETA programs. This would allow targeting of the SETA program to specific characteristics of employee behaviour and would improve the effectiveness of SETA as it will be based in a deeper understanding of employees.

## 4.2 Behaviour and Behavioural Goals

The social marketing focus is on the understanding and transforming of employee behaviour. The transformation is implemented through (1) analysis of the target behaviour, (2) identifying the desired behaviour, and (3) implementing the transformation program. There was consensus amongst participants that the aim of SETA programs is to raise employees’ awareness of the organisation’s security directives. CISO1 reported that *“the primary aim of our SETA is to make people aware of our security policies”* similarly MGR1 said *“Most of the time it is policy itself that people were made aware of”*. In terms of setting goals, participants stated that they set goals and objectives for SETA during planning *“we set objectives for the short campaigns for example, security and fraud week is develop to achieve specific objectives. We also have very high-level objectives that we'd like to achieve for the overall security awareness program”* MGR2.

Whilst participants made several references to building a culture of security and changing behaviour, no specific behaviour goals and objectives were mentioned. For example, CISO2 stated that *A SETA program should drive your information security strategy, translate your vision into reality. It should make people share your vision of security and in such way help you to build a security culture within the organisation so you can modify the behaviour of the people”*. Even though behaviour goals were not explicitly mentioned by the participants, the ultimate aim of developing SETA programs is to change employees’ behaviour to comply with security directives.

Participants recognise the importance of setting objectives and target goals for a SETA program. This is in line with the literature as almost all best practice standards and guidelines (the primary source of guidance to organisations) advise organisations to set goals for their SETA programs (Tsohou et al. 2015). However, objectives are usually limited to knowledge objectives and do not go beyond, to belief and behaviour objectives (Alshaikh et al. 2019). A SETA program that includes knowledge, belief and behaviour objectives is more likely to be effective in changing employees’ behaviours.

There was no explicit evidence given by participants that any analysis of employee behaviour was undertaken by organisations prior to SETA development, although there may be implicit indications given to the SETA team as a result of an internal security incident for example that current behaviour is not the desired behaviour. Thus, there is a lack of development around behavioural goals. However, post SETA development, study participants reported that evaluation is a real challenge, although they all employ various methods to measure effectiveness of SETA and to monitor the changes to employee behaviour. For example, the respondents stated that the number of reports of security incidents around threats addressed in the SETA program is used as an indication for the level employee’s security

awareness. However, the number of security incident reports does not necessarily reflect the extent to which the SETA program is effective in imparting an awareness of security directives for two reasons. First, ‘incidents’ are variably defined and not every “event” is an incident. Second, increases in incident reports may occur because of an increase in the number of, or sophistication of, attacks.

Therefore, it is still unknown to organisations how effective their SETA programs are in changing employee behaviour and how much they should invest on SETA to achieve an effective outcome. We argue that having specific behavioural goals and objectives helps organisations to plan as to how to measure changes in employee behaviour as a result of the implemented interventions within SETA programs.

### 4.3 Theory Based

Theory-based interventions are more successful and lead to longer lasting behaviour change ([Michie et al. 2014](#)). Theories are important for providing guidelines to organisations on conducting in-depth analyses of the behaviours that they wish to change and selecting the appropriate SETA strategies that are most likely to achieve the intended outcomes.

However, there is no evidence reported by participants to suggest the use of theories to investigate and understand employee’ behaviour, nor to guide their selection of appropriate strategies that can effectively change behaviour. This is not surprising as organisations rely on “best practice” and industry guidelines which have no empirical evidence or theoretical foundation that assists with understanding which strategies are effective in which contexts ([Alshaikh et al. 2018](#); [Ng et al. 2009](#); [Siponen and Willison 2009](#)). Additionally, despite the large number of information security behavioural studies that have made recommendations to practice, there is no basis for developing a SETA program with confidence that it will yield the intended behaviour change outcomes ([Ng et al. 2009](#); [Ögütçü et al. 2016](#)). As [Ögütçü et al. \(2016\)](#) points out, this may be because SETA programs are not informed by behavioural change theories. Therefore, it is unclear to organisations which method (or mix of methods) can be used to successfully change behaviour. Consequently, existing SETA programs tend to be less than optimal in changing behaviour.

We argue that there is a lack of explicit rationale for the development of SETA programs that can provide practical guidance on the analysis of employees’ behaviour and the selection of the appropriate strategies and techniques (*methods*) to change behaviour. As a result, practitioners face the problem of how the theoretical constructs that determine employees’ behaviour can inform the development of SETA programs.

### 4.4 Develop ‘Insight’

Social marketing suggests that genuine insight into key factors and issues (often in the form of emotional or physical barriers) relevant to positively influencing specific behaviour is required to be able to change that behaviour. One of the key areas in SETA development suggested by all participants is the identification of the needs for the SETA program. All participants suggest that the needs for SETA can be identified in policy, whilst only four participants [MGR1, CISO2, MGR3 and MGR4] reported that they also use incident reports, risk assessment, threat intelligence, and users’ feedback to identify needs. For instance, MGR4 stated: *“There are numerous inputs. Understanding the threat landscape: what is currently happening or what's being advertised. There's also a component around what incidents have we seen in the past, be they to our organisation or to other industries or organisations. we also look at what user feedback we are receiving. If people are actually saying that these are their concerns--these are their issues, we'll also feed that into it, as well. Then, also, the strategic direction of where the ISO wants to build capability. That will really dictate more or less the key areas”*.

Additionally, several examples were provided by participants on how incidents were used for awareness purposes within a SETA program. MGR4 explained that phishing attacks present opportunities to raise the employees' awareness on this type of threat.

However, it seems that traditional 'needs assessment' is very limited to knowledge of what employees need to know to comply with security directives. It does not go beyond that to develop deeper understanding and insight to identify factors related to barriers and enablers to allow employees to perform the desired behaviour. The *Develop Insight* principle provides in-depth analysis of behaviour which can be translated into practical steps to change behaviour. Our findings indicate this principle is missing from current SETA programs. Therefore, adopting this principle may improve the SETA program effectiveness.

#### 4.5 Exchange Theory

An exchange, in social marketing terms, needs to be on offer for behaviour to change. The exchange is based on having participants believe that the benefits of changing their behaviour outweigh the costs of doing so. An effective social marketing campaign should maximise the benefits and minimise the costs to participants. The organisation's SETA development team can apply the exchange theory to effectively persuade employees to adopt the desired security behaviour.

The participants state that, from the organisational perspective, their SETA programs have no motivational aspects and are only seen as a compliance requirement that is mandatory for every employee to undertake once a year. MGR1 states: *"I don't think we do any motivation. We do more of ensuring compliance by showing people what they need to know from the organisation's policies"*. However, participants provided several suggestions and recommendations on how to motivate employees to change their behaviour and perceptions towards information security and complying with security policies. Participants reported that these suggestions and recommendations were learned through experience and trial and error of what worked and what did not work during many years managing the SETA program in their organisations.

CISO2 reported that to motivate people, they tried to communicate the importance of SETA to protect the organisations from various type of risks: *"We focus on explaining the consequences of not following the organisation's policies on the business and various types of risks"*. Understanding the types of risks to the organisation information systems helps to motivate employees to attend SETA sessions and to be aware of the organisation's policies which will enable them to perform their job in secure manner. *"Awareness teams have always developed material based on a compliance and policy risk culture rather than a true business enablement culture, so there's a real opportunity for us to change the conversation and sit down with the business and say, 'These are the risks. This is how security helps you. How can we properly develop and create content that is consumable for you, supports your teams, and also facilitate better customer experience'"* MGR4.

Relating information security to an employee's personal life is another way to motivate. For example, when raising employees' awareness about the organisation's policies on the use of social media (Facebook, Twitter ...etc.), the organisation should ensure that the awareness program makes references to issues like personal and child safety when using social media. MGR3 reports: *"If we are running training on social media, we make sure it's about enabling them to be more secure on their personal social media sites or talk to their parents or children about secure social media use. We find that making that personally relevant is a really good motivator to get staff to come along and be interested and engaged in the session"*.

The findings of the study indicate that a compelling exchange offer is required to motivate employees to change their behaviour. If the 'exchange' principle in social marketing is considered in the development process of a SETA program, it would certainly assist organisations to develop a program that motivate employees to change their behaviour.

## 4.6 Competition

One of the major concerns in social marketing is to examine the internal and external factors that compete for participants' attention and to minimise the impact of this competition. While the participants did not mention whether they take into account competition for their employees' time and attention during the planning process of their SETA programs, two participants in the study reported such competition as challenge to the effectiveness of a SETA program. CISO2 points out: *"There's competition now within organisations to get the attention of employees and to hold their attention for your security awareness program to be effective. It's very difficult these days. Throughout the year, they go through many training programs. They come back to me and say, 'Do you have any idea how many training sessions we go through'"*.

Organisations face a challenge in that employees only have a limited amount of attention that can be devoted to training programs such as SETA. As organisations have become more governed by rules and regulations, the amount of training of employees has increased and employees now must be trained about occupational health and safety, sexual harassment, discrimination, privacy etc. The consequence of such competition between various functions inside the organisation for the attention of employees is that it is difficult for employees to focus and remember the information provided in SETA sessions. CISO1 states: *"There's too much information, information overflow. So, if they [employees] go and come out of our training, they forget immediately everything we taught them. They forget as they have to move on to something else and get ready for more training in two days"*.

The study participants provided several suggestions and recommendations to overcome the competition challenge:

First, using multiple delivery methods and being creative and innovative in how the organisation delivers their SETA program. *"You've got to be innovative in the way that you reach out to your colleagues, constantly refresh themes to try and get the attention of workforce using things like comic heroes, and quizzes, and giving away gifts and toys to people to try to maintain the interest"* MGR3.

Second, increase the effectiveness of the SETA program by to reducing content and increasing motivation. *"We reduced the content and increased motivational aspects, making us more approachable. That was the most important thing after having realized that with all the competition we've got"* MGR3.

Third, focus on employees who deal with sensitive information and processes. The main target in some organisations is to identify those people and develop a SETA program that targets them to safeguard the information and processes they deal with in their job. CISO2 states: *"We had to let go of the people that didn't have confidential information. That was biggest thing, I think. To let go of those and really concentrate on those people who dealt with confidential information"*. MGR4 agrees: *"We do a targeted campaign for those people who are dealing with very sensitive or very critical information. We do more frequent, more high-touch awareness training and campaigning with that particular group of stakeholders"*.

Fourth, find the right balance between getting people's attention and overwhelming them with SETA activities. *"Too much awareness is not good, people are getting confused. We've got to try and get a balance, but you don't want to do it so frequently that people become fatigued. We are vying for their attention like many other parties in the organisation. You don't want it to feel like spam and become overwhelming. It's really important that we strike the right balance"* CISO2.

Last, to overcome the problem of employees' limited time and attention is to investigate successful SETA programs in organisations that have similar risk landscapes. *"What I've been finding when I've talked to other organisations that have had successful awareness campaigns,"* MGR3.

However, it was clear that SETA teams in all six organisations do not have comprehensive understanding of all factors that compete for employee' attention and time to adopt the desired behaviour. Identifying



such factors during the planning process of a SETA program is important to minimize the impact of competition.

#### 4.7 Audience Segmentation

Social marketing uses segmentation of participants to better tailor intervention strategies. Participants indicate that their organisations group employees according to their roles and responsibilities. Then, they develop SETA programs to fulfil the needs of each segmented group. For example, CISO2 stated that, *“In my organisation, there are three kinds of training and awareness programs: one for executive management, the second type of security training and awareness is general awareness messages for all employees from all the departments and the third type is target-specific group awareness.”*

Participants agreed that the SETA program should be tailored to address the needs of each target group. In other words, different types of SETA should be designed. As MGR4 states: *“There is no one size fits all approach. [...] we need to tailor our awareness campaigns depending on the stakeholder group that we are dealing with”*. Each type should have its own characteristics in terms of the content, length/duration, frequency, and delivery methods required to meet the needs of different groups in the organisation. For instance, SETA for executive level management would be short and concise.

This finding is in line with the literature. For example, [Whitman and Mattord \(2017\)](#) state that the audience can be divided into groups based on their job descriptions, required skills and knowledge etc. In theory ‘audience segmentation’ principle is not new in the cyber security literature. However, audience segmentation in SETA literature does not involve gaining a deeper and comprehensive understanding of each segment to avoid the use of generalised SETA approach to all employees. Therefore, applying ‘audience segmentation’ should be emphasised as main principle in SETA programs to improve its effectiveness to influence behaviour. Although the study findings suggest some the organisations implemented the segmentation principles focusing on knowledge required by each segment, more need to be done to fully utilize this important social marketing principle.

#### 4.8 Method Mix

Social marketing uses an appropriate mix of methods to intervene in current behaviour, altering it to desired behaviour. These methods must be integrated to achieve synergy in the message being presented. The study participants use of multiple methods to deliver SETA. These methods vary according the message and the target group. Examples of delivery methods include email, computer-based training (CBT), classroom training and posters. For example, MGR4 states: *“We have our newsletter which is also via our email. [...] We do use some poster materials. So, there are several channels depending on what it is that we are trying to achieve”*. Likewise, MGR3 also offers that numerous techniques are used: *“It’s a program that should run throughout the year. With all sort of component such as flyers souvenirs, workshops, small groups, you can have different messages targeted to different people”*.

Similar to recommendations provided in the literature ([e.g., Abawajy 2014](#)), participants suggest that the use of a mixture of delivery techniques is an effective way to convey SETA messages. However, recommendations usually focused on raising awareness using multiple-channel approaches and not mix intervention strategies suggested in the ‘Method Mix’ in social marketing. The latter approach is a far broader concept aimed at effectively influencing the target audience behaviour. As explained previously, the social marketing approach utilises five intervention strategies: design (to alter the environment), inform (to communicate facts and attitudes) control (to regulate and enforce), educate (to enable and empower) and service (to provide support services) ([French et al. 2011](#)). We argue to successfully change employees’ behaviour, SETA programs should adopt the ‘Method Mix’ and not just focus on education and training.

#### 4.9 Summary of the assessment of SETA programs using the Social Marketing Triangle

The aim of this study is to assess the practices of current SETA programs in organisations against key social marketing principles that are essential to make sustainable behaviour change in employees' behaviour. Table 4 maps social marketing key concepts to gaps identified in existing SETA approaches.

**Table 4 A mapping of social marketing key principles to gaps in current SETA approaches**

Key Social Marketing Principles	Findings
1: Customer Orientation	Existing SETA programs aim to fulfil compliance requirements. Motivations behind employee behaviour are not investigated.
2: Behaviour and Behavioural Goals	Objectives are typically limited to knowledge acquisition and do not address deeper belief and behaviour objectives. Behaviour of target audiences' is not analysed.
3: Theory Based	The selection of intervention strategies in SETA programs is not informed by theory.
4: Develop 'Insight'	Traditional 'needs assessment' in current SETA programs is limited and does not develop a deeper understanding of employees such as emotional or physical barriers to behaviour change.
5: Exchange	Current SETA programs do not make a compelling offer to persuade employees to change their behaviour.
6: Competition	External and internal competing factors are usually not considered.
7: Audience Segmentation	Existing SETA programs mainly provide computer-based training (CBT) to all employees without paying attention to the specific needs of different segments of the employees.
8: Method Mix	SETA programs focus on raising awareness using multiple channels rather than implementing a mix of intervention strategies.

Although the maturity of SETA programs in the six organisations varies, the data shows that the social marketing key principles were not utilized in the planning and implementation of SETA programs. This may have undermined the ability of these SETA programs to change employee behaviour.

Customer orientation and insights principles were not identified in current SETA programs. SETA programs were developed to meet compliance requirements rather than addressing the needs of employees and developing in-depth understanding of how to influence their behaviours. No investigations of how employees behave took place, so the organisations were only guessing what motivates employees to behave in the way that they do. Likewise, any barriers to being able to change the behaviour, either physical or emotional were not identified. Subsequently, any interventions implemented in SETA to change behaviour is only speculation.

Exchange and competition were also not considered in the development of the SETA programs in organisations under investigation. Some of the study participants state that they have had feedback from participants stating that they face competition getting employees' attention from other parts of the organisation. However, none of the participants had examined the internal and external factors that compete for employees' attention. Further, there was no indication that the concept of providing a compelling offer had been employed to convince employees to adopt the desired behaviour and comply with security directives.

The role of theory and setting specific behavioural objectives is limited in practice. This is because organisations do not have adequate guidance to develop a theory-informed SETA program as information systems security behaviour research has mainly focused on making theoretical contributions rather than translating the theoretical insights into practical guidance to organisations.

Use of segmentation was partially applied in some organisations as they developed tailored SETA programs to different employees based on their level and job descriptions. However, there was no comprehensive understanding of each segment of the target audience leading to prioritisation of specific segments based on their influence on other segments -groups in the organisation- and susceptibility to cyber risks. Particularly, the organisations do not consider learning styles of employees when developing SETA programs.

Subsequently, we argue that there is no employee oriented systematic approach to the development of SETA programs in organisations. Developed programs tend to be compliance driven and a focus on many of the aspects that social marketing uses to drive behaviour change is missing. In the next section we propose a SETA development process grounded in the social marketing approach.

## 5 A Social Marketing SETA Development Process

The process for developing a strategic social marketing plan is outlined in detail in [Lee and Kotler \(2015\)](#). As shown in Figure 2, the process consists of ten steps divided into five key phases: scoping, selecting, understanding, designing, and managing. The five phases are described below with examples from the information security context to demonstrate to how these phases can be applied to the domain.

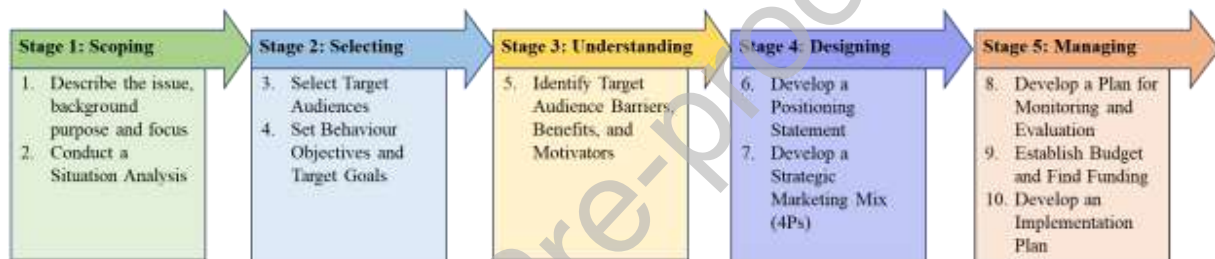


Figure 2 The Proposed SETA Planning Process Adopted from [Lee and Kotler \(2015\)](#)

The process is a logical step-by-step approach, from scoping through to managing, giving a clear progression for how the project will be conducted. These steps are spiral in nature – not linear. The steps would usually progress linearly but going back and adjusting prior steps may be necessary. For example, it may be necessary to refine the goals after gaining more understanding of the target audience or change the communication channel based on the available budget. The following discussion is based on the detail outlined in [Lee and Kotler \(2015\)](#).

### 5.1 Scoping Phase

The scoping phase aims to build foundational knowledge about the issues and problems that the social marketing campaign is to address. The scoping phase consists of two steps: 1) describe the issue, background purpose, and focus and 2) conduct a situation analysis.

#### 5.1.1 Step 1: Describe the issue, background purpose and focus

In this step, the social issue that the project is intended to address is identified and described in detail. A series of questions around the problem need to be answered to form a sound understanding of the issue. To support the decision to focus on specific issues, data can be used from sources such as scientific research and publicly available reports by government and other organisations. A purpose statement is then developed to outline the benefits of a successful campaign, and the focus of the campaign is selected from the factors identified through the research. A compelling purpose statement at the start of the social marketing plan is essential for building a strong motivation to conduct a campaign to influence and change behaviour.

In this paper, the example of phishing attacks is used to demonstrate how a social marketing approach can be applied in a SETA program. In this step, several resources (e.g. literature review and cyber security

reports) can be used to describe the issue (phishing attack), provide the background and purpose of the campaign and identify the focus.

An example issue statement might be: *recent security reports indicate that security incidents caused by employees clicking on phishing links constitute 90% of the total number of security incidents. Our Organisation has lost X amount of money/data/reputation as a result of incidents of employee noncompliance with our organisation's policy on dealing with phishing emails. The broader purpose of the campaign to address phishing attacks is to protect our organisation by improving employees' responses to phishing emails.*

### 5.1.2 **Step 2: Conduct** a Situation Analysis

Once the purpose and focus of the campaign plan are described, the team should start to analyse the external and internal factors that might affect the campaign planning process. A SWOT (strength, weaknesses, opportunities, and threats) analysis is conducted to identify organisational strengths to maximise, weaknesses to minimise, opportunities to utilise and threats to overcome. Strengths and weaknesses are internal factors (such as available resources, expertise, management support, current alliances, and partners etc.), while opportunities and threats are external factors. The result of the analysis should be a list of factors that will guide the campaign's planning process ([French et al. 2011](#); [Lee and Kotler 2015](#)).

A possible SWOT analysis for the phishing emails campaign can be as follows: The greatest organisational *strength* going into the phishing campaign is the high awareness level of top management of the importance of protecting the organisation from evolving cyber threats. The awareness should result in management's commitment to protecting the organisation from cyber threats and supporting the campaign effort. *Weaknesses* include limited resources (e.g., full time staff and budget) to: a) conduct the awareness campaign, b) maintain the campaign and c) measure the effectiveness of the campaign.

External *opportunities* to take advantage of may include: aligning the campaign effort with general awareness of cyber security international days/public campaigns (e.g., Safer Internet Day, Stay Smart Online) and using resources developed by government and other organisations such as templates, emails and twitter hashtags to amplify your message. The organisation's SETA team should build alliances with other organisations' teams (private and public sector) to share their expertise and resources and therefore take advantage of and build into the organisation's campaign plan.

A *threat* to prepare for is the level of sophistication of phishing emails. Attackers use advanced tools and strategies to deceive the employees into clicking on phishing links by taking advantage of information people disclose on their social media, or information freely available about the organisation, which makes it difficult for the organisation to change their employees' behaviour to effectively identify and report these emails.

## 5.2 Selecting Phase

The selecting phase consists of two steps: 3) select target audiences and 4) set behaviour objectives and goals.

### 5.2.1 **Step 3: Select** Target Audiences

The target audience is the group whose behaviour is targeted by the campaign effort. Developing a thorough description of the target group includes determining its demographics, social networks, and size. It is advisable that the marketing plan focuses on one primary target audience. Selecting the target audience involves segmenting the market (population) into similar groupings, evaluating these segments based on a set of criteria, choosing one or more main groups and finally specifying the desired behaviour. The decision on which segment of the target audience to select is based criteria, such as *needs* (problem incidence, problem severity), *readiness for action* (readiness and willingness to change), *reach*

(communication channel) and *best match* (organisational mission, expertise and resources) ([Lee and Kotler 2015](#)).

In the phishing attack example, the organisation's SETA development team should carefully select the target audience for the campaign, and then segment it into smaller groups based on roles and responsibilities, departments and level (e.g., management level top and middle management). Each segment of the target audience should be evaluated based on size, ability to reach and susceptibility to phishing attacks. For instance, the SETA team should conduct a review of the type and number of cyber security incidents caused by clicking on a phishing link. This will provide valuable information about which group in the organisation is targeted the most by phishing attacks/email/links.

### 5.2.2 Step 4: Set Behaviour Objectives and Target Goals

Once the campaign target audience is selected and described, the team should set specific behaviour objectives and goals to be achieved. The selection of the target audience will enable the team to establish specific behaviour objectives that will influence the behaviour of the selected audience.

There are three type of objectives a social marketing campaign should aim for. First, *knowledge objectives* aim to raise awareness in the target group about the issues and make them willing to perform the desired behaviour. Second, *belief objectives* aim to change the target group's feelings and attitudes toward the issue. Third, *behaviour objectives* aim to change the target group's behaviour to either accepting, rejecting, modifying, abandoning, switching to, or continuing, a target behaviour. The campaign goals have to be SMART (specific, measurable, achievable, relevant and time-bound) goals that quantify the desired behaviour outcome and changes in knowledge, beliefs and behaviour intent ([Lee and Kotler 2015](#)).

Phishing campaign strategies should be developed to support the three types of objectives: (a) *knowledge objectives* of raising awareness (e.g., what are phishing attacks, risks phishing emails pose to the systems, how to identify and report phishing emails), (b) *belief objectives* of convincing (target audience) employees to believe that the behaviour of clicking on a phishing link has negative consequences on the systems, and (c) *behaviour objectives* of influencing the target audience to change their behaviours. The overall goal of the phishing campaign is to protect the organisation by reducing security incidents resulting from employees clicking on phishing links. Specific and measurable goals of the phishing campaign are an increase in the number of phishing emails reported and a decrease in the number of clicks on phishing links.

## 5.3 Understanding Phase

After selecting the campaign's target audience and the desired behaviour, it is time to understand the target audience in relation to the desired behaviour. The understanding phase consists of one step: 5) identify target audience barriers, benefits, and motivators.

### 5.3.1 Step 5: Identify Target Audience Barriers, Benefits, and Motivators

In this step, a thorough and detailed analysis of the selected segment of the target audience is conducted. The analysis process involves understanding the target audience's knowledge and attitudes toward the target behaviour and the real and perceived barriers to the target behaviour ([Lee and Kotler 2015](#)). The analysis also aims to identify the benefits the target audience expect in exchange for performing the desired behaviour. It also identifies strategies to motivate the target audience to adopt the desired behaviour, the behaviour / forces that compete with the desired behaviour and who has the power to influence the target audience.

To perform the behavioural analysis, data should ideally be collected from multiple sources to obtain as much detailed and accurate information as possible. Different data collection methods can be used, including literature reviews, interviews, focus groups, direct observation and questionnaires ([French et al.](#)



2010). The selection of the data collection techniques depends on the type of behaviour being targeted. There are specific questions that could be asked to identify barriers, benefits, and motivators. These questions can be adapted to cyber security behaviour and context.

For our phishing example, focus groups can be conducted with a selected sample of employees from the target audience of the phishing campaign. The SETA team should ask questions to determine existing knowledge about phishing attacks, the barriers to avoiding clicking on links and the motivators for doing the right thing (report the phishing emails). Examples of expected answers to the questions might be that they do not have adequate knowledge to identify phishing emails and they do not have the time to thoroughly examine emails to determine whether they are phishing emails. Answers related to motivation to report phishing may refer to receiving feedback on their report (confirmation it is phishing and acknowledgment that they are protecting the organisation) or linking the behaviour to their personal life (protecting their children and personal computers). Direct observation of the targeted employees could also be conducted.

## 5.4 Designing Phase

The designing phase involves two steps: 6) develop a position statement and 7) develop a strategic marketing mix.

### 5.4.1 Step 6: Develop a Positioning Statement

The positioning statement describes how the social marketing team want the target audience to see the behaviour they would like adopted instead of the competing behaviour (Grier and Bryant 2005; Lee and Kotler 2015). This step is usually achieved by branding that helps to secure the desired position. The positioning statement and brand identity is informed by the data collected in the previous 'understanding' phase. The positioning statement is important as it guides the development of the strategic marketing mix. Positioning strategies can have a behaviour, barriers, benefits, or competition focus depending on the desired behaviour and the stage of adoption. For example, if the behaviour is new and/or very specified, then behaviour-focused positioning that describes and highlights the behaviour would be the most appropriate positioning strategy.

In the cyber security domain, the positioning statement for phishing attacks could be that *we want employees to believe that clicking on phishing links will have detrimental consequences for the organisational information resources and that appropriately responding to phishing emails (avoid clicking on links and report it) will protect the organisation.*

### 5.4.2 Step 7: Develop a Strategic Marketing Mix (4Ps)

The 4Ps (product, price, place, and promotional strategies) are intervention tools that campaigns can use to influence the target audience to adopt the desired behaviour. The 4Ps are used to reduce barriers, and to create and deliver the value that the target audience expects in exchange for adopting the new behaviour.

There are three types of product levels: core, actual and augmented. The core product represents the benefits the target audience values and will experience if they do the desired behaviour. The actual product consists of actual features of the desired behaviour and any services and resources that will support the desired behaviour. The augmented product includes any additional tangible services that will be added in the offer or that will be promoted to the target audience.

Concerning price, the social marketing team should mention any related financial costs that the target audience will pay (e.g., cost for buying a service) and any financial benefits they will receive as an incentive for performing the desired behaviour. Price should also include non-financial incentives (e.g., appreciation for performing the desired behaviour) and disincentives (e.g., warning letter).

The place is when and where the target audience will perform the desired behaviour.

In the promotion section of the 4Ps, persuasive communication strategies are described using four main elements: the key messages of the social campaign that will influence the target audience, who is going to deliver the messages (messengers), the communication channel that is going to be used to communicate the messages to the target audience and the creative elements such as the logo, taglines and graphics. The promotion plan is essential for ensuring that the target audience knows about the offer (product, price and place), that they believe they will gain benefits from performing the desired behaviour and that they are inspired to act ([Lee and Kotler 2015](#)).

In our cyber security example, the product could be launching a new service (reporting and support services) for employees who receive email that they suspect is a phishing email. Once the reported email is received by the help desk it will be checked, and if it is a phishing email, the employee will receive an email to thank them for their help in protecting the organisation. In our phishing example, there would be no direct costs for the service and no financial incentives. However, employees showing irresponsible behaviour by clicking on a phishing link that causes the system to be compromised can cost the employees their job or affect their performance and therefore their promotion. In the cyber security domain, place is the organisation context or anywhere that uses the organisation's systems.

Effectively addressing the issues that have been identified that prevent employees from responding appropriately to phishing emails is based on an understanding of the target audience. Different strategies can be used to promote the desired behaviour, including awareness training for essential skills in identifying and reporting phishing emails and raising awareness about the impact of opening phishing emails and clicking on their links. The channel for communicating the campaign messages would be emails, the organisation's website, and/or internal social media networks (e.g., Yammer).

## 5.5 Managing Phase

The managing phase consists of three steps: 8) develop a plan for monitoring and evaluation, 9) establish budget and find funding sources, and 10) develop an implementation plan.

### 5.5.1 Step 8: Develop a Plan for Monitoring and Evaluation

The monitoring and evaluation plan should include measures that will be used to evaluate the success of the campaign effort and how and when these measurements will be taken. The evaluation strategies are developed based on the purpose and goals of the social marketing campaign (the desired level of behaviour change, knowledge and beliefs) ([French et al. 2010](#); [Lee and Kotler 2015](#)). It is recommended that the evaluation plan be developed before the budget is established to ensure this step is considered when it comes to determining the availability of resources. There are four types of measures: *input measures* (resources used in the campaign), *output measures* (campaign activities), *outcome measures* (target audience responses and changes in knowledge, beliefs and behaviour) and *impact measures* (contribution to the effort's purpose) ([Lee and Kotler 2015](#); [Sowers et al. 2007](#)).

In the phishing example, developing a plan to monitor and evaluate the success of the SETA campaign is vital. The plan should have a detailed description of each type of measure. This example focuses on the last two types of measures (outcome measure and impact measure). As mentioned in Section 5.2.2, the goal of the phishing campaign is to increase the number of reports and decrease the number of clicks on phishing links. The outcome measure should look at the number of phishing reports and the number of clicks on phishing links before and after the campaign. The impact measure is the overall protection of the organisation's information systems as a result of the decrease in phishing-related security incidents. Although some cultural change aspects can be difficult to measure precisely, such as positive attitudes and supporting co-workers in dealing with phishing emails, they can be observed by team managers and the security team.

### 5.5.2 **Step 9: Establish Budget and Find Funding Sources Budget**

The team ensures that all the resources required to undertake the steps in the social marketing plan are available and if not, what source of funding is available to acquire these resources. This step may trigger a revision of previous steps, such as the purpose and the target audience, so that the team can work within the allocated resources if funding for the original plan cannot be secured. The final budget is presented in this section of the social marketing campaign.

In this step, the SETA team should prepare the budget for the costs associated with the phishing campaign. These usually include the cost of segmenting and understanding the target audience, designing products (e.g., posters), training sessions and monitoring and evaluation (phishing simulations exercises). The team should identify the required resources and potential sponsors within the organisation (security managers and/or chief information security officer).

### 5.5.3 **Step 10: Develop an Implementation Plan**

The implementation plan is referred to as the real marketing plan as it provides detailed information about the roles and responsibilities (who is going to do what), specific tasks and the schedule of campaign activities. This detailed plan should then be shared with relevant stakeholders in the organisation. To achieve sustainable behaviour change, it is recommended that the implementation plan should include what efforts will be made in subsequent years to maintain the behaviour change ([Lee and Kotler 2015](#)).

In the cyber security context, a list of related tasks, the roles and responsibilities and an overall timetable of the campaign activities should be developed. The implementation plan should also include piloting and testing prior to rollout. The SETA team should also continue their intended efforts to ensure that the behaviour change is maintained.

## 6 Discussion

In this section, we map stages of the proposed SETA development process to social marketing principles to show how the proposed model addresses gaps in existing SETA approaches. Further, we discuss how the proposed model, when compared to existing approaches, can provide comprehensive and systematic guidance to develop an effective SETA program.

The proposed SETA development process can address the gaps in existing SETA programs identified as shown in Table 4. In the *scoping phase* of the process, the SETA team develops background information about the problem(s) that the SETA campaign will address and identifies the required resources, strengths, and weaknesses. Building a thorough understanding of the problem and its impact on the organisation is essential in developing effective SETA (**Principle 1: Customer Orientation**).

The *selecting phase* involves identifying and selecting the target audience for the SETA campaign (**Principle 7: Audience Segmentation**) which assists in developing tailored SETA programs to address the needs of each segment of the target audience rather than providing a generic “one size fits all” program. The *selecting phase* also includes setting behaviour-related goals and objectives that the SETA campaign should achieve (**Principle 2: Behaviour and Behavioural Goals**). Including behaviour objectives for the SETA campaign addresses the gap in existing SETA programs which focus on knowledge and overlook behaviours, beliefs, and attitudes.

As the name suggests, the *understanding phase* provides a comprehensive and thorough understanding of the target audience (i.e. why do they behave in this way, what motivates them? etc). Such understanding will help to generate useful insights (**Principles 4 & 1: Develop ‘Insight’ & Customer Orientation**) for developing effective SETA strategies to change employee behaviour. Further, the *understanding phase* encompasses identifying factors that compete for the time and attention of employees for them to adopt the induced behaviours (**Principle 6: Competition**). Moreover, during the *understanding phase*, theories can be used to develop theory-informed interventions (**Principle 3: Theory Based**) which addresses the lack of theory-informed SETA programs.

In the *designing phase* the value exchange and method mix are both considered to convince and enable the target audience to adopt the induced behaviour and/or give up the undesired behaviours (**Principles 5 & 8: Exchange & Method Mix**). The positioning step highlights how the development team wants the target audience to see the behaviour and develops a convincing offer for the target audience. Further, developing the strategic marketing mix (4Ps) goes above and beyond providing awareness into implementing mix intervention strategies such as design (to alter the environment), inform (to communicate facts and attitudes) control (to regulate and enforce), educate (to enable and empower) and service (to provide support services) to change and influence employees' security related behaviours.

There are several academic and industry publications that provide useful practical recommendations and strategies to assist organisations developing SETA programs. Academic literature in IS security behaviour mainly focuses on investigating why employees do not comply with policy. The research applies various theories (e.g., deterrence theory, neutralization theory, protection, motivation theory and organisational justice). For instance, [Willison et al. \(2018\)](#) studied the effect of perceived organisational injustice on the employee intention to violate security. The study proposed model based on organisation justice theory (procedural and distributive). The authors used deterrence and neutralisation techniques as moderators on the effect of perceived injustice on employee intent to violate the policy. The study found that employees may form intentions to commit computer abuse if they perceive the presence of procedural injustice and that techniques of neutralization and certainty of sanctions moderate this influence. A practical implication of the study is that "managers should pay particular attention to the transparency and communication associated with review structures that are designed to assist employees in understanding their accordance with the expectations of management and with their peers." ([Willison et al. 2018](#)). While many IS security behaviour studies provide considerable contributions, they approach the problem from an individual level rather than providing comprehensive organisational strategies to develop effective SETA programs.

Practitioner literature (e.g., [Beyer et al. 2015](#); [Carpenter 2019](#); [ENISA 2012](#); [ENISA 2017](#); [ISF 2014](#); [SANS 2019](#)) on the other hand, suggest strategies based on experience (and opinion) for organisations to develop engaging and relevant SETA programs.

Several authors argued that the focus should be on employee behaviour and that disseminating policy directives through annual and mandatory web-based training is not effective in changing employee behaviour ([Beyer et al. 2015](#); [Carpenter 2019](#); [SANS 2019](#)). [Carpenter \(2019\)](#) reviewed marketing, behavioural and culture management to draw lessons from these three domains that can be applied in developing SETA programs. Intervention strategies provided by [Carpenter \(2019\)](#) are similar to those recommended by other publications. These include developing cyber security champions, aligning SETA objectives to organisational needs and risk profile, integrating security communications to other organisational messages, and enabling employees to protect themselves and their family ([Beyer et al. 2015](#); [ENISA 2017](#); [SANS 2019](#)). [SANS \(2019\)](#) and [Beyer et al. \(2015\)](#) both provided frameworks to guide organisations from compliance driven SETA to behavioural focused SETA programs.

Our proposed SETA development process enables organisations to leverage the insights in academic and industry literature. Behavioural insights from academic studies can be used in developing in depth understanding of the target audience at the '*understanding phase*' of proposed model. While the practical strategies provided in industry literature are valuable in guiding organisations during the '*designing phase*' of the proposed model. Thus, the proposed SETA development process can integrate available knowledge in the security literature as well as using social marketing principles to influence employee's security related behaviours.

The proposed SETA development is novel and systematic for three reasons. First, it provides a systematic planning process that integrates social marketing principles to successfully influence behaviour. Second, it develops a thorough and in depth understanding of the target audience to guide the development of effective SETA strategies. Last, it applies multiple strategies to change and influence behaviours.

## 7 Conclusion, Contributions and Future Work

This paper investigates the use of the social marketing approach in SETA. Our review of the literature shows that there is little evidence that the social marketing approach has been applied for SETA development, even though it has been used in other domains to effectively change behaviour. To further investigate this in practice, we undertook six expert interviews with experienced practitioners in the SETA field. These expert interviews reveal that despite awareness training, by definition, being about changing employee behaviour, organisations tend not to have an in depth, behaviour driven focus to their SETA programs. Like [Tan et al. \(2010\)](#), we find that organisations are still compliance driven –this is why they have SETA programs in the first place. Our findings show that organisations only consider one of the 8 social marketing principles (audience segmentation) when they develop SETA programs. The other seven principles are either not used at all or are only minimally considered. The paper also presents a systematic and theory-informed development process for SETA programs based on the social marketing approach. We illustrate how such an approach can be used for the development of SETA programs in organisations, using a scenario focused on phishing.

This paper makes a major contribution to how organisations practice information security awareness training. Using the social marketing approach, the paper describes a process of how a SETA program could be designed for the specific alteration of behaviour of employees towards phishing. The process is adaptable for all behaviours related to information security exhibited by employees. Thus, the paper informs practice of how employee security behaviour can be changed, using a proven technique – social marketing, which should be more effective than the currently used methods in organisations. One limitation of this paper is that it does not report on the implementation of this process in practice. This is the target of a future publication.

From a theory perspective, this research applies the social marketing approach to a new domain – SETA. This addresses the identified gap in the literature of there being no systematic SETA development process. The lack of a systematic development process which is focussed on the behaviour of employees has resulted in ineffective SETA programs that are ineffective in influencing behaviour. Therefore, using the social marketing approach and its planning process can guide organisations in selecting a specific behaviour, identifying the target audience, understanding the barriers, benefits and motivators for performing the desired behaviour and then designing a SETA program with mix intervention and marketing strategies to achieve behaviour change.

Our proposed SETA process provides a sound basis for further work. First, embedding our process for social marketing-based SETA development in an organisation would be the initial step. Then research can occur that measures the effectiveness of this approach within a single organisation. Second, a measurement tool based on social marketing key principles can be developed to help organisations assess their SETA programs. This will enable organisations to identify gaps to address and areas to improve to develop effective SETA programs that can successfully change employees' behaviour.

CRedit author statement

**Moneer Alshaikh:** Conceptualization, Methodology and Writing-Original draft preparation.

**Sean B Maynard and Atif Ahmad** Reviewing and Editing-final draft.

### Declaration of interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.



☒The authors declare the following financial interests/personal relationships which may be considered as potential competing interests:

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

## 8 References

- Abawajy, J. 2014. "User Preference of Cyber Security Awareness Delivery Methods," *Behaviour & Information Technology* (33:3), Mar 4, pp 237-248.
- Accenture & HfS Research. 2016. "The State of Cybersecurity and Digital Trust: Identifying Cybersecurity Gaps to Rethink State of the Art." Retrieved from <https://www.accenture.com/us-en/insight-cybersecurity-digital-trust-2016>
- Ahmad, A., Desouza, K.C., Maynard, S.B., Naseer, H., and Baskerville, R.L. 2020. "How Integration of Cyber Security Management and Incident Response Enables Organizational Learning," *Journal of the Association for Information Science and Technology* (71:8), pp 939-953.
- Almestahiri, R.d., Rundle-Thiele, S., Parkinson, J., and Arli, D. 2017. "The Use of the Major Components of Social Marketing: A Systematic Review of Tobacco Cessation Programs," *Social Marketing Quarterly* (23:3), 2017/09/01, pp 232-248.
- Alshaikh, M. 2020. "Developing Cybersecurity Culture to Influence Employee Behavior: A Practice Perspective," *Computers & Security* (98), 2020/11/01/, p 102003.
- Alshaikh, M., Ahmad, A., Maynard, S.B., and Chang, S. 2014. "Towards a Taxonomy of Information Security Management Practices in Organisations," *25th Australasian Conference on Information Systems*, Auckland, New Zealand, p. 10.
- Alshaikh, M., Maynard, S.B., Ahmad, A., and Chang, S. 2018. "An Exploratory Study of Current Information Security Training and Awareness Practices in Organizations," in: *Proceedings of the 51st Hawaii International Conference on System Sciences*. Hawaii, US: pp. 5085-5094.
- Alshaikh, M., Naseer, H., Ahmad, A., and Maynard, S.B. 2019. "Toward Sustainable Behaviour Change: An Approach for Cyber Security Education Training and Awareness," *In Proceedings of the 27th European Conference on Information Systems (ECIS)*, Stockholm & Uppsala, Sweden.
- Andreasen, A.R. 2002. "Marketing Social Marketing in the Social Change Marketplace," *Journal of Public Policy & Marketing* (21:1), 2002/04/01, pp 3-13.
- Ashenden, D., and Lawrence, D. 2013. "Can We Sell Security Like Soap?: A New Approach to Behaviour Change," in: *Proceedings of the 2013 New Security Paradigms Workshop*. Banff, Alberta, Canada: ACM, pp. 87-94.
- Bada, M., Sasse, A.M., and Nurse, J.R. 2019. "Cyber Security Awareness Campaigns: Why Do They Fail to Change Behaviour?," *arXiv preprint arXiv:1901.02672*.
- Beyer, M., Ahmed, S., Doerlemann, K., Arnell, S., Parkin, S., Sasse, M., and Passingham, N. 2015. "Awareness Is Only the First Step," *A framework for progressive engagement of staff in cyber security*, Hewlett Packard, Business white paper).

- Boudreau, M.-C., and Robey, D. 2005. "Enacting Integrated Information Technology: A Human Agency Perspective," *Organization science* (16:1), pp 3-18.
- Bowen, P., Hash, J., and Wilson, M. 2006. "Sp 800-100. Information Security Handbook: A Guide for Managers." Retrieved from
- Carpenter, P. 2019. *Transformational Security Awareness: What Neuroscientists, Storytellers, and Marketers Can Teach Us About Driving Secure Behaviors*. John Wiley & Sons.
- Chatterjee, S., Sarker, S., and Valacich, J.S. 2015. "The Behavioral Roots of Information Systems Security: Exploring Key Factors Related to Unethical It Use," *Journal of Management Information Systems* (31:4), 2015/01/01, pp 49-87.
- Chaudhry, P.E., Chaudhry, S., and Reese, R. 2012. "Developing a Model for Enterprise Information Systems Security," *Economics, Management & Financial Markets* (7:4), pp 587-599.
- Corbin, J., and Strauss, A. 2015. *Basics of Qualitative Research*. sage.
- 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), pp 525-554.
- Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., and Baskerville, R. 2013. "Future Directions for Behavioral Information Security Research.," *Computer & Security* (23), pp 90-101.
- D'Arcy, J., and 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), pp 643-658.
- 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), pp 79-98.
- De Maeyer, D. 2007. "Setting up an Effective Information Security Awareness Programme," in: *Isse/Secure 2007 Securing Electronic Business Processes*. Vieweg, pp. 49-58.
- Eisenhardt, K.M. 1989. "Building Theories from Case Study Research," *Academy of management review* (14:4), pp 532-550.
- ENISA. 2012. "Collaborative Awareness Raising for Eu Citizens & Smes." Retrieved from <https://www.enisa.europa.eu/publications/eisas-large-scale-pilot>
- ENISA. 2017. "Cyber Security Culture in Organisations." Retrieved from <https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations>
- Fertig, T., Schütz, A.E., and Weber, K. 2020. "Current Issues of Metrics for Information Security Awareness," In *Proceedings of the 28th European Conference on Information Systems (ECIS)*, An Online AIS Conference.
- French, J., and Blair-Stevens, C. 2005. *Social Marketing Pocket Guide*.
- French, J., Blair-Stevens, C., McVey, D., and Merritt, R. 2010. *Social Marketing and Public Health: Theory and Practice*. Oxford University Press.
- French, J., Merritt, R., and Reynolds, L. 2011. *Social Marketing Casebook*. Sage.
- Glanz, K., and Rimer, B.K. 1997. *Theory at a Glance: A Guide for Health Promotion Practice*. US Dept. of Health and Human Services, Public Health Service.
- Grier, S., and Bryant, C.A. 2004. "Social Marketing in Public Health," *Annual Review of Public Health* (26:1), 2005/04/21, pp 319-339.
- Grier, S., and Bryant, C.A. 2005. "Social Marketing in Public Health," *Annu. Rev. Public Health* (26), pp 319-339.
- Guo, K.H., Yuan, Y., Archer, N.P., and Connelly, C.E. 2011. "Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model," *Journal of Management Information Systems* (28:2), 2011/10/01, pp 203-236.
- Hanus, B., and Wu, Y.A. 2016. "Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective," *Information Systems Management* (33:1), pp 2-16.
- Herold, R. 2010. *Managing an Information Security and Privacy Awareness and Training Program*. CRC press.
- ISF. 2014. "From Promoting Awareness to Embedding Behaviours," Information Security Forum (ISF). Retrieved from
- ISO/IEC. 2013. "Iso/Iec 27002 Interntional Standard: Information Technology - Security Techniques- Code of Practice for Information Security Controls."
- Jampen, D., Gür, G., Sutter, T., and Tellenbach, B. 2020. "Don't Click: Towards an Effective Anti-Phishing Training. A Comparative Literature Review," *Human-centric Computing and Information Sciences* (10:1), pp 1-41.
- Johnston, A.C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS quarterly*, pp 549-566.

- Karjalainen, M., Sarker, S., and Siponen, M. 2019. "Toward a Theory of Information Systems Security Behaviors of Organizational Employees: A Dialectical Process Perspective," *Information Systems Research* (30:2), 2019/06/01, pp 687-704.
- Karjalainen, M., and Siponen, M. 2011. "Toward a New Meta-Theory for Designing Information Systems (Is) Security Training Approaches," *Journal of the Association for Information Systems* (12:8), pp 518-555.
- Khan, B., Alghathbar, K., and Khan, M. 2011. "Information Security Awareness Campaign: An Alternate Approach," in: *Information Security and Assurance*, T.-h. Kim, H. Adeli, R. Robles and M. Balitanas (eds.). Springer Berlin Heidelberg, pp. 1-10.
- Ki-Aries, D., and Faily, S. 2017. "Persona-Centred Information Security Awareness," *Computers & Security* (70), 2017/09/01/, pp 663-674.
- Klein, H.K., and Myers, M.D. 1999. "A Set of Principles for Conducting and Evaluating Interpretive Fields Studies in Information Systems.," *MIS Quarterly* (23:7), pp 67-94.
- Kritzinger, E., and Smith, E. 2008. "Information Security Management: An Information Security Retrieval and Awareness Model for Industry," *Computers & Security* (27:5-6), 10//, pp 224-231.
- Lebek, B., Uffen, J., Breitner, M.H., Neumann, M., and Hohler, B. 2013. "Employees' Information Security Awareness and Behavior: A Literature Review," *The 46th hawaii international conference on system sciences (HICSS)*, pp. 2978-2987.
- Lee, N.R., and Kotler, P. 2015. *Social Marketing: Changing Behaviors for Good*. Sage Publications.
- McKenzie-Mohr, D. 2011. *Fostering Sustainable Behavior: An Introduction to Community-Based Social Marketing*. New society publishers.
- Michie, S., Atkins, L., and West, R. 2014. *The Behavior Change Wheel: A Guide to Designing Interventions*. Great Britain: Silverback Publishing.
- Neuman, W.L. 2014. *Social Research Methods: Qualitative and Quantitative Approaches*, (Seventh ed.). London: Pearson Education Ltd.
- Ng, B.-Y., Kankanhalli, A., and Xu, Y. 2009. "Studying Users' Computer Security Behavior: A Health Belief Perspective," *Decision Support Systems* (46:4), 2009/03/01/, pp 815-825.
- NTT Security. 2019. "Global Threat Intelligence Report," NTT Security, Japan, p. 50. Retrieved from [https://www.nttsecurity.com/docs/librariesprovider3/resources/2019-gtir/2019\\_gtir\\_report\\_2019\\_uea\\_v2.pdf](https://www.nttsecurity.com/docs/librariesprovider3/resources/2019-gtir/2019_gtir_report_2019_uea_v2.pdf)
- Öğütçü, G., Testik, Ö.M., and Chouseinoglou, O. 2016. "Analysis of Personal Information Security Behavior and Awareness," *Computers & Security* (56), 2//, pp 83-93.
- Park, M., and Chai, S. 2018. "Internalization of Information Security Policy and Information Security Practice: A Comparison with Compliance," *Proceedings of the 51st Hawaii International Conference on System Sciences*.
- PCI. 2014. "Information Supplement: Best Practices for Implementing a Security Awareness Program." Security Awareness Program Special Interest Group PCI Security Standards Council.
- Peltier, T.R. 2005. "Implementing an Information Security Awareness Program," *EDPACS* (33:1), 2005/07/01, pp 1-18.
- Power, R., and Forte, D. 2006. "Case Study: A Bold New Approach to Awareness and Education, and How It Met an Ignoble Fate," *Computer Fraud & Security* (2006:5), 5//, pp 7-10.
- Puhakainen, P., and Siponen, M. 2010. "Improving Employees' Compliance through Information Systems Security Training: An Action Research Study," *Mis Quarterly* (34:4), pp 757-778.
- SANS. 2017. "Security Awareness Report: It's Time to Communicate." Retrieved from
- SANS. 2019. "The Rising Era of Awareness Training." Retrieved from <https://www.knowbe4.com/hubfs/SANS-Security-Awareness-Report-2019.pdf>
- Sharma, S., and Warkentin, M. 2019. "Do I Really Belong?: Impact of Employment Status on Information Security Policy Compliance," *Computers & Security* (87), p 101397.
- Shedden, P., Ahmad, A., and Ruighaver, A.B. 2011. "Informal Learning in Security Incident Response Teams," *Paper presented at the 22nd Australasian Conference on Information Systems*. , Sydney, Australia., pp. 1-11.
- Shedden, P., Smith, W., Scheepers, R., and Ahmad, A. 2009. "Towards a Knowledge Perspective in Information Security Risk Assessments—an Illustrative Case Study," *Paper presented at the 20th Australasian Conference on Information Systems*, Melbourne, Australia, pp. 74-84.
- Siponen, M., and Vance, A. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS quarterly*, pp 487-502.

- Siponen, M.T., and Willison, R. 2009. "Information Security Management Standards: Problems and Solutions," *Information and Management* (46), pp 267-270.
- Sowers, W., French, J., and Blair-Stevens, C. 2007. "Lessons Learned from Social Marketing Models in the United Kingdom," *Social Marketing Quarterly* (13:3), pp 58-62.
- Stebbins, R.A. 2001. *Exploratory Research in the Social Sciences*. Sage.
- Tan, T., Ruighaver, A., and Ahmad, A. 2010. "Information Security Governance: When Compliance Becomes More Important Than Security," in: *Security and Privacy – Silver Linings in the Cloud*, K. Rannenberg, V. Varadharajan and C. Weber (eds.). Springer Berlin Heidelberg, pp. 55-67.
- Tapp, A., and Rundle-Thiele, S. 2016. "Social Marketing and Multidisciplinary Behaviour Change," *Beyond behaviour change: Key issues, interdisciplinary approaches and future directions*, p 135.
- 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), pp 38-58.
- Warkentin, M., and Willison, R. 2009. "Behavioral and Policy Issues in Information Systems Security: The Insider Threat," *European Journal of Information Systems* (18:2), 2009/04/01, pp 101-105.
- Whitman, M.E., and Mattord, H.J. 2017. *Principles of Information Security*, (6th ed.). Course Technology, Cengage Learning.
- Willison, R., and Warkentin, M. 2013. "Beyond Deterrence: An Expanded View of Employee Computer Abuse," *MIS quarterly*, pp 1-20.
- Willison, R., Warkentin, M., and Johnston, A.C. 2018. "Examining Employee Computer Abuse Intentions: Insights from Justice, Deterrence and Neutralization Perspectives," *Information Systems Journal* (28:2), pp 266-293.
- Yin, R.K. 2018. *Case Study Research and Applications: Design and Methods*. Sage publications.

## Appendix A: Interview Questions

### 1- Direct questions about practices related to the practice area:

- What steps do you take as a security manager to conduct a security awareness program?
- Can tell me how the process of developing security awareness works?

### 2- Follow up questions and Interrelated security management area

- How can an organisation identify the needs for SETA?
- How do you plan for SETA?
- What are the things that you take into consideration when you plan for SETA?
- Can you tell me a little bit about how you use:
  - i. Policy
  - ii. Risk
  - iii. Incident response
- Does it inform what you do? How does that happen?
- When you are planning for SETA, do you review existing SETA plans?
- In your organisation, how do you identify target groups for SETA?
- What are the things that you consider when designing SETA?
- Who is responsible for developing SETA materials?

### The Implementation Stage

- How can you motivate employees to participate in SETA program? What are your strategies for convincing employees to take part in awareness campaign or training session?
- What are the steps to ensure effective implementation of SETA program?
- What are the ways that your organisation uses to deliver security awareness message?
- How training is done in your organisation? One to one – meeting – group session?

### Evaluation

- How do you know that users are aware of the security?
- How often do you review your SETA program?
- How does that happen? Is it ongoing or once a year?
  - i. Do you conduct periodic review of SETA plan?
  - ii. Reassess the needs for SETA periodically?
  - iii. Evaluate SETA materials?



## Appendix B

Social Marketing Principles	Representatives quotes
Customer Orientation	<ul style="list-style-type: none"> <li>• “we have mandatory online training that everyone must complete” CISO1</li> </ul>
Behaviour and Behavioural Goals	<ul style="list-style-type: none"> <li>• “the primary aim of our SETA is to make people aware of our security policies” CISO1</li> <li>• “Most of the time it is policy itself that people were made aware of” MGR1.</li> <li>• “we set objectives for the short campaigns for example, security and fraud week is develop to achieve specific objectives. We also have very high-level objectives that we'd like to achieve for the overall security awareness program” MGR2</li> <li>• “A SETA program should drive your information security strategy, translate your vision into reality. It should make people share your vision of security and in such way help you to build a security culture within the organisation so you can modify the behaviour of the people” CISO2</li> </ul>
Theory Based	<ul style="list-style-type: none"> <li>• Participants did not mention the use of theory to understand behaviours</li> </ul>
Develop ‘Insight’	<ul style="list-style-type: none"> <li>• “There are numerous inputs. Understanding the threat landscape: what is currently happening or what's being advertised. There's also a component around what incidents have we seen in the past, be they to our organisation or to other industries or organisations. we also look at what user feedback we are receiving. If people are saying that these are their concerns- these are their issues, we'll also feed that into it, as well. Then, also, the strategic direction of where the ISO wants to build capability. That will really dictate more or less the key areas.” MGR4</li> </ul>
Exchange	<ul style="list-style-type: none"> <li>• “I don’t think we do any motivation. We do more of ensuring compliance by showing people what they need to know from the organisation’s policies” MGR1</li> <li>• “Awareness teams have always developed material based on a compliance and policy risk culture rather than a true business enablement culture, so there's a real opportunity for us to change the conversation and sit down with the business and say, ‘These are the risks. This is how security helps you. How can we properly develop and create content that is consumable for you, supports your teams, and also facilitate better customer experience” MGR4</li> <li>• “If we are running training on social media, we make sure it's about enabling them to be more secure on their personal social media sites or talk to their parents or children about secure social media use. We find that making that personally relevant is a really good motivator to get staff to come along and be interested and engaged in the session”. MGR3</li> </ul>
Competition	<ul style="list-style-type: none"> <li>• “There's competition now within organisations to get the attention of employees and to hold their attention for your security awareness program to be effective. It's very difficult these days. Throughout the year, they go through many training programs. They come back to me and say, ‘Do you have any idea how many training sessions we go through”. CISO2</li> <li>• “There's too much information, information overflow. So, if they [employees] go and come out of our training, they forget immediately everything we taught them. They forget as they have to move on to something else and get ready for more training in two days”. CISO1</li> </ul>
Audience Segmentation	<ul style="list-style-type: none"> <li>• “In my organisation, there are three kinds of training and awareness programs: one for executive management, the second type of security training and awareness is general awareness messages for all employees from all the departments and the third type is target-specific group awareness.” CISO2</li> <li>• “There is no one size fits all approach. [...] we need to tailor our awareness campaigns depending on the stakeholder group that we are dealing with”. MGR4</li> </ul>
Method Mix	<ul style="list-style-type: none"> <li>• “We have our newsletter which is also via our email. [...] We do use some poster materials. So, there are several channels depending on what it is that we are trying to achieve” MGR4</li> <li>• “It's a program that should run throughout the year. With all sort of component such as flyers souvenirs, workshops, small groups, you can have different messages targeted to different people”. MGR3</li> </ul>

Dr Moneer Alshaikh is an Assistant Professor at the College of Computer Science and Engineering, Department of Cybersecurity, University of Jeddah, Saudi Arabia. He is also an Honorary Fellow at School of Computing and Information Systems, the University of Melbourne. Dr Moneer worked as a research fellow in cyber security at The Academic Centre of Cyber Security Excellence, School of Computing and Information Systems, the University of Melbourne. Dr Moneer is a certified Information Security Manager and ISO/IEC 27001 Implementer. His research interests include information security management, security awareness, and security behaviour change.

Sean B. Maynard is an academic in the School of Computing and Information Systems, University of Melbourne, Australia. He has over 25 years of teaching experience at the undergraduate, postgraduate and executive training levels. His research interests are in the management of information security specifically relating to security policy, security culture, security governance, security strategy, security analytics, and incident response. His research has been published in high-impact journals such as *Computers & Security* and the *International Journal of Information Management* as well as leading conferences such as the International Conference on Information Systems. For more information, please visit <https://www.seanmaynard.me/>

Atif is an Associate Professor at the University of Melbourne where he serves as Deputy Director for the Academic Centre of Cyber Security Excellence. Atif leads a unique team of Cybersecurity Management researchers drawn from information systems, business administration, security intelligence, and information warfare. He has authored over 90 scholarly articles in cybersecurity management and received over AUD\$3.9M in grant funding. Atif is an Associate Editor for the leading IT security journal, *Computers & Security*. Atif has previously served as a cybersecurity consultant for WorleyParsons, Pinkerton and SinclairKnightMerz. He is a Certified Protection Professional with the American Society for Industrial Security. For more information, please visit <https://www.atifahmad.me/>