5-15-2019

TOWARD SUSTAINABLE BEHAVIOUR CHANGE: AN APPROACH FOR CYBER SECURITY EDUCATION TRAINING AND AWARENESS

MONEER ALSHAIKH
The University of Jeddah, malshaikh@uj.edu.sa

Humza Naseer
University of Melbourne, humza.naseer@unimelb.edu.au

Atif Ahmad
The University of Melbourne, atif.ahmad@unimelb.edu.au

Sean B. Maynard
The University of Melbourne, seanmaynard@unimelb.edu.au

Toward Sustainable Behaviour Change: An Approach for Cyber Security Education Training and Awareness

Research paper

Alshaikh, Moneer [1,2], [1] University of Jeddah, Jeddah, Saudi Arabia, malshaikh@uj.edu.sa

[2] University of Melbourne, Melbourne, Australia, alshaikhm@unimelb.edu.au

Naseer, Humza, University of Melbourne, Melbourne, Australia, humza.naseer@unimelb.edu.au

Ahmad, Atif, University of Melbourne, Melbourne, Australia, Atif@unimelb.edu.au

Maynard Sean, B, University of Melbourne, Melbourne, Australia, sean.maynard@unimelb.edu.au

Abstract

Effective information security education, training and awareness (SETA) is essential for protecting organisational information resources. Whilst most organisations invest significantly in implementing SETA programs, the number of incidents resulting from employee noncompliance with security policy are increasing. This trend may indicate that many current SETA programs are not as effective as they should be. We argue that existing SETA programs are not optimal in changing employee behaviour to comply with security policy as they lack a theoretical base that can inform and guide the development of SETA programs. This study draws on knowledge from the medical domain on the use of theory to design an intervention to bring about sustainable behaviour change. The paper therefore adopts an intervention design process, based on the behaviour change wheel (BCW) framework, to develop a theory-informed SETA development process. The paper demonstrates the use of BCW in the analysis of the target behaviour and the selection of suitable strategies and techniques to change the target behaviour. The proposed SETA development process provides a sound basis for future empirical work including focus groups and action research.

Keywords: Information Security Education Training and Awareness, Behavioural Information Security, Behaviour Change Wheel, Security Interventions.

1 Introduction

Despite organisations investing a significant amount of money and resources on information security, the number of security breaches reported are still on the increase. Recent security reports show that a major proportion of non-malicious cybersecurity breaches result from employee noncompliance with the organization's information security policies (Accenture & HfS Research 2016). For example, in 2016, a staff member from a government organization clicked on an Australia Post themed email that infected the workstation with ransomware (Cryptolocker), which encrypted the files on the computer (Australian Cyber Security Centre 2016).

Security researchers have consistently argued that information security education, training and awareness (SETA) programs should be in place to raise employees' awareness of security risks, and provide them with the required skills and knowledge to comply with the organisation's security policy (De Maeyer 2007; Tsohou et al. 2015; Posey, Roberts, and Lowry 2015). Although organisations adopt and employ SETA programs to educate users, number of security breaches as a result of employees' noncompliance with security policy is still on the increase (SANS 2017). This trend may indicate that many current security training and awareness programs are not as effective as they should be.

When developing SETA programs, organisations rely on "best practice" and industrial guidelines which have no empirical evidence or theoretical explanation to assist with understanding which strategies are effective in which contexts (Ng, Kankanhalli, and Xu 2009; Alshaikh et al. 2018; Siponen and Willison 2009). Furthermore, it is unclear to organisations what process to change behaviour should be adopted to develop an effective SETA program. Consequently, existing SETA programs tend not to be effective in changing employees' behaviour.

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, Kankanhalli, and Xu 2009; Öğütçü, Testik, and Chouseinoglou 2016). As Öğütçü, Testik, and Chouseinoglou (2016) points out, this may be because SETA programs are not informed by behavioural change theories. Such theories are important for providing systematic guidelines to organisations on conducting an in-depth analysis of the behaviours that they wish to change and selecting the appropriate SETA strategies that are most likely to achieve the intended outcomes.

Therefore, this research draws on knowledge from the medical domain on the use of theory to design interventions to bring about sustainable behaviour change. The paper adopts the intervention design process which is based on the behaviour change wheel (BCW) framework in order to develop a theory-informed SETA development process (Michie, Atkins, and West 2014). The paper demonstrates the use of BCW in the analysis of the target behaviour and the selection of suitable strategies and techniques to change the target behaviour. The study addresses the following research question:

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

By answering the research question, this study addresses a highly important research problem. We define the word 'sustainable' in this context as the ability to maintain the change in behaviour. The BCW framework can bring a sustainable behaviour change by analysing the behaviour and addressing barriers to and facilitators of the target behaviour (Michie, Atkins, and West 2014).

The study is motivated by the need for a theory-informed development process for SETA programs. From our recent exploratory study of SETA practices (Alshaikh et al. 2018), we found that organisations are unable to determine how effective their SETA programs are in changing their employees' behaviour and how much they should invest in SETA programs to achieve effective outcomes. The BCW framework can address this issue by providing systematic guidance to organisation on developing effective SETA programs.

This paper is organised as follows. First, the background section discusses information security behavioural studies and their contribution to the development of SETA programs, and then presents the

theoretical framing for the study (the behaviour change wheel). Second, a theory-informed SETA development process is proposed based on the BCW framework, and examples of the behaviour analysis in the security domain are provided. Finally, we conclude with a discussion of the theoretical and practical implications of the proposed theory-informed SETA development process and a direction for future work.

2 Background

This section presents a review of IS security behavioural studies, focusing on their practical contributions to the development of SETA programs. In the second part of this section, the behaviour changing wheel is presented as the theoretical framing of this research.

2.1 Information Systems Security Behavioural Study

Information security education training and awareness (SETA) programs refer to organised information security training activities that are related to security training, and awareness raising of an organisation's employees (D'Arcy, Hovav, and Galletta 2009). The aim of a SETA program is to change the behaviour of employees towards security and to encourage good security practices (Tsohou et al. 2015; Whitman and Mattord 2008).

A review of the literature reveals consensus on the need for organisations to develop SETA programs to protect their information assets (Khan, Alghathbar, and Khan 2011; Ahmad, Maynard, and Shanks 2015). Studies that address SETA can be categorised into two main categories: 1) studies about employees' behaviour and compliance with information security policy which provide recommendations on the development of SETA programs, and 2) studies that directly address the role of SETA programs in protecting organisations and changing employees' behaviour. The following is a discussion of these two categories.

The issue of compliance with information security policy has been the focus of research in the information systems security domain (e.g., Siponen, Adam Mahmood, and Pahnila 2014; Vance, Siponen, and Pahnila 2012; Ifinedo 2014). Empirical work in this domain addresses compliance. Studies have been conducted to understand why employees do not comply with policy, and have explored factors that affect employees' compliance with information security policies (e.g., Wall, Palvia, and Lowry 2013; Molok, Ahmad, and Chang 2011). These studies use a variety of theories: general deterrence theory, rational choice theory, situational crime prevention theory, planned behaviour theory, the protection motivation theory, the theory of reasoned action, and the cognitive evaluation theory

For example, a study by Siponen, Adam Mahmood, and Pahnila (2014) applies a combination of three theories (protection motivation theory, the theory of reasoned action, and cognitive evaluation theory) to understand factors that influence employees' adherence to information security policy. The study identified five factors that have a significant impact on employees' compliance with an information security policy (*perceived severity of potential threats, perceived vulnerability to potential threats, attitude towards complying with security policy, social norms towards complying with the security policy and intention to comply with security policy*). Similar to other compliance studies, Siponen, Adam Mahmood, and Pahnila (2014)'s study provides recommendations that can assist organisations to achieve better compliance with their information security policy. These recommendations include instilling in employees the importance of information security, developing clear policies, and providing information security education, training and awareness for employees to assist employees to perform their job in a secure manner.

An extensive body of literature is devoted to understanding the effect of SETA programs on changing employee behaviour and proposing approaches for developing effective SETA programs. A comprehensive review conducted by Karjalainen and Siponen (2011) identified 32 IS training approaches, the majority of which were based on practical experience with no underlying theory or theoretical concepts to explain the rationale behind the development process of SETA programs presented in the papers. Only twelve studies applied any theory (these included: learning theories, social

psychology theories, and criminology theories). These studies present a large and sometimes overlapping array of theoretical constructs or components that has led to mixed results and limited practical value of much of the research in the area (Lebek et al. 2013). Rosemann and Vessey (2008) argue that academic literature should provide relevance for practitioners to prevent research from becoming an end unto itself. Subsequently, 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 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.

There are many useful practical contributions of existing theory-based SETA approaches. Table 1 provides examples of studies and their practical recommendations to the development of SETA. Examples of practical recommendations from theoretical grounded studies include: using past experiences and collaborative learning to achieve desired outcomes (Karjalainen and Siponen 2011), employing a combination of SETA delivery methods that activate and motivate employees (Abawajy 2014), integrating the SETA program with the normal business communication of the organisation (Puhakainen and Siponen 2010), motivating employees through effectively communicating the purpose of the SETA program (Johnston and Warkentin 2010), building trust and good relationships with stakeholders (Albrechtsen and Hovden 2010), and engaging stakeholders in managing SETA activities through providing feedback (Bulgurcu, Cavusoglu, and Benbasat 2010). However, these recommendations are fragmented and dispersed and do not build cumulatively to guide the development of SETA programs in organisations.

Study	Theory	Recommendations to SETA programs
Kajzer et al. (2014)	Personality traits (Machiavellianism, and social desirability)	SETA programs should consider the personality traits and thinking styles of users.
Vance, Siponen, and Pahnila (2012)	Habit theory and Protection Motivation Theory	SETA should address employees' past and automatic behaviour to improve compliance.
Al-Omari, El-Gayar, and Deokar (2012)	Theory of Planned Behaviour	Identifies factors that SETA approaches should emphasise to influence the users' perspectives and knowledge.
Karjalainen and Siponen (2011)	Theory of Three Levels of Thinking	SETA programs should use past experiences and collaborative learning to achieve desired outcomes

Table 1 Examples of theory-based SETA studies and their practical recommendations

Our review of the SETA studies supports the conclusion of several researchers that there is a need for a systematic approach for developing SETA programs (Puhakainen and Siponen 2010; Karjalainen and Siponen 2011; Lebek et al. 2013; Ng, Kankanhalli, and Xu 2009). We argue that the process for developing SETA programs requires a systematic approach with a strong rationale. Theory should be used to inform development of SETA programs by providing detailed guidance on the analysis of target behaviour that needs to be changed and the selection of appropriate strategies and techniques to achieve the desired outcomes.

The approach proposed by Puhakainen and Siponen (2010) includes analysis of users' current skills and knowledge, the required level of skills and knowledge and the learning objectives for the training program to bridge the gap between the current and required level. However, the analysis step is conducted at a very high level, focusing on skills and knowledge, but overlooking motivational aspects of an effective SETA program (Alshaikh et al. 2018).

The lack of systematic and theory-informed SETA development process has led organisations to adopt guidelines and best practice standards to develop SETA programs. However, these guidelines and standards are conceptual, lack support from empirical data, are generic in nature, and give no consideration to the organisational context (Siponen and Willison 2009). Further, implementing SETA practices based on best practice standards does not guarantee SETA quality (Siponen and Willison

2009). Consequently, SETA programs are often implemented ineffectively with intended outcomes not being achieved.

This paper draws on the behaviour change wheel framework that is used to design theory-informed interventions in the medical field. The next section will discuss the behaviour change wheel and how it can be adopted to inform the design of SETA programs.

2.2 Theoretical Framing –Behaviour Change Wheel

Our review of the behaviour change and intervention design literature revealed that the Behaviour Change Wheel (BCW) framework (Figure 1) could be useful for addressing the gap in the information security domain with regard to the need for a systematic and theory-informed SETA development process. The BCW consists of three key elements: sources of behaviour, intervention functions and policies categories.

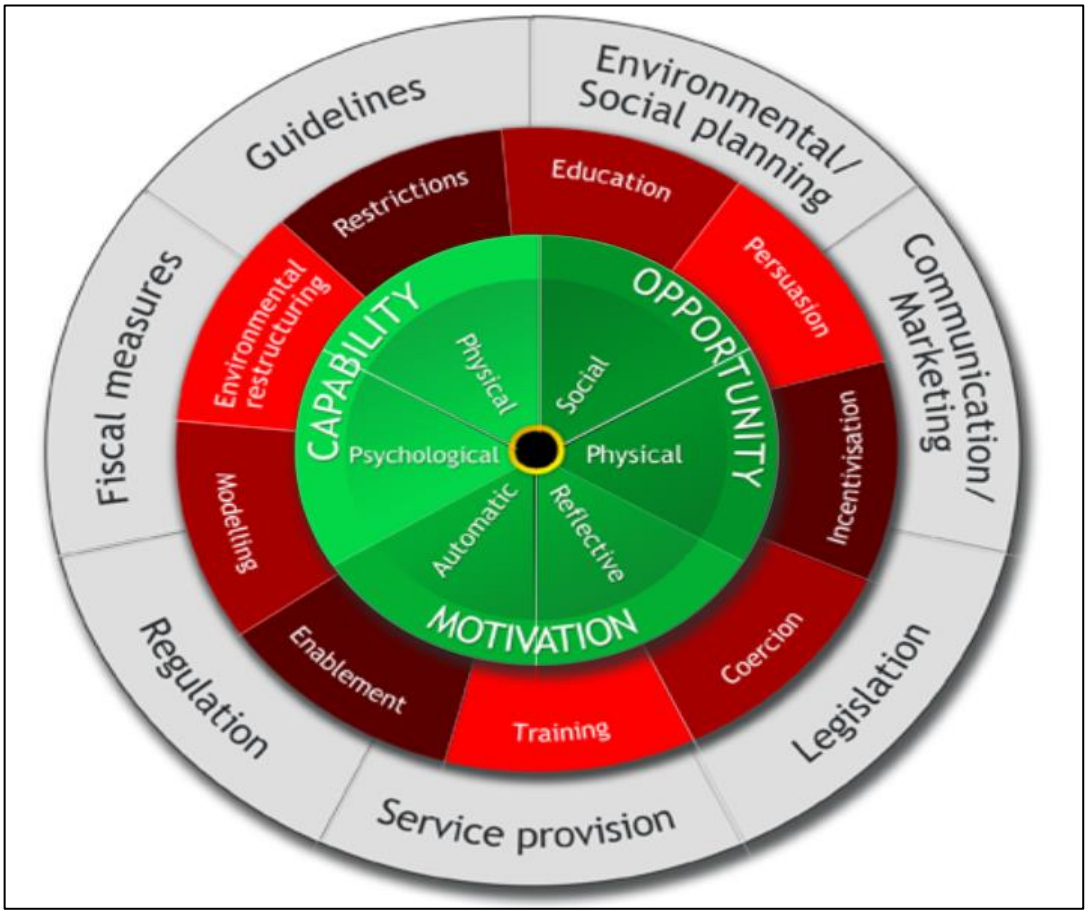

Figure 1 The Behaviour Change Wheel (BCW) Framework from (Michie, van Stralen, and West 2011)

The inner core (sources of behaviour) green part of BCW is based on the COM-B model (Michie, van Stralen, and West 2011) which consists of three necessary conditions for a given 'Behaviour' to occur: (1) *Capability*; (2) *Opportunity*; and (3) *Motivation*. Each COM-B model component is divided into two types (Michie, van Stralen, and West 2011). Table 2. shows COM-B model components including definition and explanation. The analysis of a target behaviour in relation to COM-B and its components helps to identify which psychological determinants need to be addressed in order to achieve behaviour change (Michie, Atkins, and West 2014). The BCW framework provides tools to investigate what drives and enables behaviour patterns and individual behaviours.

The red intervention functions and policies category elements of the BCW framework are derived from a systematic review and synthesis of 19 frameworks of behaviour change. An analysis of these

frameworks revealed nine broad functions of interventions and seven categories of supporting policies (Michie, Atkins, and West 2014). The BCW provides organisations with a comprehensive set of all options available for achieving behaviour change. Thus avoiding the situation where a possible effective intervention is overlooked by the organisation (Michie, Atkins, and West 2014).

COM-B Model Component	Definition	Explanation
Capability: Physical	Physical skills, strength or stamina	Having the skills to perform the target behaviour
Capability: Psychological	Knowledge or psychological skills, strength or stamina to engage in the necessary mental processes	Understanding the impact of not performing the behaviour on the systems
Opportunity: Physical	Opportunity afforded by the environment involving time, resources, locations, cues, and physical 'affordance'	Environment/systems support to perform the behaviour.
Opportunity: Social	Opportunity afforded by interpersonal influences, social cues and cultural norms that influence the way we think about things, e.g. the words and concepts that make up our language.	Social support to perform the behaviour
Motivation: Reflective	Reflective processes involving plans (self-conscious intentions) and evaluations (beliefs about what is good and bad)	Intention and plan to perform the behaviour
Motivation: Automatic	Automatic processes involving emotional reactions, desires (wants and needs), impulses, inhibitions, drive states and reflex responses	Feelings and emotions that drive the behaviour

Table 2. COM-B model components: definition and explanation

The significance of the BCW framework from other behaviour intervention classifications is its explicit linkage to a comprehensive understanding of the behaviour and the identification of all possible intervention options to achieve behavioural change. The BCW framework enables the systematic development of interventions for supporting behaviour change (Michie, Atkins, and West 2014). It can be used to design and select interventions and policies according to the analysis of the nature of the behaviour, the mechanisms that need to be altered to bring about behaviour change, and the interventions and policies required to alter those mechanisms (Michie, Atkins, and West 2014).

The intervention design process that is informed by the BCW starts with a theoretical understanding of behaviour to determine what needs to change for the behavioural target to be achieved, and what intervention functions are likely to be effective to bring about that change. The BCW has been field tested by a range of staff involved in policy and intervention work to develop prototype strategies for specific implementation targets (Michie, van Stralen, and West 2011).

The intervention process informed by the BCW framework has been used in many studies in the medical failed to change behaviour. For example, (Fulton et al. 2016) developed an application (StopApp) based on BCW to increase uptake and attendance to stop smoking services. The process also utilised in developing intervention for asthma management for pharmacies and resulted in significant adoption of the clinical guidelines for asthma management (Watkins et al. 2016).

Michie, van Stralen, and West (2011, p.2) define behaviour change interventions as "coordinated sets of activities designed to change specified behaviour patterns". The use of interventions to achieve behavioural change is common in human-computer interaction studies but less common in the field of information security (Coventry et al. 2014). However, several researchers state that the work on behaviour change interventions in the information security domain is just getting started (Briggs, Jeske, and Coventry 2017).

In the information security domain, the SETA program is an intervention that is designed to change employee behaviour towards adopting security practices (Albrechtsen and Hovden 2010; Herath and Rao 2009). A SETA program consists of three key elements: education, training and awareness. Each of these elements has specific goals and objectives that aim to provide knowledge, skills and awareness (Whitman and Mattord 2008).

The objectives of SETA program elements are very high level and are mostly focused on the knowledge aspects of SETA, neglecting motivation and attitude as well as context and environmental aspects (Alshaikh et al. 2018). Although addressing these high-level elements can influence behaviour, the effect is not optimal and sustainable. Thus, using the BCW framework provides detailed intervention strategies that go beyond the traditional three elements of SETA (education, training, and awareness) in the IS literature.

The BCW framework is useful for the development of effective SETA programs for two primary reasons (French et al. 2012). First, it provides in-depth analysis of behaviour beyond the traditional 'needs assessment process' that current SETA best-practice standards and guidelines offer. In current practice, the needs assessment for SETA uses different inputs to identify problems and issues employees need to be aware of and comply with; whereas, the BCW analysis step uses the COM-B model components to focus on the behaviour that needs to change. Second, based on the analysis results, the BCW provides detailed guidance on the selection of the most appropriate strategies to change the behaviour. The next section explains the BCW intervention development process and how it can be applied in the security management domain.

3 Toward a Theory -Informed SETA Development Process

The process of intervention development using the BCW is outlined in detail in (Michie, Atkins, and West 2014) and has been tested, validated and extensively applied in many studies (Michie, Atkins, and West 2014). As shown in Figure 3, the process consists of eight steps divided into three key stages: stage 1 - understand the behaviour, stage 2 - identify the intervention options, and stage 3 - identify the content and implementation options. The three stages are described below with examples from the information security context to demonstrate to how these steps are can be applied to the domain.

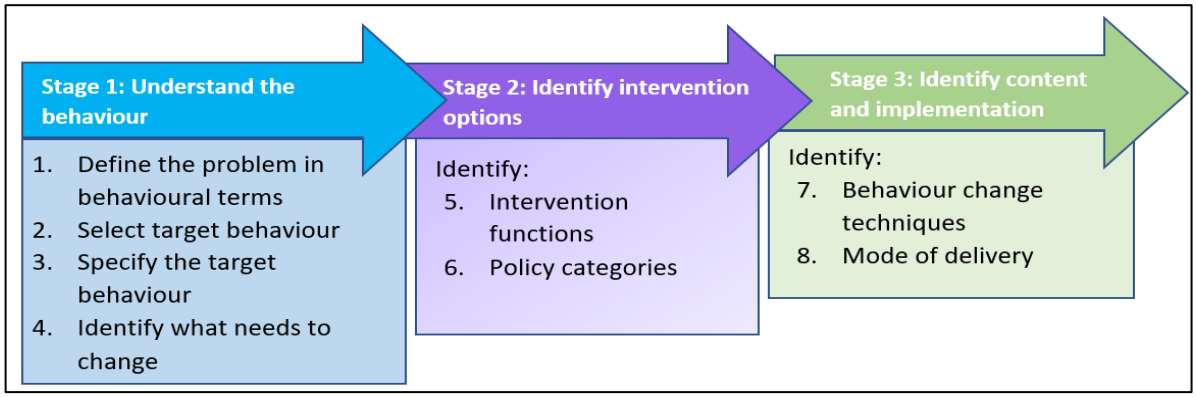

Figure 2 A Theory-Informed Intervention Development Process based on BCW (from Michie, Atkins, and West (2014))

3.1 Stage 1: Understand the Behaviour

Stage 1 of the development process of the theory-informed SETA program consists of four steps that are the foundation for understanding the target behaviour and identifying what needs to change.

3.1.1 Step 1: Define the Problem in Behavioural Terms

This step involves precisely defining the problem in behavioural terms. The definition of the problem means being specific about the target individuals, group or population involved in the behaviour. The

BCW guidelines provides three questions about the behaviour, the location where the behaviour occurs and who is involved in performing the behaviour.

In the information security context, stating that SETA is implemented to improve employee compliance with the organisation's security policies is a very general statement that does not indicate what behaviours the SETA program is trying to change. Complying with cybersecurity policies is also not a specific behaviour target. However, avoiding and reporting phishing emails, and setting a complex password are more specific target behaviours.

3.1.2 Step 2: Select the Target Behaviour

Behaviours do not occur in isolation; they are part of a system where they can be influenced by the behaviours of other groups within the context (Michie, Atkins, and West 2014). Step 2 includes two tasks. The first, is generating a list of all possible behaviours of the people involved in the target behaviour that need to change and the behaviours of other groups that might influence the target behaviour. The second task is prioritising the behaviours according to factors such as their effect in changing other behaviours and the ease to change the behaviour. For effective behaviour changing outcomes, one or two behaviours should be targeted at a time so organisations can build on successes towards changing all targeted behaviours (Michie, Atkins, and West 2014).

SETA managers should identify all possible behaviours relevant to the problem. For instance, a list of behaviours associated with improving employees' responses to phishing emails may include: identifying phishing emails, avoiding clicking links in phishing emails, reporting phishing emails. Additionally, this may include indirectly influencing employee behaviour through ensuring appropriate methods exist to report phishing emails and to acknowledge and thank employees for reporting the phishing emails. Some behaviours relevant to the problem are interconnected and some are performed by the target group. Other behaviours are related to the systems, individuals, and teams within the organisational context.

3.1.3 Step 3: Specify the Target Behaviour

In Step 3, the target behaviour should be described in detail. An accurate and detailed description of the target behaviour is important for helping with the analysis of the behaviour, which is conducted in the next step (Michie, Atkins, and West 2014). Specifying the target behaviour and content includes answering a series of questions around who needs to perform the behaviour, what needs to be done to achieve the desired change, and when and where the target behaviour should be performed (Michie, Atkins, and West 2014).

Target Behaviour	**Employees to recognise phishing emails and report it to the security team/IT services**
Who needs to perform the behaviour?	All employees in the organisation
What do they need to do differently to achieve the desired change?	The need to know how to identify phishing email They need to know how to report the phishing email
When do they need to do it?	As soon as they receive a phishing email
Where do they need to do it?	Anywhere they access the system via PC, laptop, tablet or smart phone
How often do they need to do it?	Every time they receive a suspicious email
With whom do they need to do it?	On their own or with support from their co-worker and IT support

Table 3 Specifying the target behaviour and content

This paper uses protection against phishing attacks and employees' responses to phishing emails as an example to explain how the BCW can inform the SETA development process. A phishing attack is where personal information is retrieved using deception through impersonation (Lastdrager 2014). Phishing is a significant security problem that is faced by organisations world-wide (Arachchilage and Love 2014). Table 3 provides examples of target behaviour within the information security context.

3.1.4 Step 4: Understand the Target Behaviour and Understanding What Needs to Change

After specifying the target behaviour in Step 3, Step 4 is a thorough analysis of the behaviour. The analysis of the behaviour involves identifying what needs to change in the individual and the environment / context to achieve the desired change in behaviour. A more detailed and accurate analysis of the target behaviour is more likely to result in a successful SETA program that changes behaviour. Behavioural analysis in this step is based on the COM-B model (see Table 2 for definition of three COM-B components).

To perform the behavioural analysis, data should ideally be collected from multiple sources to get as much detailed and accurate information as possible. Different data collection tools can be used, including literature reviews, interviews, focus groups, direct observation and questionnaires (Michie, Atkins, and West 2014). The selection of the data collection techniques depends on the type of behaviour being targeted. The guidelines for designing the intervention provides suggestions on questions that could be asked to assess the components of the COM-B model. Also, a self-evaluation questionnaire (COM-B-Qv1) has been developed to help analyse the target behaviour (Michie, Atkins, and West 2014). These questions can be adapted to cybersecurity behaviour and context. Once data collection is completed, the data can be analysed using the COM-B behavioural diagnosis form to make sense of the data and gain a consistent picture of the target behaviour.

To demonstrate the use of the BCW analysis process, in this paper we conducted a literature review to analyse employee responses to phishing emails. The review focused on exploring barriers and enablers for employee capabilities, opportunities, and motivations (the COM-B model components) to identify, avoid, and report phishing emails. In this step, we explain how the identified problems related to the target behaviour (employees' responses to phishing emails) from the literature are mapped to the COM-B model. Table 4 summarises how our behavioural analysis findings are mapped onto the behaviour change wheel.

A list of issues related to the target behaviour was identified based on a review of the academic and industrial literature (Jansen and van Schaik 2019; Williams, Hinds, and Joinson 2018; Aleroud and Zhou 2017; Alsharnouby, Alaca, and Chiasson 2015; Lastdrager 2014; Gowtham and Krishnamurthi 2014; Arachchilage and Love 2014; Dodge Jr, Carver, and Ferguson 2007). Then the issues were mapped to the COM-B model based on the definitions of each component. The findings aligned with 'Capability' (e.g., a lack of skills to identify phishing email), 'Opportunity' (e.g., a lack of mechanism or systems to report phishing email), and 'Motivation' to act (e.g., a lack of encouragement and support from managers and the security team to identify and report) within the COM-B model. It should be noted that the list of issues that need to be addressed using intervention is not exhaustive as it is prepared only to demonstrate how the BCW can be used in the security context. A comprehensive and complete behaviour analysis should take into consideration the organisational context and collection of data from multiple sources.

3.2 Stage 2: Identify Intervention Options

Stage 2, identify the intervention options, includes two key steps: identifying the intervention functions and identifying policy categories. The BCW framework (Figure 1) outlines two different levels of actions for changing the behaviour based on the behaviour analysis steps undertaken in the previous stage. The intervention functions are the broad categories of strategies by which intervention can change behaviour. Policy categories are types of decisions made by the authorities that help to support and enact the intervention (Michie, van Stralen, and West 2011).

3.2.1 Step 5: Identify Intervention Functions

The BCW framework enables a systematic selection of nine possible intervention functions based on the analysis of the target behaviour (Michie, van Stralen, and West 2011). COM-B identifies what needs to change to achieve the desired behaviour and therefore what interventions types are more likely to

change the target behaviour. The BCW framework maps the COM-B components (Table 2) to the appropriate type of interventions that are likely to address the problems within the components and bring about the desired change.

COM-B	Description of what Needs Addressing in the Intervention Based on Literature	Intervention Functions	Policy Categories	Behaviour Change Techniques (BCTs) Identified
Capability: Physical	A lack of skills to scan suspicious links A lack of skills to report phishing emails A lack of skills to identify phishing emails	Education Training	Communication / Marketing Guidelines Environmental/ Social planning Service provision	Instruction on how to perform the behaviour Prompts/cues
Capability: Psychological	A lack of knowledge about the consequences on the systems of clicking on phishing link.	Education Training		Information about social and environmental consequences Prompts/cues
Opportunity: Physical	A lack of mechanism or systems to report phishing email A lack of Email Filtering Systems	Environmental restriction		Adding object to the environment Prompts/cues
Opportunity: Social	Perception that reporting phishing email is a good employee security practice A lack of encouragement from managers and security team to report phishing emails	Modelling Enablement Incentivisation Persuasion		Feedback on the behaviour Feedback on the outcome of the behaviour Social reward
Motivation: Reflective	Don't like the idea of needing or seeking help in identifying or reporting phishing emails Hold the belief that reporting phishing emails will protect the systems Staff do not necessarily recognise the value of identifying and reporting skills	Modelling Enablement Incentivisation Persuasion		Demonstration of the behaviour Social support Social reward Reduce negative emotion
Motivation: Automatic	Fear of failing to identify phishing email and causing a systems compromise Need to develop a habit of identifying and reporting phishing emails	Modelling Enablement Incentivisation Persuasion		

Table 4. Example of how the findings from the behavioural analysis mapped into BCW framework

In the information security context, a security manager should use the BCW framework to determine what needs to be done to change the behaviour (intervention functions) and what tools and techniques should be used to enable the change in the behaviour based on the analysis of the target behaviour (Table 4). Of the possible nine interventions the following seven interventions were identified as being the most useful for addressing the identified barriers to the target behaviour (improving employee responses to phishing emails): (1) Education, (2) Persuasion, (3) Training, (4) Environmental restriction, (5)

Modelling, (6) enablement, and (7) Incentivisation (see Michie, Atkins, and West (2014) for list of all nine intervention functions and definitions). For example, the analysis indicated that there was insufficient knowledge to identify phishing emails, so to change behaviour requires employees' skills and knowledge around identification of phishing emails to be increased through providing two types of interventions: 'Training' (imparting skills) and 'Education' (increasing knowledge or understanding). Table 4 illustrates how the intervention function relates to the corresponding COM-B components.

3.2.2 Step 6: Identify Policy Categories

There are seven types of policies identified in the BCW guidelines for the design of the intervention (Michie, van Stralen, and West 2011). The BCW suggests which type of policies should be implemented to enact the type of interventions selected to make changes to the target behaviour. It must be noted that not all types of policies in the BCW framework are applicable to SETA programs in organisations.

Based on the definitions of the seven policy categories (Michie, van Stralen, and West 2011) four were identified as being appropriate to support and enable the selected six intervention functions to change employees' behaviour toward phishing emails: (1) Communication/Marketing, (2) Guidelines, (3) Environmental/Social planning, and (4) Service provision (see Table 4). For example, the education and training intervention functions can be enacted by conducting mass media campaigns within the organisation using print, electronic or broadcast media to raise employees' awareness about the threat of phishing and how to identify phishing emails which is communication/marketing policy category. The intervention function 'Environmental restriction' can be enabled by the policy category type 'Service provision'. In the phishing example, this can be solutions that can detect and block sophisticated phishing messages before they reach the intended targets.

3.3 Stage 3: Identify Content and Implementation Options

Stage 3 - the identify content and implementation options stage is concerned with the design of the content and the delivery. This stage involves two main steps: identifying behaviour change techniques (BCTs) and determining the mode of delivery. The following explains the two steps and demonstrates how they are applied in the security context using the phishing attack example.

3.3.1 Step 7: Identify Behaviour Change Techniques (BCTs)

According to Michie, Atkins, and West (2014, p.145) a behaviour change technique (BCT) is "an active component of an intervention designed to change behaviour". The process of a theory-informed intervention designed based on the BCW is supported by a list of possible BCTs called the BCT taxonomy. The BCT taxonomy consists of 93 BCTs organised into 16 groups (Michie, Atkins, and West 2014).

The BCW guidelines for intervention design links intervention functions with BCTs. Each intervention function has several BCTs within the BCT taxonomy that can be used to change the behaviour. The process of selecting the appropriate BCTs should include generating a list of possible BCTs that are aligned with the intervention functions, and then, through analysis and discussion, the design team should consider the most feasible, affordable, practical, acceptable and effective BCTs that can used to change the target behaviour.

Table 4 includes some possible BCTs that are identified through discussion between the authors. For example, to address the lack of skills on identifying phishing emails, the training intervention function was selected. The BCT that aligns with training is 'Instruction on how to perform the behaviour' (advise on how to perform the behaviour). Another example is addressing the lack of email filtering systems that block phishing emails before they get to employees by using an environmental restriction of 'Adding object to the environment', the BCT for which is implementing email filtering systems.

3.3.2 Step 8: Determine the Mode of Delivery

After deciding what BCTs should be used to change the behaviour, the mode of delivery needs to be selected. The BCW-based guidelines provide a taxonomy of modes of delivery for the intervention functions (Michie, Atkins, and West 2014). The mode of delivery is classified based on the type of delivery (face-to-face and distance) and level of delivery (individual, group and population level).

For example, security managers can provide training on how to identify phishing emails (BCT Instruction on how to perform the behaviour) by giving training seminars (group: face-to-face), and/or talk to an employee who was a victim of a phishing attack (individual: face-to-face), and/or prepare instructions on how to identify phishing emails and send it via the organisation's intranet or SharePoint (population: digital media). Using a combination of delivery modes is highly recommended in the information security literature (Alshaikh et al. 2018).

4 Conclusion and Future Work

This paper presents a theory-informed information security training and awareness development process based on the behaviour change wheel (BCW) framework. The need for a theory-informed SETA development process is explained, and application of the BCW and its intervention design process in the information security domain is discussed. The main contribution of this research to theory is the explanation of how the BCW can be applied in the information security domain, which addresses the gap in the literature for a theory-informed SETA development process. The theoretical nature of the existing SETA development process has resulted in ineffective SETA programs that are not able to bring about sustainable behaviour change. Therefore, using the BCW and its intervention design process can help organisations to design an appropriate SETA program after conducting in-depth analysis of the behaviour and selecting appropriate strategies to change the behaviour based on the analysis results.

Our study has several important implications for practice. The study has proposed a new process that can be used by organisations to develop an effective SETA program that can change employees' behaviour. The study has also provided practical guidance to organisations on how to use the BCW to develop their SETA programs. The example of the problem of phishing attacks was used to demonstrate the behaviour analysis step and the selection of 'intervention functions', 'policy categories', 'behaviour changing techniques (BCTs)', and 'mode of delivery' as per the BCW intervention design process.

The proposed theory-informed SETA program based on the BCW framework in this paper provides a sound basis for further work. The next step is to conduct a focus group with information security training and awareness managers/experts to validate and refine the proposed theory-informed SETA development process and explore what the experts think about the practicality and usefulness of such an approach. The final step of the research project will be conducting an action research by putting the proposed theory-informed SETA development process into practice in an organisation with a high level of maturity in SETA practices. This research will be done by selecting a specific behaviour, performing a thorough and in-depth analysis of the behaviour, and then designing a SETA program to change the target behaviour based on the BCW.

References

Abawajy, Jemal. 2014. 'User preference of cyber security awareness delivery methods', *Behaviour & Information Technology*, 33: 237-48.

Accenture & HfS Research. 2016. "The State of Cybersecurity and Digital Trust: Identifying Cybersecurity Gaps to Rethink State of the Art." In.

Ahmad, Atif, Sean Maynard, and Graeme Shanks. 2015. 'A case analysis of information systems and security incident responses', *International Journal of Information Management*.

Al-Omari, Ahmad, Omar El-Gayar, and Amit Deokar. 2012. 'Information security policy compliance: The role of information security awareness'.

Albrechtsen, Eirik, and Jan Hovden. 2010. 'Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study', *Computers & Security*, 29: 432-45.

Aleroud, Ahmed, and Lina Zhou. 2017. 'Phishing environments, techniques, and countermeasures: A survey', *Computers & Security*, 68: 160-96.

Alshaikh, Moneer, Sean B Maynard, Atif Ahmad, and Shanton Chang. 2018. "An Exploratory Study of Current Information Security Training and Awareness Practices in Organizations." In *Proceedingsofthe51st Hawaii International Conference on System Sciences*, 5085-94. Hawaii, US.

Alsharnouby, Mohamed, Furkan Alaca, and Sonia Chiasson. 2015. 'Why phishing still works: User strategies for combating phishing attacks', *International Journal of Human-Computer Studies*, 82: 69-82.

Arachchilage, Nalin Asanka Gamagedara, and Steve Love. 2014. 'Security awareness of computer users: A phishing threat avoidance perspective', *Computers in Human Behavior*, 38: 304-12.

Australian Cyber Security Centre. 2016. "2016 Threat Report." In.

Briggs, P., D. Jeske, and L. Coventry. 2017. 'Chapter 6 - Behavior Change Interventions for Cybersecurity.' in Linda Little, Elizabeth Sillence and Adam Joinson (eds.), *Behavior Change Research and Theory* (Academic Press: San Diego).

Bulgurcu, Burcu, Hasan Cavusoglu, and Izak Benbasat. 2010. 'Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness', *MIS Quarterly*, 34: 523-A7.

Coventry, Lynne, Pam Briggs, Debora Jeske, and Aad van Moorsel. 2014. "SCENE: A Structured Means for Creating and Evaluating Behavioral Nudges in a Cyber Security Environment." In *Design, User Experience, and Usability. Theories, Methods, and Tools for Designing the User Experience*, edited by Aaron Marcus, 229-39. Cham: Springer International Publishing.

D'Arcy, John, Anat Hovav, and Dennis Galletta. 2009. 'User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach', *Information Systems Research*, 20: 79-98.

De Maeyer, Dirk. 2007. 'Setting up an Effective Information Security Awareness Programme.' in, *ISSE/SECURE 2007 Securing Electronic Business Processes* (Vieweg).

Dodge Jr, Ronald C., Curtis Carver, and Aaron J. Ferguson. 2007. 'Phishing for user security awareness', *Computers & Security*, 26: 73-80.

French, Simon D., Sally E. Green, Denise A. O'Connor, Joanne E. McKenzie, Jill J. Francis, Susan Michie, Rachelle Buchbinder, Peter Schattner, Neil Spike, and Jeremy M. Grimshaw. 2012. 'Developing theory-informed behaviour change interventions to implement evidence into practice: a systematic approach using the Theoretical Domains Framework', *Implementation Science*, 7: 38.

Fulton, E. A., K. E. Brown, K. L. Kwah, and S. Wild. 2016. 'StopApp: Using the Behaviour Change Wheel to Develop an App to Increase Uptake and Attendance at NHS Stop Smoking Services', *Healthcare (Basel)*, 4.

Gowtham, R., and Ilango Krishnamurthi. 2014. 'A comprehensive and efficacious architecture for detecting phishing webpages', *Computers & Security*, 40: 23-37.

Herath, Tejaswini, and H. Raghav Rao. 2009. 'Protection motivation and deterrence: a framework for security policy compliance in organisations', *Eur J Inf Syst*, 18: 106-25.

Ifinedo, Princely. 2014. 'Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition', *Information & Management*, 51: 69-79.

Jansen, Jurjen, and Paul van Schaik. 2019. 'The design and evaluation of a theory-based intervention to promote security behaviour against phishing', *International Journal of Human-Computer Studies*, 123: 40-55.

Johnston, Allen C, and Merrill Warkentin. 2010. 'Fear appeals and information security behaviors: an empirical study', *MIS Quarterly*: 549-66.

Kajzer, Mitchell, John D'Arcy, Charles R. Crowell, Aaron Striegel, and Dirk Van Bruggen. 2014. 'An exploratory investigation of message-person congruence in information security awareness campaigns', *Computers & Security*, 43: 64-76.

Karjalainen, Mari, and Mikko Siponen. 2011. 'Toward a New Meta-Theory for Designing Information Systems (IS) Security Training Approaches', *Journal of the Association for Information Systems*, 12: 518-55.

Khan, Bilal, KhaledS Alghathbar, and MuhammadKhurram Khan. 2011. 'Information Security Awareness Campaign: An Alternate Approach.' in Tai-hoon Kim, Hojjat Adeli, RosslinJohn Robles and Maricel Balitanas (eds.), *Information Security and Assurance* (Springer Berlin Heidelberg).

Lastdrager, Elmer EH. 2014. 'Achieving a consensual definition of phishing based on a systematic review of the literature', *Crime Science*, 3: 9.

Lebek, Benedikt, Jorg Uffen, Michael H. Breitner, Markus Neumann, and Bernd Hohler. 2013. "Employees' Information Security Awareness and Behavior: A Literature Review." In *System Sciences (HICSS), 2013 46th Hawaii International Conference on*, 2978-87.

Michie, Susan, L Atkins, and R West. 2014. *The behavior change wheel: a guide to designing interventions* (Great Britain: Silverback Publishing).

Michie, Susan, Maartje M. van Stralen, and Robert West. 2011. 'The behaviour change wheel: A new method for characterising and designing behaviour change interventions', *Implementation Science*, 6: 42.

Molok, Nurul Nuha Abdul, Atif Ahmad, and Shanton Chang. 2011. "Disclosure of organizational information by employees on Facebook: Looking at the potential for information security risks." In *Proceedings of the Australasian Conference on Information Systems (ACIS)*.

Ng, Boon-Yuen, Atreyi Kankanhalli, and Yunjie Xu. 2009. 'Studying users' computer security behavior: A health belief perspective', *Decision Support Systems*, 46: 815-25.

Öğütçü, Gizem, Özlem Müge Testik, and Oumout Chouseinoglou. 2016. 'Analysis of personal information security behavior and awareness', *Computers & Security*, 56: 83-93.

Posey, Clay, Tom L. Roberts, and Paul Benjamin Lowry. 2015. 'The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets', *Journal of Management Information Systems*, 32: 179-214.

Puhakainen, Petri, and Mikko Siponen. 2010. 'Improving employees' compliance through information systems security training: an action research study', *MIS Quarterly*, 34: 757-78.

Rosemann, Michael, and Iris Vessey. 2008. 'Toward Improving the Relevance of Information Systems Research to Practice: The Role of Applicability Checks', *MIS Quarterly*, 32: 1-22.

SANS. 2017. 'Security awareness report: It's Time to Communicate', Accessed 11/08. https://www.sans.org/security-awareness-training/blog/2017-security-awareness-report.

Siponen, Mikko, M. Adam Mahmood, and Seppo Pahnila. 2014. 'Employees' adherence to information security policies: An exploratory field study', *Information & Management*, 51: 217-24.

Siponen, Mikko, and Robert Willison. 2009. 'Information security management standards: Problems and solutions', *Information & Management*, 46: 267-70.

Tsohou, Aggeliki, Maria Karyda, Spyros Kokolakis, and Evangelos Kiountouzis. 2015. 'Managing the introduction of information security awareness programmes in organisations', *European Journal of Information Systems*, 24: 38-58.

Vance, Anthony, Mikko Siponen, and Seppo Pahnila. 2012. 'Motivating IS security compliance: Insights from Habit and Protection Motivation Theory', *Information & Management*, 49: 190-98.

Wall, Jeffrey D, Prashant Palvia, and Paul Benjamin Lowry. 2013. 'Control-related motivations and information security policy compliance: The role of autonomy and efficacy', *Journal of Information Privacy and Security*, 9: 52-79.

Watkins, Kim, Liza Seubert, Carl R Schneider, and Rhonda Clifford. 2016. 'Post hoc evaluation of a common-sense intervention for asthma management in community pharmacy', *BMJ Open*, 6: e012897.

Whitman, Michael E., and Herbert J. Mattord. 2008. *Management of information security* (Thomson Course Technology: Boston, Mass.).

Williams, Emma J., Joanne Hinds, and Adam N. Joinson. 2018. 'Exploring susceptibility to phishing in the workplace', *International Journal of Human-Computer Studies*, 120: 1-13.