# Developing a framework to support SMEs operate a proactive cyber-security culture using behaviour change techniques

---


**Author:**

Keith Bollington

**Supervisor:**

Dr Yulia Cherdantseva

**Moderator:**

Jianhua Shao


A dissertation submitted in partial fulfilment of
the requirements of the degree of:

**Master of Cybersecurity**

October 8th, 2021


School of Computer Science and Informatics
Cardiff University

# Table of Contents

Abstract ..... 3
Acknowledgement ..... 4
List of Figures ..... 5
List of Tables ..... 5
Chapter 1: Introduction ..... 6
1.1 Research motivation ..... 6
1.2 Aims and objectives ..... 6
1.3 Scope ..... 7
1.4 Thesis structure ..... 8
Chapter 2: Background and Literature Review ..... 9
2.1 Overview ..... 9
2.2 The level of cyber threat that an SME is facing ..... 9
2.3 Why a business needs to build and operate a strong security culture ..... 10
2.4 Why security awareness training alone is not enough to build a security culture ..... 10
2.5 Other challenges businesses face to building a strong security culture ..... 11
2.5.1 The use of psychology in social engineering ..... 11
2.5.2 The challenges of employees using social media ..... 11
2.5.3 Security Policies do not necessarily take humans into account ..... 12
Chapter 3: Research Methodology ..... 14
3.1 Overview of Methodology ..... 14
3.2 Stage 1: Identify the problem ..... 14
3.3 Stage 2: Define objectives of a solution ..... 14
3.3.1 Building on awareness training to support behaviour change ..... 15
3.3.2 Providing behaviour change support to increase the user's digital hygiene ..... 15
3.3.3 Providing tools and processes to increase the user's digital hygiene ..... 15
3.4 Stage 3: Design and develop ..... 16
3.4.1 Using Behavioural Change Wheel to build a framework ..... 16
3.4.2 Selecting the most relevant Intervention Functions ..... 18
3.4.3 Selecting the most relevant Behaviour Change Techniques (BCTs) ..... 19
3.5 Stages 4, 5, 6: Demonstrate, Evaluate and Communicate ..... 22
Chapter 4: Framework for delivering a proactive cyber security culture ..... 22
4.1 Overview ..... 22

4.2 The Foundation ..... 23
4.2.1 Top Management ..... 23
4.2.2 Security Champion ..... 26
4.3 The Pillars ..... 27
4.3.1 Social Engineering Pillar ..... 28
4.3.2 Access Control Pillar ..... 30
4.3.3 End-User Devices Pillar ..... 33
4.4 The Overarching Support Functions ..... 35
4.4.1 Threat Intelligence ..... 35
Chapter 5: Evaluation ..... 36
5.1 Overview ..... 36
5.2 Analysis of Expert Feedback ..... 36
5.3 Evaluation and Discussion ..... 38
5.4 Summary ..... 40
5.4.1 Using certification to push a positive cyber-security culture framework ..... 40
5.4.2 Utilise the Supply Chains to request CE certification ..... 41
5.4.3 Utilise the Insurance Industry to request CE certification ..... 41
Chapter 6: Conclusion ..... 43
6.1 Conclusion ..... 43
6.2 Limitations and future work ..... 43
6.3 Reflections ..... 43
References ..... 45
Appendix 1 – Framework Description ..... 51
Appendix 8 – Answers to Questionnaire ..... 82

# Abstract

As more business is transacted online, the opportunity for cyber-criminals to conduct activities to disrupt and defraud business has increased. While larger companies have invested money, time, and resource into building systems and providing education designed to create a secure environment to work and conduct their business, the challenge for Small and Medium sized Enterprise (SME) is more significant. SMEs often do not have the funds, resources, or knowledge to adequately identify the risk and build the defences required to protect themselves adequately from Cyber Attacks. And that risk level is rising as cyber-criminals have determined that the return on investment for cyber-crime can have a potentially high return. Cyber-criminals are consistently modifying their attack methods and have identified that targeting employees is often the most straightforward entry point when looking to gain access to a computer system. Using social engineering methods such as phishing to con employees into opening unsecure attachments or clicking links that take them to unsecure websites, the cyber-criminal is developing psychological methods designed to trick an employee. Therefore, even if an SME gains certification to a secure framework (e.g., the UK Government-backed Cyber Essentials scheme), it will not provide strong protection against social engineering attacks, which account for up to 90% of the data breaches recorded.

Therefore, to assist SMEs in better protecting themselves from cyber-attacks, this study sets out to create a novel framework designed to support building a human line of cyber-defence. The framework's goal is to implement behaviour change techniques, individually selected from the Behaviour Change Wheel, to support the development of the SME employees in using and maintaining the right behaviours to identify and prevent a cyber-attack. Such behaviours will support the operation of a positive cyber-security culture.

Feedback given on the framework demonstrates that although there is clear support and agreement that a human layer of security is equally, if not more important than a technical layer, persuading the SMEs to spend time and resources on implementing such a framework will be very difficult. Therefore, the study identifies several external factors which, given the right amount of support from the right legislative or corporate bodies, could actively encourage or incentivise an SME to build the secure human layer and operate a safer, positive cyber-security culture within its employees.

# Acknowledgement

I would like to thank my supervisor, Dr Yulia Cherdantseva, for providing the guidance and support to research a topic which was quite different to many of the dissertation topics due to its focus on the human factor rather than the technical factor. It provided an equally interesting and important topic in researching human behaviours that could better secure SMEs from cyber-attacks.

I am grateful to CyberSmart for the support given throughout the project. Specifically, Anete Poriete for taking the regular meetings, providing feedback, challenging the content, and creating clarity on the academic ways. And to Dennis Palmer and Paul Sideras for their feedback, which proved most helpful.

To Andrew Rae for his feedback, which triggered a few “light bulb” moments which helped steer the project to its conclusions.

Finally, to Kath. Without whom I would not have had the courage to become a full-time student again after 28 years of full time working. Your love and support and focus on what really matters in life gave me the strength to make the change.

# List of Figures

Figure 1: Structure to achieve a positive security culture ..... 7
Figure 2: Overview of chosen methodology [40] ..... 14
Figure 3: The COM-B model [53] ..... 17
Figure 4: Behaviour Change Wheel [14] ..... 18
Figure 5: Building for Cyber Security Behaviour Change Framework ..... 23
Figure 6: Foundation Layer ..... 23
Figure 7: The Pillars ..... 27
Figure 8: Overarching Functions ..... 35

# List of Tables

Table 1: BCTs relating to health care ..... 19
Table 2: BCTs seen to have a negative connotation ..... 20
Table 3: BCTs viewed to be too time-consuming for the individual/management ..... 20
Table 4: BCTs used in the framework ..... 21
Table 5: BCTs relevant to the framework but not yet used ..... 22

# Chapter 1: Introduction

## 1.1 Research motivation

As more SMEs move to a digital way of operating, the opportunity for cyber-criminals to profit from illegal activity has increased significantly [1]. The recent proliferation of ransomware attacks [2] highlights the need for these businesses to protect themselves or fall prey to regular attacks [1].

A business with 50 employees who operate with poor digital hygiene provides a cyber-criminal with 50 additional insecure endpoints by which to gain entry to business systems and data. Cyber-criminals have quickly identified that targeting SMEs employees is one of the easiest ways to break into a company's systems [3]. These criminals have been using psychological tactics [4] to ensure that their methods are effective. Methods include targeting emails that put employees under time pressure or pray on the employee's inbuilt wish to help the sender or create a scenario in which the employee believes action is needed to protect themselves [5]. Verizon reported that in 2020, 85% of breaches they analysed involved a human element [6] and that overall, phishing was present in 35% of the breaches analysed [6]. Businesses are investing time and money into solutions that will try to identify a system breach. Such systems are a necessity moving forward, with Gartner predicting that 89% of spending to be targeted on Security Services, Infrastructure Protection, Identify Access Management and consumer security software [7]. These systems and solutions are technical in nature. Less investment is made to ensure that employees do not open the digital door to allow cyber-criminals to access the systems.

Security awareness training is a standard method that businesses use to educate their employees about the risks faced in the digital world so that employees do not allow easy access to a cybercriminal. Not all training is equal, with some solutions simply offering a quick introduction to the existing dangers [8]. For the training to be effective, the employees need to adopt new behaviours that ensure they adhere to the security policies set [9]. Importantly, these behaviours need to become second nature. Evidence is growing that awareness training is successful in educating the employee. However, training alone does not trigger the behaviour change required to turn the learnings into practice, which keeps a business safe [10] [11].

## 1.2 Aims and objectives

The project aims to design and develop a framework that, when combined with cyber-security awareness training, can be used by SMEs to support positive behaviour change amongst employees. Such an approach should strengthen the employees' digital hygiene and result in a robust cyber security culture that increases the overall security.

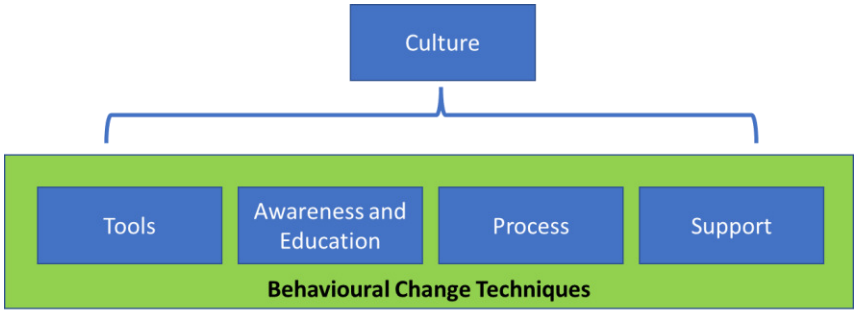



*Figure 1: Structure to achieve a positive security culture*

Figure 1 shows that behavioural change techniques within, tools, awareness and education, process and support help deliver better behaviour change and build a stronger security culture.

The objective of the project is as follows:

1. Explore the limitations of awareness training in changing the security behaviour of the recipients.
2. Identify a standard security awareness tool that can be used freely by SMEs and identify the common modules provided by this tool.
3. Identify behavioural methods to be used to change people's behaviours when supporting the delivery of the standard modules and learning objectives.
4. Using the Behaviour Change Wheel, identify a set of Intervention techniques that will support the training delivery, target the behaviour changes required and strengthen the cyber security culture.
5. Build the intervention functions into a framework that SMEs can use to support changing and sustaining security behaviours and improving security culture.
6. Assess the feedback from Industry experts of the framework and identify future development work based on the feedback received.

## 1.3 Scope

This project's scope is to concentrate on the SME category. Many SMEs have limited resources, budgets, or capability to invest in cyber-security in the way large companies are able [12]. Therefore, this project focuses on supporting SMEs.

While the project will attempt to identify the behavioural change techniques best adapted to modify an individual's behaviour, it will not look at individuals' specific psychological traits or demographics when identifying the behavioural change techniques. Although research identifies that individuals will react differently to situations based on their demographic [13] or unique psychological make-up, this adds a layer of complexity for which the potential SME user of the framework will not have time to manage [5].

During the research of the behavioural change techniques [14], a range of academic, government and standard publications were examined that identified that whilst using fear

appeals could create an initial shift in behaviour; they could ultimately create an opposite response to the behaviour change required [15] [11]. For this reason, negative behaviour change methods were excluded from the scope of this project.

## 1.4 Thesis structure

This thesis consists of 6 chapters as follows:

**Chapter 2**

This chapter introduces the background knowledge regarding the challenges that an SME faces due to the growing and evolving challenges of cyber-crime.

**Chapter 3**

This chapter presents the research methodology and the introduction and reading on the behavioural change wheel to support behavioural change.

**Chapter 4**

This chapter documents the framework design and the reasons why each of the framework elements were chosen.

**Chapter 5**

This chapter presents the results from the questionnaire feedback from security experts on the suitability of the framework.

**Chapter 6**

This chapter summarises the project findings, discusses the future study direction and reflections from having made the study.

# Chapter 2: Background and Literature Review

## 2.1 Overview

This chapter gives the reader a background into the increasing level of cyber-security attacks taking place, the reasons why an SME should therefore focus on building a strong cyber-security culture to act as a deterrent to these attacks, and why implementing awareness training alone should not be expected to change behaviours of employees so that the business becomes more secure. Several reasons are given for why employees find the needed behaviour change to be challenging to achieve.

## 2.2 The level of cyber threat that an SME is facing

Cybersecurity is quickly becoming a key focus area in many businesses worldwide, as the number of cyber-attacks significantly increase year on year [6]. In 2016, it was estimated that there were 6.2 billion cyber-attacks [4]. With over 61% of UK businesses operating a digital model where customer-related data is held electronically [4], the risk is to a more significant portion of companies.

Zurich Insurance research stated that up to 875,000 SMEs (16%) in the UK had suffered a cyber security breach in the 12 months preceding their report published mid-2017 [16]. Zurich also estimated that just under 49% of SME businesses would invest less than £1,000 into cyber security over the next year. Such a scenario points to what may become a "security divide" between SMEs and large businesses [17].

The Information Commissioners Office (ICO) published security incident trend statistics for the number of incidents reported to the ICO in Q1 2021 [18]. These figures show that of the 688 reported cases, 41% related to phishing attacks and 21% to ransomware attacks. These attack methods account for 62% of the attack types reported by businesses in the UK.

In 2020, the UK Government Department for Digital, Culture, Media and Sport (DCMS) reported that cyber-attacks on business have evolved and become more frequent [2]. It was reported that 46% of companies and 26% of charities had reported cyber security attacks in the previous twelve months. More alarmingly, within the 46% of companies who reported attacks, 32% experienced some form of attack weekly. Since 2017, the number of businesses experiencing phishing attacks has risen from 72% to 86% [2].

When viewing the negative impact of cyber-attacks on business, nearly 20% of those businesses that identified an attack reported that they lost money or data from the attack whilst two in five businesses were negatively affected due to a level of disruption to the business [2].

## 2.3 Why a business needs to build and operate a strong security culture

Businesses will invest in technology to help to identify and stop a cyber-attack [19]. However, buying and installing the latest security technology does not necessarily guarantee that it is preventing an attack. Research as far back as 2001 identified that preventing attack events meant that companies should not just focus on the technical solutions of "*locks and keys*" but also on "*the social groupings and behaviour*" [20]. The employees of a business have a significant impact on how safely and securely a business operates. If employees are not aware of the risks and do not know how to act when a potential attack occurs, even the most technically well-protected businesses can become a victim of a cyber-criminal, as the employees do not operate as the primary level of defence [21].

Businesses are addressing this risk by creating security policies for employees to follow and providing awareness training that highlights the risks and provides information on how to perform the right behaviours so that employees can operate as an effective line of defence against the prospect of an attack.

Creating and monitoring a strong security culture will make a business more secure from a cyberattack [22].

## 2.4 Why security awareness training alone is not enough to build a security culture

There is evidence to show that awareness training does educate employees and has some effect in changing the way an employee behaves [9] [21]. A case study on the effectiveness of awareness training given regarding best practice methods for using secure passwords [21], showed that in a controlled study, there was a decrease in the number of passwords cracked within a 2-minute time frame from 58% down to 35% when re-tested six months after awareness training had been delivered. Although this represents a significant reduction in the ease of a cybercriminal to crack a password, it still resulted in 35% of passwords being breakable within 15 minutes. In another research project run to test different demographics ability to identify a phishing website, it was found that training subsequently provided a 40% improvement but still resulted in 28% of people being fooled [13]. This demonstrates that although the training raised employee awareness and many users chose to follow the guidelines given, a significant number of users did not change behaviour. Nearly a third of passwords were still in an easy to crack state six months later.

The role of awareness training is to educate employees as to the risks and actions needed to reduce those risks [23]. But to ensure that an employee carries out the actions taught and turns those actions into normal behaviours in the long term, SMEs needs to support their employees through a process of behavioural change, where the knowledge gained through awareness training is developed into sustained practice.

## 2.5 Other challenges businesses face to building a strong security culture

### 2.5.1 The use of psychology in social engineering

As reported by the ICO and UK government [2] [18], cyber-criminals primarily target businesses using phishing and ransomware attacks. Often a phishing attack can lead to a ransomware attack as phishing is a cheap and effective way for a cyber-criminal to break through the security of a business, making it a cost-effective and profitable attack method that delivers a high Return On Investment (ROI) [24].

Such information raises the question of why phishing emails provide such an effective method of targeting employees within a business. One possible answer relates to the level of sophistication that cyber-criminals are using to ensure that the phishing email effectively generates the required response from the user who receives it [25]. Cyber-criminals are employing a psychology-sensitive design to their phishing mails. The receiver is led to believe that the mail is legitimate and needs to be acted upon immediately. [23].

Worryingly for businesses, the person targeted by this form of deception may not even realise that they have been the victim of an attack that successfully revealed private information to an attacker [3]. This scenario makes it even more difficult for a business to learn from attacks and thus improve its security.

Several methods of psychological manipulation are used within phishing mails to lure the receiver into unsafe behaviour. Attackers may misuse reciprocity by offering some form of gift in exchange for information. In an experiment done [26] using chocolate as the incentive, researchers extracted passwords from 30% (344) of the participants.

### 2.5.2 The challenges of employees using social media

Another issue that comes to light is people's use of social media such as Facebook and Instagram. Sharing of personal information on social media platforms allows cyber-criminals a source of information by which they could target employees using spear-phishing emails [27] [28].

In the last ten years, phishing has become the most likely used attack method by cyber-criminals. This situation coincides with a massive increase in the use of Social Media sites. Facebook grew its active user base from 100 million users in 2008 to a staggering 2.26 billion users in 2018 [29]. The business model of Facebook and other social media companies is that of selling targeted advertising. Facebook disrupted the marketing industry by using technology to collect vast amounts of detailed personal data and harvesting that data so that it could sell marketing that targeted an audience with a level of precision never previously achieved. To get that level of accuracy, Facebook collects information such as the pages a user likes, the pages they visit, the apps they use, and the purchases they make [30]. Facebook matches this information with personal data about the individual (age, sex,

location, relationship status etc.) to provide very targeted marketing. Therefore, it is within the interests of a social media company such as Facebook to gain as much personal information as possible. Social media sites compete for our time, as each subsequent click made by a user grows the knowledge about that user.

The boundaries between a personal social media account and a work social media account are becoming more and more blurred as people become used to running their own social media profiles and sharing information about their personal and work life. Also, mobile devices such as tablets and smartphones allow "24/7" style news coverage where it becomes challenging to keep corporate information within the boundaries of the corporate network [31].

The volume and ease of availability of such detailed personal information is a boon for the cyber-criminal looking to use psychological methods to trick a user into believing that a phishing mail is legitimate or simply guessing an employee's password to hack into their systems. Social media can provide an easy to access and detailed overview of a person. Within a short amount of time, an online investigation can provide an attacker with a wealth of information about an employee's company, skill set, likes, dislikes, hobbies, family, friends, pets, and purchases [28]. This data could be used in a spear-phishing email to target that individual in a way that makes it far more likely that they will click a link that provides the attacker access to their computer or other devices [25].

The cyber-criminal also matches this increased knowledge of their potential victim with known psychological tools that have increased success in making an employee take an incorrect action when faced with a possible cyber-attack.

Cyber-criminals use automated technology to create fake social media accounts that share information of interest in order to gather a list of potential targets. The user actively engages and shares information on the account, building up trust and making the user even more likely to fall for a phishing attack. In research done using social bots on Twitter over a two-week period, the researchers lured over 400 users to visit a fake website. At least 33 of those users visited while signed into an organisational network [32].

### 2.5.3 Security Policies do not necessarily take humans into account

According to the National Institute of Standards and Technology (NIST), the definition of a security policy is to "define the objectives and constraints for the security program. Policies are created at several levels, ranging from organisational or corporate policy to specific operational constraints (e.g., remote access). In general, policies answer the questions 'what' and 'why' without dealing with "how." Policies are typically written in terms that are technology independent. [33]". Simply put, policies guide employees on what to do and what not to do. They do not focus on how employees should carry out the actions, and here in lies a challenge. Where computer systems can be programmed to carry out instructions consistently, humans are far less predictable. Therefore, simply issuing a security policy and expecting adherence is not a recipe for success.

A 2015 Cyber Security report by IBM identified that over 95% of incidents were caused by human error [34]. However, many businesses still focus their time and spending on the technical infrastructure area [35]. This results in a large gap in security for those businesses that do not focus on securing the human aspects of cyber security in their organisations [35].

Research in this field has identified various security-related behaviour resulting in security policy violations [36]. Some of these behaviours are malicious; however, many of the non-compliance behaviours do not have a malicious intent by the employee but still subject the business to a much-increased risk.

Firstly, the employee may find the policy too challenging to comply with due to the requirements placed upon them, therefore finding themselves unable to carry out the required behaviours. This scenario can lead to employees ignoring security warnings [37] [38] rather than adhering to the policy. Such situations are common, and although intentional by the employee, it is not a malicious act as the employee does not mean to cause damage. Such examples of non-malicious intent could be the writing down of passwords, installing unauthorised software and copying sensitive data onto non-work devices [36].

Secondly, the employee may have completed the awareness and education training and has the knowledge and skills needed to carry out the policy requirements. However, they decide not to comply because the policy restricts their ability to do their job correctly, meet targets and be successful [36]. In these situations, the policy is not in line with the business tasks and therefore compromises an employee between delivering on their job tasks or delivering on their security tasks. The employee sees a higher risk of not performing their job tasks and acts accordingly.

Lastly, an employee may not comply with the security policy because they do not believe that any harm will happen from using insecure methods. Most of the time that employees carry out these methods (such as sharing a password), they see no negative consequences to their actions, and in many cases, feel that they received a positive outcome from their action [37]. Like driving a car without a seat belt, the person saves time by not needing to fasten or un-fasten the belt and will see the risk reducing after each journey without injury [37].

Therefore, a business must address the needs of its employees when defining its security policies, as a poorly defined policy can result in non-compliance, which its users believe to be justified [36].

# Chapter 3: Research Methodology

## 3.1 Overview of Methodology

This chapter provides information about the methodology chosen for researching, designing, and building the behavioural change framework required to assist an SME in increasing the digital hygiene of its employees. The methodology chosen is the Design Science Research Methodology [38].

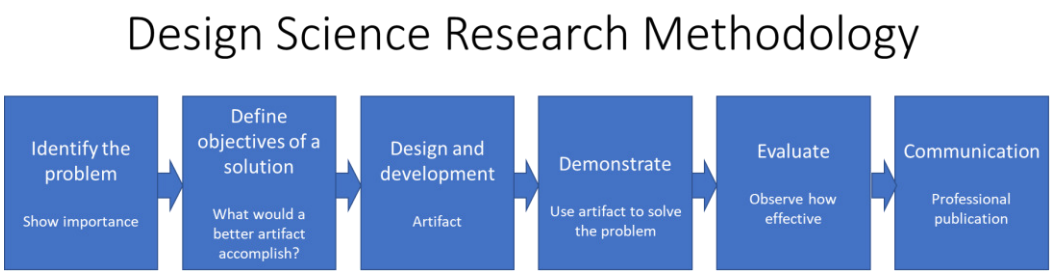



*Figure 2: Overview of chosen methodology [38]*

## 3.2 Stage 1: Identify the problem

Although a good amount of research identifies that a proactive information security culture would reduce the internal threats to an organisation, less study discusses how to create the behaviour changes necessary [39]. SMEs face many challenges, and Information Security is a relatively new topic for those SMEs when implementing digital technology. The COVID-19 pandemic speeded up the necessity for many SMEs to quickly implement new digital solutions to keep the business operating. This situation has increased the challenges regarding data security and the need for an SME to have clear policies on user and data privacy [40].

## 3.3 Stage 2: Define objectives of a solution

Several research documents guide how to build a framework for supporting the change of behaviour for cyber-security [39] [41]. However, none built a framework document that could be directly implemented as a solution. Therefore, this project sets out to create such a framework, using feedback from cyber-security experts who support SMEs in finding, fixing, and protecting against cyber security incidents.

### 3.3.1 Building on awareness training to support behaviour change

Documentation and support for the need for security training have been available for many years. The National Institute for Standards and Technology (NIST) produced guidelines in 2003 that informed how to build an information technology security awareness and training program [42].

Governments and trade bodies have been producing literature that guides SMEs to the risks and steps to reduce those risks. The Information Commissioners Office (ICO) published in 2016 a guide entitled “A practical guide to IT security. Ideal for the small business” [43], which maps out ten practical methods for keeping data safe and secure. One specific item relates to the need for employee’s awareness training.

There is a great choice [44] of offerings a company can explore when choosing awareness training packages. Due to the increase of competition in the market and the ability to deliver training digitally via a web browser, the solutions offered can be cost-effective.

Generally, businesses are aware of the risks that they face. Research done in 2017 by the Council of Better Business Bureaus surveyed SMEs in the US [45] and found that awareness of phishing attacks ranked at 73% and increased to 93% when asked about a more extensive range of cybersecurity threats. Therefore, the work by the government and other business support agencies appears to be working in creating the proper awareness of the problems.

### 3.3.2 Providing behaviour change support to increase the user's digital hygiene

Awareness training is shown to increase an employee’s knowledge of the threats faced. However, research shows a discrepancy between the level of knowledge a user believes they have gained and the activities that are subsequently undertaken to improve digital hygiene [46]. For example, one research project found that 85% of people responded positively to the question regarding using strong passwords, but 56% used the same password across multiple systems [46]. Therefore, the objective of a framework solution needs to bridge the gap between the knowledge gained via awareness training and the actions of carrying out the behaviours which match that knowledge so that employees improve and maintain their digital hygiene.

### 3.3.3 Providing tools and processes to increase the user's digital hygiene

The requirements on employees for ensuring that they operate with a good level of digital hygiene can be challenging. As hackers improve their techniques for infiltrating humans, the education requirements can be daunting for even the most computer literate employees.

For example, the Information Commissioners Office (ICO) current guidelines for ensuring a secure password [47] involve three key elements:

1. Passwords should be no less than ten characters in length (with no maximum length currently specified).
2. Special characters should be used if the service allows.
3. Commonly used passwords must be blocked.

In addition, best practice guidance tells users not to re-use the same password across other platforms/systems. For a user who is using multiple computer systems for social media, banking, music services, streaming services, news, and shopping, it is conceivable that they may need to remember over 20 individual passwords over ten characters in length which contain special characters. Such a requirement is why some users who follow such recommendations will write down the passwords to remember them [48]. Alternatively, it has been argued that the fear of writing down the passwords will result in employees choosing less secure passwords as they are easier to remember [49].

The European Union Agency for Cyber Security (ENISA) [50] highlights the need for technology to be used wherever possible to improve cyber security protection. This ensures that the employees are not carrying the entire burden of ensuring that the data is kept fully secure from an attack.

Therefore, to support employees in adhering to security policy guidelines, the framework must encourage SMEs to investigate providing their employees with software and tools which can reduce the challenges and make adherence to the policy an easier task.

## 3.4 Stage 3: Design and develop

The elements built within this stage are discussed in Chapter 4: Design and Implementation. The methods used to design the delivery is discussed below.

### 3.4.1 Using Behavioural Change Wheel to build a framework

In this project the Behavioural Change Wheel (BCW) [14] is used to build a framework that SMEs can use to change behaviours and build a strong security culture.

The behaviour change wheel was devised in 2011 when a group of experts looked at six existing behaviour change classification systems with the goal of building "*an extensive hierarchical classification of clearly labelled, well-defined BCTs (behavioural change techniques) with a consensus that they are proposed active components of behaviour change interventions, that they are distinct (non-overlapping and non-redundant) and precise, and that they can be used with confidence to describe interventions;*" [14]. Nineteen experts in behavioural change took part to create a distinct list of BCT labels and associated definitions.

The resulting framework identified 96 behavioural change techniques, which were categorised within 16 groups [14]. When identifying a behaviour to target, the behaviour change can be used standalone or grouped and combined with other change techniques.

The BCW was chosen as the basis for the framework for the following reasons:

- It is a comprehensive framework for designing behaviour interventions
- Many techniques can be used at the same time to target a behaviour
- It supports the building of policies

At the very centre of the framework is the COM-B model [51], which defines three key components that must be addressed so that behaviour change can occur. These are:

- Motivation.
- Opportunity and
- Capability.

In order for a person can perform a particular behaviour, they must have the motivation (an internal factor) to want to carry out the behaviour, the given opportunity (an external factor) in which to carry out this behaviour and have the right capability (skills) to be able to carry out the behaviour [52]. If all three interventions can be successfully adhered to, there is the best chance for a successful behaviour change.

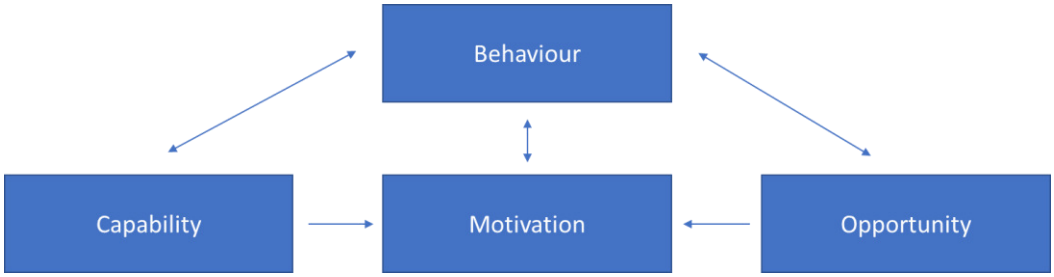



*Figure 3: The COM-B model [51]*

The behaviour change wheel takes the components defined by COM-B and adds seven policy categories and nine intervention functions.

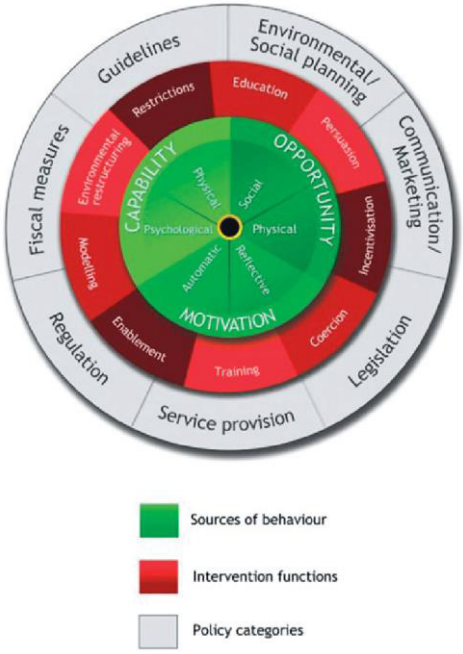



*Figure 4: Behaviour Change Wheel [14]*

Once the needed behaviour has been identified using COM-B, the BCW lists nine intervention functions and seven policy categories by which the behaviour change can be grouped. BCW then contains the taxonomy of 93 the behaviour-change techniques (BCTs), which can be used to create the behaviour change intervention desired to take place [14]. These 93 behaviours change techniques are split into 16 distinct groups, which have similar components.

### 3.4.2 Selecting the most relevant Intervention Functions

Whilst analysing the nine intervention functions, it was decided that two functions were not a good fit for developing a positive approach to behaviour change.

The 'Restrictions' intervention function was removed, as a restriction is often seen by an individual in a negative light. Employees will often take the easiest route to complete a piece of work, especially if they are operating under some form of time pressure. If a security policy has restrictions in place which prevent the employee from taking the easiest path, they may choose to ignore the restriction and continue to take the risk. Therefore, the framework will need to deliver alternate intervention functions which limit the number of restrictions and instead offer alternative solutions to the user.

Secondly, the 'Coercion' intervention function was removed. The Cambridge English dictionary terms coercion as [53] "*the use of force to persuade someone to do something that they are unwilling to do*". Rather than coerce, the framework will look to use positive engagement with employees to enable behaviour change. If the user sees methods to be coercive, such methods may be rejected by the employees. Such a decision is supported by research on "fear appeals", where caution is being suggested as to the effectiveness of

these appeals [15]. Another risk in the use of coercion and fear appeals is that employees are conditioned into simply following policies that are not as adaptive as the methods of the cyber-criminal. The use of more adaptive and proactive behaviour change techniques could ensure that employees adapt better to threats and produce a higher level of digital hygiene than the policy dictates [54].

### 3.4.3 Selecting the most relevant Behaviour Change Techniques (BCTs)

To remove the unsuitable BCTs, an analysis was made of their intended uses and then BCTs were reduced based on the unsuitability for supporting needed cyber security behaviour. Since the Behaviour Change Wheel was developed with the health care sector in focus, there were immediately several BCTs related to health care that were not so relevant to cyber-security behavioural change:

| Grouping | Behaviour Change Technique |
|---|---|
| 2 Feedback and monitoring | 2.6 Biofeedback |
| 3 Social support (emotional) | 3.3 Social support (emotional) |
| 4 Shaping knowledge | 4.2 Information about antecedents |
| | 4.3 Re-attribution |
| | 4.4 Behavioural experiments |
| 5 Natural consequences | 5.1 Information about health consequences |
| | 5.4 Monitoring of emotional consequences |
| | 5.5 Anticipated regret |
| | 5.6 Information about emotional consequences |
| 7 Associations | 7.3 Reduce prompts/cues |
| | 7.6 Satiation |
| | 7.7 Exposure |
| | 7.8 Associative learning |
| 8 Repetition and substitution | 8.2 Behaviour substitution |
| | 8.5 Overcorrection |
| 11 Regulation | 11.1 Pharmacological support |
| | 11.2 Reduce negative emotions |
| | 11.3 Conserving mental resources |
| | 11.4 Paradoxical instructions |
| 12 Antecedents | 12.4 Distraction |
| | 12.6 Body changes |

*Table 1: BCTs relating to health care*

During the research into methods of behavioural change, arguments that the use of fear as a stimulus for behaviour change had many opposing views, with arguments that fear can result in the opposite response to the one being targeted [15] [54]. Any BCTs which had a negative connotation were identified and removed from the list to be used:

| Grouping | Behaviour Change Technique |
|---|---|
| 7 Associations | 7.4 Remove access to the reward |
| 10 Reward and threat | 10.11 Future threat |
| 14 Scheduled consequences | 14.1 Behaviour cost |
| | 14.2 Punishment |
| | 14.3 Remove reward |
| | 14.4 Reward approximation |
| | 14.5 Rewarding completion |
| | 14.6 Situation-specific rewards |
| | 14.7 Reward incompatible behaviour |
| | 14.8 Reward alternative behaviour |
| | 14.9 Reduce reward frequency |
| | 14.10 Remove punishment |
| 16 Covert learning | 16.1 Imaginary punishment |
| | 16.3 Vicarious consequences |

*Table 2: BCTs seen to have a negative connotation*

To ensure that the process of using a cyber security behavioural change framework was not too time-consuming for either the business or the individual employees, BCTs that required additional time requirements from the individual or management in supporting the individuals were removed.

| Grouping | Behaviour Change Technique |
|---|---|
| 9 Comparison of outcomes | 9.3 Comparative imaging of future outcomes |
| 10 Reward and threat | 10.7 Self incentive |
| | 10.9 Self reward |
| 12 Antecedents | Avoidance/reducing exposure for cues to the behaviour |
| 13 Identity | 13.3 Incompatible beliefs |
| | 13.4 Valued self-identity |
| | 13.5 Identity associated with changed behaviour |
| 15 Self belief | 15.2 Mental rehearsal of successful performance |
| | 15.3 Focus on past success |
| | 15.4 Self-talk |

*Table 3: BCTs viewed to be too time-consuming for the individual/management*

The following list of BCTs were deemed relevant in the cyber-security behaviour change framework:

| Grouping | Behaviour Change Technique |
|---|---|
| 1 Goals and planning | 1.1 Goal setting (behaviour) |
| | 1.3 Goal setting (outcome) |
| | 1.5 Review behaviour goal(s) |
| | 1.7 Review outcome goal(s) |
| | 1.9 Commitment |
| 2 Feedback and monitoring | 2.1 Monitoring of feedback by others without feedback |

| | |
|---|---|
| | 2.2 Feedback and behaviour |
| | 2.7 Feedback on outcome(s) of behaviour |
| 3 Social support | 3.1 Social support (unspecified) |
| | 3.2 Social support (practical) |
| 4 Shaping knowledge | 4.1 Instructions on how to perform the behaviour |
| 5 Natural consequences | 5.2 Salience of consequences |
| | 5.3 Information about social and environmental consequences |
| 6 Comparison of behaviour | 6.1 Demonstration of the behaviour |
| | 6.2 Social comparison |
| | 6.3 Information about others approval |
| 7 Associations | 7.1 Prompts/cues |
| 10 Reward and threat | 10.1 Material incentive (behaviour) |
| | 10.4 Social reward |
| 12 Antecedents | 12.1 Restructuring the physical environment |
| | 12.2 Restructuring the social environment |
| 13 Identity | 13.1 Identification of self as a role model |

*Table 4: BCTs used in the framework*

The following list of BCTs were deemed relevant but have not yet been used in the cyber-security behaviour change framework:

| Grouping | Behaviour Change Technique |
|---|---|
| 1 Goals and planning | 1.2 Problem solving |
| | 1.4 Action planning |
| | 1.6 Discrepancy between current behaviour and goal |
| | 1.8 Behavioural contract |
| 2 Feedback and monitoring | 2.3 Self-monitoring of behaviour |
| | 2.4 Self-monitoring of outcome(s) of behaviour |
| | 2.5 Monitoring of outcome(s) of behaviour without feedback |
| 6 Comparison of behaviour | 6.2 Social comparison |
| | 6.3 Information about others approval |
| 7 Associations | 7.2 Cue/signalling reward |
| | 7.5 Remove aversive stimulus |
| 8 Repetition and substitution | 8.1 Behavioural practice/rehearsal |
| | 8.3 Habit formation |
| | 8.6 Generalisation of target behaviour |
| 9 Comparison of outcomes | 9.1 Credible source |
| | 9.2 Pros and cons |
| 10 Reward and threat | 10.2 Material reward (behaviour) |
| | 10.3 Non-specific reward |
| | 10.5 Social incentive |
| | 10.6 Non-specific incentive |
| | 10.8 Incentive (outcome) |
| | 10.10 Reward (outcome) |
| 12 Antecedents | 12.1 Restructuring the physical environment |

| | |
|---|---|
| | 12.5 Adding objects to the environment |
| 13 Identity | 13.2 Framing/reframing |
| 15 Self-belief | 15.1 Verbal persuasion about capability |
| 16 Covert learning | 16.2 Imaginary reward |

*Table 5: BCTs relevant to the framework but not yet used*

### 3.5 Stages 4, 5, 6: Demonstrate, Evaluate and Communicate

There is not enough time to research the subject matter, build a framework and thoroughly test the framework within several SME businesses. Therefore, the demonstrate function will deliver the completed framework to several industry experts who will evaluate and provide qualitative feedback.

Within the evaluation phase, the industry experts will answer six specific questions. Communication of the qualitative feedback and the associated actions will be delivered within the Results section of this thesis.

# Chapter 4: Framework for delivering a proactive cyber security culture

## 4.1 Overview

This chapter discusses the framework for supporting cyber-security behaviour change and how it will be delivered in a structured design. It discusses a set of foundation layers to be implemented first to ensure that subsequent pillars provide the right level of support to enable behavioural change success. Due to time constraints, three pillars have been designed which contain behavioural change techniques that will support the on-line cyber-security awareness training provided by the National Cyber Security Centre (NCSC) [55]. This link to the NCSC awareness training is made because, as a Government supported organisation that promotes the Cyber Essentials certification and offer free online awareness training, there is a compelling reason for an SME to investigate using this training.

The novel framework for delivering a proactive cyber security culture for SMEs, developed in this project, is presented in Figure 5.

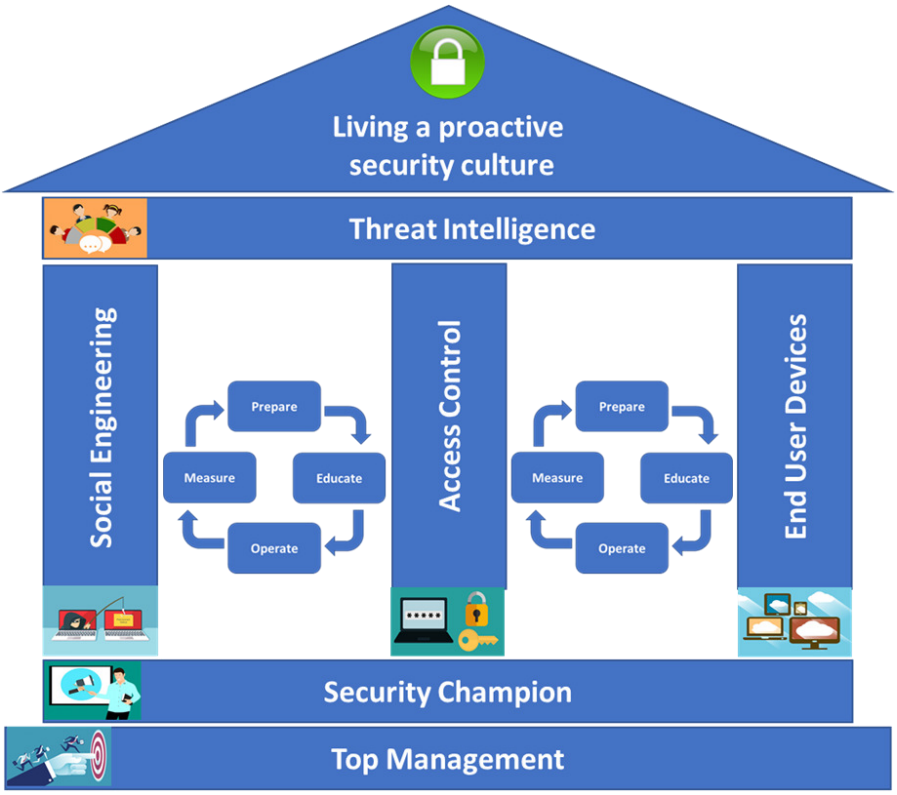



*Figure 5: Building for Cyber Security Behaviour Change Framework*

## 4.2 The Foundation

The foundation layer contains the actions required to ensure positive, security-focused behavioural change can be introduced, embraced, supported, and made permanent.

*Figure 6: Foundation Layer*

### 4.2.1 Top Management

Young at al. demonstrates [56] that without committed top management support, initiatives and projects undertaken by a business are far more unlikely to deliver a satisfactory outcome. The concept of Top Management support for IT projects was made back in 1963 when John Garrity [57], writing for the Harvard Business Review, identified some key roles which top management should do to aid and support successful IT project implementation:

1. *Devote time to the program in proportion to its cost and potential.*

*2. Review plans.*

*3. Follow up on results.*

*4. Facilitate ‘‘the management problems involved with integrating computer systems with the management process of the business”.*

ISO/ISEC 27001 [58] includes section 5.1 Leadership and Commitment, which supports these arguments and states eight specific actions expected by top management in supporting an information security management system:

*Leadership and commitment top management shall demonstrate leadership and commitment with respect to the information security management system by:*

*a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization.*
*b) ensuring the integration of the information security management system requirements into the organization’s processes.*
*c) ensuring that the resources needed for the information security management system are available.*
*d) communicating the importance of effective information security management and of conforming to the information security management system requirements.*
*e) ensuring that the information security management system achieves its intended outcome(s).*
*f) directing and supporting persons to contribute to the effectiveness of the information security management system.*
*g) promoting continual improvement.*
*h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility*

The European Union Agency for Network and Information Security (ENISA) published a report entitled “Cyber Security Culture in organisations” [50]. The report argues that cyber security has now become the responsibility of senior management as a breach of systems could lead to significant financial and reputational damage. Shareholders worried about the risks that a cyber-attack could have on the business expect senior management to take a leading role. This situation changes the dynamic of the conversation at the Senior Management level, as previously, discussions would often only happen when a security breach occurred [59].

ENISA argues that changes within the working environment can only successfully occur when senior management leads by example to visibly support such change and ensure adequate resources (both human and financial) are made available to drive forward the change.

The research into frameworks for security management identified top management support as the most significant factor that affects the success of activities undertaken to build a

strong security culture [39]. Recent research that analysed a broad range of research papers on building a security culture found that top management support was the most discussed factor [60].

**ACTIONS TO IMPLEMENT TOP MANAGEMENT SUPPORT FOUNDATION**

***BCT 12. 2 Restructure the environment***

In order that a figurehead is appointed in the organisation, a senior member of management is needed to take the visible role of top management sponsor. It is essential that this individual takes full accountability for the security culture and has a business role that highly benefits from having a strong security culture in operation.

***BCT 13.1 Identification of self as a role model***

The chosen Top Management Sponsor must undertake actions that identify themselves as a role model for supporting a proactive cyber security culture. They must be visible to all employees through communicating the importance of the culture, attending events such as education and training, and regularly sharing updates on culture development and successes.

***BCT 1.1 Goal setting behaviour + BCT 1.2 Goal setting outcome***

The Top Management Sponsor is to work with the Security Champion(s) to set achievement goals (both behaviour and outcome goals) that will be regularly measured to check progress. Goals are to be published.

***BCT 1.9 Commitment***

The Top Management Sponsor will ensure that the culture change programme is supported with the resources, time and funds required. Top Management Sponsor will work with IT/Security Champion to build a business case that details the costs and benefits.

**ACTIONS TO OPERATE TOP MANAGEMENT SUPPORT FOUNDATION**

***BCT 1.5 Review behaviour goal + BCT 1.7 Review outcome goal***

The Top Management Sponsor is to work with the Security Champion to review behaviour goals and outcome goals and identify the next steps required to keep activities on track.

***BCT 3.1 Social support (unspecified) + BCT 3.2 Social support (practical)***

The Top Management Sponsor is to provide the Security Champion with the right level of coaching and support to grow and develop in the role. This is based on giving encouragement and feedback, which helps the Security Champion to feel valued and to be able to understand their development needs. It can also be part of a more practical level, providing training or additional time or tools that help them fulfil the role.

***BCT 6.1 Demonstration of the behaviour***

The Top Management Sponsor is to ensure that they consistently demonstrate the correct behaviours and support the use of the right behaviours so that employees are led from the top regarding how to operate appropriately.

### 4.2.2 Security Champion

Traditionally, the role of undertaking Information Security has been seen as the remit of the IT department, and most tasks would be carried out by IT specialists [12]. However, as cyber-criminals continue to use attack methods directed at employees, there is a strong need for all employees to increase their digital skills and digital hygiene to keep the business safe. Therefore, there is the need to bridge the gap between IT technicians and users of the systems so that all employees understand and take an active role in the business's cyber security. For many SMEs, there will be a minimal IT department and possibly no IT department at all, and so here, there is an even greater need for a business user to take the Security Champion role.

The Security Champion concept will add a foundation layer of security to a business, which feels less formal for a user to access and could be described as more “human” in its approach [61]. The Security Champion helps bridge the gap between the security/IT professionals and the employees who need to operate a secure IT behaviour. The Security Champion supports the employees by promoting the concept of security, teaching and mentoring employees in the activities and providing non-judgmental support in answering questions and helping to deal with security issues that employees discover in their daily work.

When selecting security champions, the need for solid business knowledge ranks higher than having some form of cyber expertise. It is more important for this individual(s) to know the business processes and how data is used [62].

The concept is starting to be investigated and rolled out by businesses. Research on the feedback shows that such a concept provides valuable support to the employees who must adhere to the security policies [62] and operate securely.

**ACTIONS TO IMPLEMENT SECURITY CHAMPION FOUNDATION**

***BCT 12.2 Restructure the social environment***

The Security Champion role is vital in opening the channel to employees who need to understand cyber-security issues and carry out actions that ensure a secure operation. The choice of the Security Champion is key to a successful channel operating. The person must be respected by the business employees and knowledgeable about the work undertaken by the business. It is not a requirement that this person is a security/IT expert, but they need the capability to learn about the risks and transfer this information into a language that employees understand.

**ACTIONS TO OPERATE SECURITY FOUNDATION**

***BCT 2.1 Monitoring of others without feedback***

The Security Champion will monitor the behaviours of those around them to gauge the organisation's temperature and identify potential issues in behaviour that need investigating and supporting.

***BCT 2.2 Feedback of behaviour***

When a Security Champion observes behaviours that are not in line with the behaviours needed, they will take a conversation with the employee(s) identified and in a non-judgemental way, and with a focus on supporting, help the employee(s) to understand the issues and adopt behaviours which will be more beneficial to themselves and the business.

***BCT 6.1 Demonstration of behaviour***

The Security Champion will ensure that they use and actively demonstrate the right behaviours so that those employees around them can actively learn the behaviours to use.

***BCT 13.1 Identify of self as a role model***

The Security Champion will be encouraged to see themselves as a role model who acts as an example to those around them.

## 4.3 The Pillars

The pillars contain the behavioural change actions that should be undertaken to provide the employees with the right level of additional support to act in such a way as to keep a secure environment in operation. The pillars are each given a broad description and remit, covering an area where multiple attack types may take place. This means that the pillar description should stay consistent whilst the contents of the pillars will develop and change as the cyber-criminal adapts and defines new and different ways to carry out cyber-attacks.

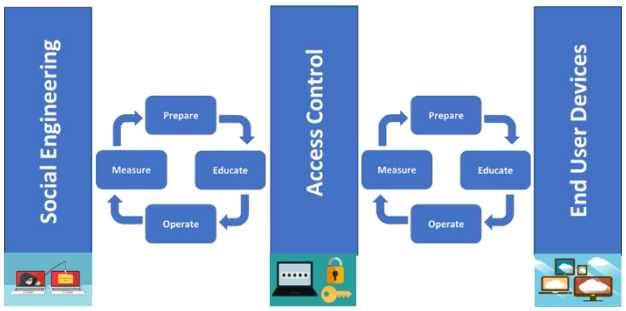



*Figure 7: The Pillars*

Three specific pillars were chosen after examining a range of online cyber security training applications available on the market and analysing the most common topics covered by these pieces of training. In this way, the framework should be flexible enough for SMEs to

choose from many awareness training options when actively building a proactive cyber security culture.

### 4.3.1 Social Engineering Pillar

The Social Engineering pillar contains actions designed to assist in implementing behavioural change techniques to support employees in taking the learnings from awareness training and operate with a higher level of digital hygiene that prevents social engineering attacks from being successful.

With the recent trend of cyber-criminals moving away from bulk sending of spam mail to a more sophisticated and targeted phishing mail [25], the need for educating secure behaviours for handling such scenarios has become even more prevalent.

Equally as concerning is the readiness of cyber-criminals to exploit world events such as the COVID pandemic [25].

Therefore, the following behaviour change techniques are identified to assist employees in gaining the correct behaviours to operate within the Social Engineering sphere:

**ACTIONS TO IMPLEMENT THE PREPARE PHASE**

***BCT 5.3 Information about social and economic consequences***

It is an important task of any process which requires a sustained change of behaviour, that the attendees understand the risks of performing poorly against these challenges. This does not mean using fear appeals, but rather treating the individuals with a level of trust and respect and allowing them to understand the challenges and persuade them that they can gain the skills to work effectively within the environment. Fogg described persuasion as an "attempt to change attitudes or behaviours or both (without using coercion or deception)" [10],

To build the required level of self-efficacy to make a behavioural change, a person needs to realise that there is a risk, know there are behaviours that will reduce this risk and finally realise they are themselves capable of carrying out these behaviours [10]. The educate BCT listed here tackles the first two elements of those topics. It informs of the risk in place and looks to create an environment where employees will be acceptable to make changes by informing that there are ways of operating that can be learned that will significantly reduce the risk.

***BCT 12.2 Restructure the social environment***

The requirements set in a security policy can be challenging and, at times, almost impossible for an employee to comply. In the situation of phishing attacks, if a user receives many legitimate emails containing links and attachments from within their own company, then opening these links becomes a normal work-related process. Therefore, it should not be surprising that a user may click the wrong link or open the wrong attachment.

To provide the employee with a better chance at being successful, the business should look at its working environment and remove (or at least significantly reduce) its use of technology targeted by the cybercriminal.

For example: instead of sending internal emails, the business could use secure apps to communicate between employees. It will be much more difficult for a cybercriminal to get security access to the App to contact employees via an internal source. It results that receiving any internal emails should immediately raise a warning to the employee.

The use of an App adds a level of security that does not exist in email. Anyone can open an email account and send an email. However, only those people given access to the corporate group within the App can communicate with employees, meaning that internal communications are generally more secure.

**ACTIONS TO IMPLEMENT THE EDUCATE PHASE**

***BCT 4.1 Instructions on how to perform the behaviour***

Within the prepare phase, the framework first educates the user on the risks that exist within the digital landscape. This was the start of helping a user build self-efficacy. They need to realise that there is a risk, know there are behaviours that will reduce this risk, and finally realise they can carry out these behaviours [10]. Within the Educate Phase, the framework looks to complete the final element of the three steps, teaching a user how to use the skills needed to carry out behaviours that will help them work within the rules of a security policy.

Such training is to be practical, allowing the employee to see precisely the behaviours and actions needed. Employees must be allowed to try out the skills learned in a safe and non-judgemental environment, with the support of the Security Champion available to ensure that questions are answered, and concerns are addressed.

**ACTIONS TO IMPLEMENT THE OPERATE PHASE**

Within the Operate Phase, the user will be encouraged to repeat the behaviours taught. Rewards will be offered for demonstrating the correct behaviours and sharing knowledge with colleagues to assist those colleagues in performing the behaviours.

***BCT 4.1 Instructions on how to perform the behaviour***

So that the business can get a clear understanding of the challenges presented via social engineering attacks and support employees in identifying these attacks, employees will be taught how to report a potential attack quickly and easily.

This activity links back to the Overarching Threat Intelligence process, where potential threats can be shared across the organisation, increasing awareness of the danger and providing employees with important information that allows them to be more successful in countering the threat.

Employees will be informed that they will not be reprimanded when reporting an attack where a link was accidentally clicked, or an attachment was accidentally opened. It is critical

to the business that these scenarios are reported as soon as possible to reduce the possibility of further damage. The Security Champion must provide a non-judgemental persona to all employees to ensure that employees do not feel concerned about reporting in this situation.

***BCT 10.1 Material incentive***

So that employees feel further encouraged to carry out the behaviour of reporting attacks, an incentive is to be planned monthly, based on a few possible criteria such as:

- Most reports of potential social media attacks
- The employee who caught the most dangerous potential attack
- The employee who assisted colleagues the most in preventing an attack

The reward is communicated to all employees to demonstrate the ongoing value placed by the business on the reporting action.

***BCT 10.4 Social reward***

As well as providing a material incentive, the business will emphasise to employees the value of community in keeping colleagues secure by notifying them of attacks that could impact them negatively. Such an approach will strengthen the security culture across the organisation by having employees acting as role models and mentors for each other and understanding the value of their actions to colleagues and the business when reporting attacks.

**ACTIONS TO IMPLEMENT THE REPORT PHASE**

***BCT 2.7 Feedback on outcomes and behaviours***

So that employees continue to use the correct behaviours, statistics on the value of the process are to be published each month. Statistics are gathered from the Overarching Threat Intelligence process and relate to the data reported by employees.

Statistics are to be evaluated by the Security Champion. Any amendments needed to the framework based on the learnings are directed back into the 'Prepare' phase so that the lifecycle supports the preparing, educating, and operating of the new change.

### 4.3.2 Access Control Pillar

The Access Control pillar contains actions designed to assist in implementing behavioural change techniques to support employees in taking the learnings from awareness training and have those employees then operating with a higher level of digital hygiene that prevents cyber-criminals from gaining information that would allow them to access accounts using the user's credentials.

Although identifying facts about the level of password hygiene is difficult because passwords are stored securely and so cannot be analysed, research is showing that large

numbers of users do not use the recommended guidelines for managing passwords [26] [36] [63].

The behaviour-change techniques identified are as follows:

**ACTIONS TO IMPLEMENT THE PREPARE PHASE**

***BCT 5.3 Information about social and economic consequences***

Just as in the Social Engineering pillar, the same need applies to prepare employees as to the task by explaining the challenges and the risks to the business of poor cyber security behaviour when controlling the access to digital devices.

To build the required level of self-efficacy to make a behavioural change, a person needs to realise that there is a risk, know there are behaviours that will reduce this risk and finally know they are themselves capable of carrying out these behaviours [10]. The Educate BCT listed here tackles the first two elements of those topics. It informs clearly of the risk in place of not securing access to personal and business devices and looks to create an environment where employees will be acceptable to make changes by informing those employees that there are ways of operating that can be learned and used which will significantly reduce the risk of their devices being compromised.

***BCT 12.2 Restructure the social environment***

The requirements set upon employees to adhere to when operating a secure behaviour can be challenging and, at times, almost impossible to comply with. In the situation of password security, a user is recommended to have a different password for each system/service they use, which is more than ten characters in length, containing no words or phrases that could be linked back to them [47]. The estimates on the average number of passwords used per person seem to vary, with claims from 27 to over 100 per individual. Whatever the true figure, the average employee, will simply not be able to remember all their passwords. It should, therefore, not be surprising that a user will write down passwords as a method of remembering them.

To give the user a much better chance at success in this situation, the business should look at its working environment and provide tools that help the employees to achieve the security requirements. In the case of password management, the business should investigate providing password management software to employees, which they could use for both business machines and personal machines. The argument that the business supports non-business systems is that by supporting a user to increase both the business and personal cyber-security, their general digital hygiene will improve across the board, and such an increase only benefits the business [50].

**ACTIONS TO IMPLEMENT THE EDUCATE PHASE**

***BCT 4.1 Instructions on how to perform the behaviour***

Training is provided, which demonstrates the steps that a user should take to secure their end-user devices. This training is dependent on the tools available. For example, if Password

managers have been provided, the training will instruct how to successfully use these. If Password Managers are not available, training will be given to best equip a user on how to use and manage passwords manually. The training should be supported by the Security Champion, who is available to give practical demonstrations and answer any question due to the non-judgemental environment that is being fostered.

**ACTIONS TO IMPLEMENT THE OPERATE PHASE**

Within the Operate Phase, the user will be encouraged to repeat the behaviours taught and will be offered rewards for demonstrating the behaviours and sharing knowledge with colleagues to assist those colleagues in also performing the behaviours.

***BCT 4.1 Instructions on how to perform the behaviour***

So that the business can get a clear understanding of the challenges presented via unauthorised access attacks and support employees in identifying these attacks, the employees will be taught how to report a potential attack quickly and easily.

This activity links back to the Overarching Threat Intelligence process, where potential threats can be shared across the organisation, increasing awareness of the danger and enabling employees with more information, allowing them to be more successful in countering the threat. Employees are informed that they will not be judged and reprimanded for reporting an attack where the employee has accidentally provided someone else access to their device or computer system. These scenarios must be reported as soon as possible to reduce the possibility of damage. The Security Champion must provide a non-judgemental persona to all employees to ensure that they do not feel concerned about reporting in this situation.

***BCT 10.1 Material incentive***

So that employees feel further encouraged to carry out the behaviour of reporting attacks, an incentive is to be planned monthly, based on a few possible criteria such as:

- Most reports of potential access control attacks
- The employee who caught the most dangerous potential attack
- The employee who assisted colleagues in preventing an attack

Rewards are communicated to all employees to demonstrate the ongoing value placed by the business on the reporting action.

***BCT 10.4 Social reward***

As well as providing a material incentive, the business will emphasise to employees the value of community in keeping colleagues secure by notifying them of attacks that could impact them negatively. Such an approach strengthens the security culture across the organisation by having employees acting as role models and mentors for each other and understanding the value of their actions to colleagues and the business when reporting attacks.

**ACTIONS TO IMPLEMENT THE REPORT PHASE**

***BCT 2.7 Feedback on outcomes and behaviours***

So that employees continue to use the correct behaviours, statistics on the value of the process are to be published each month. Statistics are gathered from the Overarching Threat Intelligence process and relate to the data reported by employees.

Statistics are to be evaluated by the Security Champion. Any amendments needed to the framework based on the learnings are directed back into the 'Prepare' phase so that the lifecycle supports the preparing, educating, and operating of the new change.

### 4.3.3 End-User Devices Pillar

The End-User Devices pillar contains actions designed to assist in implementing behavioural change techniques to prevent cyber-criminals from using employees' personal devices to attack the individual or the business.

The Pillar focuses on behaviours that encourage and support employees to keep their personal devices updated and secure. An employee's digital hygiene should be consistent across all their devices to ensure they use behaviours that are always secure.

The behaviour-change techniques identified are as follows:

**ACTIONS TO IMPLEMENT THE PREPARE PHASE**

***BCT 5.3 Information about social and economic consequences***

Just as in the previous pillars, the same need applies to prepare employees for the task by explaining the challenges and the risks to the business of poor cyber security when operating their own end-user devices.

To build the required level of self-efficacy to make a behavioural change, a person needs to realise that there is a risk, know there are behaviours that will reduce this risk and finally realise they are themselves capable of carrying out these behaviours [10]. The Educate BCT listed here tackles the first two elements of those topics. It informs of the risk of using personal devices that are not operating the latest security software and patches. It also creates an environment where employees should be acceptable to make changes by informing them that there are ways of working that can be learned and used which will significantly reduce the risk to their personal devices.

***BCT 12.5 Adding objects to the environment***

It is within the benefit of the business to ensure that its employees operate all digital devices with an understanding of keeping them secure, thus increasing their overall digital hygiene.

As the process of keeping devices up to date may seem daunting to a non-technical employee, the business should look to provide tools and techniques that make this process

easier, automating where possible and supporting the user so that they feel in control of the process.

**ACTIONS TO IMPLEMENT THE EDUCATE PHASE**

***BCT 4.1 Instructions on how to perform the behaviour***

Operating system manufacturers push regular security updates to devices such as phones, tablets, and computers. However, the user decides whether the device is updated automatically. This means that employees could be operating end-user devices which are not protected against cyber-attack.

The Security Champion will explain the risks of running old device software and educate employees on how to change settings so that devices are automatically updated. These instructions will be given for the most common operating systems run on personal devices such as Apple, Android and Microsoft.

**ACTIONS TO IMPLEMENT THE OPERATE PHASE**

***7.1 Prompts/cues***

Although operating system suppliers such as Apple, Android and Microsoft publish information regarding the availability of new updates, there is a reliance that user settings allow automatic updates. Also, many of the security issues resolved by a software update are vague in detail, as software providers appear less keen to publicise the information. For example, Apple will not list a vulnerability in its top list of software changes made within a release, requiring employees to scroll further down the page to reveal the security issues [64]. Therefore, to find the information relevant to keep employees adequately informed of the risk, the Security Champion should follow the social media accounts of security firms who issue reports on the patching issues and the dangers of the vulnerability fixed by the patch.

The Security Champion should then inform employees of the risk and prompt employees (who have not set automatic updates) to install the latest patch to ensure they stay protected.

**ACTIONS TO IMPLEMENT THE REPORT PHASE**

***5.3 Information about the social and environmental consequences***

As devices are personal, it will not be possible to report in the same way as within the other pillars as to the number of potential attacks. However, if a successful attack is linked to an employee's insecure device, that information will be reported to demonstrate the ongoing risk to individuals and the business. Reporting should not name and shame individuals. Personal data is kept private so as not to create fear amongst employees that they will be publicly named.

## 4.4 The Overarching Support Functions

Overarching functions are designed to [35] work with the pillar functions to provide additional support that increases the level of proactive security culture.

*Figure 8: Overarching Functions*

### 4.4.1 Threat Intelligence

The Threat Intelligence pillar contains actions designed to assist in implementing behavioural change techniques to support employees in reporting threat intelligence information which is shared with all employees across the business. This ensures that employees are fully aware of any potential attacks taking place and are therefore more alert to the situation

**ACTIONS TO IMPLEMENT THREAT INTELLIGENCE**

***12.1 Restructuring the physical environment***

So that employees feel empowered and able to report threat intelligence, the business should implement an easy-to-use tool. This tool will enable an employee to quickly log and send details of the threat information to the relevant person(s), who can assess the information and decide on the best course of action.

***5.3 Information about social and economic consequences***

To create the needed “buy-in” to use the reporting tool, employees will be educated about the benefits for both individuals and the business in having suspected cyber-attacks reported to a central location. Therefore, the risks of not sharing such information must be presented. This must not be done using scare tactics but instead presented in a way designed to make the employee feel empowered by receiving the knowledge.

***4.1 Instructions on how to perform the behaviour***

Practical training is given to help the user master the steps needed to report an identified potential attack. Training is delivered by the Security Champion, who can continue to sell the benefits of the process, answer questions and offer support.

**ACTIONS TO OPERATE THREAT INTELLIGENCE**

***2.7 Feedback on outcomes of behaviour***

When a potential attack is reported, the Security Champion (or IT security professional) will make a quick analysis of the report. Information that gives other employees a better understanding of a potential cyber-attack will be shared across the business.

# Chapter 5: Evaluation

## 5.1 Overview

Within this chapter, the results of the qualitative feedback from industry experts currently working in the cyber-security field, are summarised, and discussed. The detailed results are available to read in Appendix 8.

## 5.2 Analysis of Expert Feedback

The qualitative feedback received is summarised against each question asked:

**Question 1)** ***Are there any elements (foundation layers, pillars, or overarching process) which you do not believe would add enough value to make the implementation of that element worthwhile for an SME?***

The feedback was that all the elements included would have an impact and that no elements should be removed. However, one respondent required more detail, whilst another respondent needed more information on the continual service improvement element of the framework.

**Question 2)** ***Are there any sub-elements (specific behaviour change techniques within each element) that you do not believe would add enough value to warrant implementing?***

The feedback was that the sub-elements (behaviour change techniques) were valid for use, but further detail was needed to be able to give a true reflection of value. There was a further request for additional change techniques to cover the continual improvement topic.

**Question 3)** ***From your experience, are there any activities missing within the framework which could further assist an SME to change user behaviour to build a stronger security culture?***

The feedback stated that it should be investigated whether an initial study of the SME should first take place to ascertain the culture before implementing the framework. Any specific behaviours needs should then be targeted. It was also pointed out that the framework should be aligned to the SME business objectives and security goals. Additional feedback highlighted a greater need for the framework to clearly show how it can adapt to a changing world where cyber-attacks develop and change.

***Question 4) As security professionals, when assessing where limited budgets should be spent, do you believe that investing into the changing of user behaviour towards a more positive security culture is: (please choose one option)***

a) ***Less important than investing in technical solutions that counter cyber-attacks***
b) ***Equally as important as investing in technical solutions that counter cyber-attacks***

***c) More important than technical solutions that counter cyber-attacks***

The feedback here was split between “Equally as important” and “More important”. Arguments for more important being that around 90% of data breaches coming from human error, and therefore statistically, this is the “critical” area to be addressed.

Arguments for equal importance are based on the view that even with excellent training and strong behavioural support, a human cannot make the right decision 100% of the time and will still make a mistake that creates an entry point into the system. Therefore, a technical solution is equally important to mitigate the risk.

***Question 5) This model focuses on a user's digital behaviour at home and in the office, as it is perceived that a user's digital hygiene should be at an equal level for both so that the user operates a consistently high level of digital hygiene.***

***From your knowledge as security professionals and working with SMEs, do you believe that:***

***a) The concept of encouraging a user into operating a higher level of security at home would have a positive impact on overall cyber-security for the business (Yes/No)***

***a) An SME is potentially willing to invest in offering its employees help in acquiring and setting up tools for home use, like what they already provide for business end-user devices (e.g., VPN, Password Managers etc.) (Yes/No)***

Respondents agreed that the concept of employees operating a higher level of security (digital hygiene) at home would have a positive impact on the cyber-security of the business.

However, there was a disagreement about whether SMEs would be willing to invest in supporting their employees in the right tools to support end-user home devices.

***Question 6) Any other thoughts or ideas that you have considered in reviewing the framework, which you believe would be useful feedback and has not been covered in this short questionnaire?***

One respondent suggested identifying a value-add element that could sell the additional benefits to the SME for taking on this framework. One idea is to align the framework with industry standards such as the five modules of Cyber Essentials [65].

They also touched again on the use of language, linking back to the argument that it is important to know the organisation's existing culture when implementing such a framework.

## 5.3 Evaluation and Discussion

The following evaluations were made after examining the qualitative feedback provided:

***Question 1 – Elements that do not add value***

Focus was given on the need for the framework to be fit to adapt to the changing cyber-security landscape through a process of continual service improvement. Whilst the model was built with the concept of **"Prepare, Educate, Operate, Measure",** allowing measurements of operation to be taken and lessons learned fed back into the prepare stage, this was not well enough described and lacked some behaviour change techniques within the framework to facilitate this. Therefore, the framework needs to be reviewed and updated with the required change techniques which adequately describe and manage the continual improvement process.

***Question 2 – Sub-elements that do not add value***

The idea of creating mandatory and optional behavioural change techniques based on the culture of the business is an interesting challenge. Such a task would require a much greater knowledge of cultures and how to best adapt to that culture to establish the needed behaviours. The concept of the framework was that it was a one-size-fits-all (SME) business. However, that does not mean that it should not be flexible to fit business cultures better where relevant. When reviewing the behavioural change techniques identified in the framework, it can be argued that the two foundation elements (The Top Senior Management Sponsor and the Security Champion) would be the right people to review and the culture of the business and set their delivery of the framework to fit with the culture. The framework can be updated so that Top Management Sponsor and Security Champion BCTs require these individuals to consider the business culture when taking action. Further research should occur to see if the idea of mandatory and optional BCTs makes sense based on business culture.

***Question 3 – Missing activities***

The feedback states the need to ensure that continual service improvement is carried out so that the framework stays relevant and fit for purpose. Secondly, that BCTs are used that continually "nudge" the user to the right behaviour. The framework needs to be updated to cater for this feedback by examining and including more "nudge" behaviour change techniques from the Behaviour Change Wheel.

***Question 4 – How important is changing security behaviours vs technical solutions***

The feedback from security professionals' points to the belief that a business must focus equally if not more on the way its employees behave when using IT systems (the human layer) as they do on implementing technical solutions to prevent cyber-attacks (the technical layer). This position is supported by academics who argue that an SME should first make its employees more resilient [63].

Research also argues that some SMEs focus on technical measures that are easy to implement, and a gap may be growing between the security put in place and the risks that the business is facing [66]. As SMEs have more limited knowledge of cyber-security and fewer resources who are skilled and able to manage the issue, the process of defining valid risks and mitigations will become less meaningful [66], and the overall risk of a successful attack will become higher.

Future research is needed to identify what methods can be used to assist an SME in understanding the risks and allocating the right time, resources, and money into ensuring that their level of cyber security is sufficient.

***Question 5 – Employees' home security behaviour to increase digital hygiene***

Security professionals agree that improving the employees' digital hygiene at home as well as in the office will lead to more secure business computing. Some strong arguments given to support this view were that since the COVID pandemic forced people to work from home, there is an expected lightening of the rules across many businesses for where an employee can work from, meaning that home offices will become more common in the future. The UK Government is currently proposing a law to allow all new employees to request a flexible working arrangement on the first day of their employment [67]. With employees creating offices at home and working from cafes, there is an opportunity for cyber-criminals to modify their attacks to exploit items such as the weaknesses in home routers to hack into a secure business system.

The professionals differ in their view as to whether an SME will be prepared to invest time and money into ensuring that personal end-user devices are kept secure. The key point is whether the SME can make a connection between home working and the risk to the business systems. If the risk is understood, and the benefits of home working outweigh the cost of helping to secure user devices, then there is a view that the SME may support the move.

***Question 6 – Other thoughts and ideas not covered in previous questions***

One answer to question 6 focused on the possibility of aligning the framework with a standard such as Cyber Essentials. Such an alignment could demonstrate to an SME the added value that utilising the framework could have in gaining CE certification. Looking at the 5 Cyber Essentials modules, it becomes challenging to make a clean connection with the framework as Cyber Essentials is more technology-focused and concentrates on the "technical layer" of cyber security whilst the framework focuses on the "human layer". This raises a topic that will be discussed in the Conclusion chapter. If over 90% of breaches have occurred due to human error, should Cyber Essentials be modified to introduce a 6$^{th}$ module that focuses on the activities needed to secure the human layer?

## 5.4 Summary

There is consensus within the answers given by the security experts that utilising a human layer of security within an SME will increase the overall security of that business. With over 90% of security breaches reported from human error [68], the statistics show a need for a framework that implements and maintains security behaviours that increase employee's digital hygiene and support a proactive security culture.

However, persuading an SME to invest time, resources, and money into implementing and operating a framework that focuses on behaviour change will be challenging. The SME will find it hard to quantify the benefits [66], [69]. There is a need for a strong justification that an SME can fully buy into because there is a value to the framework that becomes tangible in a value such as money saved, customers won, or business increased.

A standard method would be to identify and quantify the risk and then calculate the return on investment (ROI) or return on security investment (ROSI). Such an approach would help to prove the value of an effective human layer that supports a strong security culture. However, research shows that many SMEs lack the skilled resources, knowledge and/or understanding of cyber risk that would allow a meaningful ROI calculation [66]. SMEs, therefore, are unlikely to use such a method.

Cyber security in large businesses is fast becoming a board-level topic [70], with Governmental documentation available to facilitate the process [71]. However, SMEs do not tend to have such boards. Therefore, it is important to investigate where a push for adherence to secure cyber practices could come. There are potentially two approaches that can focus on the need to adhere to a standard framework for cyber security compliance. These are [72]:

- A need to comply with market forces
- A need to comply with supply chain demands

It can be viewed as a "*market failure*" that so few SMEs have taken some form of cyber-security certification. The supply chain element is slowly beginning to take hold as SMEs understand that to do business within a supply chain, there is a growing need to prove some form of security compliance [72].

Therefore, the following options are identified as a method to attract SMEs to invest time into the human layer framework:

### 5.4.1 Using certification to push a positive cyber-security culture framework

Within the answers provided to the questionnaire, one security expert suggested tying to tie elements of the framework to Cyber Essentials (CE), a UK Government-backed certification launched in 2014 [65] specifically focused on SMEs. CE is designed around five controls:

1. *Boundary firewalls and internet gateways*

2. *Secure configuration*
3. *Access control*
4. *Malware protection*
5. *Patch management*

Once an SME can demonstrate adequate protection for each of the five controls, they gain the CE certification. Implementing these technical controls certainly makes the SME more secure. However, what the certification does not provide is an implementation of the human layer. Cyb Safe published an analysis that showed that over 90% of data breaches occur due to human error [68]. A government-sponsored project showed that whilst Cyber Essentials is strong on providing the technical layer when dealing with remote exploits; there is a gap regarding insider threats, whether malicious or accidental [73]. As the framework is behavioural-based, it becomes difficult to map the framework to the CE technical controls. Therefore, it can be argued that CE is missing a 6$^{th}$ control – the human layer control required for a proactive cyber-security culture.

The UK Government sets up CE to be attractive to SMEs by offering the ability to strengthen their security against cyber-attack and gain a recognised certification without the need to spend large sums of money on cyber-security practices [74]. Suppose CE was to be modified to provide a 6th control that supports the delivery of a simple framework for developing a human layer that delivers a robust cyber-security culture. In that case, the SME could benefit further from CE certification, having addressed security concerns regarding the 90% of breaches that currently happen via that human layer.

### 5.4.2 Utilise the Supply Chains to request CE certification

As supply chains are only as strong as their weakest point, it is becoming more common for an SME to demonstrate some form of cyber-security certification when tendering a bid for a supply chain contract [75]. This stance is therefore pushing more SMEs to gain certification. If CE were modified to include the 6$^{th}$ control for the human layer, more SMEs operating within the supply chain would by default implement a basic framework that supports a positive cyber-security culture. Education is needed for supply chain owners to understand better the benefits of a human layer of defence operating within the SMEs who support their supply chains.

### 5.4.3 Utilise the Insurance Industry to request CE certification

Leading from the United States is the concept of cyber liability insurance. As more businesses see a need to take out this type of insurance to protect themselves from losses relating to a cyber-attack, the companies who offer the insurance may offer discounts or cheaper rates for SMEs that gain a form of certification to prove their cyber security credentials [72].

If the discount leads to a significant saving, then there is a simple, straightforward, and easy to understand business case for the SME to work. Suppose Insurance Companies were canvased to adopt a standard certification such as CE and used CE certification as the tool for offering SMEs discounts on insurance. In that case, Insurers could help increase cyber-security within SMEs whilst lowering their risk and exposure to future claims [72].

# Chapter 6: Conclusion

## 6.1 Conclusion

In this project, a framework was designed and built to assist SMEs in creating a positive cyber-culture that would further protect their businesses via a human layer of cyber-security. The framework was constructed using behaviour change techniques taken from the Behaviour Change Wheel. Industry experts provided feedback on the suitability of the framework in changing security behaviours and the suitability for SMEs to implement the techniques in the framework. The main findings are a shared belief that building a human layer of security that maintains a positive security culture is very important for SMEs and that using behavioural change techniques should support the behavioural change needed. However, it will be challenging to persuade SMEs to invest the time, money and resources required to implement and operate the framework. The project, therefore, makes recommendations on building the framework into an existing certification process such as Cyber Essentials and then influencing supply chain owners and insurers to promote certification as a positive (and needed) step in conducting business in the UK.

## 6.2 Limitations and future work

The framework evaluation shows that to make a human layer framework attractive to SMEs, there will be a need for incorporating the framework into an existing certification where the SME gains significant value from holding that certification.

For this framework to be suitable for implementation as part of a cyber-security certification, it needs to be reviewed and simplified in scope. The three Pillar documents share the same behaviour change techniques. A single generic pillar document could be produced that could be easily adapted to support each of the awareness training provided to employees. The Pillar documents reinforce the learnings of awareness training. They will often change to meet the changing landscape of cyber-attacks, so a more simplified, generic model would fit this scenario.

A certification scheme needs to be identified where the owner would see the value of extending the certification to include a human layer security element alongside the existing technical layer security.

## 6.3 Reflections

From my 28 years working within Information Technology, I have already gained extensive experience in delivering projects. What has been significantly different within this experience is the requirement to research a topic properly and thoroughly via academic papers to understand better the data existing. Having the time to study in this way initially

felt like a luxury and something that would potentially slow down the delivery of the final solution. However, the learnings from the research phase were hugely beneficial in framing the final solution. The learnings also provide the knowledge required to fully justify and argue why decisions were made, resulting in a more significant justification of the final product. When viewing the Design Science [38] method, the first stage of "Identify the problem" allows the use of much deeper research to correctly identify and understand the problem that is trying to be solved. The second stage continues the approach by defining a solution using the knowledge gained via the first stage. Time spent in the first two stages should pay back during the development stage if the research ensures a higher quality artefact is being built and delivered, and limited re-working is required. On returning to the workplace, where time pressures often means more focus on delivery than research, I shall ensure that I argue for the time necessary to properly research a topic before planning and implementing the final product.

I have needed to educate myself on the method required for writing an academic thesis. Writing such a document is quite different from how I have written business documents in the past. I had never written a dissertation before, so there was a steep learning curve to ensure that I delivered the dissertation in an acceptable format. I have a better understating of how a dissertation is delivered. However, I believe that the style does not support those who respond to visual queues (a more significant portion of the population).

Developing a finished framework within twelve weeks proved to be a more significant challenge than first expected. Multiple iterations will be needed before it is ready to be presented to an SME for a live trial. This project managed the first iteration with qualitative feedback.

For each additional iteration, there will be the need to get a larger number of experts to give their feedback. It is challenging for the experts to make time for this type of project, and so project timeframes will extend for each iteration.

# References


[1] Bitdefender, “2020 consumer landscape report,” Bitdefender, 2020.

[2] m. c. a. s. Department of digital, “Cyber Security Breaches Survey 2020,” 2020. [Online]. Available: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020.

[3] J. Scheeres, “Establishing the human firewall: reducing an individual's vulnerability to social engineering attacks,” Air force institute of technology, 2008.

[4] J. McAlaney, J. Taylor and H. Thakray, “Behaviour Change: Cybersecurity,” The British Psychological Society.

[5] J. Taylor-jackson, J. McAlaney, A. Bello, A. Maurushat and J. Dale, “Incorporating Psychology into CyberSecurity Education : A Pedagogical Approach,” in *AsiaUSEC'20, Financial Cryptography and Data Security*, Kota Kinabalu, 2020.

[6] Verizon, “2021 Data breach investigations report - Executive Summary,” Verizon, 2021.

[7] Gartner, “Gartner Says Global IT Spending to Decline 8% in 2020 Due to Impact of COVID-19,” Gartner, 13 May 2020. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2020-05-13-gartner-says-global-it-spending-to-decline-8-percent-in-2020-due-to-impact-of-covid19.

[8] T. Caldwell, “Making security awareness training work,” *Computer fraud and security,* pp. 8 - 14, 2016.

[9] K. McCrohan, K. Engel and J. Harvey, “Influence of Awareness and Training on Cyber Security,” *Journal of Internet Commerce,* pp. 23-41, 2010.

[10] M. Bada and A. Sasse, “Cyber Security Awareness Campaigns - Why do they fail to change behaviour?,” Global cyber security capacity centre, 2014.

[11] K. Renaud, “Blaming Noncompliance Is Too Convenient : What really causes information breaches,” IEEE Computer and Reliability Societies, 2012.

[12] Y. Cherdantseva, “Cybersecurity Investment Decision Making - A best practice guide for SMEs,” Cardiff University, 2021.

[13] S. Sheng, M. Lanyon, P. Kumaraguru and L. Cranor, “Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions,” in *Proceedings of the 28th International Conference on Human Factors in Computing Systems*, Atlanta, 2010.

[14] S. Michie, M. Richardson, M. Johnston, C. Abraham, J. Francis, W. Hardeman, M. Eccles, J. Cane and C. Wood, “The Behavior Change Technique Taxonomy (v1) of 93 Hierarchically Clustered Techniques: Building an International Consensus for the Reporting of Behavior Change Interventions,” *Annals of Behavioural Medicine,* vol. 46, pp. 81-95, 2013.

[15] K. Renaud and M. Dupuis, “Cyber Security Fear Appeals: Unexpectedly Complicated,” NSPW 19, 2019.

[16] Zurich, “As many as 875,000 UK SMEs suffer cyber security breach in the last 12 months,” Zurich, 1 August 2017. [Online]. Available: https://www.zurich.co.uk/en/about-us/media-centre/general-insurance-news/2017/as-many-as-875000-uk-smes-suffer-cyber-security-breach-in-the-last-12-months.

[17] M. Heidt, J. Gerlach and P. Buxmann, “Investigating the security divide between SME and large companies : How SME characteristics influence organisational IT security investments,” *Information System Frontiers,* vol. 21, pp. 1285 - 1305, 2019.

[18] I. C. Office, “Data security incident trends,” 2021. [Online]. Available: https://ico.org.uk/action-weve-taken/data-security-incident-trends/.

[19] C. Nobles, “Botching human factors in cybersecurity in business organizations,” *Holista - Journal of business and public administration,* pp. 71-88, 2018.

[20] G. Dhillion and J. Blackhouse, “Current directions in IS security research: towards socio-organizational perspectives,” *Information Systems Journal,* vol. 11, pp. 127-153, 2001.

[21] M. Eminagao, E. Uc¸ar and S. Eren, “The positive outcomes of information security awareness - a case study,” Elsevier, 2010.

[22] A. Da Veiga and N. Martins, “Information security culture and information protection culture: A validated assessment instrument,” *Computer law and security review,* vol. 31, pp. 243-256, 2015.

[23] M. M. Al-Daeef, N. Basir and M. M. Saudi, “Security awareness training : A review,” in *World congress on engineering* , London, 2017.

[24] J. Parrish, J. Bailey and J. Courtney, “A Personality Based Model for Determining Susceptibility to Phishing Attacks,” University of Arkensas, 2009.

[25] A. Bhardwaj, V. Sapra, N. Kumar and A. S, “Why is phishing still successful?,” *Computer and fraud security,* vol. 2020, no. 9, pp. 15 - 19, 2020.

[26] C. Happ, A. Melzer and G. Steffgen, “Trick with treat - Reciprocity increases the willigness to communicate personal data,” *Computers in human behaviour,* vol. 61, pp. 372-377, 2016.

[27] B. Parmar, “Protecting against spear phishing,” *Computer fraud and security,* pp. 8 - 11, 2012.

[28] M. Bossetta, “The weaponisation of social media: Spear phishing and cyberattacks on democracy,” *Journal of International Affairs,* vol. 71, no. 1.5, pp. 97-106, 2018.

[29] E. Orti-Ospina, “Our world in data,” Global Change Data Lab, 19 September 2019. [Online]. Available: https://ourworldindata.org/rise-of-social-media.

[30] M. Zuckerberg, “Understanding Facebook’s Business Model,” Facebook, January 2019. [Online]. Available: https://about.fb.com/news/2019/01/understanding-facebooks-business-model/.

[31] Cyveillance, *The impact if social media on information security,* Cyveillance, 2015.

[32] M. Shafahi, L. Kempers and H. Afsarmanesh, “Phishing through social bots on twitter,” in *2016 IEEE International conference on big data*, Washington, 2016.

[33] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams and A. Hahn, “NIST: Guide to Industrial Control Systems (ICS) Security,” [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.

[34] IBM, “IBM 2015 Cyber Security Intelligence Index,” IBM, 2015.

[35] H. W. Glaspie and W. Karowski, “Human factors in Information Security Culture: A Literature Review,” Springer International Publishing, 2018.

[36] K. H. Guo, “Security related behaviour in using information systems in the workplace: A review and synthesis,” *Computers and security,* vol. 32, pp. 242-251, 2013.

[37] K. Aytes and T. Connolly, “Computer security and risky computer practices: A rational choice perspective,” *Journal of organizational and end user computing,* no. Jul-Sep, pp. 22 - 40, 2004.

[38] K. Peffers, T. Tuunanen and M. Rothenberger, “A Design Science Research Methodology for Information Systems Research,” *Journal of Management Information Systems,* vol. 24, no. 3, pp. 45 - 78, 2008.

[39] A. Alhogail and A. Mirza, “A framework for Information Security Culture Change,” *Journal of theoretical and applied information technology,* vol. 64, 2014.

[40] T. Papadopoulos, K. N. Baltas and M. E. Balta, “The use of digital technologies by small and medium enterprises during COVID19: Implications for theory and practice,” *International Journal of Information Management,* vol. 55, 2020.

[41] M. Siponen, “A conceptual foundation for organizational information security awareness,” *Information Management and Compuuter Security,* pp. 31 - 41, 2000.

[42] N. I. o. S. a. Technology, “Building an Information Technology Security Awareness and Training Program,” NIST Special Publications 800-50, 2003.

[43] I. C. Office, “A practical guide to IT security. Ideal for the small business,” Information Commissioner's Office, 2016.

[44] National Cyber Security Centre, “NCSC Certified Training,” March 2019. [Online]. Available: https://www.ncsc.gov.uk/information/certified-training.

[45] C. o. B. B. Bureaus, “2017 State of Cybersecurity Amongst Small Businesses in North America,” Council of Better Business Bureaus, 2017.

[46] M. Zwilling, G. Klien, D. Lesjak, L. Wiechetek, F. Cetin and H. N. Basim, “Cyber security awareness: A comparative study,” *Journal of computer information systems,* 2020.

[47] information commissioners office, “Passwords in online services,” ICO, [Online]. Available: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/passwords-in-online-services/.

[48] M. Zviran and W. Haga , “Cognitive passwords: The key to easy access control,” *Computers and Security,* vol. 9, pp. 723 - 736, 1990.

[49] M. Mannan and P. van Oorchot, “Digital objects as passwords,” Carleton University, Canada, 2008.

[50] European Union Agency for Information Security (ENISA), “Cyber Security Culture in organisations,” ENISA, Haraklion, 2017.

[51] R. West and S. Michie, “A brief introduction to the COM-B Model of behaviour and the PRIME Theory of motivation,” Qeios, 2020.

[52] S. Michie and R. West, “A brief introduction to the COM-B Model of behaviour and the prime theory of motivation,” Qeios, 2020.

[53] C. Dictionary, “Cambridge Dictionary,” 2021. [Online]. Available: https://dictionary.cambridge.org/dictionary/english/coercion.

[54] K. Renaud, M. Dupuis and S. Flowerday, “Moving from employee compliance to employee success in the cyber security domain,” Computer fraud and security, 2021.

[55] National Cyber Security Centre, “Top tips for staff,” National Cyber Security Centre, 2021. [Online]. Available: https://www.ncsc.gov.uk/training/top-tips-for-staff-scorm-v2/scormcontent/index.html#/.

[56] R. Young and E. Jordan, “Top management support: Mantra or necessity?,” *International Journal of Project Management,* vol. 26, pp. 713-725, 2008.

[57] J. T. Garrity, “Top Management and Computer Profits,” *Harvard Business Review,* vol. 41, pp. 6 - 13, 1963.

[58] B. Standards, “ISO/IEC 27001:2017 Information technology - Security techniques - Information security management systems,” BSI Standards Publication, 2017.

[59] D. Ashended, “Information Security Management: A human challenge,” Elsevier, 2009.

[60] B. Uchendu, J. Nurse, M. Bada and S. Furnell, “Developing a cyber security culture: Current practices and future needs,” *Computers and Security,* vol. 109, 2021.

[61] S. Moramarco, “What is a security champion? Definition, necessity and employee empowerment,” INFOSEC, 15 April 2021. [Online]. Available: https://resources.infosecinstitute.com/topic/what-is-a-security-champion-definition-necessity-and-employee-empowerment/. [Accessed 06 August 2021].

[62] M. Alshaikh, “Developing cyber security culture to influence employee behaviour: A practice perspective,” *Computers and security,* vol. 98, 2020.

[63] K. Renaud, “How small business struggle with security advice,” *Computer fraud and security,* pp. 10-19, August 2016.

[64] N. Mott, “Apple continues to hide its rotten security from consumers,” Pando Media, 14 February 2014. [Online]. Available: https://pando.com/2014/02/27/apple-continues-to-hide-its-rotten-security-from-consumers/.

[65] National Cyber Security Centre, “Cyber Essentials,” nsc.gov.uk, 2021. [Online]. Available: https://www.ncsc.gov.uk/cyberessentials/overview.

[66] E. Osborn and A. Simpson, “Risk and the Small-Scale Cyber Security Decision Making Dialogue - a UK Case Study,” *The Computer Journal : Security in Computer Systems and Networks,* vol. 61, no. 4, pp. 472 - 495, 2018.

[67] BBC, “Staff to gain right to request flexible working from first day,” BBC, 21 September 2021. [Online]. Available: https://www.bbc.co.uk/news/business-58636439.

[68] Cyb Safe, “Human error to blame for 9 in 10 UK cyber data breaches in 2019,” Cyb Safe, 2019. [Online]. Available: https://www.cybsafe.com/press-releases/human-error-to-blame-for-9-in-10-uk-cyber-data-breaches-in-2019/.

[69] M. Heidt, J. Gerlach and P. Buxmann, “Investigating the security divide between SME and Large Companies : How SME characteristics influence organisational IT security investments,” *Information Systems Frontiers,* vol. 21, pp. 1285-1305, 9 November 2019.

[70] Gartner, “Gartner Predicts 40% of Boards Will Have a Dedicated Cybersecurity Committee by 2025,” 28 January 2021. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2021-01-28-gartner-predicts-40--of-boards-will-have-a-dedicated-.

[71] National Cyber Security Centre, “Questions for boards to ask about cybersecurity,” National Cyber Security Centre, 2020.

[72] R. Henson and D. Sutcliffe, “An insurance-based approach to improving SME cyber security,” 2017.

[73] J. Such, P. Ciholas, A. Rashid, J. Vidler and T. Seabrook, “Basic Cyber Hygiene: Does it work?,” IEEE Computer Society, 2019.

[74] L. Irwin, “How Much Does Cyber Essentials Cost in 2021?,” IT Governance, 25th March 2021. [Online]. Available: https://www.itgovernance.co.uk/blog/how-much-does-cyber-essentials-cost-in-2021.

[75] G. Lloyd, “The business benefits of cyber security for SMEs,” *Computer Fraud & Security,* pp. 14-17, February 2020.

[76] A. A. Moustafa, A. Bello and A. Maurushat, “The role of user behaviour in improving cyber security management,” *Frontiers in psychology,* 2021.

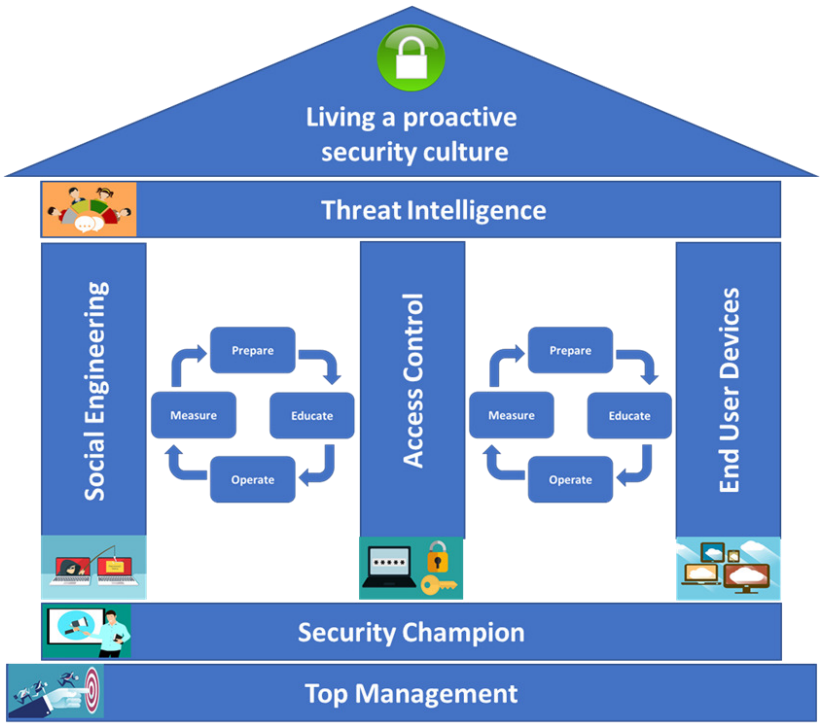
# Appendix 1 – Framework Description

# FRAMEWORK FOR BUILDING A POSITIVE CULTURE OF CYBER SECURITY

A guide on how to set up and operate a culture that enables employees to make the right decisions when a cyber-attack takes place.

## Introduction

The framework for securing cyber security behaviour change is based on a foundation that supports the implementation of pillars that support the building of a proactive security culture.




The framework is based on behaviour change techniques taken from the Behaviour Change Wheel, which is designed to assist the business employees in taking the learnings gained from activities such as awareness training, and turning those learning into behaviours which, when supported by activities within this framework, become a habit.

## How to Implement the Framework

The framework is implemented in stages.

- Firstly, the foundation stages are implemented.
    - Foundation stages build a solid foundation from which to build and are critical to the successful implementation.
- These are followed by the pillars.
    - The pillars support planning, education, operation, and reporting of key security topics.
- Finally, the Overarching process of Threat Intelligence binds the pillars together, supporting the operation within the pillars to share key knowledge of threat events.

## The Supply of Education/Awareness Training

The framework is designed to be used with a multitude of different awareness training packages which deliver some of the knowledge needed in the Pillars. The framework does not provide training but rather defines the activities to build around training to ensure that employees behaviours change to use the training given, making the organisation more secure.

# GUIDELINES FOR TOP MANAGEMENT SUPPORT FOUNDATION

## GOAL

Consistent Top Management support is the most essential element in creating a proactive and adaptive cyber security culture. Top Management must provide the vision, goals, visibility, funding, and commitment required to ensure that the undertaking is a success.

## FOUNDATION LAYERS

Top Management Support is the base foundation layer and is the first part of the model to be addressed. Additional layers and pillars will be built on top of this layer.

## BEHAVIOUR CHANGE TECHNIQUES

### Implement

| GROUPING | BCT |
|---|---|
| **1.Goals and Planning** | 1.1 Goal setting behaviour<br>1.3 Goal setting outcome<br>1.9 Commitment |
| **12. Antecedents** | 12.2 Restructure the social environment |
| **13. Identify** | 13.1 Identification of self as a role model |

### Operate

| GROUPING | BCT |
|---|---|
| **1.Goals and Planning** | 1.5 Review behaviour goal<br>1.7 Review outcome goal |
| **3. Social support** | 3.1 Social support (unspecified)<br>3.2 Social support (practical) |
| **6. Comparison of behaviour** | 6.1 Demonstration of the behaviour |

## ACTIVITIES TO IMPLEMENT TOP MANAGEMENT SUPPORT FOUNDATION

So that an SME creates a proactive cyber security culture that actively works to keep its operation safe from cyber-attack, the SME will appoint and operate a senior manager in the role of Top Management Sponsor (TMS)

### ACTIVITY: APPOINT A TOP MANAGEMENT SPONSOR

Appoint a TMS to act as the sponsor and spokesperson for management when setting direction and supporting a digital security culture within the business.

| **Intervention Function** | **Policy Category** |
|---|---|
| Enablement | Environmental Planning |
| **Grouping** | **BCT** |
| 12. Antecedents | 12.2 Restructuring the social environment |
| **Definition** | |
| A member of the Top Management must take the role of the Top Management Sponsor (TMS). This person will be the figurehead for the security culture. | |
| **Tasks** | |
| 1. Appoint a key member who takes accountability for the Cyber Security culture of the business.<br>2. The TMS will actively work on the strategy, direction, and goals of a positive Cyber Security culture within the business.<br>3. The TMS should have a responsibility within the business that would be severely affected by poor cyber security. | |

### ACTIVITY: ACT AS A ROLE MODEL

TMS must take the position of a role model and sell the concept across the business.

| **Intervention Function** | **Policy Category** |
|---|---|
| Modelling | Communication/Marketing |
| **Grouping** | **BCT** |
| 13. Identify | 13.1 Identification of self as a role model |
| **Definition** | |
| Top Management Sponsor to be a visible and proactive sponsor of a proactive security culture. | |
| **Tasks** | |
| 1. Communicate to all employees how management sees the importance of a strong security culture.<br>2. Be visible at training and education events and be seen as a role model<br>3. Provide regular follow-up on progression of culture and of management support | |

### ACTIVITY: SET GOALS FOR CREATING A SECURITY CULTURE

TMS must ensure the setting of goals for identifying the security culture required.

| **Intervention Function** | **Policy Category** |
|---|---|

| Modelling | Communication/Marketing |
|---|---|
| **Grouping** | **BCT** |
| 1. Goals and planning | 1.1 Goal Setting (Behaviour)<br>1.3 Goal Setting (Outcome) |
| **Definition** | |
| TMS to work with Security Champion and other relevant employees to set achievement goals for both the security behaviours needed and the desired outcomes wanted. | |
| **Tasks** | |
| 1. Work with a group of relevant employees to identify the correct goals.<br>2. Publish the goals<br>3. Use the goals to tailor the training requirements of the business | |

### ACTIVITY: PROVIDE RESOURCE AND FUNDING

TMS must ensure the resources and funding are in place to deliver on the security culture.

| **Intervention Function** | **Policy Category** |
|---|---|
| Modelling | Communication/Marketing |
| **Grouping** | **BCT** |
| 1. Goals and planning | 1.9 Commitment |
| **Definition** | |
| Top Management Sponsor to ensure that resources are appointed, time is allocated, and funding is provided to be able to deliver on the security plan. | |
| **Tasks** | |
| 1. Build a business case for the funding required and get the approval of funds. | |

## ACTIVITIES TO OPERATE TOP MANAGEMENT SUPPORT FOUNDATION

### ACTIVITY: DEMONSTRATE THE CORRECT BEHAVIOURS TO EMPLOYEES

TMS to demonstrate the correct behaviours when working in the office environment.

| **Intervention Function** | **Policy Category** |
|---|---|
| Persuasion | Environmental Planning |
| **Grouping** | **BCT** |
| 6. Comparison of behaviour | 6.1 Demonstration of behaviour |
| **Definition** | |
| The TMS must ensure that they always use and demonstrate the correct behaviours so that employees have a visual guide as to how to properly behave in the work environment. | |
| **Tasks** | |
| 1. TMS to actively demonstrate the correct security behaviours | |

## ACTIVITY: REVIEW AND ACT UPON MEASUREMENTS

Review and modify goals based on data

| **Intervention Function** | **Policy Category** |
|---|---|
| Modelling | Communication/Marketing |
| **Grouping** | **BCT** |
| 3. Social support | 3.1 Social support (unspecified)<br>3.2 Social support (practical) |
| **Definition** | |
| TMS to provide the Security Champion with coaching and support which helps them adapt to and grow within the role. Support can be on a social level (encouragement and feedback) as well as a more practical level (providing additional training, time, or tools) | |
| **Tasks** | |
| 1. Take a meeting with Security Champion to gauge their comfort with the role<br>2. Offer assistance when required | |

# GUIDELINES FOR SECURITY CHAMPION FOUNDATION

## GOAL

The Security Champion role provides a human interface between the technical requirements of a Cyber Security policy and the users who must adhere to the policy. The goal of a Security Champion is to support the building and operation of a strong cyber-security culture across the organisation.

## FOUNDATION LAYERS

To ensure the success of these guidelines, the following foundation layers **must** be operating:

1. Top Management Support Foundation

## BEHAVIOUR CHANGE TECHNIQUES

### Implement

| GROUPING | BCT |
|---|---|
| **12. Antecedents** | 12.2 Restructure the Social Environment |

### Operate

| GROUPING | BCT |
|---|---|
| **2. Feedback and monitoring** | 2.1 Monitoring of behaviour of others without feedback |
| **2. Feedback and monitoring** | 2.2 Feedback on behaviour |
| **6. Comparison of Behaviour** | 6.1 Demonstration of behaviour |
| **13. Identify** | 13.1 Identify of self as a role model |

## ACTIVITIES TO IMPLEMENT SECURITY CHAMPION FOUNDATION LAYER

So that an SME creates a proactive cyber security culture that actively works to keep its operation safe from cyber-attack, the SME should look to implement the role and associated activities of a Security Champion.

### ACTIVITY: APPOINT A SECURITY CHAMPION

Appoint a Security Champion to support employees in operating a proactive security culture within the business.

| **Intervention Function** | **Policy Category** |
|---|---|
| Enablement | Environmental Planning |
| **Grouping** | **BCT** |
| 12. Antecedents | 12.2 Restructuring the social environment |
| **Definition** | |
| The business will appoint a Security Champion who will provide a communication channel for all Cyber Security topics and issues. The person must be respected by the employees and be able to carry authority. The Security Champion must guide and support users with their digital hygiene so that they become part of a proactive security culture. The Security Champion must be non-judgemental of any mistakes made by employees when handling cyber-security issues.<br>The choice of the Security Champion is key to ensuring a positive cyber-security culture can be built and function effectively. The Security Champion does not need to be a member of an IT/Security Team but can instead be a representative from the User community who is trusted and respected by their peers. | |
| **Tasks** | |
| 1. Select and appoint one or more Security Champions (dependent on the number of employees)<br>2. Provide training to the Security Champion on how to coach employees when supporting cyber-security topics and issues.<br>3. Top Management to promote the role of the Security Champion | |

## ACTIVITIES TO OPERATE A SECURITY CHAMPION FOUNDATION LAYER

**The following activities support behaviour change techniques designed to support the Security Champion in enabling positive behaviour change across the organisation.**

### ACTIVITY: OPERATE AS A ROLE MODEL

Security Champion to act as a role model on best practice cyber-security behaviours

| **Intervention Function** | **Policy Category** |
|---|---|
| Persuasion | Environmental Planning |
| **Grouping** | **BCT** |
| 13. Identify | 13.1 Identify of self as a role model |
| **Definition** | |

| |
|---|
| Explain to the Security Champion of their behaviour as being an example to others and how positive security behaviour will help to build a stronger security culture. Encourage the Security Champion to behave as a role model. |
| **Tasks** |
| 1. Provide encouragement and incentives to the Security Champion to undertake the role of a role model. |

## ACTIVITY: DEMONSTRATE THE CORRECT BEHAVIOURS TO EMPLOYEES

Security Champion to demonstrate the correct behaviours when working in the office environment.

| **Intervention Function** | **Policy Category** |
|---|---|
| Persuasion | Environmental Planning |
| **Grouping** | **BCT** |
| 6. Comparison of behaviour | 6.1 Demonstration of behaviour |
| **Definition** | |
| The Security Champion must ensure that they always use and demonstrate the correct behaviours so that employees have a visual guide on how to behave in the work environment. | |
| **Tasks** | |
| 1. Security champion to actively demonstrate the correct security behaviours | |

## ACTIVITY: MONITOR AND GIVE FEEDBACK ON SECURITY BEHAVIOURS

Security Champion to monitor and give feedback where incorrect behaviours are used.

| **Intervention Function** | **Policy Category** |
|---|---|
| Persuasion | Environmental Planning |
| **Grouping** | **BCT** |
| 2. Feedback and monitoring | 2.2 Feedback on behaviour |
| **Definition** | |
| The Security Champion must use the correct security behaviours and look out for and identify examples where an employee does not adhere to those behaviours. When a situation is identified, the Security Champion shows the user in a non-judgmental way how the correct behaviour should be carried out and explains the risks of not using the correct behaviours. | |
| **Tasks** | |
| 1. Security champion to actively demonstrate the correct security behaviours<br>2. If an employee is seen demonstrating incorrect behaviours, Security Champion will explain the dangers of such behaviour and how a change to the behaviour will result in a better outcome for both the individual and the business. | |

## ACTIVITY: MONITOR BEHAVIOURS TO MEASURE AGAINST GOALS

Security Champion to monitor and record data on adherence to goals

| Intervention Function | Policy Category |
|---|---|
| Persuasion | Environmental Planning |
| **Grouping** | **BCT** |
| 2. Feedback and monitoring | 2.1 Monitor of behaviour of others without feedback |
| **Definition** | |
| The Security Champion will record instances of behaviours where attacks were caught, attacks were successful etc., to build up KPIs to match against the pre-set goals. | |
| **Tasks** | |
| 1. Security champion to record instances of relevant information related to goals<br>2. KPIs to be reviewed to gauge the success of the program. | |

# GUIDELINES FOR PREVENTION OF SOCIAL ENGINEERING ATTACKS

## GOAL

Preventing the user from unknowingly taking a course of action that could open the door to a cybercriminal

## FOUNDATION LAYERS

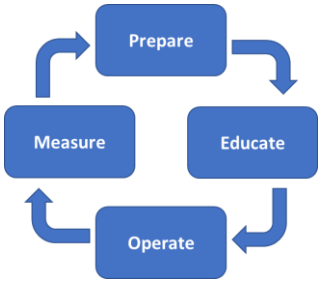
To ensure success, the following foundation layers must be operating:

2. Top Management Support Foundation
3. Security Champion Support Foundation

## ACTIVITIES CATEGORIES

Activities required to enable and sustain behavioural change are broken down into the following four categories:

- Prepare
- Educate
- Operate
- Measure



## BEHAVIOUR CHANGE TAXONOMIES

### PREPARE

| GROUPING | BCT |
|---|---|
| **5. Natural Consequences** | 5.3 Information about Social and Economic consequences |
| **12. Antecedents** | 12.2 Restructure the social environment |

### EDUCATE

| GROUPING | BCT |
|---|---|
| **4. Shaping Knowledge** | 4.1 Instructions on how to perform the behaviour |

### OPERATE

| GROUPING | BCT |
|---|---|
| **4. Shaping Knowledge** | 4.1 Instructions on how to perform the behaviour |
| **10. Reward** | 10.1 Material incentive |
| | 10.4 Social reward |

### REPORT

| GROUPING | BCT |
|---|---|
| **2. Feedback and monitoring** | 2.7 Feedback on Outcomes of behaviour |

## ACTIVITIES THAT SUPPORT THE PREPARE CATEGORY

So that awareness training is given the best opportunity to succeed, the following activities are designed to build a culture where employees are prepared and understand the need to embrace the training and engage in positive change behaviour so that they operate securely. Activities in the PREPARE category are designed to modify the environment in such a way that users are given the best support to behave in the best way.

### ACTIVITY: CREATE BUY-IN

Create "Buy-in" to the need for training by informing about the dangers of being tricked by Social Engineering.

| **Intervention Function** | **Policy Category** |
|---|---|
| Education | Communication |
| **Grouping** | **BCT** |
| 5. Natural Consequences | 5.3 Information about Social and Economic consequences |
| **Description** | |
| To understand why training is important and therefore gets "buy-in", the employees need to understand the risks that phishing provides both themselves and the business. This must not be scare tactics but rather a grown-up discussion about real-world events and the impact that these events are having. It should be delivered in such a way that the user feels educated and empowered by receiving the information. | |
| **Action Points:** | |
| 1. Provide information about how Cyber-criminals target individuals<br>2. Provide information about how strong digital hygiene can be a benefit first and foremost in a person's private life and subsequently benefit their work-life<br>3. Provide real-world examples of the impact of poor security on individuals and business | |

### ACTIVITY: CHANGE THE ENVIRONMENT TO REDUCE FALSE POSITIVES

Remove the practice of sending internal emails to employees which include links or attachments.

| **Intervention Function** | **Policy Category** |
|---|---|
| Environmental Restructure | Environmental Planning |
| **Grouping** | **BCT** |
| 12. Antecedents | 12.2 Restructure the social environment |
| **Description** | |
| If employees normally receive internal emails which include links or attachments, they will be used to clicking such links, and it will become an everyday habit. Therefore, the business should provide a method of information and data sharing for employees that are not done via e-mail. This could be done by using secure Apps which are designed for collaborating and data sharing and negate the need for e-mails with attachments or clickable links.<br>By removing internal emails, the practice of regularly clicking links or opening attachments will be significantly reduced, making it an oddity rather than a normal practice. Oddities are more likely to trigger caution in the eyes of a user. | |
| **Action Points** | |
| 1. Create a team (which has user representatives and a Security Champion) to investigate and choose a secure App that is to be used for internal communication and collaboration.<br>2. Educate the users as to why the use of the App provides more significant benefits than email<br>3. Rollout and train the users on how to collaborate using the App<br>4. Modify the security policy to ban the use of internal emails.<br>5. Monitor and follow-up with the policy, supporting users throughout the process | |

## ACTIVITIES THAT SUPPORT THE EDUCATE CATEGORY

So that people understand and buy into what is being asked of them, activities are required to support the education of users.

### ACTIVITY 3: PROVIDE PRACTICAL TRAINING

Equip users with the skills needed to carry out the behaviour.

| **Intervention Function** | **Policy Category** |
|---|---|
| Training | Service Provision |
| **Grouping** | **BCT** |
| 4. Shaping Knowledge | 4.1 Instructions on how to perform the behaviour |
| **Description** | |

| |
|---|
| Training is provided, which demonstrates the steps that a user should take each time an email instructs to click a link or open an attachment. Training should build on the Education function by enabling the user with the skills needed to spot and prevent phishing attacks from taking place. The training should be supported by the Security Champion, who is available to give practical demonstrations and answer any question due to the non-judgemental environment that is being fostered. |
| **Action Points** |
| 1. Security Champion to provide demonstrations of the correct behaviours<br>2. Users to be allowed to test themselves in a safe environment by repeating the taught behaviours in pre-prepared scenarios<br>3. Security Champion to monitor the results and provide positive support and advice to users who need further assistance in gaining positive results. |

## ACTIVITIES THAT SUPPORT THE OPERATE CATEGORY

To create ongoing behaviour change, users need to be reminded of the correct behaviours and incentivised to carry these out.

### ACTIVITY 4: REPORTING OF SOCIAL ENGINEERING ATTACKS

Capture all phishing attacks that take place.

| **Intervention Function** | **Policy Category** |
|---|---|
| Enabling | Environmental Planning |
| **Grouping** | **BCT** |
| 4. Shaping Knowledge | 4.1 Instructions on how to perform the behaviour |
| **Description** | |
| Employees will be trained to report 100% of all phishing emails discovered (whether or not they clicked the link) by **enabling** simple to use reporting process. Once a phishing email has been detected, the information should be shared across the organisation to pre-warn employees that an attack is happening. Reporting must be easy to carry out and be seen as a positive action that can benefit the social group. If a user accidentally clicks the phishing link, they must know that subsequently reporting the phishing attack will not lead to any repercussions. | |
| **Action Points** | |
| 1. Introduce the Threat Intelligence Overarching process and explain the benefits of using such a tool.<br>2. Explain to the user how they can check with a Security Champion if they are unsure and need clarification about the correct steps to take.<br>3. Show the users how to quickly and easily report a potential social media attack via a Threat Intelligence tool. | |

### ACTIVITY 5: INCENTIVISE USERS TO CATCH AND REPORT ATTACKS

Incentivise the users to continue with the correct behaviour of reporting attacks

| **Intervention Function** | **Policy Category** |
|---|---|
| Incentivisation | Environmental Planning |
| **Grouping** | **BCT** |

| 10. Reward | 10.1 Material Incentive<br>10.4 Social reward |
|---|---|
| **Description** | |
| Users will be incentivised to report 100% of all phishing emails discovered. Users who accidentally clicked a link must not be discouraged from reporting the attack through fear of judgement or reprisal. Reporting of a phishing mail should be seen to reward the individual and the group (social reward), as the individual detecting the attack can supply knowledge that can support their colleagues in staying safe from the attack.<br>Reporting of the mail could also lead to a Material Reward for the user identifying that attack. An incentive scheme such as “Monthly cash reward for the user who reports the most phishing attacks could be operated, thus giving an additional reason to actively report attacks. | |
| Actions: | |
| 1. Management and Security Champion to agree on a reward system<br>2. Security Champion to communicate the reward system to employees<br>3. Monthly rewards to be presented and publicised. | |

# GUIDELINES FOR BEHAVIOURAL CHANGE IN SECURING ACCESS CONTROL

## GOAL

Preventing unauthorised people from accessing your secure systems and services by ensuring strong, secure password protection

## FOUNDATION LAYERS

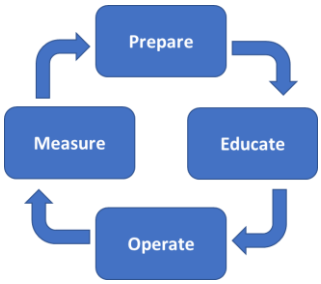
To ensure success, the following foundation layers must be operating:

4. Top Management Support Foundation
5. Security Champion Support Foundation

## ACTIVITIES CATEGORIES

Activities required to enable and sustain behavioural change are broken down into the following four categories:

- Prepare
- Educate
- Operate
- Measure



## BEHAVIOUR CHANGE TAXONOMIES

### PREPARE

| GROUPING | BCT |
|---|---|
| **5. Natural Consequences** | 5.3 Information about Social and Economic consequences |
| **12. Antecedents** | 12.2 Restructure the social environment |

### EDUCATE

| GROUPING | BCT |
|---|---|
| **4. Shaping Knowledge** | 4.1 Instructions on how to perform the behaviour |

### OPERATE

| GROUPING | BCT |
|---|---|
| **4. Shaping Knowledge** | 4.1 Instructions on how to perform the behaviour |
| **10. Reward** | 10.1 Material incentive |
| | 10.4 Social reward |

### REPORT

| GROUPING | BCT |
|---|---|
| **2. Feedback and monitoring** | 2.7 Feedback on Outcomes of behaviour |

## ACTIVITIES THAT SUPPORT THE PREPARE CATEGORY

So that awareness training is given the best opportunity to succeed, the following activities are designed to build a culture where employees are prepared and understand the need to embrace the training and engage in positive change behaviour so that they operate securely. Activities in the PREPARE category are designed to modify the environment in such a way that users are given the best opportunity and support to learn and operate in the best way.

### ACTIVITY: CREATE BUY-IN

Create “Buy-in” to the need for users to practice digital hygiene before the training begins.

| **Intervention Function** | **Policy Category** |
|---|---|
| Education | Communication |
| **Grouping** | **BCT** |
| 5. Natural Consequences | 5.3 Information about Social and Economic consequences |
| **Description** | |
| To understand why training is essential and therefore gets “buy-in”, the employees need to understand the risks that poor password hygiene delivers to both themselves and the business. This must not be scare tactics but rather a grown-up discussion about real-world events and the impact that these events are having on ordinary people and businesses. It should be delivered in such a way that the user feels educated and empowered by receiving the information. | |
| **Action Points:** | |
| 1. Provide information to the users about how Cyber-criminals target individuals to gain password information.<br>2. Provide information about how strong digital hygiene can be a benefit first and foremost in a person’s private life and subsequently benefit in their work-life | |

| |
|---|
| 3. Provide real-world examples of the impact that poor password hygiene has had on individuals and businesses |

### ACTIVITY: RESTRUCTURE THE CURRENT ENVIRONMENT

Investigate supplying all users with a password management tool rather than have users manually managing their passwords.

**DESCRIPTION OF ACTIVITY**:

Provide supporting software which makes it easy for a user to adhere to password security rules.

| **Intervention Function** | **Policy Category** |
|---|---|
| Environmental Restructure | Environmental Planning |
| **Grouping** | **BCT** |
| 12. Antecedents | 12.2 Restructure the social environment |
| **Description** | |
| A password management tool will support the user by automatically creating a password using long, random mixes of letters, numbers, and characters. These passwords far exceed the guidelines set by security professionals and are managed by the password management tool rather than the user, meaning the user only needs to remember one administration password, thus making it much easier for a user to be compliant with security guidelines. | |
| **Action Points** | |
| 1. Investigate and choose a password management tool that is to be used by users for managing their passwords<br>2. Educate the users as to why the use of the App provides greater benefits than manually creating their passwords<br>3. Rollout and train the users on how to manage passwords using the password management tool<br>4. Modify the security policy to state that passwords should only be created and maintained using the password management tool.<br>5. Monitor and follow-up with the policy, supporting users throughout the process | |

## ACTIVITIES THAT SUPPORT THE EDUCATE CATEGORY

So that people understand and buy into what is being asked of them, activities are required to deliver and support the education of users.

### ACTIVITY: PROVIDE PRACTICAL TRAINING

Equip users with the skills needed to carry out the behaviour.

| **Intervention Function** | **Policy Category** |
|---|---|
| Training | Service Provision |
| **Grouping** | **BCT** |

| 4. Shaping Knowledge | 4.1 Instructions on how to perform the behaviour |
|---|---|
| **Description** | |
| Training is provided, which demonstrates the steps that a user should take to secure their end-user devices. This training is dependent on the tools available. For example, if Password managers have been provided, the training will instruct how to use these successfully. If Password Managers are not available, training will be given to best equip a user on how to use and manage passwords manually. The training should be supported by the Security Champion, who is available to give practical demonstrations and answer any question due to the non-judgemental environment that is being fostered. | |
| **Action Points** | |
| 1. Security Champion to provide demonstrations of the correct behaviours<br>2. Users given the opportunity to test themselves in repeating the same behaviours in pre-prepared scenarios<br>3. Security Champion to monitor the results and provide positive support and advice to users who need further assistance in gaining positive results. | |

## ACTIVITIES THAT SUPPORT THE OPERATE CATEGORY

To create ongoing behaviour change, users need to be reminded of the correct behaviours and incentivised to carry these out.

### ACTIVITY: REPORTING OF ATTEMPTED ACCESS BY UNKNOWN PERSONS

Capture information about attempts to access your secure systems and report these.

**DESCRIPTION OF ACTIVITY**:

Users will be trained to report an attempt by a third party to extract details from them that allows unauthorised access.

| **Intervention Function** | **Policy Category** |
|---|---|
| Enabling | Environmental Planning |
| **Grouping** | **BCT** |
| 4. Shaping Knowledge | 4.1 Instructions on how to perform the behaviour |
| **Description** | |
| Once a potential attempt at unauthorised access into a device or system has been detected, the information should be shared across the organisation to pre-warn employees that an attack is happening. Reporting must be easy to do and be seen as a positive action that can benefit the social group. Even if a user unwittingly divulges their credentials, they must know that subsequently reporting the unauthorised access will not lead to any repercussions, as there will be an even greater need to act upon stopping a potential breach. | |
| **Action Points** | |
| 1. Introduce the Threat Intelligence Overarching process and explain the benefits of using such a tool.<br>2. Explain to the user how they can check with a Security Champion if they are unsure about a situation in which they find themselves. | |

| |
|---|
| 3. Show the users how to report a potential unauthorised access attack quickly and easily via a Threat Intelligence tool. |

### ACTIVITY: INCENTIVISE USERS TO CATCH AND REPORT ATTACKS

Incentivise users to continue with the correct behaviour of reporting attacks

**DESCRIPTION OF ACTIVITY**:

Users will be incentivised to report 100% of all end-user device access attacks. Users who accidentally provided unauthorised access must not be discouraged from reporting the attack.

| **Intervention Function** | **Policy Category** |
|---|---|
| Incentivisation | Environmental Planning |
| **Grouping** | **BCT** |
| 10. Reward | 10.1 Material Incentive<br>10.4 Social reward |
| **Description** | |
| Reporting of an unauthorised attack should be seen to reward the individual and the group (social reward), as the individual detecting the attack supplies knowledge that can support their colleagues in staying safe from the attack.<br>Reporting of the attack could also lead to a Material Reward. An incentive scheme such as a monthly cash reward for employees who reports the most unauthorised access attacks could be operated, thus giving an additional reason to actively report attacks. | |
| Actions: | |
| 1. Management and Security Champion to agree on a reward system<br>2. Security Champion to communicate the reward system to employees<br>3. Monthly rewards to be presented and publicised. | |

## ACTIVITIES THAT SUPPORT THE MEASURE CATEGORY

Activities are required to measure the success of the operation, give feedback to employees and gain lessons learned, which can be fed back into the PREPARE stage.

### ACTIVITY: REPORT THE SUCCESS OF THE ACTIONS TAKEN BY USERS

Provides regular reporting of suspected unauthorised access attacks thwarted so that users can see that their continued actions have value

| **Intervention Function** | **Policy Category** |
|---|---|
| Education | Communication |
| **Grouping** | **BCT** |
| 2 Feedback and monitoring | 2.7 Feedback on Outcomes of behaviour |
| **Description** | |
| Monthly reporting published to all employees by the Security Champion, informing of the number of attempted access attacks made. This is done to keep the activity of | |

| |
|---|
| unauthorised access prevention highlighted and ensure it stays in the general focus of all employees. |
| **Actions** |
| 1. Statistics from the reported catches are to be gathered monthly<br>2. Security Champion to publish data to users, showing the benefit of the behaviour in catching attacks, thwarting the cyber-criminals, and keeping the business safe |

# GUIDELINES FOR BEHAVIOURAL CHANGE IN SECURING END-USER DEVICES

## GOAL

Ensure that an employee's end-user devices are operating securely, resulting in an increased level of security for the user, and therefore the business.

It is expected that an SME is already protecting business devices used by the user. The focus here is on the personal devices of end-users which may/may not be used for handling work e-mail or apps. By encouraging the user to protect all their devices, their overall digital hygiene will improve.

## FOUNDATION LAYERS

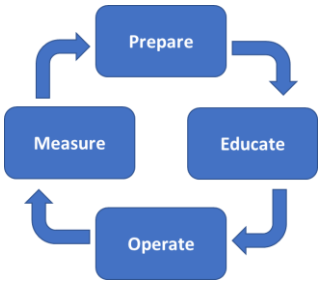
To ensure success, the following foundation layers must be operating:

6. Top Management Support Foundation
7. Security Champion Support Foundation

## ACTIVITIES CATEGORIES

Activities required to enable and sustain behavioural change are broken down into the following four categories:

- Prepare
- Educate
- Operate
- Measure



## BEHAVIOUR CHANGE TAXONOMIES

### PREPARE

| GROUPING | BCT |
|---|---|
| **5. Natural Consequences** | 5.3 Information about Social and Economic consequences |
| **12. Antecedents** | 12.5 Adding objects to the environment |

### EDUCATE

| GROUPING | BCT |
|---|---|
| **4. Shaping Knowledge** | 4.1 Instructions on how to perform the behaviour |

### OPERATE

| GROUPING | BCT |
|---|---|
| **7. Associations** | 7.1 Prompts/cues |

### REPORT

| GROUPING | BCT |
|---|---|
| **5. Natural consequences** | 5.3 Information about social and environmental consequences |

## ACTIVITIES THAT SUPPORT THE PREPARE CATEGORY

So that awareness training is given the best opportunity to succeed, the following activities are designed to build a culture where employees are prepared and understand the need to embrace the training and engage in positive change behaviour.

The focus is on the end-users personal devices. It is expected that business devices are already protected by the IT department, and therefore such devices are being kept at a secure level as per the IT policies.

### ACTIVITY: CREATE BUY-IN

Create "Buy-in" to the need for digital hygiene on end-user devices before the training begins.

| **Intervention Function** | **Policy Category** |
|---|---|
| Education | Communication |
| **Grouping** | **BCT** |
| 5. Natural Consequences | 5.3 Information about Social and Economic consequences |
| **Description** | |
| Users will be educated as to the risks that exist around their end-user devices and why being able to secure the devices is a valuable skill both in their home and work lives. They will be informed how such skills will benefit themselves in their personal lives and jointly then benefit the company as the employees increase their digital hygiene. To understand why training is important and therefore gets "buy-in", the employees need to understand the risks that operating an insecure device will put on both the individual and the business. This must not be scare tactics but rather a grown-up discussion about real-world events and the impact that these events are having on normal people and businesses. It should be delivered in such a way that the user feels educated and empowered by receiving the information. | |
| **Action Points:** | |

| |
|---|
| 1. Provide information to the users about how Cyber-criminals target individuals<br>2. Provide information about how strong digital hygiene can be a benefit first and foremost in a person's private life and subsequently benefit in their work-life<br>3. Provide real-world examples of the impact of poor security on individuals and business |

### ACTIVITY: PROVIDE TOOLS TO DO THE TECHNICAL WORK

Provide employees with the technical tools needed so that a solution for the user is easy to implement on all devices they use, as insecure personal devices can impact business security.

| **Intervention Function** | **Policy Category** |
|---|---|
| Education | Communication |
| **Grouping** | **BCT** |
| 12. | 12.5 Adding objects to the environment |
| **Description** | |
| Although it should be expected that a business computer is running anti-virus software, it cannot be assumed that an employee's personal devices are doing the same. To ensure good digital hygiene, a user should be ensuring that all devices they use have protection from a cyber-attack. | |
| **Action Points:** | |
| 1. Put together a small team to investigate possible software solutions which can be provided to users.<br>2. Include the Security Champion and some end-users in the process to ensure end-user buy-in to the process and chosen solution<br>3. Put together a business case to support the time and costs of rolling out software for employees personal devices.<br>4. Once approval is gained, produce a pack for employees on how to install and use the software – if needed, a process can be included in the "Educate" area to support this. | |

## ACTIVITIES THAT SUPPORT THE EDUCATE CATEGORY

Awareness training works best when users can actively participate in practical training, which is proven to increase the users understanding and ability to re-create the correct behaviours when required.

### ACTIVITY: PROVIDE PRACTICAL TRAINING

Explain to users the importance of security patches regarding their personal devices and show the users how to keep their devices running on the latest versions of the OS.

| **Intervention Function** | **Policy Category** |
|---|---|
| Training | Service Provision |
| **Grouping** | **BCT** |
| 4. Shaping Knowledge | 4.1 Instructions on how to perform the behaviour |
| **Description** | |

| |
|---|
| User's personal devices should be running on the latest version of the operating system to ensure that any security patches launched by the software provider are installed in a timely fashion on the user's devices (PC, tablet, phone etc.). To assist users in making the required changes, instructions on performing the desired behaviour will be given, along with support when carrying out the behaviour. |
| **Action Points** |
| 1. Security Champion to explain the risk of running a mobile device which is not having the latest update of the operating system installed.<br>2. Security Champion to demonstrate how to check and update to the latest version of the operating system on a few of the most popular devices (E.g. iOS, Android, Windows)<br>3. Security Champion to encourage users to follow the guidelines and update their devices. |

## ACTIVITIES THAT SUPPORT THE OPERATE CATEGORY

As the goal is to have users running their personal devices, there is only a limited number of tasks that can be done in the Operation category as the company will not have any knowledge of user-specific device status and usage.

### ACTIVITY: INFORM OF CRITICAL UPDATES

Prompt users if critical updates are released by software vendors for the primarily used devices (iOS, Windows, Android)

| **Intervention Function** | **Policy Category** |
|---|---|
| Environmental Restructure | Environmental Planning |
| **Grouping** | **BCT** |
| 7 Associations | 7.1 Prompts/cues |
| **Description** | |
| Not all software vendors tend to highly publicise the release of important security updates and so providing information on the availability of updates can bring user understanding to the risk and provide a trigger to install the update. | |
| **Action Points** | |
| 1. Security Champion sign-up for alerts from Major Vendors for security update notifications<br>2. When an alert is issued, the Security Champion will communicate to the users that an update to their personal devices can be made. | |

## ACTIVITIES THAT SUPPORT THE REPORT CATEGORY

As the focus is on personal devices, the business will not be able to gather data and report on personal device security and usage.

However, the business can still publish information regarding attacks via personal devices if an attack is traced back to a personal device.

### ACTIVITY: INFORM OF SUCCESSFUL BREACHES VIA PERSONAL DEVICES

| Intervention Function | Policy Category |
|---|---|
| Environmental Restructure | Environmental Planning |
| **Grouping** | **BCT** |
| 5 Natural consequences | 5.3 Information about social and environmental consequences |
| **Description** | |
| Inform the users if a successful attack took place via an unsecured personal device. Inform of the business consequences of the successful attack so that users understand the business impact of such an attack.<br>The User whose device was used must not be named as such an approach could lead to users being reluctant to inform of attacks and to adhere to the security policies | |
| **Action Points** | |
| 1. Gather the information needed<br>2. Publish and inform users of the attack in such a way that they understand the consequences for the business of such an attack<br>3. Ensure that no user information is divulged as part of the communication so as not to label blame on an individual | |

# GUIDELINES FOR BEHAVIOURAL CHANGE IN THREAT INTELLIGENCE

## GOAL

Provide an easy-to-use method of sharing threat intelligence information that can be shared with all users across the business. This will ensure that users are fully aware of any potential attacks taking place and are therefore more alert to the situation.

## FOUNDATION LAYERS

To ensure success, the following foundation layers must be operating:

1. Top Management Support Foundation
2. Security Champion Support Foundation

## PILLAR CATEGORIES

For the Threat Intelligence overarching process to operate successfully, one or more of the framework Pillars must be in operation:

1. Social Engineering
2. Access Control
3. End-User Devices

## BEHAVIOUR CHANGE TAXONOMIES

### Implement

| GROUPING | BCT |
|---|---|
| **4 Shaping knowledge** | 4.1 Instructions on how to perform the behaviour |
| **5 Natural consequences** | 5.3 Information about Social and Economic consequences |
| **12 Antecedents** | 12.1 Restructuring the physical environment |

### Operate

| GROUPING | BCT |
|---|---|
| **2. Feedback and monitoring** | 2.7 Feedback on Outcomes of behaviour |

## ACTIVITIES THAT SUPPORT THE IMPLEMENT CATEGORY

So that Threat Intelligence can operate successfully, supporting activities and systems must be put in place, which makes the reporting and communication of threats easy to do.

### ACTIVITY: PREPARE A ROBUST AND EASY TO USE INCIDENT REPORTING PROCESS

Implement a system for users to easily report threats that are taking place so that an expert can quickly act in preventing further harm.

| **Intervention Function** | **Policy Category** |
|---|---|
| Enablement | Environmental Planning |
| **Grouping** | **BCT** |
| 12 Antecedents | 12.1 Restructuring the physical environment |
| **Description** | |
| So that users can quickly notify of an attack, a system must be in place so that a user can quickly and efficiently inform the right person(s). | |
| **Action Points:** | |
| 1. Evaluate the best method for informing of an attack. This will consider issues such as the number of users, location of users, time of day/night users are working, and equipment supplied to users as part of the job role.<br>2. Working with Security Champion and user representatives, implement a process by which a user can immediately report a potential attack.<br>3. Define the process around the receiving and acting on the reported incident.<br>4. Ensure a feedback loop to the user who raised the incident. | |

### ACTIVITY: CREATE BUY-IN

Create “Buy-in” to the need for users to report security incidents that they find.

| **Intervention Function** | **Policy Category** |
|---|---|
| Education | Communication |
| **Grouping** | **BCT** |
| 5. Natural Consequences | 5.3 Information about Social and Economic consequences |
| **Description** | |
| To understand why training is important and therefore gets “buy-in”, the employees need to understand the benefits that reporting security incidents provides both themselves and the business around them and the risks of not reporting said incidents. This must not be | |

| |
|---|
| scare tactics but rather a grown-up discussion about real-world events and the impact that these events are having on employees and businesses. It should be delivered in such a way that the user feels educated and empowered by receiving the information. |
| **Action Points:** |
| 1. Provide information to the users about how Cyber-criminals target individuals<br>2. Provide information about how reporting of incidents allows quick intervention and shared knowledge which can alert a colleague to a potential attack.<br>3. Provide real-world examples of reporting incidents and the benefits gained – and the cost of ignoring an incident. |

### ACTIVITY: PROVIDE USERS PRACTICAL TRAINING ON USING THE PROCESS

Equip users with the skills needed to carry out the behaviour.

| **Intervention Function** | **Policy Category** |
|---|---|
| Training | Service Provision |
| **Grouping** | **BCT** |
| 4. Shaping Knowledge | 4.1 Instructions on how to perform the behaviour |
| **Description** | |
| Training is provided, which demonstrates the steps that a user should take each they identify a potential attack and need to report it. The training should be supported by the Security Champion, who is available to give practical demonstrations and answer any question due to the non-judgemental environment that is being fostered. | |
| **Action Points** | |
| 1. Security Champion to provide demonstrations of the correct behaviours<br>2. Users given the opportunity to test themselves in repeating the same behaviours in pre-prepared scenarios<br>3. Security Champion to monitor the results and provide positive support and advice to users who need further assistance in gaining positive results. | |

## ACTIVITIES THAT SUPPORT THE OPERATION CATEGORY

So that people understand how to report threats, activities are required to deliver and support the education of users.

### ACTIVITY: (IF RELEVANT) INFORM ALL USERS OF AN POSSIBLE ATTACK

Report details of an attack if that information could raise user awareness and prevent another security incident from happening.

| **Intervention Function** | **Policy Category** |
|---|---|
| Education | Communication |
| **Grouping** | **BCT** |
| 2 Feedback and monitoring | 2.7 Feedback on Outcomes of behaviour |
| **Description** | |

| |
|---|
| Information found promptly can be used to increase the awareness of all users to help prevent subsequent attacks. |
| **Actions** |
| 1. Reported incident to be quickly analysed and a decision made whether to share the information across the company<br>2. If communication is to take place, the information must be easy to understand and descriptive in the actions needed by the user to prevent a further attack. |

# Appendix 8 – Answers to Questionnaire

## Questions

1. ***Are there any elements (foundation layers, pillars, or overarching process) which you do not believe would add enough value to make the implementation of that element worthwhile for an SME?***

   The elements themselves appear reasonable but need more details pulling out.

2. ***Are there any sub-elements (specific behaviour change techniques within each element)that you do not believe would add enough value to warrant implementing?***

   This is harder to assess as although the model has many classifications and taxonomies the description of the interventions/tasks feels quite vague, so it is hard to fully appreciate the value of implementing stated actions and the impact they may have. Also, it's not clear what sub-elements may be applicable to every organisation so in order to ensure relevance is achieved it may be useful separating these out into mandatory and optional type elements.

3. ***From your experience, are there any activities missing within the framework which could further assist an SME to change user behaviour to build a stronger security culture?***

   The first stage is typically assessing what are the SME's existing cultures and behaviours to then have defined what the target behaviours are being planned for. Using the type of model proposed can then be introduced but it also appears to miss the use of nudging techniques, e.g. maybe add a section which can define what applicable nudges could be introduced to assist in ensuring that behaviours are both achieved and maintained. This would need the introduction of something like Nudge Theory into the framework.

   Also, any framework needs to connect with the business' overall objectives and their security objectives to help align both perceived relevance and value into implementing such a framework. Certainly, smaller organisations require this to assess the effort to reward ratio of implementing such a framework.

4. ***As security professionals, when assessing where limited budgets should be spent, do you believe that investing into the changing of user behaviour towards a more positive securityculture is: (please choose one option)***

   a) ***Less important than investing into technical solutions that counter cyber-attacks***
   b) ***Equally as important as investing into technical solutions that counter cyber-attacks]***
   c) ***More important than technical solutions that counter cyber-attacks***

   ***Please give a few words to support your answer…..***

Around 90% of data breaches have come from human error and so secure behaviours are critical to this. Technical solutions are still important but should be there to support and provide defence-in-depth rather than overly relied upon for the complete security posture of an organisation.

5. ***This model focuses on a user's digital behaviour at home and in the office, as it is perceivedthat a user's digital hygiene should be at an equal level for both so that the user operates aconsistently high level of digital hygiene.***

   ***From your knowledge as security professionals and working with SMEs, do you believe that:***

   a) ***The concept of encouraging a user into operating a higher level of security at homewould have a positive impact on overall cyber-security for the business. Yes***

   ***a) An SME is potentially willing to invest in offering its employees help in acquiring and setting uptools for home use, like what they already provide for business end user devices (e.g., VPN, Password Managers etc.) No***

   ***Please give a few words that support your answers….***

   Point a – I have no doubt that transformation of mindset into positive security behaviours at home would translate into improved work behaviours. However, I do not believe it would be a 1:1 ratio in terms of those two environments. It depends how the behaviour change was implemented as home life will be very personal and relevant to a user whereas at work, they may care less about the potential outcomes as they do not perceive the same threat and consequences personally as they would do at home. It's how relevant and applicable you make it to that user.

   Point b – I think unless you can provide a clear ROI on investing in home life or that the user will be working at home, this would be a tough sell that most SMEs would not do just due to the pure cost element. It is hard to get investment decisions around cyber security in the actual business environment of SMEs, let alone for their employee's home life. There would need to be compelling evidence to demonstrate such an investment can have a positive impact on the SMEs growth or revenue protection aspects.

6. ***Any other thoughts or ideas that you have considered in reviewing the framework, which you believe would be useful feedback and has not been covered in this short questionnaire?***
   I think it would also be good to align the said behaviours with standards such as Cyber Essentials (CE) and potentially ISO 27001. With CE, you could have behaviour inventions and nudges mapped against all 5 technical control domains of CE as they supposedly address 80% of the cyber-attacks being faced. It would then also provide additional value that the work done with your framework could then translate into a % of work required for achieving CE certification. CE also feels the right level for

SMEs.

I would also caution the connection with IT functions as we need security behavioural change not fully aligned to IT or technical functions but more seen as strategic and operationally aligned. I did note a few tasks did state IT which is fine in areas but needs additional functions added to not give the perception of it being an "IT issue" which many businesses still perceive cyber risk to be.

Also, research has shown messaging and what words are used in how we try to elicit behavioural change is important so you would need to also understand the profile of the audience in order to better refine the effectiveness of said framework in how you provide guidance on interventions etc.

Finally, it would be good to understand how you would intend to measure the success of interventions and/or your proposed framework.

## Questions

1. ***Are there any elements (foundation layers, pillars, or overarching process) which you do not believe would add enough value to make the implementation of that element worthwhile for an SME?***

A: No. The only note I would mention is to add something about continuous improvement and change.

2. ***Are there any sub-elements (specific behaviour change techniques within each element) that you do not believe would add enough value to warrant implementing?***

A: No. Similar to the point above, the only things mentioned about continuous and on-going behaviour is to implement phishing emails and encourage everyone to keep reporting incidents. There are many yearly/bi-yearly/quarterly things the company can do like refresher courses, or run fake experiments to encourage these behaviours as well.

3. ***From your experience, are there any activities missing within the framework which could further assist an SME to change user behaviour to build a stronger security culture?***

A: Just the points about about continuous improvements, changes and adaptions. This document does not clearly outline how the culture can adapt to changing worlds.

4. ***As security professionals, when assessing where limited budgets should be spent, do you believe that investing into the changing of user behaviour towards a more positive security culture is: (please choose one option)***

    d) ***Less important than investing into technical solutions that counter cyber-attacks***
    e) ***Equally as important as investing into technical solutions that counter cyber-attacks***
    f) ***More important than technical solutions that counter cyber-attacks***

    ***Please give a few words to support your answer…..***

Although statistically people are the weakest link in the security chain, I don't think putting the more resources and relying on humans always being correct is the right idea. No matter how intelligent or educated any one human is, it only takes a very short lapse in concentration to make a mistake and potentially an entry point into the companies

security system. I would invest equally into technology which would be the layer deeper than humans (which are the first layer). Without relavant technological measures in place, the company is putting most of its faith into one layer.

5. ***This model focuses on a user's digital behaviour at home and in the office, as it is perceived that a user's digital hygiene should be at an equal level for both, so that the user operates a consistently high level of digital hygiene.***

   ***From your knowledge as security professionals and working with SMEs, do you believe that:***

   ***b) The concept of encouraging a user into operating a higher level of security at home would have a positive impact on overall cyber-security for the business (Yes/No)***

   ***b) An SME is potentially willing to invest in offering its employees help in acquiring and setting up tools for home use, like what they already provide for business end user devices (e.g., VPN, Password Managers etc.) (Yes/No)***

   ***Please give a few words that support your answers….***

   a) Although the risks are lower with employees working from home and by not having strangers in their home, connecting to their home internet and more, people are more relaxed and slack at home which leaves space for malicious attackers. As more people work from home, the more the 'hackers' will look to exploit that and change their attacking profile. So if the attackers are changing, why should the individuals not also adapt to the ways of working from home.

   b) The company should always support their employees in all manners, especially digital security when working from home - the one thing the individual is reliant on, being digital and effective. With individuals now having the freedom to work from home, that also means they can work from anywhere they want, if that's a coffee shop, a beach abroad or in the park via a hotspot. So without the company physically controlling (being in the office with measures in place) how the individual is connecting to confidential information, the company should defiantly provide the individuals with the necessary tools to protect themselves, which will protect the company.

6. ***Any other thoughts or ideas that you have considered in reviewing the framework, which you believe would be useful feedback and has not been covered in this short questionnaire?***

   No

## Questions

7. ***Are there any elements (foundation layers, pillars, or overarching process) which you do not believe would add enough value to make the implementation of that element worthwhile for an SME?***

Structurally the architecture of the model in the "house" diagram is effective. However, in the context of SMEs and the physical human resource capability within an SME it points to a commitment for multiple people. The recognition in the model at the earliest point of the scope for combining of TM and SC etc would make more sense and eliminate a conceptual barrier. The paper as presented does not, in the Executive Summary, provide any benefits table that would immediately engage a time/resource pressured SME to push further into the Framework and scope delivery within their organisation.

8. ***Are there any sub-elements (specific behaviour change techniques within each element) that you do not believe would add enough value to warrant implementing?***

There is confusion in the presentation of BCT and the requirements for individuals i.e. TM Sponsor is the "Figure Head" in 12.2 yet they have active positive behavioural steps that are not connected to the assumption of figure head i.e. 13.1 "promotion and marketing". As the figure head they are then the Role Model and Sponsor - consistency is key to behavioural change and a role model/figure head is more apt when described as setting the standard by living the framework not selling it. Similarly, across the other elements i.e., 6.1 the scope is limited to "working in the office environment" yet the behaviour for the framework to have full effect must encompass all engagement with the SME systems and security not just the office environment.

9. ***From your experience, are there any activities missing within the framework which could further assist an SME to change user behaviour to build a stronger security culture?***

The tasks are not particularly precise enough to add real value i.e. 3.1 and 3.2 have tasks that are weak and undefined for purpose or scope "Take meeting with Security Champion to gauge their comfort with the role" "Offer assistance when required" as a senior manager in a business I am always looking for clear decision making opportunities and if I need guidance then it needs to have purpose and outcome/output potential identified. The Framework could do with a critical review of all the tasks to make them SMART - then they will have both immediate relevance to the business, the business leaders and anybody engaged with the Framework for delivery.

10. ***As security professionals, when assessing where limited budgets should be spent, do you believe that investing into the changing of user behaviour towards a more positive security culture is: (please choose one option)***

***g) Less important than investing into technical solutions that counter cyber-attacks***
***h) Equally as important as investing into technical solutions that counter cyber-attacks***
***i) More important than technical solutions that counter cyber-attacks***

***Please give a few words to support your answer…..***

C - an individual or organisation that has a healthy awareness of and actively engages in their own security behaviours has inherently a lower risk of the human dependant cyber-attack. Technology and its application and maintenance with embedded in systems and processes reinforce the behaviour and provide a discrete technical element of a holistic defence Framework. But the technology is dependent on the human for deployment, maintenance and embedding into process in order to be of immediate and lasting value

***11. This model focuses on a user's digital behaviour at home and in the office, as it is perceived that a user's digital hygiene should be at an equal level for both, so that the user operates a consistently high level of digital hygiene.***

***From your knowledge as security professionals and working with SMEs, do you believe that:***

***c) The concept of encouraging a user into operating a higher level of security at home would have a positive impact on overall cyber-security for the business (Yes/No)***

***c) An SME is potentially willing to invest in offering its employees help in acquiring and setting up tools for home use, like what they already provide for business end user devices (e.g., VPN, Password Managers etc.) (Yes/No)***

***Please give a few words that support your answers….***

For the Framework to be applicable to the SME market then it needs to fundamentally address the physical environment(s) and devices that it must cover. There are a significant number of businesses, not just SMEs, who permit BYOD as a policy or business cost decision and the paper makes little reference directly to how this must be addressed. Every mobile phone in service today owned by an employee probably has the capability to access SME systems as an example is only lightly referenced or addressed in the Framework

***12. Any other thoughts or ideas that you have considered in reviewing the framework, which you believe would be useful feedback and has not been covered in this short questionnaire?***

The structure of the paper is relatively sound and has a logical sequence. However, I personally find the tone and language not particularly SME business focused and at

times ambiguous. As it is written I would not engage much further past the executive summary and section 1. i.e 2.1 Feedback and Monitoring The Security Champion will record instances of behaviours in such instances as potential attacks that were caught, attacks that were successful etc.. in order to build up KPIs to match against the pre-set goals. I have multiple issues with this: 1. Grammar, construct, language and tone. As a statement it is not written to build confidence in a business leader that the Framework is sound. 2. The statement asks that the Security Champion captures the instances - this abrogates the responsibility of the individuals to engage in the Framework et