Global Cyber Security Capacity Centre

Global Cyber Security Capacity Centre: Draft Working Paper

Cyber Security Awareness Campaigns
Why do they fail to change behaviour?

Dr. Maria Bada
Global Cyber Security Capacity Centre,
University of Oxford

Professor Angela Sasse
Department of Computer Science
Science of Cyber Security Research Institute
University College London

July 2014

Contents

Cyber Security Awareness Campaigns: Why do they fail to change behaviour?

Dr. Maria Bada
Global Cyber Security Capacity Centre, University of Oxford, maria.bada@cs.ox.ac.uk

Professor Angela Sasse
Department of Computer Science, Science of Cyber Security Research Institute, University College London, A.Sasse@cs.ucl.ac.uk

Abstract
The present paper focuses on Security Awareness Campaigns, trying to identify factors which potentially lead to failure of these in changing the information security behaviours of consumers and employees. Past and current efforts to improve information security practices have not had the desired effort. In this paper, we explain the challenges involved in improving information security behaviours. Changing behaviour requires more than giving information about risks and correct behaviours – firstly, the people must be able to understand and apply the advice, and secondly, they must be willing to do – and the latter requires changes to attitudes and intentions. These antecedents of behaviour change are identified in several psychological models of behaviour (e.g. theory of reasoned action, theory of planned behaviour, protection motivation theory). We review the suitability of persuasion techniques, including the widely used fear appeals. Essential components for an awareness campaign as well as factors which can lead to a campaign's failure are also discussed.

In order to enact change, the current sources of influence-whether they are conscious or unconscious, personal, environmental or social, which are keeping people from enacting vital behaviours, need to be identified. Cultural differences in risk perceptions can also influence the maintenance of a particular way of life. Finally, since the vast majority of behaviours are habitual, the change from existing habits to better information security habits requires support. Finally, we present examples of existing awareness campaigns in U.K., in Australia, in Canada and Africa.

1 Introduction

1.1 Scope and purpose

Governments and commercial organizations around the globe make extensive use of information and computing (ICT) systems, and need to keep them secure. To achieve this, they deploy technical security measures, and develop policies that specify 'correct' behaviour of employees, consumers and citizens. There is ample evidence that many people do not comply with specified behaviours - some because do not know the risks or the correct behaviour, but most people who do not comply know the correct behaviour when asked.

The primary purpose of security awareness is to influence the adoption of secure behaviours. In this report, we will identify first what behaviours help to deliver information security, and to what extent they are adopted. We will then examine existing approaches to change information security behaviours through awareness campaigns - what works, and what not, and why.

The aim of this paper is to take a first step towards understanding better the reason why changing information security behaviour is such a challenge. IT requires more than simply telling people what they should and should not do: they need first of all to accept that the information is relevant, secondly understand how they ought to do, and thirdly be willing to do this, in the face of many other demands. In order to enact change, the current sources of influence- whether they are conscious or unconscious, personal, environmental or social, which are keeping people from enacting vital behaviours, need to be found. Cultural differences in risk perceptions can also influence the maintenance of a particular way of life.
Finally: even when people are willing to change, the process of learning a new behaviour needs to be supported.

We discuss components for an awareness campaign as well as factors which can lead to a campaign's failure.

1.2 Structure of the paper

Section 2 of this paper reviews existing knowledge about behaviour and behaviour change in general. Models such as the theory of reasoned action, the theory of planned behaviour, protection motivation theory, as well as the importance of self-efficacy as a personal factor are being presented.

Section 3 reviews current information security awareness campaigns and their effectiveness. In section 4, we examine persuasion techniques used in past campaigns. Many campaign designers use fear to encourage people to adopt better practices. Psychological research findings show the importance of fear in attitude and / or behavior change Influence strategies. Also factors which influence change, such as personal, social and environmental factors, are described.

In Section 5 we consider the importance of cultural differences as a factor which influences or prohibits behavioural change. Messages and advertisements are usually preferred when they match a cultural theme of the message recipient.

Section 6, discusses rewards and punishments as a method of influencing people in order to follow a desired behaviour. Section 7, presents the importance of message framing and their persuasiveness.

Section 8, summarises the essential components for a campaign, and section 9 presents the factors which can lead to a campaign's failure.

The last part of this paper, section 10, presents examples of existing awareness campaigns in U.K., in Australia, in Canada and Africa.

1.3 Audience

This paper is written primarily for experts on awareness campaigns, influence strategists as well as experts on education and training.

2 Theoretical Background

In order to change behaviour, there has to be a change in attitudes and intentions. These antecedents of behaviour change are key indices of a person's mental readiness for action and are described in several psychological models of behaviour (e.g. theory of reasoned action, theory of planned behaviour, protection motivation theory).

2.1. Theory of reasoned action

The theory of reasoned action (Ajzen & Fishbein, 1980) proposes an internal decision mechanism in which the formation of intention of behavior is immediately preceding the same behavior and mediates between that and the impact of other variables. According to this theory, the psychological requirements of intended behavior are attitudes and perceived social norms.

Overall, the model supports a linear process in which changes in behavior and normative beliefs of an individual will ultimately affect the actual behavior. Perceived control, the sense one has that he/she can drive specific behavior has been found to affect the intention of behavior but also the real behavior.

2.2. Theory of planned behaviour

The theory of planned behaviour (TPB) was developed by Ajzen in 1988. The theory proposes a model which can measure how human actions are guided. It predicts the occurrence of a particular behaviour, provided that behaviour is intentional.

The theory was intended to explain all behaviours over which people have the ability to exert self-control. The key component to this model is behavioural intent. Behavioural intentions are influenced by the attitude about the likelihood that the behaviour will have the expected outcome and the subjective evaluation of the risks and benefits of that outcome.

The TPB states that behavioural achievement depends on both motivation (intention) and ability (behavioural control). It distinguishes between three types of beliefs - behavioural, normative, and control. The TPB is comprised of six constructs that collectively represent a person's actual control over the behaviour.

1. Attitudes - refer to the degree to which a person has a favourable or unfavourable evaluation of the behaviour of interest. It entails a consideration of the outcomes of performing the behaviour.
2. Behavioural intention - refers to the motivational factors that influence a given behaviour where the stronger the intention to perform the behaviour, the more likely the behaviour will be performed.
3. Subjective norms - refer to the belief about whether most people approve or disapprove of the behaviour. It relates to a person's beliefs about whether peers and people of importance to the person think he or she should engage in the behaviour.
4. Social norms - refer to the customary codes of behaviour in a group or people or larger cultural context. Social norms are considered normative, or standard, in a group of people.

5. Perceived power - refers to the perceived presence of factors that may facilitate or impede performance of a behaviour. Perceived power contributes to a person's perceived behavioural control over each of those factors.
6. Perceived behavioural control.

2.3. Protection motivation theory

Protection motivation theory was originally developed to explain the influence of fear invocations on attitudes and health behaviors (Rogers, 1975).
Protection motivation theory is organized around two cognitive processes: the process of threat assessment and the process of handling assessment.

Based on only one factor of protection motivation theory, vulnerability, we can say that many other factors prevent people to appreciate properly the possibilities of a result. It is important to note that the final threat assessments and handling reflections will react through measurements of intent and behavior.

2.4. Self-efficacy

According to theory of Self-efficacy (Bandura 1977), the adoption of a preventive health behavior, depends on three factors:

- the realization that the person is at risk,
- the expectation that behavior change will reduce this risk and
- the expectation that the person is capable enough to adopt preventive behavior or to refrain from risky health behavior.

It is not simply a matter of how capable is someone but how capable he/she considers to be. Bandura (1977), successfully showed that people with different levels of self-efficacy perceive the world differently. Individuals with a high sense of self-efficacy are generally of the opinion that they have absolute control over their lives. That their personal actions and decisions shape their lives. In contrast, individuals with low sense of self-efficacy feel that their lives do not depend on them.

Our beliefs about self-efficacy, affect the way we think and of course affect our emotional reactions.

2.5. Expected utility hypothesis

In economics, game theory, and decision theory the expected utility hypothesis refers to a hypothesis concerning people's preferences with regard to choices that have uncertain outcomes (gambles). This hypothesis states that if certain axioms are satisfied, the subjective value associated with a gamble by an individual is the statistical expectation of that individual's valuations of the outcomes of that gamble (Bernoulli, Daniel, 1954).
According to the expected utility approach, behavioural change can be explained because individuals perceive it as a 'useful' decision. In the presence of risky outcomes, a decision maker could use the expected value criterion as a rule of choice: higher expected value investments are simply the preferred ones. This hypothesis has proved useful to explain some popular choices

that seem to contradict the expected value criterion (which takes into account only the sizes of the pay-outs and the probabilities of occurrence), such as occur in the contexts of gambling and insurance.

3. Information Security Awareness Campaigns

There is a need to move from awareness to tangible behaviours. Governments and Organizations need to secure their information assets and systems, and develop policies that specify the expected, 'correct' behaviours for their employees. Governments encourage citizens to transact online – and dispense advice on how to do so. But there is ample evidence that major cyber events continue to occur (Kirlappos & Sasse, 2012, Kirlappos, Parkin, & Sasse, 2014). Training as conceived is not working. Caputo, et al., (2013) having spear phishing as an example showed that framing had no significant effect. The study suggested that effective embedded training must take into account not only framing and security experience but also perceived security support, information load, preferred notification method and more.

The fact is that people know the answer to awareness questions but they do not act accordingly to their real life (ISF, 2014, NIST, 2003). The Coventry, et al., report (2014, Government Office for Science, UK) proposes that it is essential for security and privacy practises to be designed into a system from the very beginning. A system difficult to use will eventually lead users to make mistakes and avoid it.

The primary purpose of security awareness is to render people amenable to change (Winkler, I. & Manke, S, 2013). Influence strategists need to identify vital behaviours, meaning behaviours which they wish to change before they start trying to change them. Equally important is identifying the crucial moments when they are most likely to fail in meeting these goals (Patterson, Gremm, Maxfield, McMillan & Switzler, 2011).

Awareness is defined in NIST Special Publication 800-16 (Wilson and Hash, 2003) as follows: "*Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly.*

Questions rise on what exactly is not working and the majority of security awareness campaigns cannot secure the human element. The most recent ISF report (2014), identifies the following reasons:

1. Solutions are not aligned to business risks
2. Neither progress nor value are measured
3. Incorrect assumptions are made about people and their motivations
4. Unrealistic expectations are set
5. The correct skills are not deployed
6. Awareness is just background noise

Persuasiveness of recommendations for health, among other things, is a function of assessing the cost of the recommended behaviour - such as money, time, effort and discomfort - and the reaction efficiency, defined as the probability that compliance with the recommendation will lead to the desired goal.

Various behavioural theories consider the cost and efficiency of a reaction and have independent effects on persuasion. Among health messages, more effective are those tailored to the

individual's needs (Simons-Morton, et. Al., 1997). However, even when the design of the message is taken into account, there is a big gap between the recognition of the threat and the manifestation of the desired behaviour at regular intervals. The attempt to change a certain behaviour is much more difficult when the person is bombarded by a large number of messages about certain issues.

Naturally, an individual who is faced with so many warnings and advice, may be tempted to abandon all efforts to protect himself, and not worry about any danger (Fisher & Rost, 1986). Threatening or intimidating messages are not particularly effective, for the reason that they increase the stress of the individual to such an extent that the individual may even be repulsed or deny the existence of any problem.

An awareness and training program is crucial in that it is the vehicle for disseminating information that users, including managers, need in order to do their jobs. In the case of an IT security program, it is the vehicle to be used to communicate security requirements across the enterprise. An awareness and training program can be effective, if the material is interesting and current. Any presentation that "feels" impersonal and so general as to apply to any audience, will be filed away as just another obligatory session (NIST, Wilson and Hash, 2003).

Briefly, a persuasive message must have four characteristics: First, it needs to attract attention, secondly, it must be understood, thirdly, it must relate to a matter worthy processing and fourthly, its contents will need to be stored and recalled easily from memory.

Research findings show that it is better to present the arguments on both sides. In that case the recipient is able to autonomously decide which of the two would believe. If only convinced by the arguments in favour of a view and then opposing arguments are presented, then it is likely that the initial convictions falter and weaken.

Findings of studies on persuasion, highlighted the existence of an important phenomenon, called ''retardant effect of persuasion'', which refers to persuasion brought about the desired results after a long time later. This phenomenon occurs when the initial belief of a message is changing, and the recipient cannot remember what caused the change (Cook & Flay, 1978).

4. Persuasion Techniques

4.1. Behaviour Change

Persuasion can be defined as an "*Attempt to change attitudes or behaviors or both (without using coercion or deception)" (Fogg, 2002).* There are basically two ways of thinking about changing behaviour (Dolan, et al., MINDSPACE, 2010). The first is based on influencing what people consciously think about, rational or cognitive model. This model suggests that citizens and consumers will analyse the various pieces of information from various sources, the numerous incentives offered to them and act in their best interests. The second model of shaping behaviour focuses on the more automatic processes of judgment and influence. This shifts the focus of attention away from facts and information, and towards altering the context within which people act, the context model. The context model recognises that people are sometimes seemingly irrational and inconsistent in their choices, often because they are influenced by surrounding factors. It focuses more on 'changing behaviour without changing minds'. This route has received rather less attention from researchers and policymakers.

Three factors are particularly useful for understanding controversy around behaviour change (Dolan, et al., MINDSPACE, 2010).

1. **Who the policy affects.** Any behaviour change that will affect a group in particular is likely to require careful justification–there may be particular controversy if the behaviour concerned is seen as integral to a group's identity or culture.
2. **What type of behaviour is intended.** If the harm is seen to be more distant from the individual, it may be seen as a less pressing case for changing behaviour. Making the desired behaviour change clear, salient and justified can balance out people's tendency to care less about "distant" harms. The availability and prestige of evidence and experience may be crucial factors in doing so.
3. **How the change will be accomplished.** MINDSPACE effects depend at least partly on automatic influences on behaviour. This means that citizens may not fully realise that their behaviour is being changed – or, at least, how it is being changed.

4.2. Influence Strategies

Messages which are most concerned on persuading us, are found in advertising, public relations and advocacy. These "persuaders" use a variety of techniques to grab our attention, to establish credibility and trust, to stimulate desire for the product or policy, and to motivate us to act (buy, vote, give money, etc.).

We call these techniques the "language of persuasion".[1] They're not new. Aristotle wrote about persuasion techniques more than 2000 years ago, and they've been used by speakers, writers, and media makers for even longer than that. The basic persuasion techniques include:

- Fear

[1] Media Literacy Project, Language of Persuasion, Retrieved from http://medialiteracyproject.org/language-persuasion

- Association
- Beautiful people (a way to attract attention)
- Experts
- Explicit claims (So are specific, measurable promises about quality,
- Effectiveness, or reliability)
- Humour
- Intensity (comparatives, exaggeration)
- Testimonial
- Repetition

Intermediate persuasion techniques include:

- Nostalgia
- Rhetorical questions
- Scientific evidence
- Symbols. Symbols are words or images that bring to mind some larger concept, usually one with strong emotional content

Advanced persuasion techniques include:

- Analogy (an analogy compares one situation with another)
- Denial
- Group dynamics
- Majority belief
- Scapegoating
- Timing (Sophisticated ad campaigns commonly roll out carefully-timed phases to grab our attention, stimulate desire, and generate a response).

Clearly, lecturing and other attempts at verbal persuasion haven't managed to effect all of the change we need. Usually, single-source strategies are rarely the answer to complex problems (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008).

People do not just follow advice or instructions even if they come from a person of authority. Especially, security education is a field that requires background and experience in the varied subject areas within the security environment that are only accomplished through learning over time (Roper et al., 2006).

In many of the cases listed above, end users do know about the dangers. Security experts have warned them, confused them, and filled them with fear, uncertainty and doubt. People base their conscious decisions on whether they have the ability to do what is required and whether the effort will be worth it[2].

[2] Robinson A., The SANS Institute, 2013. https://www.sans.org/reading-room/whitepapers/awareness/influence-strategies-improve-security-awareness-programs-34385

4.3. Factors influencing change

The increased availability of information has significant effects, most of them positive. But providing information per se often has surprisingly modest and sometimes unintended impacts when it attempts to change individuals' behaviour (Dolan, et al., MINDSPACE, 2010).
A considerable amount of money is being spent by Governments on influencing behaviour, and the success in doing so will be maximised if they draw on robust evidence of how people actually behave. Dolan et al., (MINDSPACE, 2010) outline nine robust influences on human behaviour and change.

1. **Messenger** (who communicates information)
2. **Incentives** (our responses to incentives are shaped by predictable mental short cuts, such as strongly avoiding losses)
3. **Norms** (what others do strongly influences us)
4. **Defaults** (we follow pre-set options)
5. **Salience** (what is relevant to us draws our attention)
6. **Priming** (our acts are often influenced by sub-conscious cues)
7. **Affect** (emotional associations can powerfully shape our actions)
8. **Commitments** (we seek to be consistent with our public promises, and reciprocate acts)
9. **Ego** (we act in ways that make us feel better about ourselves)

To really enact change, we must find the current sources of influence-whether they are conscious or unconscious, personal, environmental or social, which are keeping people from enacting vital behaviours (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008).

Personal motivations refer to feelings associated with an action, while social motivations come from peer pressure and interactions with others in a group. Environmental motivations can be coming either from the physical environment or the ways the culture of an organization rewards and punishes certain activities (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008).

4.3.1. Personal Factors

The individuals and their knowledge, skills and understanding of cybersecurity as well as their experiences, perceptions, attitudes and beliefs are the main influencers on behaviour (Coventry, et al., 2014, Government Office for Science, UK). Personal motivation and personal ability, are the most powerful sources of influence (Patterson, Gremm, Maxfield, McMillan & Switzler, 2011)**.** Awareness professionals can tap into the source of motivation by linking people's actions to their values. By giving people an image of their best selves, and showing them how to stay true to that image, enacting "secure" behaviours can be made inherently satisfying (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008)**.** When values align with actions, people are more excited to work and be more productive (Meyerson, 2011).

In many cases, people will have to overcome existing patterns in order to form new habits. If asked, the conscious mind will invent stories to rationalize these things that the unconscious mind is telling them to do (Hogan, 2005). The desire to behave consistently will drive people to honour a previous commitment to an ideal or an activity (Cialdini, 2009). As users begin to think of themselves as people who are security-conscious, they then begin to act in accordance with this image.

In many cases, these behavioural changes can lead to attitudinal changes. In order people to change their behaviour they have to start by doing something (Hogan, 2005). If a security practitioner is trying to sell an idea or a behaviour, then first he has to present users with a more difficult, more unpleasant or more expensive behaviour.

Changing the emotion associated with an activity is a powerful way to motivate this change in behaviour (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008). "Vicarious experience", using vivid stories that allow the listener to become a participant by identifying with the characters, is a powerful technique for affecting this emotional change (Hogan, 2005).

4.3.1.1. Security Fatigue[3]

People can sometimes get tired of security procedures and processes, especially if the perception is that security is an obstacle, disturbing them all the time. It can also be stressful to remain at a high level of vigilance and security awareness. These feelings can be a sign of Security Fatigue and they can be hazardous to the overall health of an organization or society.

In the security world there is something called the Security vs. Usability Triangle. The basic premise behind the triangle is that you are trying to create a balance between security and usability. If the triangle leans too far in either direction, then this can lead to a super secure system that no one can use, or an insecure system that everyone can use, even hackers. Therefore, there has to be a balance. Security fatigue becomes an issue when the triangle swings too far to the security side.

If security fatigue sets in at an organizational level, it could cause users and administrators to become lax and could open up the doorways for hackers and malicious social engineers.

4.3.2. Social Factors

Another powerful influence source available to security awareness professionals is peer pressure. The majority of people will conform to the social norm. Leadership is a key component of security culture (Coventry, et al., 2014, Government Office for Science, UK). Influential leaders derive their power from four perceptions (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008):

- They are knowledgeable and continue learning
- They have others' best interests at heart
- They are generous with their time and well connected
- They speak their minds directly

4.3.3. Environmental Factors

To change behaviour, the easiest thing to do may often be to change the environment and make the desired behaviour easier to achieve. Environmental influencers reflect the design of the

[3] O'Donnell Andy, How to Prevent IT 'Security Fatigue. Retrieved from: http://netsecurity.about.com/od/advancedsecurity/a/How-To-Avoid-IT-Security-Fatigue.htm

environment, the physical environment such as the workplace, and the technology, but also the economic factors (Coventry, et al., 2014, Government Office for Science, UK).

4.4. Fear

A meta-analysis (Sutton, 1982) research conducted on communication invoking fear held between 1953 and 1980, showed that increases in perceived level of fear led to increases in the acceptance of the proposed adjustment or behavioural intention.

4.4.1. Fear as a persuasion approach

The invocation of fear is "*a persuasive message designed to scare the world, describing the terrible things that will happen if they do not do what the message recommends*» (Witte, 1992). Surveys have shown that fear can be a quite persuasive tactic to specific situations or counterproductive tactic in other (Ahluwalia, 2000). Psychological research findings show the importance of fear in attitude and / or behaviour change (Levanthal, 1970; Girandola, 2000).

Various theoretical approaches have been used to explain the effect of fear persuasion e.g. The Drive Model-Janis, (1967), The Parallel Reaction Model (Levanthal, 1970) and the Protection Motivation Theory (Rogers, 1975; 1983).

Culturally sensitive interventions have been found to cause more effective changes in behaviour in high-risk populations, such as adolescents. This finding suggests that interventions based on major theoretical knowledge to change behaviour (e.g., social learning theory or the theory of self-efficacy) take into account the cultural beliefs and attitudes, and are more likely to succeed (Arthur, Quester, 2004).

O'Keefe (1990), makes an important distinction between the two definitions of fear invocations (message content - public reactions) and he notes that messages with horrible content may not cause fear and that fear may be caused without frightening contents. However, the majority of research on invoking fear have combined both definitions to handle fear invocations.

When researchers refer to a strong condition of fear invocation, usually they mean that the message represents a big threat and the recipient perceived a big threat. Typically, the invocations of fear offer recommendations that are as efficacious in preventing the threat. Thus, the three central structures in fear invocations is fear, threat and efficacy.

4.5. Control

''Perceived Control'' is a core construct that can be considered as an aspect of empowerment (Eklund, & Backstrom, 2006). It refers to the amount of control that people feel they have, as opposed to the amount of ''Actual Control'' that they have. In contrast, ''Vicarious Control'' and ''Vicarious Perceived Control'' refer to the amount of control that outside entities have over the subject.

The positive effects of perceived control mainly appear in situations where the individual can improve its condition through its own efforts. Also, the greater the actual threat, the greater the

value that perceived control can play. When we apply this theory to information security, we could assume that home computer users often experience high levels of actual control over their risk exposure. They can choose which websites to visit, whether to open email attachments and whether to apply system updates. In contrast, employees in big organisations, lack the sense of control, since IT experts control every aspect of security (More Josh, 2011).

Ajzen (2002), introduced a new concept concerning the relationship between self-efficacy and perceived behavioral control. He argued that "*the central concept of perceived behavioral control consists of two factors: self-efficacy (on the ease / difficulty of performing a behavior) and the ability to control (the extent to which performance depends entirely on the person)*."

5. Culture

Culture is also an important factor that can influence the process of persuasion. Messages and advertisements are usually preferred when they match a cultural theme of the message recipient. As a result, cultural factors are being in consideration when designing messages (Kreuter & McClure, 2004).

The role of culture in the persuasion process is until now under research. How can cultural factors impact the persuasion process? Is persuasiveness of a message determined by the cultural background of the message recipient and its framing in order to be congruent with culturally divergent motivational styles?

Cultural systems shape a variety of psychological processes. Motivational orientation is one potential process behind cultural differences. Messages that match regulatory focus can ''feel right'' and this feeling leads us to an evaluation of the content of the message, which increases persuasiveness (Uskul, A. et. al., 2009).

Messages are more persuasive when there is a match between the recipient's cognitive, affective or motivational characteristics and the content of framing of the message. Also, messages are more persuasive if they match and individual's ought or self-guides, or self-monitoring style (Uskul, A. et. al., 2009).

The Regulatory focus theory (Higgins, 1998), proposes that in a promotion-focused mode of self-regulation, individuals' behaviours are guided by a need for nurturance, the desire to bring one's actual self into alignment with one's ideal self, and the striving to attain gains. In a prevention-focused mode of self-regulation individual's behaviours are guided by a need of security, the need to align one's actual self with one's ought self by fulfilling one's duties and obligations and the striving to ensure non-losses.

The values that distinguish country cultures from each other could be categorised into four groups (Hofstede at al., 2010)[4]. The Hofstede dimensions of national culture are a) Power Distance (PDI) b) Individualism versus Collectivism (IDV) c) Masculinity versus Femininity (MAS) and d)Uncertainty Avoidance (UAI). Culture can be only used meaningfully by comparison. The forces that cause cultures to shift tend to be global or continent-wide. This means that they affect many countries at the same time, so if their cultures shift, they shift together and their relative positions remain the same. Exceptions to this rule are failed states and societies in which the levels of wealth and education increase very rapidly.

In Western more individualistic cultures, people tend to define themselves in terms of their internal attributes such as goals, preferences and attitudes. Individuals tend to focus on their personal achievements and tend to favour promotion over prevention strategies focusing on positive outcomes that they hope to approach, rather than the negative outcomes they hope to avoid (Lockwood, Marshall, & Sadler, 2005). Providing messages that fit the dominant regulatory focus of individuals may lead to a ''feeling right'' experience and thus to an increased persuasion (Cesario et al., 2004).

[4] http://geert-hofstede.com/national-culture.html

In Eastern more collectivist cultures, individuals tend to define themselves in terms of their relationships and social group memberships (Triandis, 1989). In this cultural context, individuals tend to avoid behaviours that cause social disruptions and they favour prevention over promotion strategies focusing on the negative outcomes which they hope to avoid rather than the positive outcomes they hope to approach (Lockwood et al., 2005).

5.1. Culture and Risk perception

Risk perception refers to people's responses to questions regarding the riskiness of their decisions and actions (Weber E. & Hsee Ch., 2000). Perception of risk can be a collective phenomenon (Douglas, M., & Wildavsky, A., 1982). Each culture selects some risks for attention and chooses to ignore others.

Cultural differences in risk perceptions are explained in terms of their contribution to maintaining a particular way of life. There are different patterns of interpersonal relationships such as archical, individualist, egalitarian, fatalist and hermitic. Risk is also seen as the other side of trust and confidence, as the result of the way in which the theory see risk perception as being imbedded in social relations (Douglas, M., & Wildavsky, A., 1982).

6. Rewards and Punishments

Rewards and punishments can be used in order to influence people follow a desired behaviour. Both rewards and punishments, however, can have unintended consequences[5]. Rewarding people for an activity that they already enjoy makes that activity less desirable, while the receiver of the reward begins to question the intrinsic value of the activity (Kohn, 1994). Even honouring certain employees that follow the new standards may backfire, causing others to feel resentful (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008).

This process is called, "Incentivized Awareness Programs" (Winkler & Manke, 2013)[6]. That better represents what we are talking about, as a comprehensive awareness program does not limit itself to a single tool. With incentivized awareness (Gamification), you create a reward structure that incentivizes people to exercise the desired behaviours, which could include seeking out additional training. The incentives ideally make demonstrating or learning about awareness behaviours fun.

Rewarding people for doing the right behaviours makes them more security conscious. In general, extrinsic rewards should not be the first strategy. They could be used them only in conjunction with motivational strategies that encourage intrinsic satisfaction and social support (Kohn, 1994). Short-term goals need to be created and small improvements in those vital behaviours can be celebrated.

Economists argue that we are more inclined to avoid actual loss than to strive for conditional benefits. This tendency is called loss aversion and it refers to not setting the stakes too high.

[5] Robinson A., Using influence strategies to improve security awareness programs, The SANS Institute, 2013. Retrieved from: https://www.sans.org/reading-room/whitepapers/awareness/influence-strategies-improve-security-awareness-programs-34385

[6] Winkler & Manke (2013).

1. 7. Media-Framed Messages

Media constructions often serve as a heuristic for citizens, whose understanding of issues is powerfully shaped by the values involved (Domke D. et al., 1998). Prevention messages typically try to convey either the benefits of performing a behaviour (gain-framed messages) or the costs associated with failing to perform a health-promoting behaviour. Gain-framed messages are usually more persuasive when they are used to promote prevention behaviours. Messages which are congruent with a person's predominant motivational orientation are more effective than messages that are not congruent.

Most studies on framing have compared the persuasive power of messages emphasizing the benefits of performing a behaviour, to messages highlighting the cost of not performing a behaviour (similar framing effects). The distinction between positive and negative messages, with respect to either the presence or absence of pleasant or unpleasant results seem to be a useful conceptual tool for studying the role of pre-existing perceptions about safety issues. Broemer, P. (2002), states that the framework would be relevant even when given only negative results.

2. 8. Essential Components for a Campaign

In order a Campaign to be successful, there are several essential components which need to be taken into consideration (Winkler Ira and Manke Samantha, 2013)[7].

1. **Communication**. A significant part of a campaign is communication. This can be accomplished by collateral, internally distributed materials. These are things like newsletters, blogs, and other internal communications. Also, posters are a very crucial method of raising awareness. While some people believe they are old-fashioned and outdated, they can be very effective when they are well designed.
2. **Computer Based Training.** CBT is the most omnipresent component of security awareness programs, as it is the most clearly accepted method of achieving compliance.
3. **Events.** Well-executed events bring the Security Awareness program, and the whole security effort for that matter, to life.
4. **Security Portal.** An internal security portal provides several functions. It provides a Knowledge base that can provide a huge return on investment with includes information on security related topics. It is also important to include information on home and personal security strategies, such as protecting children online and securing social media accounts.
5. **Behavioural Testing and Teachable Moments.** Phishing, USB drive drops, and Social Engineering tests require some care, but are important components to give your employees a "teachable moment."
6. **Teaching New Skills Effectively**. What looks like a lack of motivation is sometimes really a lack of ability (Patterson, Gremm, Maxfield, McMillan & Switzler, 2011). As teachers, security awareness professionals must break down complex goals in short, clear achievable steps.

[7] Winkler & Manke (2013).

3. 9. Factors which lead to a Campaign's failure

In order a Campaign to be successful, there are several factors which need to be avoided (Winkler and Manke, 2013)[8].

1. **Not understanding what security awareness really is.** Information must be provided in a way that relates to how people think and behave. There must be a personal association of how knowledge would impact their actions. There is also a difference in providing an individual information on a one time basis, and delivering information in different formats over the course of time to effect change.
2. **Compliance.** In short, saying your awareness program is compliant does not necessarily equate to create the desired behaviours.
3. **Illustrate that awareness is a unique discipline.** A good security awareness professional will have good communication ability, be familiar with learning concepts, understand that awareness is more than a check the box activity, knowledge of a variety of techniques and awareness tools, and an understanding that there is a need for constant reinforcement of the desired behaviours.
4. **Lack of engaging and appropriate materials.**
5. **Not collecting metrics.** By collecting regular metrics, you can adjust your program to the measured effectiveness. By determining what is working and what is not, you can tailor future programs based upon lessons learned. The appropriate metrics also allow for the determination of which components are having the desired impact. They should be taken prior to starting any engagement effort, at least once during the engagement, and also post-engagement.
6. **Unreasonable expectations**. No security countermeasure will ever be completely successful at mitigating all incidents. There will always be a failure.
7. **Arrange multiple training exercises**. Focusing on a specific topic or threat does not offer the overall training needed.

[8] Winkler & Manke (2013).

4. 10. Case Studies

10.1. Cyber Security Awareness Campaigns in U.K.

10.1.1. GetSafeOnline Campaign[9]

This campaign focuses on users at home and businesses. Get Safe Online is a jointly funded initiative between several Government departments and private sector businesses. It provides practical advice on how to protect yourself, your computers and mobiles device and your business against fraud, identity theft, viruses and many other problems encountered online. It contains guidance on many other related subjects too – including performing backups and how to avoid theft or loss of your computer, smartphone or tablet. Every conceivable topic is included on the site – including safe online shopping, gaming and dating. The site also keeps you up to date with news, tips and stories from around the world. Unfortunately, there is too little information regarding cyberbullying and how to act when you are a victim.
The site offers easy access by listing information. All information appears on the home page. Also a question Fag and possibility to apply your own question.

Message: The positive message of ''get safe online'' again gives the responsibility to users for staying safe.
The campaign covers, topics such as:

- Protecting Your Computer
- Protecting Yourself
- Smartphones & Tablets
- Shopping, Banking & Payments
- Safeguarding Children
- Social Networking
- Businesses

The campaign offers a repository of threats and how-to advice but its tone and approach is based on essential fear tactics. As previously discussed, messages with horrible content may not cause fear and that fear may be caused without frightening contents. Fear invocations cannot be successful in changing behaviour if the three central structures of fear invocations - fear, threat and efficacy - are combined.

It is very important to embed positive information security behaviours, which can result to thinking becoming a habit. Messages and advertisements are usually preferred when they match a cultural theme of the message recipient. Messages also can be more persuasive when there is a match between the recipient's cognitive, affective or motivational characteristics and the content of framing of the message.

[9] www.getsafeonline.org

10.1.2. The 'Cyber Streetwise' campaign[10]

This campaign focuses on users at home and businesses. The campaign advices home users to use social media responsibly, to keep a child's identity safe. In short, this campaign presents users as the weakest links in the cyber security chain.

The new Home Office Cyber Streetwise site advises businesses to adopt five basic measures. These include, using strong, memorable passwords, installing antivirus software on all work devices, checking privacy settings on social media, checking the security of online retailers before loading card details and patching systems as soon as updates are available. The service will be of particular use to small and medium-sized businesses.

A survey of FTSE 350 companies by the Department for Business, Innovation and Skills last month revealed that only 14 per cent are regularly considering cyber threats, with a significant number not receiving any intelligence about cyber criminals.

It is a campaign which tries to cause a behavioural change by providing tips and advice on how to improve online security.

- It urges businesses to get online
- To take control of their online behaviour
- Suggests to companies that a well-designed site provides a sense of security and business reliability.
- Suggests that the good reputation of a company for safety and security online will lead to business growth and will boost sales.

Message: The campaign uses a positive message method to influence the behaviour of users. ''*In short, the weakest links in the cyber security chain are you and me*''. This campaign represents several advances on past government-supported efforts:

1. The campaign targets specific demographic groups: based on Experian's MOSAIC product of UK demographics, X target users groups have been identified by age, gender and education/profession: small and medium businesses, seniors, middle aged men who know it all, etc.). Specific cyber threats, and how to protect against them been designed by communication professionals, is visually appealing and engaging, and avoids the 'scare factor'. It also presents the materials in the context of everyday tasks that people recognise: banking
2. The effect of targeted campaigns is measured through a set of Key Performance Indicators (KPI) for secure online behaviours.

The campaign covers, topics such as:

1. Passwords
2. Bank safely online / on your mobile
3. Common shopping scams
4. Computer health
5. Identity theft

[10] www.cyberstreetwise.com

6. Operating system and software updates
7. Online payment options
8. Online shopping
9. Phishing
10. Social media
11. Smart phone health
12. Wireless network security

These are the main advice suggestions on security for users. The advice usually comes from security experts and service providers, who monotonically repeat suggestions such as 'use strong passwords'. That advice pushes responsibility and workload for issues that should be done by the service providers and product vendors onto users, not caring that following this advice would be a near-full-time job for those who can understand it.

One of the main reasons why users do not behave optimally is that security systems and policies are poorly designed. Security awareness, education and training cannot just 'fix' security problems (Coventry, et al., 2014, Government Office for Science, UK). If security is difficult to use, too complex, too effortful, people will not do it. Perceived control, the sense one has that he/she can drive specific behaviour has been found to affect the intention of behaviour but also the real behaviour. Currently users' time and goodwill is being wasted on security that is too difficult to use, and not effective (Kirlappos, I., & Sasse, M. A., 2012).

10.1.3. Webwise Campaign[11]

This campaign focuses mainly on parents and home users. It provides basic knowledge on various cyber risks and basic protection tips. The site offers Information, games, news, resources and video relating to disability.

Message: The campaign urges users to ''*Make the most of being online*''. It offers an online course, whereas basic technology is used.

The campaign covers, topics such as:

- Home
- Your computer
- Using the web
- Email & sharing
- Living & interests
- Safety & privacy
- Glossary

[11] http://www.bbc.co.uk/webwise/0/

1.1.4. Good to know Google's[12]

This campaign targets the general public but mainly families. It provides basic knowledge on various cyber risks and basic protection tips. The site offers Information, games, news, resources and video relating to disability.

Message: The campaign uses a more collective/collaborative message ''*Working together to stay safe online*''. It is friendly to users with a step by step guide.

The campaign covers, topics such as:

- Manage your privacy and security
- Prevent cybercrime
- Getting started
- Explore with confidence
- Manage your online reputation

Google launched the "*Good to Know*" campaign promoting online safety in association with the Citizens Advice Bureau (CAB).

10.1.5. Behind the Screen[13]

Behind the Screen is a hub of free computing resources for your GCSE students, complete with lesson plans and mark schemes. The resources are developed with industry to provide authentic projects mapped to computing, ICT and computer science qualifications.

The Behind the Screen projects and resources are currently free to use for all UK schools. There are eight projects live on the site. Projects are developed with key industry partners who provide the real life business cases and ideas for each, and supply industry resources and software for students to use. Projects are presented as problems through a brief, and students are guided through to their solution. All resources they need to achieve the outcomes are provided. Projects take from 6 to 15 hours to complete, depending on the route taken. Extension activities are also provided.

Projects are supported with lesson plans, guides, mapping to current Key Stage 4 qualifications, and presentations to support delivery. Assessment is through a Student Log, and teachers are provided with an exemplar to make assessment straightforward.

10.1.6. Cyber Security Challenge UK[14]

Cyber Security Challenge UK is helping to fill the cyber security skills gap by tapping into untapped talent. It is a not-for-profit organisation which operates primarily through sponsorship. Its main role is to run a national programme of competitions which are designed to attract and inspire new talent into the UK cyber security profession.

[12] https://www.google.co.uk/goodtoknow/
[13] http://www.behindthescreen.org.uk/
[14] http://www.cesg.gov.uk/awarenesstraining/Pages/Cyber-Security-Challenge-UK.aspx

Sponsored by over 50 organisations from government, industry and academia and leading sponsor Government Communications Headquarters (GCHQ), the Challenge sets competitions that test existing cyber security skills, runs cyber camps to help individuals develop new skills, and provides information through networking events on cyber security career changes.

CESG have produced two posters for the Palace of Westminster to help raise IA awareness which can be customised with your own logo for use in your own government department (or supporting industry partner).

10.1.7. The Devil's In Your Details[15]

In the first campaign of its kind involving both the private and public sectors, The Devil's in Your Details campaign brings together Action Fraud, The Telecommunications UK Fraud Forum (TUFF) and Financial Fraud Action UK - the name under which the financial services industry coordinates its fraud prevention activity, in a powerful demonstration of what can be achieved when industry and government work together.

The National Fraud Authority backed campaign is raising awareness of the importance of protecting personal information and aims to remind the public to check that who they share their details with is genuine**.** The Devil's In Your Details campaign encourages consumers to suspect anyone or anything they are uncertain about, to keep asking questions and to challenge or end an engagement if it feels uncomfortable. As an introduction to a wider campaign against fraud, this awareness activity aims to increase reporting of fraud, making it harder for fraudsters to target consumers in the future.

The campaign includes professional videos which are very well presented. But it scared less experienced people away from online transactions, which is not what government intends to achieve. Fear invocations cannot be successful in changing behaviour if the three central structures of fear invocations - fear, threat and efficacy - are combined. It is crucial to decide the target group of a campaign and try to match a cultural theme of the message recipient but also match the recipient's cognitive, affective or motivational characteristics with the content of framing of the message.

It is very important to embed positive information security behaviours, which can result to thinking becoming a habit, instead of using fear invocations often leading to pure avoidance of the suggestion.

10.1.8. VOME[16] Visualisation and Other Methods of Expression

VOME is a three year collaborative research project bringing together researchers from the Information Security Group (ISG) at Royal Holloway, University of London, Salford and Cranfield Universities, working with consent and privacy specialists at Consult Hyperion and Sunderland City Council, to explore how people engage with concepts of information privacy and consent in on-line interactions.

[15] http://www.actionfraud.police.uk/thedevilsinyourdetails
[16] http://www.vome.org.uk/

The purpose of VOME (Visualisation and Other Methods of Expression) is to explore how user communities engage with concepts of information privacy and consent in on-line interactions. The aim is to develop alternative conceptual models of on-line privacy which enable users to make clearer on-line disclosure choices. These decision making models will facilitate a better dialogue between the designers of privacy and consent functionality and their customers.

This project offers benefits to on-line service providers, the manufacturers of technology used to deploy on-line services, as well as the general public. To date there has been considerable interest in this project from each of these communities.

This is a more innovative approach to raising awareness including games, theatre and other methods of expression.

10.2. Cyber Security Awareness Campaigns in Australia

10.2.1. Stay Smart Online[17]

This is a one-stop shop providing information for Australian Internet users on the simple steps they can take to protect their personal and financial information online. The site has informative videos, quizzes and a free Alert Service that provides information on the latest threats and vulnerabilities**.**

10.2.2. ThinkUKnow - Internet Safety Program[18]

ThinkUKnow is an Internet safety program delivering interactive training to parents, carers and teachers. Created by the UK Child Exploitation and Online Protection (CEOP) Centre, ThinkUKnow Australia has been developed by the Australian Federal Police (AFP) and Microsoft Australia. Users will need to subscribe to the site to gain access to its tools and resources.

10.2.3. Tagged (CyberSmart) - ACMA[19]

Developed by the ACMA's Cybersmart program, Tagged has received acclaim for its realistic depiction of teenagers and the problems they can face in a digital world. Since its launch in September 2011, Tagged has become a popular resource for Australian teachers and parents. More than 10,000 copies of the film and posters have been distributed nationwide and it has attracted nearly 50,000 views on YouTube.

10.2.4. Smart online, safe offline (SOSO) - National Association for Prevention of Child Abuse and Neglect (NAPCAN)[20]

By using social networking environments to target children and young people directly, the SOSO initiative educates children and young people about the dangers that exist online and on how they can manage their personal safety.

[17] http://www.staysmartonline.gov.au/
[18] http://www.thinkuknow.org.au/site/
[19] http://www.cybersmart.gov.au/Home/Teens/Games%20and%20videos/tagged.aspx
[20] http://napcan.profero.com.au/soso

10.2.5. Make cyberspace a better place - KIDS Helpline[21]

Kids Helpline campaigns to help children enjoy the freedom and fun of using the Internet and to and help make cyberspace a fun and safe place.

10.2.6. The Alannah & Madeline Foundation - Keeping children safe from violence[22]

This national charity aims to protect children from violence and its devastating impact. The website provides a range of information and resources for parents and children, including an evidence-based educational program (eSmart Schools), and a variety of other resources about bullying and cybersafety.

Some campaigns are delivered in collaboration with a wide variety of public and private agencies. As a result, there is a large degree of crossover in the material of various contributors presented across the websites. Furthermore, initiatives may target a specific issue (such as cyberbullying), or they may be delivered as part of a broader social awareness campaign (child protection).

10.2.7. Who's chatting to your kids? - Queensland Police Resource[23]

A brochure published by the Queensland Police Service's Task Force Argos. This brochure provides information to parents on Internet safety for children and young people. It discusses social networking, mobile phones, webcams and online gaming, and provides information about the types of things to look out for that may indicate that children could be at risk.

Some of the more popular social networking sites provide information specifically tailored to help parents understand their child's use of the site.

10.2.8. Keep it Tame[24]

Keep it Tame Campaign tries to Promote Online Safety and Measure Behaviour Change in Young People. This is an online campaign targeting Australian teenagers, drawing attention to the consequences of thoughtless and hurtful use of social media and empowering them to act with respect online.

Unique to the campaign is the application of an innovative digital tracking methodology which – in conjunction with a cohort study that will survey and interview young people over time – will measure its impact on behaviour change.

The campaign guides teenagers through a series of mock social media posts. As things turn nasty, an animated creature slowly becomes more grotesque, highlighting the hurtful effects of the online exchanges and ultimately encouraging people to act with respect. The Keep it Tame

[21] http://www.kidshelp.com.au/teens/get-info/cyberspace/
[22] http://www.amf.org.au/bullying/
[23] http://www.police.qld.gov.au/programs/cscp/personalSafety/children/childProtection/
[24] http://www.youngandwellcrc.org.au/keep-tame-campaign-promote-online-safety-measure-behaviour- change-young-people/

campaign is the first in a series of campaigns to come out of the Young and Well CRC'sSafe and Well Online project, a five-year study of the most effective ways to design, deliver and evaluate online social marketing campaigns aimed at improving safety and wellbeing.

This project is an initiative of the Young and Well CRC and is led by the University of South Australia in conjunction with the University of Western Sydney, Zuni and the Queensland University of Technology. Safe and Well Online builds upon the original Smart Online Safe Offline initiative developed by NAPCAN.

10.3. Cyber Security Awareness Campaigns in Canada

10.3.1. Get Cyber Safe[25]

Get Cyber Safe is a national public awareness campaign created to educate Canadians about Internet security and the simple steps they can take to protect themselves online. The campaign's goal is to bring together all levels of government, the public and private sectors, and the international community, to help Canadians be safer online.

The campaign is an important component of Canada's Cyber Security Strategy, which is dedicated to securing government systems, partnering to secure vital cyber systems outside the federal government, and helping Canadians to be secure online.

The campaign is being led by Public Safety Canada on behalf of the Government of Canada.

10.3.2. Stop Hating Online[26]

Stop Hating Online is the Government of Canada's anti-cyberbullying public awareness campaign. It focuses on cyberbullying in terms of social impacts and potential legal consequences. As a comprehensive resource for parents and youth, GetCyberSafe.ca provides information, advice and tools to prevent and stop hate, cyberbullying and the non-consensual distribution of intimate images that can take place online, including through social networks and mobile messages. The campaign encourages everyone to stand up against cyberbullying.

10.4. Cyber Security Awareness Campaigns in Africa

10.4.1. ISC Africa[27]

A coordinated, industry and community-wide effort to inform and educate Africa's citizens on safe and responsible use of computers and the internet so that we can minimise the inherent risks and increase consumer trust.

[25] http://www.getcybersafe.gc.ca/cnt/bt/index-eng.aspx
[26] http://www.getcybersafe.gc.ca/cnt/blg/pst-20140109-eng.aspx
[27] http://iscafrica.net/#home

10.4.2. Parents corner[28]

The effort is intended to co-ordinate the work done by government, industry and civil society. Its objectives are to protect children, empower parents, educate children and create partnerships and collaboration amongst concerned stakeholders. Parents' Corner tips for a safer internet include:

1. People aren't always who they say they are.
2. Think before you post.
3. Likewise, children need to think before they respond to things that other people have posted.
4. It's not just about computers. Many parents don't understand that the Internet their children can access via their cell phones is the same Internet accessed via a computer.
5. Finally, just as they would in real life, friends must protect friends.

[28] http://www.parentscorner.org.za/

11. Conclusions

The ISF report (February 2014), proposes that simple transfer of knowledge is not enough. Knowledge and awareness is a prerequisite to change behaviour but not necessarily sufficient and this is why it has to be implemented in conjunction with other influencing strategies. It is very important to embed positive information security behaviours, which can result to thinking becoming a habit, and a part of an organisation's information security culture. One of the main reasons why users do not behave optimally is that security systems and policies are poorly designed.

Moreover, the advice usually comes from security experts and service providers, who monotonically repeat suggestions such as 'use strong passwords'. But, security awareness, education and training cannot just 'fix' security problems. If security is difficult to use, too complex, too effortful, people will just not accept it (Coventry, et al., 2014, Government Office for Science, UK). Currently users' time and goodwill is being wasted on security that is too difficult to use, and not effective (Kirlappos, I., & Sasse, M. A., 2012). Behaviour change in an information security context could be measured through risk reduction, but not through what people know, what they ignore or what they do not know.

Culture is also an important factor that can influence the process of persuasion. Messages and advertisements are usually preferred when they match a cultural theme of the message recipient. As a result, cultural factors are being in consideration when designing messages (Kreuter & McClure, 2004). Messages also can be more persuasive when there is a match between the recipient's cognitive, affective or motivational characteristics and the content of framing of the message. Also, messages are more persuasive if they match and individual's ought or self-guides, or self-monitoring style (Uskul, A. et. al., 2009).

As previously discussed while reviewing existing awareness campaigns fear invocations are often used, as influence strategies. But, fear invocations are proved insufficient to change behaviour. They cannot be successful in changing behaviour if the three central structures of fear invocations - fear, threat and efficacy - are not combined. As previously discussed, messages with horrible content may not cause fear and fear may be caused without frightening contents.

Following that rationale of the expected utility approach, perhaps increasing the 'perceived utility' of cybersecurity could be one additional factor to improve the effectivity of awareness campaigns. Also, perceived control and personal handling ability, the sense one has that he/she can drive specific behaviour has been found to affect the intention of behaviour but also the real behaviour. A campaign should use simple consistent rules of behaviour that people can follow. This way, their perception of control will lead to better acceptance of the suggested behaviour.

We suggest that the following factors can lead to more sufficient awareness campaigns:

1. Awareness has to be professionally prepared and organised in order to work.
2. Causing feelings of fear to people is not an effective tactic, since it will put off people who can least afford to take risks. To make the internet accessible, risks should not be exaggerated.
3. Awareness alone is not enough. Usually all it does is catch attention.

4. Security education has to be more than providing information to people - it needs to be targeted, actionable, and doable. At the moment, what is correct behaviour is far too difficult and complex. We need simple consistent rules of behaviour that people can follow.
5. Once people are willing to change, training and feedback is needed to sustain them through the change period.

References

Ajzen, I. (1988). Attitudes, personality, and behaviour. Dorsey Press, Chicago.

Bernoulli, Daniel, "Exposition of a New Theory on the Measurement of Risk". Originally published in 1738, translated by Dr. Louise Sommer. (January 1954). *Econometrica* (The Econometric Society) **22** (1): 22–36. doi:10.2307/1909829.

Caputo, D., Lawrence Pfleeger, Sh., Freeman, D.J., Johnson, E.M. Going Spear Phishing: Exploring Embedded Training and Awareness, IEEE Security & Privacy, vol. 12, no. 1, pp. 28-38, Jan.-Feb. 2014, doi:10.1109/MSP.2013.106.

Cesario, J., Grant, H., & Higgins, T.E. (2004). Regulatory fit and persuasion: Transfer from ''feeling right''. *Journal of Personality and Social Psychology, 86,* 388-404.

Cook, T., & Flay, B. (1978). The temporal persistence of experimentally induced attitude change: An evaluative review. In L. Berkowitz (Ed.), *Advances in experimental social psychology* (vol. 11). New York: Academic Press.

Coventry, D.L., Briggs, P., Blythe, J., Tran, M. (2014). Using behavioural insights to improve the public's use of cyber security best practices. Government Office for Science, London, UK. Retrieved from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/309652/14-835-cyber-security-behavioural-insights.pdf

Dolan P., Hallsworth, M., Halpern, D., King,D., Vlaev, I. MINDSPACE Influencing behaviour through public policy, Institute for Government, Cabinet Office, 2 March 2010. Retrieved from: http://www.instituteforgovernment.org.uk/sites/default/files/publications/MINDSPACE.pdf

Domke David, Shah V. Dhavan and Wackman B. Daniel (1998). Media Priming Effects: Accessibility, Association and Activation. *International Journal of Public Opinion Research, 1(1),* 51-74.

Douglas, M., & Wildavsky, A. (1982). *Risk and culture: An essay on the selection of technological and environmental dangers.* Berkeley: University of California Press.

Eklund, M., & Backstrom, M. (2006). The role of perceived control for the perception of health by patients with persistent mental illness. *Scandinavian Journal of Occupational Therapy, 13,* 249-256.
Fogg, B. J. (2002). Persuasive Technology: Using Computers to Change What We Think and Do. Morgan Kaufmann.

Fisher, E.B., & Rost, K. (1986).Smoking cessation: A practical guide for the physician. *Clinics in Chest Medicine, 7,* 551-565. Hofstede, G., Hofstede, J.G., Minkov, M. Cultures and Organizations: Software of the Mind. 3rd Edition, McGraw-Hill USA, 2010.

Higgins, E.T. (1998). Promotion and prevention: Regulatory focus as a motivational principle. *Advances in Experimental Social Psychology, 30*, 1-46.

Information Security Forum (ISF). From Promoting Awareness to Embedding Behaviours, Secure by choice not by chance, February 2014. Retrieved from: https://www.securityforum.org/shop/p-71-170

Kirlappos, I., Sasse, M. A. (2012). Security Education against Phishing: A Modest Proposal for a Major Rethink. *IEEE Security and Privacy Magazine* 10(2), 24-32

Kirlappos, I., Parkin, S., Sasse, M. A. (2014). Learning from "Shadow Security": Why understanding non-compliance provides the basis for effective security. *Workshop on Usable Security*Kreuter, M. W., & McClure, S. M. (2004). The role of culture in health communication. *Annual Review of Public Health, 25*, 439-455.

Lapowsky Issie (2013). Reward vs. Punishment: What Motivates People More? Retrieved from: http://www.inc.com/magazine/201304/issie-lapowsky/get-more-done-dont-reward-failure.html

Lockwood, P., Marshall, T., & Sadler, P. (2005). Promoting success or preventing failure: Cultural differences in motivation by positive and negative role models. *Personality and Social Psychology Bulletin, 31,* 379-392.

Media Literacy Project, Language of Persuasion, Retrieved from http://medialiteracyproject.org/language-persuasion

More Josh (2011). Measuring Psychological Variables of Control In Information Security, - January 12, Retrieved from http://www.sans.org/reading-room/whitepapers/awareness/measuring-psychological-variables-control-information-security-33594

NIST, National Institute of Standards and Technology. Building an Information Technology Security Awareness and Training Program. Wilson, M. and Hash, J. Computer Security Division Information Technology Laboratory. October 2003. Retrieved from:http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

O'Donnell Andy, How to Prevent IT 'Security Fatigue. Retrieved from: http://netsecurity.about.com/od/advancedsecurity/a/How-To-Avoid-IT-Security-Fatigue.htm

Palmer, C.G.S. (1996). Risk perception: An empirical study of the relationship between worldview and the risk construct. *Risk Analysis, 16*, 717-724.

Robinson Alyssa, Using influence strategies to improve security awareness programs, The SANS Institute, 2013. Retrieved from: https://www.sans.org/reading-room/whitepapers/awareness/influence-strategies-improve-security-awareness-programs-34385

Roper, C., Fischer, L., Grau, J. Security Awareness, Education and Training, Elsevier Inc. UK, 2006. ISBN-13: 978-0750678032.

Simons-Morton, B.G., Donohew, L.C., Aria, D. (1997). Health communication in the prevention of alcohol, tobacco and drug use. *Health Education and Behaviour, 24,* 544-554.

Triandis, H.C. (1989). The self and social behaviour in differing cultural contexts. *Psychological Review, 96,* 506-520.

Uskul K. Ayse, Sherman K. David, Fitzgibbon John (2009).The cultural congruency effect: Culture, regulatory focus, and the effectiveness of gain- vs. loss- framed health messages. *Journal of Experimental Social Psychology, 45,* 535-541. doi: 10.1016/j.jesp.2008.12.005

Weber U. Elke, Hsee K. Christopher (2000). Culture and Individual Judgement and Decision Making. *Applied Psychology: An International Review, 49(1),* 32-61.

Winkler Ira and Manke Samantha (2013). 7 Reasons for Security Awareness Failure, CSO Magazine, July 10. Retrieved from http://www.csoonline.com/article/2133408/network-security/the-7-elements-of-a-successful-security-awareness-program.html

Winkler Ira and Manke Samantha (2013). 6 essential components for security awareness programs. Retrieved from http://www.csoonline.com/article/2133971/strategic-planning-erm/6-essential-components-for-security-awareness-programs.html

Winkler Ira and Manke Samantha (2013). How to create security awareness with incentives. Retrieved from http://www.csoonline.com/article/2134189/strategic-planning-erm/how-to-create-security-awareness-with-incentives.html

Links to Campaigns in U.K.

1. **The 'Cyber Streetwise' campaign** www.cyberstreetwise.com
2. **GetSafeOnline Campaign** www.getsafeonline.org
3. **Webwise Campaign** http://www.bbc.co.uk/webwise/0/
4. **Good to know Google's** https://www.google.co.uk/goodtoknow/
5. **Behind the Screen** http://www.behindthescreen.org.uk/
6. **Cyber Security Challenge UK**
7. http://www.cesg.gov.uk/awarenesstraining/Pages/Cyber-Security-Challenge-UK.aspx
8. **The Devil's In Your Details** http://www.actionfraud.police.uk/thedevilsinyourdetails
9. **VOME Visualisation and Other Methods of Expression** http://www.vome.org.uk/

Links to Campaigns in Australia

1. **Stay Smart Online** http://www.staysmartonline.gov.au/
2. **ThinkUKnow - Internet Safety Program** http://www.thinkuknow.org.au/site/
3. **Tagged (CyberSmart) – ACMA** http://www.cybersmart.gov.au/Home/Teens/Games%20and%20videos/tagged.aspx
4. **Smart online, safe offline (SOSO) - National Association for Prevention of Child Abuse and Neglect (NAPCAN)** http://napcan.profero.com.au/soso
5. **Make cyberspace a better place - KIDS Helpline** http://www.kidshelp.com.au/teens/get-info/cyberspace/
6. **The Alannah & Madeline Foundation - Keeping children safe from violence** http://www.amf.org.au/bullying/

7. **Who's chatting to your kids? - Queensland Police Resource**
8. http://www.police.qld.gov.au/programs/cscp/personalSafety/children/childProtection/

9. **Keep it Tame** http://www.youngandwellcrc.org.au/keep-tame-campaign-promote-online-safety-measure-behaviour- change-young-people/

Links to Campaigns in Canada

1. **Get Cyber Safe** http://www.getcybersafe.gc.ca/cnt/bt/index-eng.aspx

2. **Stop Hating Online** http://www.getcybersafe.gc.ca/cnt/blg/pst-20140109-eng.aspx

Links to Campaigns in Africa

1. **ISC Africa** http://iscafrica.net/#home

2. **Parents corner** http://www.parentscorner.org.za/