Can We Sell Security Like Soap? A New Approach to Behaviour Change

Debi Ashenden
Dept of Informatics & Systems Engineering
Cranfield University
Shrivenham, Swindon
+44 (0)1793 785479
d.m.ashenden@cranfield.ac.uk

Darren Lawrence
Dept of Informatics & Systems Engineering
Cranfield University
Shrivenham, Swindon
+44 (0)1793 785276
d.lawrence@cranfield.ac.uk

ABSTRACT
Many organisations run security awareness programmes with the aim of improving end user behaviours around information security. Yet behavioural research tells us that raising awareness will not necessarily lead to behaviour change. In this paper we examine the challenge of changing end user behaviour and put forward social marketing as a new paradigm. Social marketing is a proven framework for achieving behavioural change and has traditionally been used in health care interventions, although there is an increasing recognition that it could be successfully applied to a broader range of behaviour change issues. It has yet to be applied however, to information security in an organizational context. We explore the social marketing framework in relation to information security behavioural change and highlight the key challenges that this approach poses for information security managers. We conclude with suggestions for future research.

Categories and Subject Descriptors
K.6.5: [**Management of Computing and Information Systems**]: Security and Protection.

General Terms
Security, Human Factors, Design

Keywords
Information security, social marketing, security awareness, behavioural change.

1. INTRODUCTION
We have seen an increase in the number of security awareness programmes run by organisations in recent years. End user awareness has become a key element in the defence of organisational security. In the UK the information security risks realised by end user behaviours came to the fore with the data handling incidents at Her Majesty's Customs & Excise (HMRC) and the Ministry of Defence (MoD). The reports that investigated these events concluded that they occurred largely as a result of poor end user behaviours [34][7][10].

Similar incidents occurred in the private sector (for example, at Nationwide Building Society and HSBC) resulting in legal and regulatory requirements for organisations to run programmes on information security awareness, education and training for end users [11]. Such programmes tend to focus on raising awareness, increasing knowledge and changing attitudes as a way of changing behaviour. Behavioural research, however, tells us that raising awareness does not necessarily translate to a change in behaviour. Furthermore stated attitudes are often different to enacted behaviour. We know that data breaches are still occurring so it seems legitimate to ask how well our security awareness programmes are working. It is, however, very difficult to evaluate the effectiveness of such programmes – not least because there is often no clear understanding of what behaviours the programmes are aiming to change. Given this, it is unsurprising that we are still seeing poor information security behaviours from end users.

There is limited but growing research looking at information security awareness, training and education programmes. Conceptual studies have used theories from psychology and marketing to build models and frameworks and develop guidelines but they have not been tested [38][39]. There has been some research carried out looking at information security behaviours, attitudes and organisational culture more generally but these studies too are often conceptual and do not take account of the social context of end users' behaviour [44][20][24]. The key empirical studies of information security attitudes and behaviours are Adams & Sasse [3], Stanton et al. [41] and Albrechtson [4]. We have found no empirical research though that evaluates information security awareness, training and education programmes in terms of real-world behaviour change, although a conceptual model for doing this has been suggested by Drevin et al, [13]. Awareness and behaviour are often conflated in security campaigns and rather than measuring occurrences of behaviour before and after a campaign, reliance is placed on self reporting by end users of intended future behaviours. We consider this issue in the discussion section of the paper where we review a UK campaign called 'The Devil's in Your Details' [1] that was designed to address the problem of online fraud.

NSPW'13, September 9–12, 2013, Banff, AB, Canada.

http://dx.doi.org/10.1145/2535813.2535823

This paper addresses the challenge of changing end user behaviours around information security. Social marketing is put forward as a new paradigm for behaviour change in information security. It is a framework that has been used extensively in the health sector and in campaigns that encourage behaviours for social good in general populations. In the wider social context there have been a number of social marketing campaigns that are not in the security arena – for example, the 'Click It or Ticket' campaign [8] which is aimed at getting people to wear seat belts or the 'Truth' campaign [45] which is an anti-smoking campaign aimed at young people. We believe that social marketing could be used for security in this wider social context as well as in the corporate environment.

When information security is working nothing happens – there are no incidents, but it is difficult to know whether to attribute this to fewer vulnerabilities or fewer attacks. Social marketing offers a way of improving organizational resilience through end user behaviour. In the UK the Director of GCHQ said that 80% of security problems could be solved with good preventative measures [19]. If attackers are probing systems for weaknesses to find a soft target to attack then the good behaviours that can be inculcated through social marketing will serve to harden the organisation as a target. Social marketing won't solve all security problems but it offers a way of mitigating security risks by addressing the vulnerabilities posed by human behaviour. The process is structured to guide decision-making so that the investment in behaviour change maximizes the return on investment.

We describe the basic process of social marketing and then apply it to information security. The overarching challenge for information security managers is that they are often trying to implement change with insufficient resources and authority. This is compounded by the complexity of information security issues that encompass technology, processes and human factors. Within this, the challenges are to define clear targets for behavioural change, understanding the behaviour of end users from their own perspective, entering into a negotiation to develop an exchange proposition so that it becomes beneficial to change behaviour, developing an effective intervention and evaluating how successful it is in changing behaviour.

The paper concludes with a review of the UK campaign, 'The Devil's in Your Details', from a social marketing perspective to highlight the contribution that the social marketing framework could make. We then outline areas for further research and highlight how social marketing could have a broader impact on how organisational information security is perceived.

2. SOCIAL MARKETING

Social marketing developed in response to the question 'Why can't you sell brotherhood like you sell soap?' (Wiebe quoted in [26]) and has since been defined as the 'systematic application of marketing concepts and techniques to achieve specific behavioural goals relevant to a social good' [16]. Social marketing focuses on behaviours and uses traditional marketing principles and techniques but oriented towards achieving a 'social good' rather than commercial gain. There is now a body of research underpinning social marketing [27][5][21][17]. Social marketing is most often used as a paradigm for behaviour change in public health but its broader applicability has also been recognised [6][22] and it is increasingly being applied to broader domains.

The framework of social marketing starts with generating insight into end user behaviours by identifying specific behavioural goals and applying behavioural theory to discover how end users see their current behaviour. The next step is to take this insight and segment end users using psychographic variables in addition to demographic or role-based variables. This segmentation process also facilitates an understanding of the competition faced by the target behaviour - revealing the perceived benefits to the end user of the current behaviour and the perceived drawbacks to the end user of the target behaviour. With this rich understanding of the end users' perspective an exchange proposition can be designed and developed in the form of an intervention that goes beyond messaging and that decreases the perceived benefits of the current behaviour while increasing the perceived benefits of the target behaviour.

Social marketing is a structured approach that brings together marketing and social science and has been used to successfully deliver behavioural change initiatives over a number of years and across a range of countries. It is a framework into which a number of theories and applications can be plugged to develop an effective behaviour change programme. For example, behavioural economics (popularised by the book 'Nudge'[43]) is an approach that is often discussed as part of behavioural change interventions. Behavioural economics seeks to explain why people behave as they do and why they do not necessarily make rational decisions. The studies carried out within behavioural economics offer useful practical and theoretical additions that can be incorporated into the social marketing framework. The simple framework offered by social marketing means that it can be used effectively by individuals who are not trained social scientists. For example, a fireman now runs a highly successful campaign that aimed to stop young people deliberately setting grass fires, from the South Wales Fire Service [36]. We believe that information security managers will be able to use the social marketing framework to achieve similar successes.

3. THE CHALLENGES FOR SECURITY

Information security issues are complex because they bring together technology, processes and human factors in a variety of contexts. In an organisational setting change is often managed through a structured change management programme but this is difficult to apply to information security for two reasons. Firstly, deconstructing complex information security issues into clear behavioural change targets is difficult. Secondly, information security managers frequently don't have the resources or authority to manage a top-down change management programme. Information security managers tend to operate at the boundary between the operational and delivery functions of most organisations. They are often disempowered and unsure of their own position in the organisational hierarchy.

To add to the complexity of information security issues end users are increasingly difficult to contain within the logical perimeter of the organisation's technology. We have Bring Your Own Device (BYOD) issues as end users expect to have the same technology experiences at work as at home. Spear phishing attacks prey on the social aspects of end users' behaviour and there is a tension in many organisations over the use of social media. In global organisations there are cross-cultural issues to address and often

this is set against the need to let customers cross the organisational boundary through the online delivery of services.

Against this backdrop we should consider organisational reasons for running security awareness programmes. The stated reason will usually be to make end users more aware of the need for information security and for this to translate into improved behaviours with a corresponding decrease in the number of security incidents. There is another reason, however, and this is often not overtly stated. The authors believe that, while not admitting it publicly, many organisations run security awareness programmes to demonstrate compliance rather than to deliver genuine behaviour change in end users. The benefit of achieving compliance is important and shouldn't be dismissed – it is a legitimate business decision for an organisation to take but it seems sensible to be clear on an organisation's motive for undertaking security awareness activities at the outset. As we shall see this becomes especially important when the cost and resources necessary for a successful behavioural change programme are taken into consideration. Social marketing has a role to play in encouraging the information security manager to reflect on these reasons as the step by step approach and the questions it raises soon force an organisation to acknowledge if compliance is their primary concern.

This brings us to the overarching challenge posed by social marketing for the information security manager – the realisation that awareness and behaviour change are not the same and increasing awareness will not automatically lead to a change in behaviour although it can be a very useful first step. This has been recognised in social marketing research for a long time and is best exemplified by the following quote:

> *'It would be easy to give the public information and hope that they change behaviour but we all know that doesn't work very satisfactorily. Otherwise none of us would be obese, none of us would smoke and none of us would drive like lunatics' [33]*

This revelation is something that we are all aware of but often fail to directly acknowledge. This recognition is at the heart of social marketing and forces the information security manager to reflect on his or her activities in a more critical way than is usually the case.

One problem with many security awareness programmes is that they give the end user information and expect that they will see the rationality of the argument that information security is important and act on it accordingly. The difficulty with this is that it fails to take into account that the end user may have a completely different perspective on the problem space. The difference in the information security manager's rational view of security and that of the end user has been demonstrated in recent research [25].

Current security awareness programmes also tend to provide information and aim to educate but don't usually articulate what the end user should do differently. Social marketing forces the information security manager to answer the question, 'if end users did do what they were supposed to do, what would it look like and how much of the information security problem would be solved?' This brings us to our first challenge, which is identifying the specific behaviour to be addressed.

3.1 Identifying Target Behaviours

The first task in social marketing is to select the behaviour that you want to change. The behaviour needs to be 'non-divisible' [29]. A non-divisible behaviour is one that cannot be divided further. For example, a divisible behaviour for information security could be to protect customer confidential information. This is a divisible behaviour because it could be achieved in a variety of ways – by not emailing the information or by not revealing it on the telephone or even by locking a filing cabinet and having a clear desk policy. It is also dependent on how 'confidential' is defined - is this a recognised protective marketing that is used in a rigorous way or is there an expectation that the end user will be able to make a judgement on what is 'confidential'? A non-divisible behaviour on the other hand could be not to send customer documentation marked 'confidential' via email. The non-divisible behaviour gives the end user a clear idea of what they need to do.

Information security managers should aim to identify a small number of non-divisible behaviours that could be targeted and then to establish the behaviour to change that would give them the best return on investment. To do this they will need to have some metrics or indicators for how widespread the current behaviour is and what the impact is on security. This could be evaluated in a variety of ways from counting the number of incidents or by the size of fines from a regulator. Clearly identifying target behaviours and evaluating the size of the problem will be critical when it comes to evaluating the intervention and proving the return on investment.

From our experience, information security managers find it quite difficult to identify non-divisible target behaviours and they often need assistance to quantify them. While target behaviours should be specific to the organisation some more general suggestions could include: constructing secure passwords, reporting suspicions that an incident has happened, not downloading executable files from the Internet, not clicking on links from unrecognised senders, shredding sensitive waste, not opening email attachments from unrecognised senders, not sharing passwords.

3.2 Generating Insight

Our next challenge is generating insight into why end users behave the way they do. This requires information security managers to engage with and listen to end users. If they've participated in a security awareness programme why are they still persisting with poor information security behaviours? A range of behavioural theories can be called upon to help with this part of the social marketing process. Two such theories seem to offer particular insight into the problem of information security behavioural change. The first is attribution theory, which aims to uncover the link between attitudes and behaviours. An attribution is the link that the end user makes between cause and effect. Heider [23] laid the foundations of attribution theory. An attribution is any answer to the question 'Why?' [31], and attributions are the explanations that we give for things that make us believe our environment is more predictable and controllable (Silvester, in [38]). As Taylor [42] points out attributions can have a real impact on behaviour because how you assign a cause to an event is likely to determine how you respond to it behaviourally.

This means that by using attribution analysis we should have a better understanding of the cause and effect linkages and assumptions that individuals make. For example, some individuals believe that events such as identity theft occur by chance or by simply being in the wrong place at the wrong time. End users who hold this attitude often believe that there's nothing they can do to protect themselves online. A different individual, however, may make a different attribution and believe that the cause of identity theft is due to their poor information security practices and that they could take steps to prevent it happening. By revealing these patterns of cause and effect and understanding these attributions we can develop more effective ways of working with them, or overcoming them, in order to encourage good information security behaviours. Using attributions as a methodological approach can also overcome the problem of end users just saying what they believe they should say.

By understanding end users better we can also ascertain how ready they are to change their behaviour. This brings us to a second theory - stages of change theory (also known as the transtheoretical model) [35]. By applying this the information security manager recognises that the journey of end users from becoming aware of the risks to information security to being motivated to change behaviour is a gradual process that moves from pre-contemplation of the need to change, to contemplation of behaviour change, and then from preparation for change to taking action – that is actually changing behaviour. The final stage is maintaining the new behaviour (so it becomes a habit) and avoiding lapsing back into the old behaviour. This theory has been used in many social marketing campaigns as it offers a way of segmenting end users into those who are at the pre-contemplation stage (in information security this would be the equivalent of the end user asking 'what does information security mean?') through contemplation and preparation ('oh I've heard about malware, is there anything I can do to stop it?') to action ('I'm not going to open that link in case it infects my pc with a virus'). This is a good demonstration of where security awareness programmes can add value. An organisation can keep its security awareness programme running knowing that it will help those end users who really aren't aware of why information security is important while a behaviour change intervention will tackle those ready to take action.

3.3 The Exchange

At the heart of social marketing, as in traditional marketing, is the concept of exchange. Exchange has been defined as 'the exchange of resources or values between two parties with the expectation of some benefits' (MacFadyen et al., quoted in [30]). In the absence of a physical product the 'product' in social marketing is the benefit that people will get from changing their behaviour [28]. As part of generating insight into end user behaviour we need to understand the trade-offs end users make when they decide how to behave. These trade-offs demonstrate the competition, benefits and barriers that will impact on whether a new behaviour is taken up or rejected. The aim is to explore how end users perceive the benefits provided by the problem behaviour and the barriers to adopting the desired behaviour while also understanding what benefits the desired behaviour might be able to offer end users and what would increase the costs of the problem behaviour. When expressed as a statement the exchange should look something like the following, 'If I (carry out the new behaviour) instead of (the old behaviour) I will receive (something I perceive as a benefit). I know this will happen because (support in the form of education and messaging)'.

Security incidents are often low-probability but high impact events. The exchange proposition needs to make it clear what the benefits are to end users of changing their behaviour – this is similar to persuading people to wear seat belts even though the probability of a crash is probably quite low, or paying for insurance even though most people don't expect their house to burn down. In terms of information security behaviours the benefits of writing down a password might be that the end user doesn't have the cognitive load of memorising it and the barrier to changing this behaviour and not writing it down might not be obvious. For example, it could be that the end user believes he or she has too many passwords that already need to be remembered and doesn't believe that this one warrants being committed to memory. This indicates the competition that the new behaviour is up against. In order for it to be memorised this password has to be perceived to be more important than others and this will come down to risk perceptions and understanding the impact of the risk being realised. In this scenario the exchange statement could look like the following, 'If I (memorise my password) instead of (writing it down) I will receive (a reduction in the number of passwords I have to remember and/or use delivered through the design of better processes). I know this will happen because (the new processes have been designed to take account of the problems I currently face).

3.4 Designing the Intervention

The next step is to design an intervention using an innovative mix of approaches that increase the benefits of the desired behaviour and the costs of the problem behaviour while decreasing the barriers to adopting the desired behaviour and the benefits provided by the problem behaviour. To do this social marketing uses a mix of approaches that can be tailored to deliver the most attractive exchange offering. This will include a marketing mix of elements of education to inform and create awareness, design of the environment and processes that support the change, control through the use of regulation or disciplinary processes to act as an inhibitor to continuing with the old behaviour, services that support the new behaviour and messages that inform and communicate the new behaviour [16].

Current interventions for information security awareness tend to rely on what marketers call SPLAT (Some Posters, Leaflets, Ads 'n' Things). This approach is also referred to as 'spray and pray' because it relies on messaging as widely as possible rather than using a more targeted approach with a more innovative marketing mix in the intervention. Increasingly such campaigns in information security are brilliantly executed but they still rely primarily on messaging without digging beneath the surface of human motivation and decision-making to understand the end user or to construct an intervention that has a clear behavioural target. Recent research, however, has suggested the value of using more sophisticated approaches to information security messages such as using stories [37] and working with the heuristics and biases of end users as an input to the design of an intervention so that they are 'targeted according to the user's mental model' [18]. Technology itself can form the basis of the intervention and there has been a significant amount of work done using computers as a means to change behaviour that could usefully be incorporated at this stage [14][15].

If a target behavior for information security was to prohibit the use of personal internet access in the office the exchange could be as simple as providing internet zones (similar to smoking areas) at designated points in the organisation. Some organisations provide internet cafés for this purpose but they are rarely introduced as part of a targeted intervention. In this instance the information security manager could use a design element (in the development of the internet zones) and couple this with controls in the form of sanctions for accessing the internet for personal use outside of an internet zone. A more traditional awareness campaign would then focus on messaging the potential vulnerabilities that could impact on the corporate network if unfettered access was allowed. Finally support could be offered in the form of an advice service for protecting home internet access from the same vulnerabilities.

Desai [12] points out that co-creation in the development of interventions increases dialogue between the target audience and the social marketer. This type of co-creation is also known as a participatory approach where the end user becomes part of the team that solves the problem – in this case by co-designing the intervention. In the example given above, a panel could be established of interested end users to help guide the design of the overall intervention but particularly the design of the internet zone. They could also become advocates for the scheme and start to establish a social norm of using the new internet zones. This type of co-creation is not always straightforward though and there are various lessons to be learned by the information security manager [9]. These include managing the tension that often exists between the information security manager and the end user, as well as considering how much control can be ceded to the end user without losing sight of the purpose of the behaviour change project.

3.5 Evaluating the Impact

This brings us to the final challenge, which is measuring the impact. Relying on self-reporting to understand the impact of training and awareness programmes may be flawed – people are generally very good at not knowing why they do things and they will often make things up to be helpful.

There are different stages of implementation and different points at which impact can be assessed. Interventions should be piloted first before being rolled out on a larger scale. Having clear and measurable objectives for a behaviour change intervention is vital if we are to understand the impact. This brings us back to the idea of non-divisible target behaviours. We need to have some way of measuring the behaviour before the intervention is implemented so that we can measure it afterwards and compare and contrast. This can be difficult for information security end user behaviours because in many organisations this information isn't gathered but it should be possible to do so. For example, we may need to understand how many end users have been responsible for sending out sensitive information via email or how many have been found with passwords written on post-it notes.

Hastings [21] identifies two different types of measurements for behavioural change – the first is response and the second is reaction. Response measurements are the way that most information security behavioural change programmes are currently assessed. Such measurements gauge end user awareness, participation in programmes, understanding and how many end users the programme has reached. The more useful measurement, however, is reaction and this is harder to assess. Reaction to behavioural change is likely to be small and gradual, for example, road safety interventions typically expect to see only a 10% change in behaviour in the short term (Elliot cited in [30]). From this statistic it is apparent that a behavioural change programme is not a quick fix for information security problems and, for this reason, careful thought should be given to why the programme is being implemented and what is expected to be achieved. This takes us back to the point made in Section 3 around reflecting on whether the aim is to demonstrate compliance rather than achieve behavioural change. If it is the former, then there are probably less expensive ways of demonstrating compliance.

Social marketing programmes are iterative and action-oriented so that early results from impact measurements are incorporated into future iterations. There are hierarchies of evidence for measuring the impact of social marketing programmes [30]. These hierarchies start from randomised control trials (RCTs) as the most rigorous form of assessment. At the bottom of the hierarchy surveys could be used but as we know that attitudes do not necessarily translate to behavioural change these should be used with caution and are more useful for assessing response rather than reaction.

RCTs are used extensively in measuring the impact of clinical interventions but there are has recently been moves both in the UK and the US to use RCTs more widely to assess the impact of Government policy. As French et al. [17] point out, however, RCTs are much harder to use in a social rather than a laboratory environment and similar difficulties would apply to using them in an organisational environment. Some of the reasons that they give for these difficulties include the fact that social marketing interventions are often preventative and so nothing observable happens, they are also multi-faceted which means there is a lot of 'noise' that could contribute to the effect that is generated and this makes statistical conclusions difficult to draw. In addition RCTs randomly assign individuals to experiments conditions but this is much harder to achieve for social marketing where such control of individuals may not be possible. Ensuring internal validity is a problem too as it can be difficult to design and implement a placebo. Finally there is a very high risk that a control group would be exposed to an intervention.

While RCTs may provide the standard for clinical interventions it's likely that the information security manager would need to look at other methods for understanding the impact of social marketing interventions. These could include cohort studies where groups of individuals are selected for observation and follow up after an intervention. Alternatively case-control studies could be used where naturally occurring cases are studied. This could be particularly useful for information security behavioural interventions within an organisation where some business units could be exposed to the intervention while others wouldn't and the effect would be measured across the case groups. This is not as rigorous as an RCT but would ensure ecological validity and would be more practical to implement.

3.6 Reviewing a Campaign Through the Social Marketing Framework

The 'Devil's in Your Details' [1] was a campaign launched in the UK in 2012 by a private/public sector partnership called Action Fraud. Action Fraud is the UK's national fraud reporting centre.

We have taken open source material about the campaign and reviewed it through the framework of social marketing.

On the Action Fraud web site [2] the stated aim of the campaign is to 'help people better protect themselves' against fraud. A non-divisible target behaviour is also identified – 'to increase the reporting of fraud'. This target behaviour offers a clear way of measuring the success of the campaign as presumably there will be a baseline measurement of the level of fraud reporting before the campaign and it would be possible to measure the level of fraud reporting after the campaign and ascertain how behaviour of the target audience has changed.

A significant amount of target audience analysis was carried out. Ipsos Mori [2] was commissioned to carry out a survey benchmarking fraud awareness and behaviour change. In addition the National Fraud Agency [32] carried out a quantitative segmentation of the UK population to determine how, why and when citizens became the victim of fraud. Two target audiences were identified for the campaign. The first target audience for the campaign was men and women in the 18-25 age bracket. Research had shown that this age group was more likely to worry about image than becoming the victim of fraud and was more often the victim of online ticketing scams and bogus career opportunities. The second target audience was women in the 35-55 age bracket as they believe they are helpless to stop fraudsters. This target audience was most often the victim of online shopping scams and property investment scams.

There are three interventions in the campaign consisting of three videos. The first tackles online fraud and shows a fraudster slowly turning into the woman whose identity he is stealing online. The advice given at the end of the video is (i) be certain who you're dealing with, (ii) learn to spot scams and (iii) if in doubt, don't enter details. The second video focuses on 'phone fraud and depicts a phone conversation between a fraudster and a female victim but positions both as sitting on a park bench next to each other. The advice given at the end is (i) know who you're speaking to, (ii) stay in control and (iii) if in doubt end the call. The third video uses the end user's Facebook account to access personal details and create a personalised video. To watch the video the end user has to allow access to their Facebook profile and details of their friends. The application also requests permission to post to friends (which the authors declined to give). The resulting video is a mock-up of a news report with a video clip supposedly filmed by an undercover journalist. There is no final advice given at the end of a fairly hard-hitting video.

While the videos are gripping and cleverly executed they seem designed to raise awareness rather than change behaviour. Given the stated aim of the campaign is to 'increase the reporting of fraud' this is not articulated by the interventions. The advice given in the interventions is sound as far as it goes but it doesn't tell the end user exactly how they should behave in order to protect themselves. For example, the first video gives the advice that the end user should 'learn to spot scams' but doesn't detail how they can achieve this.

One of the comments on YouTube in response to the first video is, 'instead of providing useful information this video just demonises the Internet'. The response provided by Action Fraud is, 'the video raises awareness of the user and of Action Fraud as an organisation', but neither of these aims support changing the behaviour of end users so that they report more fraud. The Action Fraud response also draws attention to the link on their web site for tips to stay safe. On reviewing these tips it is apparent that they do offer sound behaviours for end users but they are rather remote from the videos that will have been watched and do require some searching of the web site in order to locate them.

The impact of the campaign [32] seems to have been measured by the number of viewings of the videos, the position of the videos in online searches and the reactions of end users. The last measure is probably the most useful in terms of understanding whether behaviour has changed, but it does rely on self reporting of changes in attitude and behavioural intent which is often unreliable as stated attitudes are often at odds with enacted behaviours. In the open source material on the evaluation of this campaign there is no indication that instances of the desired behavioural change of increasing fraud reporting were measured before and after the campaign.

Using a social marketing framework to guide the development of the campaign would have kept the focus on the behavioural aim of increasing the number of instances of fraud that are reported and ensured that it was a thread running through the whole campaign. With this target behaviour identified and the insight gained through the Ipsos Mori survey and the National Fraud Authority survey the interventions would have been more strongly focused on ensuring the take up of this new behaviour. The insight activities would also have focused on understanding why people don't currently report instances of fraud and what it would take for them to do so. While the interventions have obviously been designed with the target audiences in mind the exchange proposition is not clear (hence the YouTube comment that the video 'just demonises the Internet'). The exchange is implied rather than explicit (if end users are more careful they won't be the victim of fraud). By maintaining the focus on behaviour rather than awareness, the interventions may have been more clearly linked to the specific behavioural advice on the Action Fraud web site. Finally, by measuring the instances of fraud reporting before and after the campaign the impact could have been much stronger than relying on self reporting.

Reviewing this campaign through a social marketing lens suggests that the focus on behaviour change was confused with raising awareness very early on. This campaign was obviously well researched and probably did raise awareness of the issues of online fraud but it is unclear whether it achieved a change in end user behaviour. In turn this makes it difficult to judge the return on investment for the money spent on the campaign. We also know that raising awareness doesn't necessarily lead to behaviour change. The social marketing framework would have given the campaign a clear process that would have encouraged the focus to stay on the behavioural target.

4. CONCLUSIONS AND FUTURE WORK

In recent years we've seen a sharp increase in the number of organisations across both the public and private sector running security awareness programmes. Such programmes are often mandated by regulatory requirements. Our understanding, however, of the aims of such programmes is limited and their ability to deliver behavioural change is doubtful. This paper has proposed using social marketing as a new paradigm to move us from raising awareness to changing information security end user behaviours. This paradigm shift is particularly timely as it provides a way of incorporating and leveraging ongoing research

in behavioural economics and 'nudge' theories, both in the wider behavioural change environment, and as applied to information security.

By applying a social marketing framework to information security behaviours we are immediately faced with the realisation that raising awareness is unlikely to be sufficient to change behaviour. For organisations currently running security awareness and training programmes this will be a significant paradigm shift. The social marketing framework reveals at least five challenges for information security behaviours. Firstly we need to identify the specific target behaviour that we want end users to change. Secondly, we need to generate insight into how and why end users behave as they do and understand this from their perspective not that of the information security manager. Thirdly, we need to develop an exchange proposition that minimises the barriers to taking up the desired behaviour while maximising the barriers to carrying on with the existing behaviour. Fourthly, we need to design a targeted intervention using a judicious use of the marketing mix. Fifthly we need to measure the impact of the intervention in a defensible way.

To address these challenges further research is necessary. We need to develop processes for helping information security practitioners to identify non-divisible target behaviours. An element of this will include methods for estimating which behaviours will give the best return on investment if they are changed. To develop our understanding of target audiences we need to evaluate the benefits of different behavioural theories for different environments – attribution theory and the stages of change model are just two that are currently being explored and there are many others. Developing an exchange proposition will require taking a broader approach to information security interventions than is currently the case as successful interventions are likely to combine education, design, control mechanisms, support services as well as messaging. Successful interventions are also likely to be co-created and this will be a new way of working for many information security managers. Finally we need methods for evaluating the impact of interventions beyond surveys and RCTs.

If we can achieve this, however, by decreasing user generated information security incidents through effective behavioural change programmes information security practitioners will have more time and resources to focus on complex technological threats. The interventions designed can help encourage positive perceptions of security so that rather than being adversarial interventions will work with end user attitudes and behaviours and information security managers will be less likely to be seen just as the people who like to say no or who trade on fear, uncertainty and doubt.

The social marketing paradigm offers a reusable process that starts small, pilots and tests an intervention before full implementation and evaluation. If carried out methodically it is a way of proving which interventions deliver behaviour change and provides demonstrable return on investment.

5. REFERENCES

[1]Action Fraud. 2012. *The Devil's in Your Details* [Online]. Available at: http://www.actionfraud.police.uk/thedevilsinyourdetails [Accessed 11th August, 2013].

[2]Action Fraud 2013. *Pre-Campaign Surveys* [Online]. Available at: http://www.actionfraud.police.uk/majority-of-women-feel-falling-victim-to-fraud-is-inevitable-according-to-new-study [Accessed 11th August, 2013].

[3] Adams, A. and Sasse M. A. 1999. Users are not the enemy, *Communications of the ACM*. 42(12), 40-46.

[4] Albrechtsen, E., 2007. A qualitative study of users' view on information security, *Computers & Security*. 26, 276-289.

[5] Andreason, A. R., 2006. *Social Marketing in the 21st Century*. California, Sage.

[6] Andreason, A. R. and Herzberg, B. 2005. Social Marketing Applied to Economic Reforms, *Social Marketing Quarterly*, 11:2, 3-17.

[7] Burton, E. 2008. *Report into the Loss of MOD Personal Data: Final Report*. London, MOD.

[8] Click it or Ticket 2013. *Click it or Ticket* [Online]. Available at: http://www.texasclickitorticket.com [Accessed 11th August, 2013].

[9] Coles-Kemp, L. and Ashenden, D. 2012. Community-centric engagement: lessons learned from privacy awareness intervention design, *Proceedings of HCI 2012 – People & Computers XXVI*, Birmingham, UK, 12-14 September 2012.

[10] *Data Handling Procedures In Government: Final Report*. 2008. London, Cabinet Office.

[11] *Data Security in Financial Services*. 2008. London, Financial Services Authority.

[12] Desai, D., 2009. Role of Relationship Management and Value Co- Creation in Social Marketing. *Social Marketing Quarterly*, 15:4, 112-125.

[13] Drevin, L., Kryger, H.A. and Steyn, T. 2007. Value-focused assessment of ICT security awareness in an academic environment, *Computers & Security*, 26, 36-43.

[14] Fogg, B. J., 2002. Persuasive technology: using computers to change what we think and do, *Ubiquity*, 2002, December, 5, 89-120.

[15] Fogg, B. J., 2009. Creating persuasive technologies: an eight-step design process, *Persuasive '09,* Proceedings of the 4th International Conference on Persuasive Technology, Article No. 44.

[16] French, J. and Blair-Stevens, C. 2010. Key Concepts & Principles of Social Marketing, in French, J., Blair-Stevens, C., McVey, D. and Merritt, R. (eds). *Social Marketing & Public Health: Theory & Practice*, Oxford, OUP.

[17] French, J., Merritt, R. and Reynolds, L. 2011. *Social Marketing Casebook,*. London, Sage.

[18] Garg, V. and Camp, J., 2013. Heuristics and Biases: Implications for Security Design, *IEEE Technology and Society Magazine*, Spring, 73-79.

[19] GCHQ. 2011. *IISS Cyber Speech* [Online]. Available at: http://www.gchq.gov.uk/Press/Pages/IISS-CyberSpeech.aspx [Accessed 11th August, 2013].

[20] Gonzalez, J.J. and Sawicka, A. 2002. A framework for human factors in information security, *WSEAS International Conference on Information Security,* Rio de Janeiro.

[21] Hastings, G. 2007. *Social Marketing: Why should the devil have all the best tunes?*, Oxford, Elsevier.

[22] Hastings, G., MacFadyen, L. and Anderson, S. 2010. Whose behavior is it anyway? The broader potential of social marketing, *Social Marketing Quarterly* 6:2, 46-58.

[23] Heider, F. 1958. *The Psychology of Interpersonal Relations*. New York, Wiley.

[24] Helokunnas, T. and Kuusisto, R. 2003. Information Security Culture in a Value Net, Managing Technologically Driven Organizations: The Human Side of Innovation and Change, *IEEE*, 190-194.

[25] Herley, C. 2010. So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users, *NSPW '09*, 133-144.

[26] Kotler and Zaltman 1971. Social Marketing: An Approach to Planned Social Change, *Journal of Marketing*, Vol 35, 3-12.

[27] Kotler, P. and Lee, N. R. 2008. *Social Marketing: Influencing Behaviors for Good* (3rd edn), London, Sage.

[28] Levitt, T. 1960. Marketing Myopia, *Harvard Business Review*, 38, July-Aug, 29-47.

[29] McKenzie-Mohr, D. 2011. *Fostering Sustainable Behaviour: An Introduction to Community-Based Social Marketing*, (3rd edn), New Society Publishers.

[30] McVey, D., Crosier, A. and Christopoulos, A. 2010. Evaluation in in French, J., Blair-Stevens, C., McVey, D. and Merritt, R. (eds). *Social Marketing & Public Health: Theory & Practice,* Oxford, OUP.

[31] Munton, A. G., Silvester, J., Stratton, P. and Hanks, H. 1999. *Attributions in Action: A Practical Guide to Coding Qualitative Data*, Chichester, Wiley.

[32] National Fraud Authority 2013. *Awareness & Behaviour Change in the UK* [Online]. Available at: http://korrupciomegelozes.kormany.hu/download/a/15/60000/Budapest%2019%20Mar%20Main%20Pres.pdf [Accessed 11th August, 2013].

[33] Potter, I., 2007, *New Zealand Herald*.

[34] Poynter, K. 2008. *Review of information security at HM Revenue and Customs: Final Report*. London, HMSO.

[35] Prochaska, J. O. 1992. In Search of How People Change: Applications to Addictive Behaviours, *American Psychologist*, Vol 47, No 9, 1102-1114.

[36] Project Bernie. 2013. *Project Bernie* [Online]. Available at: http://www.bernie.uk.com/ [Accessed 12th April 2013]

[37] Rader, E., Wash, R. and Brooks, B., 2012. Stories as Informal Lessons about Security, *Symposium on Usable Privacy and Security (SOUPS)*, July 11-13, 2012, Washington, DC, USA.

[38] Silvester, J. 2004. Attributional Coding, in Cassell, C. and Symon, G. (eds.) *Essential Guide to Qualitative Methods in Organizational Research*, London, Sage.

[39] Siponen, M.T. 2000. A conceptual foundation for organizational information security awareness, *Information Management & Computer Security*, 8(1), 31-41.

[40] Siponen, M.T. 2001. Five dimensions of information security awareness, *ACM SIGCAS Computers and Society*, 31(2), 24-29.

[41] Stanton, J.M., Stam, K.R., Mastrangelo, P. and Jolton, J. 2005. Analysis of end user security behaviors, *Computers & Security*, 24(2), 124-133.

[42] Taylor, S. 2007. Attitudes, in Langdridge, D. and Taylor, S. (eds.) *Critical Readings in Social Psychology,* Maidenhead, OUP.

[43] Thaler, R. H. & Sunstein, C. R. 2009. *Nudge*, London, Penguin.

[44] Thomson, M.E. and Solms, R. V. 1998. Information security awareness: educating your users effectively, *Information Management & Computer Security*, 6(4).

[45] Truth. 2013. *Truth* [Online]. Available at: http://www.thetruth.com/about/ [Accessed 11th August, 2013]