Cyber security in the workplace: Understanding and promoting behaviour change

John M Blythe

PaCT Lab, Department of Psychology, Northumbria University, Newcastle-upon-Tyne, UK
NE1 8ST
john.blythe@northumbria.ac.uk

Abstract. Cyber security and the role employees play in securing information are major concerns for businesses. The aim of this research is to explore employee security behaviours and design interventions that can motivate behaviour change. Previous research has focused on exploring factors that influence information security policy compliance; however there are several limitations with this approach. Our work-to-date has explored the behaviours that constitute 'information security' and potential influencers of these behaviours. These findings will aid the design of behaviour change interventions.

Keywords: Cyber security; Information security; Behaviour change

1 Introduction

The advancement of technology in the workplace has allowed employees ubiquitous access to information, permitting employees to work in a number of different locations and on numerous devices enhancing individual productivity and the efficiency of business operation. Businesses utilize a number of services to achieve this operation including remote access and cloud-based storage to name a few and a number of technological devices including laptops, tablets, PDAs and mobile phones.

However, this adoption of newer technology has also increased their risk to cyber threats as organisations and individuals are increasingly affected by misuses of information that result from security lapses. Current cyber security practices and approaches cannot cope with this increased dependency and as a result, the UK cyber security strategy was developed with the intention to protect citizens, businesses and critical infrastructures from cyber-attacks [1].

Organisations adopt a range of technical and procedural approaches to secure information (e.g. encryption and security awareness campaigns, respectively). However, these efforts are not enough as security breaches continue to plague companies. Statistics show that 93% of large organisations and 76% of small businesses experienced a security breach in the last year [2]. Employees appear to be a large source of the prob-

adfa, p. 1, 2011.

lem as estimates show approximately half of all data breaches are due to compliance failure (indirectly or directly) to their company's security policy [3].

Although employees have been identified as one of the most significant vulnerabilities in information security of organisations, research to date is fragmented and little attention has been given to designing theoretically based and empirically validated behavioural interventions.

1.1 What influences security behaviour?

Research has been dedicated to exploring the causes and determinants of secure behaviour. The main body of research has focused on positive behaviours, which help serve the organisational goal of information security. These are compliant behaviours such as encrypting removable media. The other type of research has explored negative, potentially damaging, behaviours such as employee computer misuse/abuse.

Studies focusing on positive behaviours have primarily been through a "policy-compliance" lens, exploring the extent to which employees' conform to organisational rules and guidelines as laid out in their organisation's information security policy (ISP). There is a plethora of research in this domain investigating the factors that relate to compliance to these policies. Numerous theories have been employed to identify these factors such as the theory of planned behaviour (TPB) [4] and protection motivation theory (PMT) [5] to name a few.

Consistently researched factors have been identified using a number of different theories and conceptualizations. These include internal influences such as self-efficacy [e.g. 4, 5, 6], and attitude towards security [e.g. 7]; external influences such as social pressures i.e. the extent to which an individual is influenced by what relevant others (e.g. management) expect him/her to do [e.g. 4, 5, 6, 7] and an individuals' threat and response evaluation. Threat perception has been studied in terms of perceived vulnerability (an individual's assessment of the probability of threatening events) [e.g. 5] and perceived severity (severity of consequences to the organisation arising from non-compliance) [e.g. 6]. Finally, an individuals' assessment of response (i.e. security) has been investigated in terms of response efficacy (belief that the security action will reduce threats) [e.g. 5] and response cost (costs associated with the security behaviour such as time and effort) [e.g. 6].

Whilst the "policy-compliance" approach has identified a number of factors that can help provide an understanding of why individuals comply with their ISP, there are a number of limitations with this paradigm. Firstly, there is an over-reliance on exploratory research that has largely adopted non-experimental methodologies, which have limitations in terms of understanding cause-and-effect relationships between the factors. Previous research [e.g. 5, 6, 7] has implemented hypothesized regression models to understand security behaviour and factors that account for the most variance in compliance intention. Whilst these help us understand the relationships between several factors, they cannot tell us which factors are most efficacious in promoting secure behaviours.

Secondly, research investigating policy-compliance operationalise their outcome variable as "intention to comply with the information security policy" [e.g. 5, 6, 7].

This narrows information security to a single behaviour - compliance. However, this is an over simplification. ISPs actually dictate a variety of security behaviours that cannot be simplified to a single behaviour.

Thirdly, there are organisational differences with regards to approaches to ISPs. There is a lack of consensus for the content of these policies so there is diversity in their described and expected employee security behaviours. Furthermore, companies differ in deployment of their policies and newer forms of security documents that complement the ISP (e.g. home working policies) makes this area more complex. Different levels of organisational security maturity and legislative obligations (e.g. Freedom of Information Act (2000)) also mean that there are inconsistencies in policies across organisations.

The theoretical implications of this "policy-compliance" approach are that the researched behavioural determinants may not be applicable to the large amount of security behaviours. For example, factors such as social pressures may have more of an influence on password behaviour than preventative anti-virus behaviour. It is therefore important to understand how factors might differ in their influence on behaviours. Research in other domains such as [8] has emphasized the importance of assessing the degree to which behavioural determinants influence specific behaviours and how they may vary depending upon the behaviour and the population being studied. However, previous research studies have not explored these differences in employee information security behaviour.

It is important to consider other influences of security behaviour including the usability of the security systems and employees' working environment. A security system that considers usable design will help generate fewer insecure behaviours compared to a poorly designed system which will lead employees to 'workaround' their security guidelines simply in order to get their main job done, thus resulting in insecure practice. It is important to consider these different influences when promoting behaviour change. Future research also needs to understand security behaviour with regards to Bring Your Own Device (BYOD) and home working, both of which have limited research but provide challenging issues for workplaces to manage security [2].

Additionally, research needs to provide more focus on the context of behaviour in organisations. Two potentially important factors could be psychological ownership (perception that a physical/non-physical target is "theirs") and organisational citizenship behaviour (discretionary behaviours that go beyond the job role). These factors have only been studied within security in relation to non-work users [9], however could play an important role in employee security behaviour.

1.2 Security behaviour change

Despite efforts to understand the security behaviour of employees, there has been little attention dedicated to improving this behaviour. Behaviour change is a large research area, particularly within the health and sustainability domain. However, there is a distinct lack of research within the arena of cyber security particularly in the context of the workplace.

In organisations, previous behaviour change methods have been implemented such as training. A recent review [10] suggests that current approaches are based upon practical experience and lack empirical evidence and a theoretical grounding. There are, however, examples of empirically and theoretically based cyber security behaviour change in non-work domains such as [11] who used the game anti-phishing Phil and the health belief model to deliver tailored risk messages to improve financial security behaviour. However, despite previous research investigating the influences of ISP compliance using behaviour change models, the findings have not been utlised in intervention design within in the workplace.

Models from health psychology are particularly relevant to this area as health behaviours are similarly sensitive to that of security. Within health, individuals have to undertake a number of preventative behaviours (e.g. sanitising hands in hospitals to prevent contamination). Similar to security, individuals have to take preventative action to prevent a security breach (e.g. running anti-virus scans). Best practice and guidance for successful behaviour change from other domains may therefore have applicability to cyber security.

2 Proposed Research

There are two parts to this PhD research. The first part (stages 1-2) aims to define information security behaviours, the potential determinants of these, and identify behaviours for intervention. The second part (stages 3+) will consist of designing interventions driven by the findings of the earlier exploratory studies. The research questions proposed so far are:

1. What security behaviours are employees expected to perform? (Stage 1)
2. Are vignettes a suitable tool for cyber security research? (Stage 2a)
3. What are the behavioural determinants of security behaviours and how might they differ across the diverse security behaviours? (Stage 2b)
4. What behaviour change approaches are most suitable for cyber security? (Stage 3)

This research will entail a pragmatic research approach through use of both qualitative and quantitative methodologies. Stage 1 and 2a are complete however stage 2b is currently on-going.

2.1 Stage 1.

The first stage involved the development of a behavioural inventory by identifying employees' expected security behaviours. To achieve this, an internet search was carried out to collate information security policies available and accessible online. 25 policies were collated from healthcare (n=7), universities (n=10) and councils (n=8). Policies were excluded if they only consisted of an executive summary or they referenced supplementary documents that were unavailable online or if they were not a UK institution (due to legislative differences between countries).

Inductive content analysis was adopted using guidelines outlined by [12]. The purpose of this analysis was to establish the categorical structure of the data within ISPs. The findings revealed eleven categories with designated behaviours for employees as shown in Table 1.

Table 1. Categories with designated security behaviours

Category	*Description*
Remote working	Actions for working on mobile devices and in external locations
Removable media	Portable storage devices that can be connected to and removed from a computer (e.g. USB sticks)
User access management	How access controls are allocated and managed
Prevention of malicious software	Actions to prevent malicious software
Breaches of security	Steps for recovering and reporting security incidences
Physical security	Strategies to physically protect infrastructures, information and information resources
Information control	Responsibility in protection, storage and processing of information
Software & Systems	Software and system acquisition, installation and maintenance
Acceptable usage	Appropriate usage of information systems, email and the internet
Continuity planning	Outlines prevention and recovery from internal and external threats
Compliance to legislation	Compliance to legislation acts such as the data protection act (1998)

2.2 Stage 2a

Security can be considered a sensitive issue for employees to discuss as behaving insecure could be perceived as poor job performance. It is important to address why employees behave insecurely and therefore methodologies or tools to engage employees in this discussion are required.

Vignettes are considered one such useful tool and have been shown to be useful when dealing with sensitive issues [13] as they allow participants to control whether they disclose personal information. These are fictional scenarios describing a character and a story that allow exploration of participants' views on the issues arising from the scenario. In this research, a vignette described a security scenario (e.g. recycling passwords) but did not discuss the consequences or whether the behaviour was secure/insecure. See figure 1 for example vignette.

Remote computing:

Miles is a merchandiser for a large menswear store and constantly travels to other stores within the local area. One of the benefits of Miles's job is that he is given a company laptop as he is constantly mobile. Miles has a 15 year old daughter, who he lets use his laptop when he doesn't need it as his laptop is of much better quality than his daughter's PC. Mile's daughter uses the laptop for playing computer games, however she often disables the anti-virus software as it slows down her favourite game.

Fig. 1. Example cyber security vignette

A pilot study was run with 8 employees from multiple organisations to assess the suitability of vignettes. This was undertaken by allocating participants to a vignette or non-vignette condition. Those in the vignette condition were given short stories for each of the categories in Table 1. Those in the non-vignette condition were given a short description of the category. A semi-structured interview guide was used covering the elicitation of the factors (see stage 2b). The results from stage 2a indicated that participants in the vignette conditions were more open in their discussion of insecure behaviours and reasons for this, compared to the non-vignette condition and required less questioning from the researcher. Vignettes were therefore deemed a useful tool to use to help aid and engage participants in security discussion and allow rich and detailed data to be collected.

2.3 Stage 2b

This stage is exploring the influences of security behaviours, aiming to analyse the degree to which factors may differ depending upon specific security behaviours. This approach will help examine user perceptions and usage of security solutions, within the workplace, allowing the identification of poor security practices which require further exploration and targeted behaviour change.

A deductive approach was adopted for this stage using factors that have previously been investigated for compliance to ISP. The factors of interest are influences including internal (self-efficacy & attitude) and external (social pressures). Furthermore, individuals' threat evaluation (perceived vulnerability & severity), and their response evaluation (response efficacy & cost). Semi-structured interviews will be used with employees' from recruited organisations, using the vignettes based on stage 1 and questions focusing on the elicitation of the factors outlined above. Participants will also be required to complete a questionnaire, assessing psychological ownership and organisational citizenship behaviour. This is to categorise participants into high/low groups to allow comparisons to be made dependent upon these measures.

3 Future Work

On completion of stage 2b, the data will be analysed using framework analysis [14] as this deductive approach allows the assessment of the influences to be identified *a priori* and refined through further analysis. The findings will also help identify behaviours that will be targeted in interventions. These interventions could take many forms such as manipulating influences of the targeted security behaviour (e.g. increasing individual's perceived severity) and investigating whether this leads to behaviour change. This could, for example, involve re-designing security software so interventions target a specific behavioural determinant, or, use individuals' data from security software to provide a tailored intervention to the individual. Whilst the current behaviour change studies are yet to be designed. The following sections outline the proposed methodology of the behavioural interventions, measurement of security behaviour and an example intervention to illustrate behaviour change within the cyber security domain.

3.1 Stage 3

Behaviour change interventions

Currently, there is an abundance of guidance for the development, running and evaluation of behaviour change interventions. Within the behaviour change domain, interventions aiming to change behaviour are often poorly reported and difficult to replicate [15]. It is therefore important that when designing the interventions for this PhD that they follow previous research and guidance to enhance replicability and help inform future cyber security research and practice.

For example, appropriate guidance includes the Medical Research Council (MRC) framework for complex intervention development, implementation and evaluation [16]. Other useful guidance is the nine principles for developing interventions based on models [17] which is developed by the Government Social Research and provides practical guidance on intervention development using theoretical underpinnings. These guidelines highlight the importance of interventions being theory-driven, piloted and evaluated effectively. They emphasise understanding the target behaviour, its key influencing behavioural determinants, and where possible, identifying effective intervention techniques that have previously worked for the targeted factors. As discussed, in terms of this PhD research, stages 1 and 2 are aiming to explore the determinants of security behaviour and will inform potential areas for intervention. Once target behaviours have been identified, the subsequent studies of stage 3 will aim to improve the chosen security behaviour of interest using interventions.

Evaluating successful behaviour change

It is important that any changes resulting from an intervention are due to the intervening factors at play and not due to extraneous variables. It is therefore necessary that the most appropriate evaluation methods are in place to assess the effectiveness of the intervention and provide empirical evidence of its efficiency. Random control trials (RCTs) are considered the gold standard for evaluation and have been widely

used within the health domain for clinical trials and also within the psychology discipline. They provide valid and reliable evidence of the effectiveness of an intervention and are considered the best way to evaluate a behaviour change attempt. To design RCTs, participants are allocated to either an experimental condition (behaviour change attempt) or a comparison (control) condition. This design endeavours to overcome confounding variables by exposing participants in the experimental and control condition to the same experimental factors except the behaviour change intervention. It is assumed that differences in behaviour resulting from the research are due to the intervention and not extraneous variables. To achieve this it is important that participants in the intervention condition and those in the control condition are as 'closely matched' as possible by recruiting participants from the same recruitment sample and randomly allocating them to conditions. Randomisation to conditions reduces selection bias by ensuring that the only differences between the intervention and control condition will be due to chance and any observed differences will be due to the intervention condition. The use of RCTs for behaviour change is advocated extensively throughout behaviour change literature including the MRC framework and Cabinet Office guidance for developing public policy related to changing behaviour [18]. The behaviour change studies of stage 3 will therefore adopt RCTs as they are deemed the most appropriate methodology for assessing intervention efforts.

Measuring security behaviour

Behaviour is complex making it equally complex to quantify and measure it. Previous research exploring security behaviour in employees has primarily adopted self-report measures to assess an individual's security performance. Typically this has explored the extent to which they comply to information security policies and specific security behaviours such as email-related security behaviour [19]. Despite many advantages to using self-report data, they are a type of subjective measure as they rely on individual awareness. Therefore, they are open to many biases and are potentially unreliable. Objective measures, on the other hand, are considered to be more robust and accurate indicators of behaviour because they are less vulnerable to biases. In the context of security, an objective measure could be a password log to give an indication of frequency of password changes. Where possible, the behaviour change studies in this PhD research will measure both subjective and objective measures of behaviour in order to increase reliability, validity and measurement of behaviour change effectiveness.

Cyber Security behaviour change: An example

Current security systems within in the workplace (such as anti-virus software, for example) can be considered quite passive as they are often mandated by IT support and require little input from employees. Furthermore employees are often unaware of the function and utility of this software on their work computer. An active intervention could be designed to utilise the information from anti-virus software and other security systems to tailor risk messages to employees regarding their behaviour when online and ultimately improve their virus prevention behaviour. The intention of the intervention would be to increase perceived susceptibility to receiving a virus. This

would be achieved by providing information about the consequences of visiting insecure websites and downloading attachments. Furthermore, indicating the level of risk associated with the employees' behaviour would provide a "visualisation" of their actions (e.g. an insecure website would be more noticeable if the colour red was used in a message). Individuals are influenced by sub-conscious cues and this "priming" through visualisation is important for behaviour change [20]. It would be anticipated that by enhancing perceived susceptibility to viruses and priming secure behaviour would lead to behaviour change in employees.

4 Contributions

It is hoped that this research will help understand how to promote security behaviour change within the workplace and in doing so, aid evaluation of current approaches to information security. The main contribution is to develop interventions that are theory based and provide empirical evidence of their efficiency. Furthermore, the findings from this research will aid in the re-development of security solutions and provide resolutions for how they can be designed to encourage secure behaviour.

5 Acknowledgements

I would like to thank my PhD supervisors, Lynne Coventry and Linda Little, for their support and guidance with this research.

6 References

1. Cabinet Office. The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world. (2011)
2. Price Waterhouse Coopers. 2012 Global State of Information Security Survey
3. Stanton, J.M., Stam, K.R., Mastrangelo, P., Jolton, J.: Analysis of end user security behaviours. Computers & Security. 24, 124-133 (2005)
4. Bulgurcu, B., Cavusoglu, H., Benbasat, I.: Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Quarterly. 34, 523-548 (2010)
5. Ifinedo, P.: Understanding information systems security policy compliance: An integration of the theory of planned behaviour and the protection motivation theory. Computers & Security. 31, 83-95 (2012)
6. Herath, T., Rao, H. R.: Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems. 18, 2, 106-125 (2009)
7. Herath, T., Rao, H. R.: Encouraging information security behaviours in organisations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems. 47, 2, 154-165 (2009)
8. Fishbein, M., Cappella, J. N.: The role of theory in developing effective health communications. Journal of Communication. 56, S1-S17 (2006)

9. Anderson, C. L., Agarwal, R.: Practicing safe computing: a multimedia empirical examination of home computer user security behavioural intentions. MIS Quarterly. 34, 3, 613-643 (2010)
10. Puhakainen, P., Siponen, M.: Improving employees' compliance through information systems security training: An action research study. MIS Quarterly. 34, 757-778 (2010)
11. Davinson, N., Sillence, E.: It won't happen to me: Promoting secure behaviour among internet users. Computers in Human Behaviour. 26, 1739-1747 (2010)
12. Elo, S., Kyngäs, H.: The qualitative content analysis process. Journal of advanced nursing. 62, 1, 107-115 (2008)
13. Barter, C., Renold, E.: 'I wanna tell you a story': exploring the application of vignettes in qualitative research with children and young people. International Journal of Social Research Methodology. 3,4, 307-323 (2000)
14. Ritchie, J., Spencer, L.: Qualitative data analysis for applied policy research. In: Bryman, A. & Burgess, R.G. [eds.] "Analyzing qualitative data". Sage, London. (1994)
15. Abraham, C., Michie, S.: A taxonomy of behavior change techniques used in interventions. Health psychology. 27, 3, 379 (2008)
16. Campbell, M., Fitzpatrick, R., Haines, A., Kinmonth, A. L., Sandercock, P., Spiegelhalter, D., Tyrer, P.: Framework for design and evaluation of complex interventions to improve health. BMJ: British Medical Journal. 321,7262, 694 (2000)
17. Darnton, A.: GSR Behaviour Change Knowledge Review. Practical Guide: An overview of behaviour change models and their uses. HMT Publishing Unit, London (2008)
18. Haynes, L., Goldacre, B., Torgerson, D.: Test, learn, adapt: developing public policy with randomised controlled trials. Cabinet Office-Behavioural Insights Team (2012)
19. Ng, B.-Y., Kankanhalli, A., Xu, Y.: Studying users' computer security behaviour: A health belief perspective. Decision Support Systems. 46, 4, 815-825 (2009)
20. Cabinet Office. MINDSPACE: Influencing behaviour through public policy. (2010)