Human aspects of cyber security: Behaviour or culture change?

Received (in revised form): 1st February, 2018

Adam Joinson

holds the post of Professor of Information Systems at the University of Bath, School of Management. His research focuses on the interaction between psychology and technology, with a particular focus on how technology can shape behaviour, social relations and attitudes. Recently this work has covered privacy attitudes and behaviours, the social impact of monitoring technology, computer-mediated communication and the human aspects of cyber security and security compliance. The EPSRC, ESRC, EU, British Academy and UK Government have funded this work. He has published over 80 articles in the field, as well as editing the *Oxford Handbook of Internet Psychology* (OUP, 2007) and authoring two books on psychology and technology. He is principal investigator for the Cyber-Security Across the LifeSpan project (www.cSALSA.uk) and co-investigator for the Centre for Research and Evidence on Security Threats (www.crestresearch.ac.uk).

School of Management, University of Bath, Claverton Down, Bath BA2 7AY, UK
Web: www.joinson.com; E-mail: A.Joinson@bath.ac.uk

Tommy van Steen

is a postdoctoral research associate at the University of Bath, School of Management. His research focuses on advancing behaviour change knowledge and applying behaviour change theories to a variety of themes and behaviours. Currently, this involves applying behaviour change theories to address cyber security questions. These questions include the role of end users, management, and organisational structures that can hinder or support the occurrence of meaningful and lasting behaviour change. His work is funded by the UK Government.

School of Management, University of Bath, Claverton Down, Bath BA2 7AY, UK
E-mail: T.van.Steen@bath.ac.uk

Abstract For security professionals, addressing the role of the human in cyber security is becoming ever more important as systems are technically increasingly secure and threat actors shift their focus towards exploiting human vulnerabilities. This paper looks at three ways that the role of humans in cyber security has been addressed and suggests integrating culture, behaviour and the design of security tools and policies to properly define the role of the human in protecting cyber security.

KEYWORDS: cyber security, behaviour change, organisational culture, human vulnerabilities

INTRODUCTION

Despite increased efforts to improve cyber security for organisations and individuals, growing reports of breaches and attacks suggest that not only are we more vulnerable than ever, but also that there 'is no obvious solution to the problem of cyber security'.[1]

It has become accepted wisdom that cyber security is a 'socio-technical' system, encompassing both technical and human elements.[2,3] However, making advances based on this understanding has proved difficult. Within cyber security, people have traditionally been viewed as the 'weakest link', an unpatchable part of the system, who often undermine the efforts of information security professionals to protect systems.[4,5] This attitude is best summarised

by Van Niekerk and Von Solms, who note that 'Employees, whether intentionally or through negligence, often due to a lack of knowledge, are the greatest threat to information security'.[6]

This concern about user behaviour has led to three main strands of academic research and intervention efforts focused at different levels: 1) the behavioural, to be addressed using 'nudge' and social marketing techniques;[7,8] 2) the cultural, to be addressed by changing organisational security culture;[9] and 3) the human-design process approach, addressed by designing policies and systems around human tasks and capabilities, and organisational goals.[10,11,12] In the following sections, each of these approaches is briefly outlined.

BEHAVIOURAL APPROACHES TO CYBER SECURITY

The behavioural approach to cyber security began with an appreciation that often security procedures require users to engage in behaviours that are difficult, if not impossible, to adhere to.[13] For instance, requiring complex ('strong') passwords that cannot be used across multiple sites, cannot be written down and need to be changed frequently leads to cognitive overload, which ultimately may be counter-productive in terms of protecting accounts from external intrusion.[14] More recently, researchers have taken methods and approaches from health behaviour change and 'nudge' approaches to attempt to change security behaviour.[15] However, the degree of success when implemented has been somewhat limited. For example, Caputo et al.[16] reported no impact of different versions of behavioural science-inspired training on people's susceptibility to simulated spear phishing attacks, leading them to conclude that 'changing security behaviour is difficult', although the research conclusions were hampered by employees not reading the training material that contained the experimental materials.

Many behavioural approaches to cyber security take as inspiration theories and approaches used in health interventions to change behaviour. For instance, Briggs et al.[17] apply protection motivation theory (PM Theory) to understand how a combination of threat and response/coping appraisals leads to the type of response behaviour users engage in (see Figure 1).

PM Theory links the potential damage/threat that a cyber security breach could cause (divided into how severe the threat is seen, and how vulnerable the user believes themselves to be), in combination with the possible costs (eg financial, time) and effectiveness of the response to predict people's likelihood of engaging in defensive action. PM Theory has been used successfully in the cyber security field to study a variety of protective behaviours (eg use of firewalls, passcodes etc.), usually with some degree of success.[19,20,21] So, for instance, we can alter the likelihood a user engaging in protective behaviour by increasing perceived threat (severity or vulnerability) and by providing training that increases the perceived ability to complete protective action.

An alternative behavioural approach comes from the 'nudge' or 'behavioural insights' approach, whereby a range of lessons from (mostly) behavioural economics and social psychology is used to encourage the desired cyber security behaviour. There are various approaches to 'nudging' behaviour,[22] the usual goal being to alter the 'choice architecture' in such a way that people's behaviour is 'nudged' towards the desired pattern. Across government, various models for behaviour change have been adopted and refined, including the 'E-A-S-T' model promoted by the Behavioural Insights Team, originally at the Cabinet Office.[23] According to this model, behaviour can be moved in the desired direction by making it:

- **Easy**: It has been argued that taking cyber security protective steps exerts a cost on individuals, many of whom have a

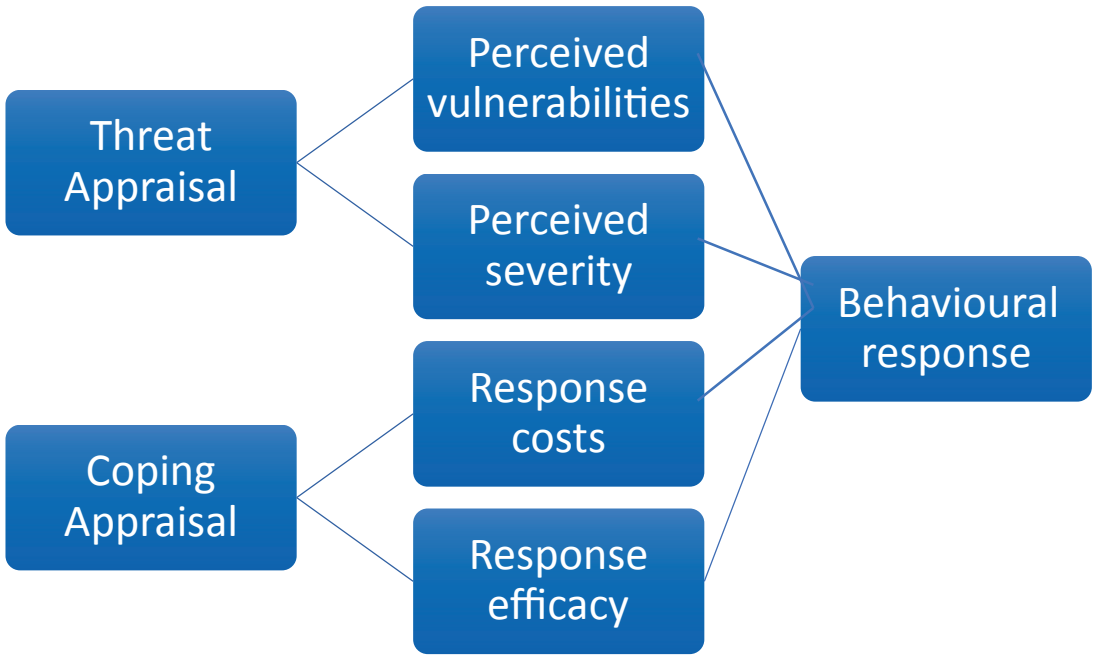

Figure 1: Protection Motivation Model (adapted from Rippetoe & Rogers)[18]

limited 'compliance budget'.[24] However, if security is a default option, with acting insecurely being the costlier action (in terms of time or effort), then it is much more likely that people will retain the default settings. At the same time as being a default (eg setting a passcode when setting up a smartphone), it should be as easy as possible for users to interact with the system (eg by using a fingerprint to open a device), so that security reduces hassle. Finally, part of making something easy is to also make it as simple as possible to understand — by avoiding technical language, being specific in terms of what is required (and by whom) and removing unnecessary information.

- **Attractive**: For many cyber security professionals, the focus is on compliance and the punishment of misdemeanours. While there is some evidence that sanctions can improve compliance,[25] they may also be counter-productive, especially if a policy stops someone doing their main job. There is remarkably little evidence on the impact of positive rewards for compliance,[26] although there is ample evidence that providing a variety of incentives (eg via gamification) can change workplace behaviours such as energy use. Another aspect of attractive is to make something draw attention (also called 'salient') — for instance, by adopting the 'traffic light' approach to food labelling for technology products, or by displaying warnings before a potentially insecure action (eg sending a confidential document to an external recipient). There is some evidence that these kinds of 'salience' prompts can be effective.[27]
- **Social**: There is extensive evidence that people will look to others for guidance on how to behave (called 'social proof'). While culture will be discussed later, suffice to say that many people have noted the importance of behavioural and social norms of cyber security behaviour in the workplace[28,29,30] and that there is

evidence that manipulating social norms changes individual behaviour.[31] There are various ways to use the power of others to manage behaviour — for instance, having people make public commitments to others greatly increases compliance to the promised behaviour.[32]

- **Timely**: The most effective behavioural interventions are those that are presented at the right time — eg to wash your hands immediately you leave a toilet, to remove a pass on leaving a building, or to check an e-mail attachment before it is clicked. For this reason, many training courses tend to be rather disappointing in changing behaviour — the opportunities to engage in the correct action are too far removed from the prompt. At the same time, people do tend to change their behaviour if they have made plans for how (and when) to complete the behaviour (called an 'implementation intention'). Often cyber security is presented as providing a long-term (distant, uncertain) reward ('remain safe') while providing a short-term, immediate cost ('no, you can't access/share/open …'). This provides a particular challenge for cyber security practitioners since a cognitive bias, known as 'hyperbolic discounting', means that humans tend to over-value short-term rewards over long-term ones.

In combination, approaches such as E-A-S-T and social/cognitive models such as PM Theory provide an approach to understanding why people behave in a certain way, and how interventions can be designed in such a way as to encourage them to behave in the desired way. There are multiple alternative approaches to understanding and changing behaviour, but most incorporate this same approach of understanding behaviour followed by attempts to change. In all cases, a behavioural approach should (ideally) measure an actual behaviour (eg using multiple sites to log incidents, with each site receiving a different intervention). For this reason, it is normal to measure a baseline for the behaviour (either before the intervention, or by running a control group which receives no behavioural intervention).

The second, related, approach to human aspects of cyber security is the cultural, which is discussed below.

CULTURAL APPROACHES TO CYBER SECURITY

As noted earlier, end-user behaviour is vital to a strong and secure cyberspace. However, this behaviour does not occur in a vacuum. It is influenced by, and in turn affects, other factors surrounding the end user. This wider view of cyber security behaviour and the influence of the environment are captured in research on security culture, the cultural system in which the cyber security threats, solutions and behaviours occur. As such, cultural norms, habits and views specific to an organisation can affect end-user behaviour. For instance, an organisation where cyber security is of the utmost importance may choose not to take on projects if they know in advance that they cannot adhere to their internal cyber security standards due to time constraints or otherwise.

The importance and value of creating a cyber security culture is advocated in the literature as fundamental to long-term behavioural changes and sustainable cyber security habits.[33,34] This focus on a culture of cyber security is not merely an academic suggestion, but has also been supported by standard bodies such as the International Organization for Standardization (ISO). However, there is as yet no clear definition of what actually is a cyber security culture. The existing definitions vary on which factors are included and how 'culture' is viewed. For example, some definitions focus strongly on values,[35] whereas others tend to view specific sets of behaviour as exemplars of a cyber security culture.[36] More elaborate models integrate several factors, such as the above-mentioned behaviours and values.[37]

As definitions vary and no clear successful definition has been established so far, the focus has pointed towards devising methods of measuring relevant cultural factors, rather than theorising about possible models. For example, Da Veiga and Eloff[38] devised a framework and assessment instrument of security culture, in which seven important factors emerged: leadership and governance, security management and operations, security policies, security programme management, user security management, technology protection and operations and change.

Creating a security culture rather than running a short behaviour change campaign that focuses on a single behaviour is, of course, more challenging. This challenge does not only lie in the complexity of the behavioural patterns that need to be influenced, but also in getting a whole organisation on board, from the CEO down to the new intern. Compared to a single behavioural intervention, this is a long-term project that requires significant investment. Such a cultural change would not only address the behaviour of end users, but also consider how employees view their own roles and where they see themselves in the organisation, establish a sense of responsibility for cyber breaches beyond their own job security and create a team spirit where employees are not afraid to question colleagues' behaviour when this behaviour is breaching security guidelines and policies. It is not just the end users that would need to be educated and persuaded, but also the higher management, as establishing a security culture can (seemingly) clash with a focus on maximising profit. To date there are no clear guidelines for how best to communicate the importance of cyber security to a board who are often more fixated on return on investment and/or easily understood and benchmarked measures (eg click rates on phishing simulations or breaches detected). All too often the example provided by senior management is still to treat security as an impediment to be worked around rather than essential to the sustenance of the business.

Additionally, a security culture would need to be embedded in the existing organisational culture. The pitfall can be to treat security as a simple add-on to the existing habits, methods and procedures. However, for security to be effective, it needs to be fully ingrained in the wider organisational culture, rather than a separate factor. To achieve this, continuous efforts are required in which security practices are shared, guidelines updated and training provided.

A starting point for an organisation seeking to implement such a security culture is to analyse their current situation. Is there currently a 'strong' security culture and if so, what does it consist of? Perhaps employees feel security is more of a nuisance rather than seeing its value. Similarly, how is security supported within the organisation, and is this support equally strong at the level of end users as well as at board level? (See Ashenden and Sasse[39] for a discussion of the interaction of chief information security officers [CISO] with organisational culture.) By understanding the security culture present in an organisation, the required changes and improvements quickly become clear, even if the ways to engender change are more challenging.

HUMAN-CENTRED DESIGN APPROACHES

In their discussion of why security awareness campaigns can fail, Bada, Sasse and Nurse[40] note that security policies often do not align with business goals. As far back as 1999, Adams and Sasse were noting that for some users it is impossible to both complete their main work task in a timely manner and comply with security policies. In these circumstances, employees may well engage in 'shadow security'.[41] Shadow security is a form of non-compliance, but rather than simply ignoring the security policy,

employees instead attempt a workaround that allows them to complete their job while also providing a modicum of security. For instance, a security policy may not allow for a bidding team to share documents via a commercial cloud service. However, if the potential client requires that method of sharing, then the bidding team is faced with a dilemma: they can comply with the policy (and definitely lose the business), work around the policy (non-compliance) and potentially win the business, or try and convince the client to use a more secure method of data transfer. In many cases the latter is unrealistic, so the team is faced with two choices. They may, however, adopt a third, shadow approach, which is like non-compliance (ie they use the cloud service) but which retains an element of information protection (eg password protected or encrypted files, or deletion of the files upon transfer). Kirlappos et al.[42] propose that security professionals should learn from shadow security in order to design security protocols that support employees' workplace goals.

This approach to designing security to support business goals and processes is a natural development of the movement towards 'usable security' and 'human-centred security',[43,44] whereby cyber security considers human capabilities as well as the context in which security is enacted (eg as part of a workplace process, within an organisational culture). This interactive approach draws on both the behavioural and cultural, although tends to place the focus on the design of security tools and processes. For instance, there has been much work from a human-centred design approach to consider passwords, in particular the lack of usability inherent in many password guidance and requirements.[45] As is well known, password guidance is mostly unusable for individuals — the rules on complexity, non-reproduction across services and not writing down is an almost impossible ask for most humans — so we end up either adopting a technical solution (eg password manager) or breaking some rules (eg using the same password for sites seen as relatively trivial, or writing down in paper form).

COMBINING THE BEHAVIOURAL, CULTURAL AND DESIGN PERSPECTIVES

Sasse and Flechais[46] divide security as a socio-technical system into three elements: product (the design of the tool or process); process (who designs the tools, who is responsible for security, and how they support work processes); and panorama (what is the wider context, such as security culture or training/awareness programmes). Within the health behaviour change field, similar approaches are common — for instance, Michie, van Stralen and West[47] outline a 'behaviour change wheel', with the sources of behaviour at the centre, intervention type on the next outer ring, and finally, policy on the outermost ring. These three layers allow for practitioners to consider: 1) the causes and sources of the behaviour (eg lack of skills/knowledge); 2) appropriate intervention type (eg education or training, incentivisation); and 3) the policy level response (eg regulation, fiscal measures).

We suggest that cyber security practitioners take a similarly integrated approach to considering the human aspects of cyber security. First, it is important to understand what the problematic behaviour is, to what it would ideally be changed and how you would measure success. In terms of identifying the human aspect to be addressed, it may be useful to apply the 'capability-motivation-opportunity-behaviour' (COM-B) method developed by Michie and colleagues[48] (see Figure 2).

- **Capability**: Is the person capable of conducting the appropriate behaviour? For instance, do they have the knowledge, skills and appropriate tools to take the right cyber security decision?

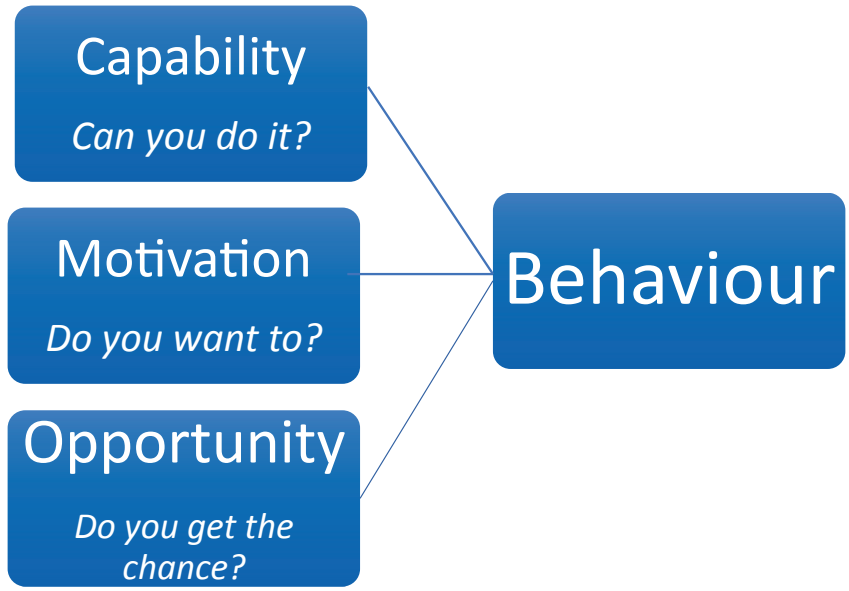

Figure 2: COM-B model (adapted from Michie et al.[49])

- **Motivation**: Are they motivated to take the right steps? For instance, do they perceive there to be a cost (eg a threat to the organisation) if they do not act in a secure manner? Do they intend to be (in)secure?
- **Opportunity**: Do they have the opportunity to behave in a secure manner? For instance, is there a cue that they need to respond to where they can decide to follow policy? Does following cyber security policy lead to problems with their work?

Next, the role of the human in cyber security needs to be understood in terms of the wider workplace, in particular the business goals and work processes they are engaged in as their main task. As noted by Sasse and Flechais[50] and Beris, Beautement & Sasse,[51] cyber security policies and processes can often get in the way of individuals' main task at work, causing frustration among employees. This wider workplace context will determine the likely balance of capability, motivation and opportunity as a cause of the non-compliance behaviour, as well as suggesting that policy and process may need to be amended to reflect the business processes within the organisation.

Alternatively, a human-oriented cyber security problem may be due to lack of awareness, knowledge or skills, in which case an educational and/or awareness programme is the appropriate response.

Finally, within a workplace, cyber security behaviour (and possible interventions) needs to be understood in the wider context — Sasse and Flechais' idea of panorama.[52] As discussed above, cyber security behaviour is (in part) determined by organisational culture, in particular information security culture. While some of this culture is 'bottom up' in terms of the norms of behaviour within a workplace, the role of leadership in establishing the importance and value of cyber security cannot be understated. Only by thoroughly unpicking the causes of a potential human issue in cyber security and placing that behaviour in the context of work processes and organisational culture can we begin to design interventions that address the behaviour — which in some cases might be to reconsider security products and tools, or even board level support for cyber security — rather than the standard training and awareness package (see Figure 3).

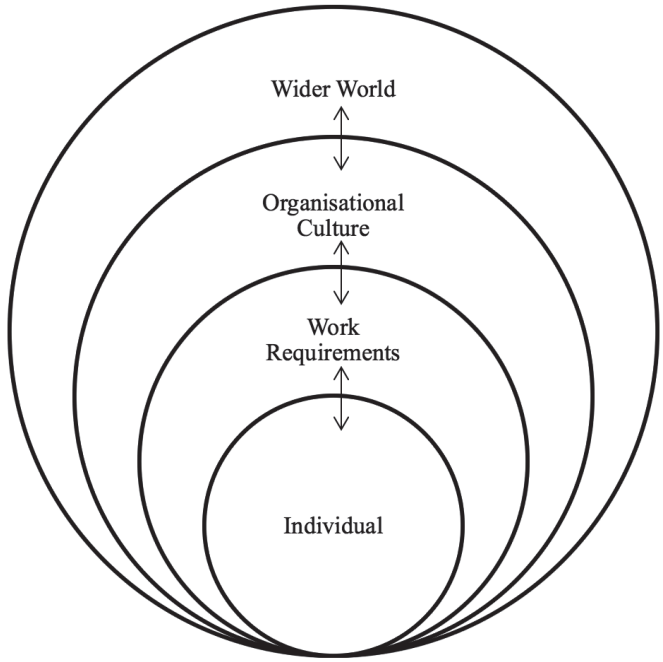

Figure 3: The integrated cyber security behaviour model

The integrated cyber security behaviour model allows us to visualise how cyber security behaviour at the core (the end user who is vulnerable to phishing attacks, who deals with sensitive information and who can report possible cyberattacks) needs to be understood as placed within, and influenced by, the environment in which the behaviour occurs. The layer immediately surrounding the end user consists of the work environment and requirements. Factors in this layer include the expectations from line managers, external contractors and direct colleagues, work processes, clashes between policy and work requirements, etc. When these factors conflict with the security policies and guidelines within the organisation, the end user must decide whether it is more important to follow the guidelines or satisfy work demands. These work requirements are likely to change when old projects are completed and new projects are started. Therefore, this layer of work expectations is constantly changing, hence any tension between work tasks and security policies will also vary across time. Of course, this tension can also be alleviated by ignoring policy and developing work arounds (ie shadow security).

The next level beyond the work requirements is the organisational culture in which the work is carried out. Organisational culture influences decisions on every aspect of the organisation. It is at this level where a general approach to cyber security can be supported or hindered, but it is also likely to be resistant to easy change. For instance, habits, organisational structure, the value put on security by line managers and board members, and 'how things are handled around here' all influence the views and value placed on cyber security practices and adherence to policies and guidelines.

On the final, outer layer of the model, there is the wider world context, including factors such as the regulatory environment, competitive threats, general threats to cyber security and public opinion — all of which influence an organisation's strategies and prioritising of resources.

One advantage of visualising the relationship between behaviour and the

wider context is that it encourages managers to consider not only the specific user behaviour, but also how that behaviour relates to specific tasks and workplace pressures, wider organisational culture and the external pressures acting on the organisation. It can also serve as a starting point for organisations that want to change employees' cyber behaviour — so while a behavioural analysis can be conducted using the COM-B approach outlined above, this only deals with a small part of the wider picture. While training at the individual level (for example, to detect phishing e-mails, how to safely share data or how to use encryption when sending confidential messages) is important, we suggest that it is also important to consider how that behaviour occurs within the context of work tasks and policies, organisational culture and leadership and wider pressures on the organisation.

ACKNOWLEDGMENT

The writing of this paper was, in part, supported by EPSRC grant 'Cyber-Security Across the LifeSpan (cSALSA) reference: EP/P011454/1.

References

1. Garfinkel, S. L. (2012), 'The cybersecurity risk', *Communications of the ACM*, Vol. *55*, No. 6, p. 29.
2. McKenna, S., Staheli, D. and Meyer, M. (2015), 'Unlocking user-centered design methods for building cyber security visualizations', *2015 IEEE Symposium on Visualization for Cyber Security (VizSec '15)*, Vol. 9, No. 1–9, p. 8.
3. Pfleeger, S. L. and Caputo, D. D. (2012), 'Leveraging behavioral science to mitigate cyber security risk', *Computers and Security*, Vol. 31, No. 4, pp. 597–611.
4. Kolkowska, E., Karlsson, F. and Hedström, K. (2017), 'Towards analysing the rationale of information security non-compliance: Devising a value-based compliance analysis method', *Journal of Strategic Information Systems*, Vol. 26, No. 1, pp. 39–57.
5. Siponen, M. T., Adam Mahmood, M. and Pahnila, S. (2014), 'Employees' adherence to information security policies: An exploratory field study', *Information and Management*, Vol. 51, No. 2, pp. 217–224.
6. Van Niekerk, J. F. and Von Solms, R. (2010), 'Information security culture: A management perspective', *Computers & Security*, Vol. 29, No. 4, pp. 479–486.
7. Ashenden, D. and Lawrence, D. (2013), 'Can We Sell Security Like Soap? A New Approach to Behaviour Change', New Security Paradigms Workshop 2013, pp. 87–94.
8. *Ibid.*, note 5.
9. Von Solms, B. (2000), 'Information security: The third wave', *Computers & Security*, Vol. 19, No. 7, pp. 615–620.
10. Ashenden, D. and Lawrence, D. (May/June 2016), 'Security Dialogues: Building Better Relationships between Security and Business', *IEEE Security & Privacy,* Vol. 14, No. 3, pp. 82–87.
11. Kirlappos, I., Parkin, S. and Sasse, M. A. (2014), 'Learning from "Shadow Security": Why understanding non-compliant behaviors provides the basis for effective security', *Usec '14*, Workshop on Usable Security, San Diego, CA, USA, pp. 1–10.
12. Siponen, M. T. (2001), 'Five dimensions of information security awareness', *Computers and Society*, Vol. 31, No. 2, pp. 24–29.
13. Adams, A. and Sasse, M. A. (1999), 'Users are not the enemy', *Communications of the ACM*, Vol. 42, No. 12, pp. 41–46.
14. *Ibid.*, note 15.
15. Briggs, P., Jeske, D. and Coventry, L. (2017), 'Behavior Change Interventions for Cybersecurity', in Little, L., Sillence, E. and Jounson, A., *Behavior Change Research and Theory: Psychological and Technological Perspectives*, Academic Press, London, pp. 115–136.
16. Caputo, D. D., Pfleeger, S. L., Freeman, J. D. and Johnson, M. E. (2014), 'Going spear phishing: Exploring embedded training and awareness', *IEEE Security and Privacy*, Vol. 12, No. 1, pp. 28–38.
17. *Ibid.*, note 17.
18. Rippetoe, P. A. and Rogers, R. W. (1987), 'Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat', *Journal of Personality and Social Psychology: Personality Processes and Individual Differences*, Vol. 52, No. 3, pp. 596–604.
19. Chenoweth, T., Minch, R. and Gattiker, T. (2009), 'Application of protection motivation theory to adoption of protective technologies', Proceedings of the 42nd Annual Hawaii International Conference on System Sciences, HICSS.
20. Mutchler, L. A. (2012), 'Expanding protection motivation theory: The role of individual experience in information security policy compliance', BMC, available at https://bmcpsychology.biomedcentral.com/articles/10.1186/s40359-017-0182-3 (accessed 5th February, 2018).
21. Siponen, M. T., Pahnila, S. and Mahmood, M. A. (2010), 'Compliance with information security policies: An empirical investigation', *Computer*, Vol. 43, No.2, pp. 64–71.
22. Thaler, R. H. and Sunstein, C. R. (2008), *Nudge*, Yale University Press, New Haven.
23. Service, O., Hallsworth, M., Halpern, D., Algate, F., Gallagher, R., Nguyen, S., Ruda, S. and Sanders,

M. (2015), 'EAST Four simple ways to apply behavioural insights', Cabinet Office, available at http://38r8om2xjhhl25mw24492dir.wpengine.netdna-cdn.com/wp-content/uploads/2015/07/BIT-Publication-EAST_FA_WEB.pdf (accessed 5th February, 2018).
24. Beautement, A., Sasse, M. A. and Wonham, M. (2008), 'The compliance budget: Managing security behaviour in organisations', Proceedings of the 2008 Workshop on New Security Paradigms, pp. 47–58.
25. *Ibid*., note 23.
26. Herath, T. and Rao, H. R. (2009), 'Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness', *Decision Support Systems*, Vol. 47, No. 2, pp. 154–165.
27. *Ibid*., note 17.
28. Godlove, T. (2012), 'Examination of the factors that influence teleworkers' willingness to comply with information security guidelines', *Information Security Journal*, Vol. 21, No. 4), pp. 216–229.
29. *Ibid*., note 28.
30. Ion, I., Langheinrich, M., Kumaraguru, P. and Čapkun, S. (2010), 'Influence of user perception, security needs, and social factors on device pairing method choices', Proceedings of the Sixth Symposium on Usable Privacy and Security — SOUPS '10, p. 1.
31. Das, S., Kramer, A. D. I., Dabbish, L. A. and Hong, J. I. (2014)', 'Increasing Security Sensitivity With Social Proof', Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security — CCS '14, pp. 739–749.
32. *Ibid*., note 25.
33. Reid, R. and Van Niekerk, J. (2014), 'Towards an Education Campaign for Fostering a Societal, Cyber Security Culture', 8th International Symposium on Human Aspects of Information Security & Assurance, pp. 174–184.
34. *Ibid*., note 11.
35. Schlienger, T. and Teufel, S. (2003), 'Analyzing information security culture: Increased trust by an appropriate information security culture', Proceedings — International Workshop on Database and Expert Systems Applications, DEXA, Vol. 2003–Janua, pp. 405–409.
36. Dhillon, G. (1997), *Managing Information System Security*, Macmillan, Hampshire.
37. Ramachandran, S., Rao, C., Goles, T. and Dhillon, G. (2013), 'Variations in information security cultures across professions: A qualitative study', *Communications of the Association for Information Systems*, Vol. 33, No. 1, pp. 163–204.
38. Da Veiga, A. and Eloff, J. H. P. (2010), 'A framework and assessment instrument for information security culture', *Computers & Security*, Vol. 29, No. 2, pp. 196–207.
39. Ashenden, D. and Sasse, A. (2013), 'CISOs and Organisational Culture: Their own worst enemy?', *Computers & Security*, Vol. 39, No. B, pp. 396–405
40. Bada, M., Sasse, M. A. and Nurse, J. R. C. (2015), 'Cyber security awareness campaigns: Why do they fail to change behaviour?', Proceedings of the International Conference on Cyber Security for Sustainable Society, pp. 118–131.
41. *Ibid*., note 13.
42. *Ibid*., note 13.
43. Balfanz, D., Durfee, G., Smetters, D. K. and Grinter, R. E. (2004)' 'In search of usable security: Five lessons from the field', *IEEE Security and Privacy*, Vol. 2, No. 5, pp. 19–24.
44. Sasse, M. and Flechais, I. (2005), 'Usable Security: Why Do We Need It? How Do We Get It?', in Cranor, L. F. and Garfinkel, S., *Security and Usability: Designing Secure Systems that People can Use*, O'Reilly, Sebastopol. pp. 13–30.
45. *Ibid*., note 46.
46. *Ibid*., note 46.
47. Michie, S., van Stralen, M. M. and West, R. (2011), 'The behaviour change wheel: A new method for characterising and designing behaviour change interventions', *Implementation Science*, Vol. 6, No. 1, p. 42.
48. *Ibid*., note 49.
49. *Ibid*., note 49.
50. *Ibid*., note 46.
51. Beris, O., Beautement, A. and Sasse, M. A. (2015), 'Employee rule breakers, excuse makers and security champions: Mapping the risk perceptions and emotions that drive security behaviors', Proceedings of the 2015 New Security Paradigms Workshop (ACM), pp. 73–84.
52. *Ibid*., note 26.