SCENE: A Structured Means for Creating and Evaluating Behavioral Nudges in a Cyber Security Environment

Lynne Coventry[1], Pam Briggs[1], Debora Jeske[1], and Aad van Moorsel[2]

[1] Psychology & Communication Technology Lab, Northumbria University, Newcastle-upon-Tyne, UK
[2] Head of Computing Science, Newcastle University, Newcastle-upon-Tyne, UK
{lynne.coventry,p.briggs,debora.jeske}@northumbria.ac.uk, aad.vanmoorsel@newcastle.ac.uk

Abstract. Behavior-change interventions are common in some areas of human-computer interaction, but rare in the domain of cybersecurity. This paper introduces a structured approach to working with organisations in order to develop such behavioral interventions or 'nudges'. This approach uses elements of co-creation together with a set of prompts from the behavior change literature (MINDSPACE) that allows resesarchers and organisational stakeholders to work together to identify a set of nudges that might promote best behavioral practice. We describe the structured approach or framework, which we call SCENE, and follow this description with a worked example of how the approach has been utilised effectively in the development of a nudge to mitigate insecure behaviors around selection of wireless networks.

Keywords: stakeholder involvement, user-centred design, user experience, management of design, methodology, MINDSPACE framework, decision-making, nudging.

1 Introduction

The cyber security community is increasingly concerned with changing the security behaviors of individual Internet users. In a 2013 survey of UK organizations across different sectors, 93% of large organizations reported having a security breach in the previous year, and 87% of small businesses. 36% of the worst breaches were attributed to "inadvertent human error" including accidental leakage of confidential information (pwc, 2013). A National Cyber Security Association (NCSA, 2012) survey of small businesses in the US, conducted in 2012, suggested a cyber security disconnect where 47% of companies believed a data breach would have no impact on their business, yet 87% did not have a formal written Internet security polity and 69% did not even have an informal one. Finally, 18% said they would not even know if their computer network was compromised. This leaves us with a situation where many companies do not have security policies which outline the online behaviors they

A. Marcus (Ed.): DUXU 2014, Part I, LNCS 8517, pp. 229–239, 2014.

expect from their employees, and for those that do, employees do not always comply with that policy. This problem is further compounded by the increased use of mobile devices that blur the boundaries between personal and work-related use. Mobile technology users typically lack the expertise to effectively protect themselves (Ho et al 2010; Furman et al 2012), thus the rise of Bring Your Own Device (BYOD) practices in the workplace can leave many businesses open to cyber security attack.

There are a number of human behaviors which are required to maintain cyber security. A review of the websites dedicated to raising awareness of cyber security issues has resulted in the following list of required requirements of users . Each of these requirements has multiple behaviors associated with it. This makes studying cyber security behaviors difficult as we are not talking about a single behavior.

- Use strong passwords and manage them securely.
- Use security software including anti-virus, anti-spyware and firewalls, and ensure they are up-to-date.
- Always run the latest and official version of software (including operating system). Update as soon as update released..
- Log out of sites when you finish, disconnect from the internet and switch off your computer.
- Only use trusted and secured connections, and devices (including Wi-Fi)
- Only use trusted and secure sites and services and connect securely
- Stay informed about scam/phishing risks (knowledge, common sense, intuition) and try to avoid them
- Always opt to provide the minimal amount of personal information needed for any online interaction and keep your identity protected.
- Be aware of your physical surroundings to prevent theft and shoulder surfing etc.
- Report suspicious or criminal online activities to the authorities

To address the human component of cyber security we need to understand the factors which affect the cyber security behaviors of individual internet users. A significant research literature documents the efficacy of behavior change interventions in other domains (Abraham & Michie, 2008). However, only a small number of researchers have considered behavioral approaches to address the cybersecurity issues (Blythe, 2013; Pfleeger & Caputo, 2012). Little is currently known and much needs to be understood if we are to be effective in changing vulnerable behaviors in order to lower cyber-security threats. In particular, we lack the following:

- Reliable behavioral data on individual users' cybersecurity behaviors.
- Research on the factors influencing an individual's cybersecurity practices or lack thereof.
- A theory of human behavior or how to change human security behavior with validated predictive power.
- Agreement between stakeholders on the size of the problem, the risks and the necessary behaviors required.

Traditional thinking in the organizational sphere is that insecure behaviors simply reflect poor awareness of key security policies and practices. Many organizations implement awareness training as a solution (Leach, 2003). Mainstream information security awareness programs are typically top-down, and try to bring about changes in individual behavior by introducing an expert who delivers relevant information using various media and approaches (Ashford, 2012). However, awareness training is not always effective (Schneier, 2013). This suggests that while awareness is necessary (and may change intentions) it is rarely sufficient as a means of engineering behavior change. We present a structured methodology that allows us to work with organizational stakeholders to identify vulnerabilities and develop relevant technology-based, behavior change interventions (based on theories of behavior) that may prove more effective than simple training.

Telling people how they should behave does not always have an effect on how they actually behave. This certainly applies to security policy compliance (Bulgurcu et al., 2010). Factors such as willpower, motivation, risk perception, cost and convenience are often more important than a lack of knowledge. Various models of behavior exist that identify factors that influence behavior - and some have been applied to the cybersecurity context. These include threat avoidance theory (Liang, 2010), the theory of planned behavior (Burns & Roberts, 2013), deterrence theory, protection motivation theory and the health belief model (Davinson & Sillence, 2010). While such developments offer promise, researchers have yet to fully exploit these behavior models as a basis for developing cybersecurity interventions. Theories tend to assume that people behave reasonably and make good use of all the information available to them when deciding between choices and that people consider the implications of their choices. This may not always be the case and research into decision making suggests that people are subject to a number of cognitive shortcuts and biases when making a decision about how to behave at any particular point in time (Gilovich, Griffin and Kahneman 2002). While we may intend to act in a particular way we may not always act according to that intention.

People can, however, be persuaded to act in particular ways when technologies are designed with user behavior in mind. While we are addressing cyber security behaviors, persuasive technology has been applied to many domains relevant to HCI including ecommerce and mobile health apps. Such persuasive technology (Fogg 2003) is based on three principal assumptions: that a person is motivated to change, that they have the ability to change and that there is an effective environmental trigger (cue to action) for the desired behavior to happen. Thaler and Sunstein (2008) popularized this idea that people can be nudged towards a particular choice or behavior by the careful design of cues in the environment, recognizing that people do not make decisions in a vacuum. They make them in an environment where many features, noticed and unnoticed, can cue their decisions.

Their goal is to show how ‘choice architectures’ can be designed to help nudge people towards make better choices without forcing certain outcomes upon anyone. The tools they highlight are: effective defaults, designing for error, understanding mappings, giving feedback, structuring complex choices, and creating incentives. We should note that these are concepts that human computer interaction practitioners are

already familiar with, as they have been traditionally associated with designing for ease of use. Note, too, that nudging is already common within the ecommerce domain - the example in Figure 2 shows how choice can be presented to dissuade people from the free version towards paying for the upgrade. The "Upgrade Now" option is bright green and highlighted, where as "download now" is dark grey with "No Thanks" written below. Both serve as cues towards the upgrade option.

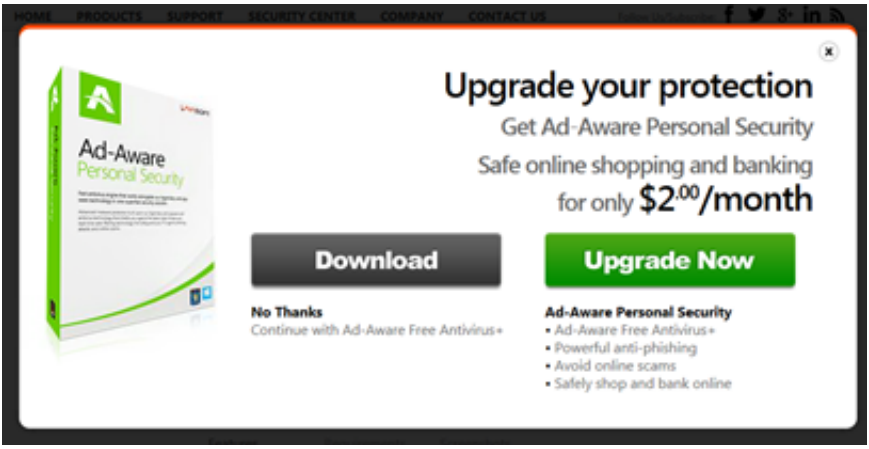

Fig. 1. A nudge towards paying for a premium version of security software (http://www.lavasoft.com/products/ad_aware_free.php#)

1.1 MINDSPACE and Nudging

The MINDSPACE framework (Dolan et al., 2012) is a useful framework for drawing together a number of the 'influencing factors' that have been identified across different economic and psychological models of behavior change. MINDSPACE has been used by the UK government's Behavioral Insight Team to create policies and inform practice in the field. Each of the nine influencers in the framework has been shown to be effective in influencing behavior and decision making. There is overlap between the factors summarised in Nudge and MINDSPACE. The influencing factors identified in MINDSPACEare as follows:

1. **Messenger:** We are influenced by the person and/or method by which the message is delivered (Hayes, 2008).
2. **Incentives**: We are influenced by the rewards and punishments (losses) we receive. This includes our evaluation of the cost of behaving appropriately and the cost of the consequences if we do not. For instance, Herath and Rao (2009) found that the severity of the punishment has a negative effect on security behaviors.
3. **Norms:** We are influenced by the behaviors demonstrated by influencial others, such as senior managers, colleagues and family (Leach, 2003).
4. **Defaults:** We go with the flow of preset options. The default option will be chosen more often (Thaler & Sunstein, 2008).

5. **Salience**: We are attracted by what is either novel or particularly relevant to ourselves (Lamy, Leber, & Egeth, 2004).
6. **Priming**: Our acts are influenced by sub-concious cues (Kay et al, 2004). For instance green represents safety and red represents danger in many cultures.
7. **Affect:** Our emotional associations influence our behavior (Hareli & Rafaeli, 2008). For example, initial emotions formed when visiting a new and unfamiliar shopping websites can influence whether or not a visitor to these sites will disclose information (Li, Sarathy, & Xu, 2011).
8. **Commitments**: We seek to be consistent with our public statements and reciprocate the acts of others (Shore & Wayne, 1993).
9. **Ego**: We act in ways that make us feel better about ourself.

We believe the MINDSPACE framework provides a useful tool to keep the many different potential influencers in mind when developing technology based nudges. For example, using messenger effects and social norms the example in Figure 2 could be further enhanced by adding that 99% of customers choose the upgrade.

Lack of an evidence base to determine what will effectively change peoples' security behaviors has led us to develop an approach, based on MINDSPACE, for working interactively with companies to identify their current security behavior problems and identify possible technology based nudges. These nudges would allow us to influence security behaviors at the specific point in the interaction where decisions relevant to security must be made.

This is a general approach that can be used to identify different problems and solutions may not necessarily involve technology. However, in our work, the focus is on redesigning the technology to persuade people to follow a secure path. We assume that, while people may intend to act securely, their primary goal is very rarely security and therefore it is important to influence decisions at the point the decision has to be made. The goal of our approach is therefore to help organisations identify their most pressing problems (in the form of scenarios) and the most appropriate behavioral design interventions for them.

1.2 Approach

Our iterative behavior design approach - with the acronym SCENE - involves stakeholders in (i) Scenario elicitation; (ii) Co-creating nudges; (iii) Election of nudge(s) for further development; (iv) Nudge prototyping and (v) Evaluation of prototype(s) - (See Fig. 1).

Three important points are worth noting in terms of the application of this methodology. First, every stage utilises numerous stakeholders. This ensures that the solution focuses both on the needs of the end users as well as on the various other individuals directly or indirectly involved or affected by any changes in procedures. Second, the methodology is not a one-time cycle. Instead, the process provides a methodological framework for carefully assessing proposals for change in defaults, settings, and choice architecture based on numerous established practices and findings (Thaler & Sunstein, 2008; Johnson et al., 2012). Thirdly, we believe that the sense of

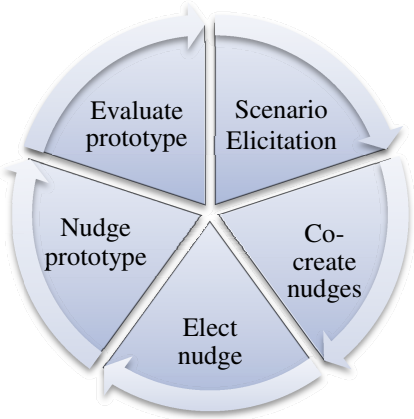

Fig. 2. Five stages in the development and evaluation of a behavioral nudge

joint ownership of security problems at work can be increased by involving stakeholders in the fashion we envision in our framework.

Scenario Elicitation. In this first stage, the aim is to capture poor security behaviors within the organization and understand more about the context for these behaviors. To achieve this, we carry out a group workshop (or series of workshops for larger organizations) where the eventual output is in the form of a security-related scenario or set of scenarios that can feed into the second stage in order to prompt thinking about behavior change. Our contention is that the company benefits from an open discussion of the behaviors which occur within the organization and an open discussion about why users act the way they do. This requires trust within the organization to ensure that these behaviors can be revealed and no blame will be attributed. Participants may be unaware of problematic behaviors. Managers may become aware that their Information Security Policy is too restrictive and employees are utilizing workarounds to optimize productivity. The act of taking part in this process can thus improve awareness of inappropriate behaviors and their consequences. Researchers can provide a back-ground on known user behaviors and vulnerabilities, but the organizational stakeholders should provide information on relevant information systems, usage modes and security behaviors, as well as the relevant security controls, the vulnerabilities of the system and the threats to which the vulnerabilities expose the organization and users.

Output: Identification of selected security scenario(s) where a behavioral change intervention would be beneficial for the organization.

Co-create Using MINDSPACE Workshop. In the second stage, all parties come together in a co-creation activity in which they brainstorm how the different influencing factors from MINDSPACE (described above) could be used to change vulnerable behaviors in the selected scenario(s). Thus a scenario can be reviewed in terms of whether or each of the MINDSPACE influencers would be fruitful to be

exploited through "nudges" in order to instill more secure behaviors. The workshop allows for an open, uncritical discussion of the problem and allows participants the opportunity to explore a number of different perspectives. The very act of taking part in the process will have made users more aware of how their security behavior may be influenced.

Output: A list of nudge possibilities.

Elect Nudge for Development. In the third stage, participants assess the nudge(s) generated and elect one or more for implementation. All parties can contribute to this prioritization process and consider whether these approaches have been tried before (generally or within this company) and whether they practically possible within the scenario and company. In addition, different stakeholders can independent prioritize which nudge they would support. We use a rating scheme to demonstrate the level of support for a proposed solution (as low agreement may reduce the chances that the nudge will be adopted in its final form by all the stakeholders). It is also a means to assess communication and commitment to the process across the board.

Output: Agreement on nudge to employ and its initial design.

Nudge Prototype. In this fourth stage, the final nudge or intervention is developed in detail. In doing this we are involved in creating the choice architecture (Thaler & Sunstein, 2008) which can take many different forms – e.g. an application prototype or particular form of communication. We know that the work context may attenuate the effectiveness of a nudge (if cyber security compliance is onerous it can lead to productivity loss) and so consideration of the work context is vital to ensure nudges do not interrupt the work flow unduly.

Output: A prototype intervention.

Evaluation of Nudge. In the fifth stage, the new nudge prototype is evaluated. It is important to use quick evaluations as part of the prototype process and feedback early to developers if the suggested nudge does not appear to be effective. Researchers and practitioners need to formulate clear success criteria, capture baselines and to record change in self-reports and actual behavioral changes. These data then serve as a means to assess the extent to which the intervention had a reliable and noticeable effect on behaviors. When the evaluation has shown a significant group difference in relation to the behaviors exhibited by the experimental group that was subject to the intervention compared to the control group, the intervention can be rolled out to further groups or applied to a larger sample. Care must be taken to ensure that the intervention is appropriate for all groups.

Output: Roll out and evaluation of intervention to add to evidence base.

2 Piloting the Framework

Any framework also needs to prove itself in practice. In this section we briefly outline an initial evaluation of the framework, in terms of its general effectiveness in

generating useful nudges in our own organizations - addressing known security problems for university staff and students (see Jeske et al., 2014; Turland et al., 2014 for a more detailed description of the resulting nudge application). The development of nudges in the university context followed the SCENE methodology, as follows:

Scenario elicitation: This was undertaken by a research team consisting of psychologists, computer scientists, mathematicians and security experts who worked for two universities in the North East of England, working with other university users. The team identified several scenarios relating to security vulnerabilities, including USB use, failure to update security software on personal computers and the use of social media. A particular scenario around the use of personal computers to carry out (sometimes confidential) work in public places, using insecure public wireless networks was identified as a particularly promising. The use of insecure wireless networks creates a number of security vulnerabilities that can be exploited (man in the middle, spoofing, hacking, e.g., Herzberg & Jbara, 2008). Human biases (e.g., selecting the first, familiar networks) can also be exploited to mislead individuals to utilize the wrong wireless access points (Ferreira et al., 2013).

Co-creation: The team explored the wireless scenario in more detail, looking at current systems and the defaults that might lead the user to make insecure choices. Using the MINDSPACE framework, a number of potential nudges were identified, with the most promising of these listed in Table 1.

Table 1. Application of MINDSPACE influencers for nudge development

	Influencers	Description of possible nudges (for chosen scenario)
Criteria chosen	Messenger	Warning messages should come from a trusted provider not generic, perhaps from the university. Perhaps a celebrity should be used to deliver warning messages.
	Incentives	When connected to unsecure network hamper productivity by reminding people they are on an unsecured network (negative). Provide free printing to students using a secure network.
	Norms	Tell the user the % of people who lost/infected data within the company that have used that network. Tell the user of the % of people using the preferred network.
	Defaults	Present most secure as first option – order list by Security.
	Salience	Prompt 'Not a secure network' etc. Trusted network list produced by company.
	Affect	Use of emotive colors. Mark insecure networks as red.

Election of a nudge for development: Ideas were collated in a spread sheet and sent to each workshop participant a week later. Given time for reflection, participants could then elect their top three ideas. The research team also assessed which of the potential nudges were technically feasible.

***Nudge prototyping*:** Our final decision was to develop a prototype application that would change the presentation of wireless networks available to the user. We created a trusted network list, which would be managed by the chief security officer of a company in tandem with an application that would nudge users towards this 'white list' by changing the menu order of available wireless networks (change default list) and to color code the options available using colors with affective associations (red=danger, green=safe). This nudge was developed as a new app for the Android platform (see Turland et al., 2014 for technical details).

Evaluation: A laboratory-based evaluation was conducted to determine whether the application effectively improved security decisions. The two manipulations (menu order and color) were assessed independently and in combination in a study in 67 students were asked to connect to a wireless network The results of the nudge prototype suggested that color could be a very effective nudge (see Jeske et al., 2014 for a full description of the evaluation method and results).

Next steps: We believe the best way to solve cybersecurity issues is to research how and why people make decisions, and then design products, services and places to nudge people to make better decisions in the future. In addition, using this process over time and across various security scenarios, organizations can develop a stakeholder-informed and needs-based nudge decision model that provides them with a procedural framework for their independent and continuous improvement. We have presented the methodology to several SME's, who have previously asked for technical support as a result of a security breach, and are currently starting to utilize this process with these companies to help prevent further breaches.

3 Conclusion

The use of a framework based on behavioral change literature and in the area of cyber security is still relatively novel (see Pfleeger & Caputo, 2012; Siponen, 2000). The fact that our framework considers the importance of co-creation in the design of nudges acknowledges the role that users increasingly play in the security decision-making process. Another benefit of the model is that our framework is not context specific, which makes it more readily transferable to other settings. For instance, our approach can be used to evaluate if an interface is optimized to achieve the intended behavior. We therefore believe that this framework can make an important contribution to cybersecurity, HCI and awareness initiatives. In conclusion, we believe this methodology can help practitioners and academics to develop a strong evidence base for different interventions at the same time as achieving practical results for organizations.

Acknowledgements. This research is supported by EPSRC Grant EP/K006568 Choice Architecture for Information Security, part of the GCHQ/EPSRC Research Institute in Science of Cyber Security. We would also like to acknowledge the support of several colleagues from Computing Sciences at Newcastle University and the HCII reviewers for their suggestions.

References

1. NCSA (2012). 2012 NCSA / Symantec National Small Business Study. National Cyber Security Alliance, Symantec, JZ Analytics (October 2012)
2. Abraham, C., Michie, S.: A taxonomy of behavior change techniques used in interventions. Health Psychology 27(3), 379–387 (2008)
3. Ashford, W.: IT security awareness needs to be company-wide, says (ISC)^2 (2012), http://www.computerweekly.com/news/2240163342/IT-security-needs-to-be-company-wide-says-ISC
4. Blythe, J.M.: Cyber security in the workplace: Understanding and promoting behavior change. In: Proceedings of CHI Italy Doctoral Symposium, Trento, September 1-10 (2013)
5. Bulgurcu, B., Cavusoglu, H., Benbasat, I.: Information security policy compliance: A study of rationality-based beliefs of information security awareness. MIS Quarterly 34(3), 523–548 (2010)
6. Burns, S., Roberts, L.: Applying the Theory of Planned Behavior to predicting online safety behavior. Crime Prevention and Community Safety 15(1), 48–64 (2013)
7. Davinson, N., Sillence, E.: It won't happen to me: Promoting secure behavior among internet users. Computers in Human Behavior 26(6), 1739–1747 (2010)
8. Dolan, P., Hallsworth, M., Halpern, D., King, D., Metcalfe, R.: Influencing Behavior: The MINDSPACE way. Journal of Economic Psychology 33, 264–277 (2012)
9. Ferreira, A., Huynen, J.-L., Koenig, V., Lenzini, G., Rivas, S.: Socio-technical study on the effect of trust and context when choosing wifi names. In: Accorsi, R., Ranise, S. (eds.) STM 2013. LNCS, vol. 8203, pp. 131–143. Springer, Heidelberg (2013)
10. Fogg, B.J.: Persuasive Technology: Using computers to change what we think and do. Morgan Kaufman (2002)
11. Furman, S.M., Theofanos, M.F., Choong, Y.-Y., Stanton, B.: Basing Cyber security Training on User Perceptions. IEEE Security and Privacy, 40–49 (March/April 2012)
12. Furnell, S., Rajendran, A.: Understanding the influences on information security behavior. Computer Fraud & Security, 12–15 (March 2012)
13. Gilovich, T., Griffin, D., Kahneman, D.: Heuristics and Biases: The Psychology of Intuitive Judgement. Cambridge University Press (2002)
14. Hareli, S., Rafaeli, A.: Emotion cycles: On the social influence of emotion in organizations. Research in Organizational Behavior 28, 35–59 (2008)
15. Hayes, D.: Does the messenger matter? Candidate-media agenda convergence and its effect on voter issue salience. Political Research Quarterly 61, 134–146 (2008)
16. Herath, T., Rao, H.R.: Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems 47, 154–165 (2009)
17. Herzberg, A., Jbara, A.: Security and identification indicators for browsers against spoofing and phishing attacks. ACM Transactions on Internet Technology 8(4). Article 16, 36 (2008)

18. Ho, J.T., Dearman, D., Truong, K.N.: Improving users' security choices on home wireless networks. In: Symposium on Usable Privacy and Security, SOUPS (2010)
19. Jeske, D., Coventry, L., Briggs, P., van Moorsel, A.: Nudging whom how: IT proficiency, impulse control and secure behavior. Paper submitted to "Personalizing Behavior Change Technologies" Workshop, Toronto, Canada (April 27, 2014)
20. Johnson, E.J., Shu, S.B., Dellaert, B.G.D., et al.: Beyond nudges: Tools of a choice architecture. Marketing Letters 23, 487–504 (2012)
21. Kay, A.C., Wheeler, S.C., Bargh, J.A., Ross, L.: Material priming: The influence of mundane physical objects on situational construal and competitive behavioral choice. Organizational Behavior and Human Decision Processes 95(1), 83–96 (2004)
22. Lamy, D., Leber, A., Egeth, H.E.: Effects of task relevance and stimulus-driven salience in feature-search mode. Journal of Experimental Psychology: Human Perception and Performance 30(6), 1019–1031 (2004)
23. Leach, J.: Improving user security behavior. Computers & Security 22(8), 685–692 (2003)
24. Li, H., Sarathy, R., Xu, H.: The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. Decision Support Systems 51, 434–445 (2011)
25. Li, Y.: Theories in online information privacy research: A critical review and an integrated framework. Decision Support Systems 54, 471–481 (2012)
26. Liang, H.: Understanding security behaviors in personal computer usage: A threat avoidance perspective. Journal of the Association for Information Systems 11(7), 394–403 (2010)
27. Pfleeger, S.L., Caputo, D.D.: Leveraging behavioral science to mitigate cybersecurity risk. Computers & Security 31, 597–611 (2012)
28. Pwc. 2013 Information Security Breaches Survey. Survey conducted by pwc for UK government Business and Innovation Department (2013), http://www.pwc.co.uk/assets/pdf/cyber-security-2013-technical-report.pdf
29. Schneier, B.: Security Awareness Training. Schneier on Security (2013), https://www.schneier.com/blog/archives/2013/03/security_awaren_1.html (retrieved November 26, 2013)
30. Shore, L.M., Wayne, S.J.: Commitment and employee behavior: Comparison of affective commitment and continuance commitment with perceived organizational support. Journal of Applied Psychology 78(5), 774–780 (1993)
31. Siponen, M.T.: A conceptual foundation for organizational information security awareness. Information Management & Computer Security 8(1), 31–41 (2000)
32. Thaler, R.H., Sunstein, C.R.: Nudge. Improving Decisions About Health, Wealth and Happiness. Penguin (2008)
33. Turland, J., Jeske, D., Coventry, L., Briggs, P., Laing, C., van Moorsel, A., Yevseyeva, I.: Nudging secure wireless network. Developing an application for wireless network selection for android phones. Conference paper, Mobile HCI, Conference, Toronto (September 2014)