Using the IKEA Effect to Improve Information Security Policy Compliance

O. Olivos

ISC2 Peru Chapter
e-mail: olivosomar@gmail.com

Abstract

In this paper, we propose the use of the IKEA effect to develop a deeper sense of value and ownership of security policies so that employees appreciate them more and therefore comply with them. In order to achieve this, we propose that Bloom's Taxonomy be used to prepare the awareness sessions. The main emphasis should not be on the use of the Lower Order Thinking Skills (LOTS) but on the Higher Order Thinking Skills (HOTS). The main goal is for employees to be part of the 'creation' process of the security policies which will develop the IKEA effect in them. They get the chance to analyse the current policies, procedures and rules; evaluate, assess and criticize their relevance from their point of view and; through a negotiation process with the security officer adapt, devise and assemble 'new policies'. After this process, we find that employees not only have a more positive attitude towards following the security policies – they are not seen as an obstacle anymore – but also towards enforcing them as they feel that they are part of the creation of the policies, they take ownership of them and as a consequence value them more.

Keywords

IKEA effect, Bloom's Taxonomy, Security Policy Compliance, Behavioural Economics

1 Introduction

In order to achieve information security policy compliance, information security practitioners usually suggest that employees go through a security awareness program and that they take some kind of training related to it. The main goal of these programs is usually to make sure that employees know the policies, understand the risks and are able to apply some techniques to reduce these risks. However, we constantly see employees circumventing the policies even right after the training sessions (Beautement et al, 2009; Schlienger & Teufel, 2003; Blythe et al, 2013; Pfleeger et at, 2014; Kirlappos et al, 2014). This paper proposes that employees participate actively in policy development so that they value policies more, take ownership them and as a result improve compliance information security policy compliance. Therefore, we have to go beyond the simple knowing and understanding of the policies (LOTS). To achieve this, it is suggested to make use of the IKEA effect (Norton et al, 2012) by making employees part of the policy creation process.

2 The IKEA effect and Bloom's Taxonomy

The IKEA effect has been defined as the increased valuation that people have for self-assembled products compared to objectively similar products which they did not assemble. The experiments suggest that when people imbue products with their own labour, their effort can increase their valuation. The authors also state that successful completion is an essential component for the link between labour and liking to emerge. (Norton et al, 2012). Previous research demonstrates that people prefer goods with which they have been endowed. (Kahneman et al., 1990). This concept, the IKEA effect, can also apply to ideas and points of view. Some researchers state that once we take ownership of an idea, we prize it more than it is worth. And most frequently, we have trouble letting go of it because we cannot stand the idea of its loss (Ariely, 2008). Paraphrasing Norton et al, we would confirm the IKEA effect – employees' increased valuation for security policies that they helped assemble when compared to objectively similar policies not written by the self – by comparing employees' willingness to follow and enforce the policies that they had helped assemble to identical policies created by others. (Based on Norton et al, 2012)

It is important to distinguish the IKEA effect from the endowment effect. Regarding the latter, this bias occurs when people overvalue something that they own, regardless of its objective market value (Kahneman et al., 1991). In other words, people place a greater value on things once they have established ownership. The IKEA effect appears as a result for effort and the positive feelings that accompany successful completion of tasks, not the mere ownership. (Norton et al, 2012; Ariely, 2008). However, the IKEA effect can also be reinforced by the endowment effect (Yates and Hattie, 2013).

Bloom's taxonomy is possibly one of the most cited and widely used models of human cognitive processes. The original taxonomy was developed by Bloom et al in 1956 and remained in use more or less unchanged until recently. A revised version of the taxonomy was published in Anderson et al in 2001. This revised taxonomy has become accepted as more appropriate in terms of current educational thinking (Krathwohl, 2002). In this paper, the focus will be on the revised taxonomy.

The following is a brief explanation of each of the six levels (Krathwohl, 2002)

- **Remember** – Retrieving relevant knowledge from long-term memory
- **Understand** – Determining the meaning of instructional messages, including oral, written, and graphic communication.
- **Apply** – Carrying out or using a procedure in a given situation.
- **Analyse** – Breaking material into its constituent parts and detecting how the parts relate to one another and to an overall structure or purpose.
- **Evaluate** – Making judgments based on criteria and standards.

- **Create** – Putting elements together to form a novel, coherent whole or make an original product.

The bottom levels of the pyramid are considered Lower Level Thinking Skills (LOTS) and the ones closer to the top are considered Higher Order Thinking Skills (HOTS).

Bloom's taxonomy has been used by other researches as a way to actively engage students and to arouse their interest in information security. (Yuan et al, 2010; Yuan et al, 2010b; Nkhoma et al, 2016). It has also been suggested that information security educational programs would be more effective if they adhered to pedagogical principles like Bloom's taxonomy (Van Niekerk & Von Solms, 2008; Olivos 2012). However, in this paper it is argued that it can also be used to develop the IKEA effect in employees regarding security policies which will in turn improve compliance.

3 Information Security Policy Compliance

There is evidence that even when employees know the policies, procedures and rules they will still not comply because these security policies are seen as an obstacle to fulfill their main task. (Beautement et al, 2009) or because it conflicts with their beliefs and values (Schlienger & Teufel, 2003). Most of the time, employees do not intend to cause harm but circumvent the policies as a way to achieve their job activities and organizational goals (Blythe et al, 2013; Pfleeger et at, 2014). There are also situations where security-conscious employees create a more fitting alternative to the policies and mechanisms created by the organization's security staff. The authors called it shadow security (Kirlappos et al, 2014). This is why we believe that the typical training and awareness programs that only make use of the LOTS (Figure 1) are ineffective. These programs usually focus on providing knowledge, making sure that employees understand the importance of the policies and providing best practices and tips that employees can apply. But as it has been stated, it does not guarantee that employees will comply.

It is therefore important to also ensure that the users have the correct attitude, and thus the desired behaviour, towards information security (Van Niekerk & Von Solms, 2006; Kruger et al, 2006). We believe that the IKEA effect can help us achieve this because as has been stated by other authors, the effort we put into something does not just change the object – in this case the security policies –. It changes the way we evaluate that object and how important it becomes to us (Kahneman et al, 1991; Kruger et al 2004). It can also be reinforced by the endowment effect (Kahneman et al, 1990; Yates and Hattie, 2013) which is an illustration of the status quo bias and can be explained by loss aversion (Kahneman et al, 1991).

Pierce et al, 2003, emphasize the concept of psychological ownership (or subjective ownership) as the state in which individuals feel an object as theirs and then propose three major mechanisms through which psychological ownership emerges:

- Controlling the ownership target (object)
- Coming to know the target intimately, and
- Investing the self into the target. (Pierce et al, 2003).

Regarding the latter, the authors argue that "we are likely to feel that we own that which we create, shape, or produce" because through our labor, we not only invest our time and physical effort but also our psychic energy into the product of that labor. The stronger this feeling of psychological ownership is, the higher one's appraisal of an object's value will be (Franke et al, 2010). This is the feeling that should be developed in employees regarding information security policies. Then they will not see the policies as externally imposed but as something they own and they value and that is worth following and even enforce.

Initially the IKEA effect was described for activities in which consumers had to physically assemble or build some products (Norton et al, 2012). However, a similar effect had already been described by other authors and that it could also apply to ideas. Whether the thing created is a material object or an abstract thought, the creator retains an identity in the object for as long as it retains a mark or some other association with the person who brought it into existence. (Belk, 1988; Belk and Coon, 1993). Other researchers have also found that customer participation has a positive impact on satisfaction and behavioural intentions and that they find themselves psychologically tied to the service as a result of their participation at the specification stage (Strauss et al, 2016). In this paper, it is suggested that the employee's participation should not only be during the specification stage but specially during the design/creation stage because simply working on a project, contributing to it without seeing it through to closure, does not appear to produce the effect at all (Norton et al, 2012). "The IKEA effect appears to be entirely the result of investing energy to complete a worthwhile project and then being able to stand back and admire its successful outcome." (Yates and Hattie, 2013)

Other researchers have also pointed out that in an organizational context participating in decision making has a positive effect on satisfaction with the decision making process as well as with the decision itself (Driscoll, 1978). Therefore these same principles – IKEA effect – can also apply to jobs for employees and not just to consumers. (Norton et al, 2012)

Regarding information security compliance, some authors have asserted that employee involvement in the development of information security policy is critical, given that 'involvement' is a foundational social control. (Hsu et at, 2015). There is also evidence that where employees are encouraged to make local decisions and voice their opinions within the organization, they are more likely to comply with security policies and procedures. Excluding employees from the conversation around security encourages non-compliance (Becker et al, 2017).

4 Developing the IKEA effect

To achieve this, we suggest that more emphasis is put on the higher order thinking skills: analyze, evaluate and create. We present some activities that could help us develop the IKEA effect.

1. **Analyze** – Breaking material into its constituent parts and detecting how the parts relate to one another and to an overall structure or purpose.

    - Have employees **compare** the different versions of the policies. They may notice that the security policy document that they got by email is not exactly the same as the one published on the organization's intranet or the printed version.

    - **Classify** some of the rules as not possible to be applied in real situations.

    - Get employees to **debate** if the same rules/procedures/policies should apply to all departments/branches of the organization.

    - Employees **analyze** if the policies/procedures can actually be applied during the different seasons when there are different demands.

    - Have employees **point out** inconsistencies in the policies.

    - Get employees to **explain** why they think some procedures are a barrier to their productivity.

2. **Evaluate** – Making judgments based on criteria and standards.

    - Encourage them to **critique** the security policies, they may provide a point of view that you never took into account.

    - Employees **judge** the policies by providing examples of situations when the rules and policies make no sense and just cannot be applied.

    - Have them **assess** the policies. They may find two policies/procedures that seem to contradict each other.

    - Encourage employees to **recommend** better ways of enforcing the policies.

3. **Create** – Putting elements together to form a novel, coherent whole or make an original product.

    - Some employees may even be able to **design** better flyers than the ones you have or they may come up with more catchy phrases to use.

- **Compose** new slogans.
- **Modify** parts of the policies where employees suggest a better wording for different parts of the policies or suggest the use of a different word because -even if it is the same language- a particular word has a different connotation in another country
- **Produce** shorter versions of the documents
- Employees may **rewrite** part of the documents because they correct some grammar mistakes you may have made while writing the policies or procedures
- **Adapt** the wording to a particular office branch.
- **Role-play** situation where it is difficult or even illogical to follow the set rules.
- Encourage employees to **formulate** alternative solutions.

During these activities the Information Security Officer should be receptive to the proposals, explain carefully when changes cannot be made (due to legal restrictions) and be open to negotiation. It is important to take all comments into account. As has been pointed out, simply working on a project - contributing to it without seeing it through to closure- does not appear to produce the IKEA effect at all. This process may be difficult as the officer may be affected by the endowment and IKEA effects himself.

5 Conclusions and the future

This paper suggested that information security awareness, training and/or educational programs can be more effective if higher emphasis is placed in the use of higher order thinking skills. Especially if the activities make employees part of the 'creation' process of the security policies. This process will develop the IKEA effect in employees which can be reinforced by the endowment effect. As a result, employees will take ownership of the policies and rules, will value them more and will be more willing to comply with them compared to policies and rules imposed by the organisation.

The primary weakness of this paper is the lack of empirical evidence to support the suggested use of the IKEA effect to ideas to improve information security policy compliance. However, multiple studies in the area of Behavioural Economics have demonstrated that labour leads to love and that the IKEA effect appears when customers (employees) put effort into developing a product (security policies) and see it through completion. Another issue to consider is how scalable it is and if it can realistically be applied in large organizations. We also need to consider if Information

security practitioners have the soft skills necessary to conduct this process and are open to criticism by non-security experts.

6 References

Anderson, L. W., Krathwohl, D. R., Airasian, P. W., Cruikshank, K. A., Mayer, R. E., Pintrich, P. R., & Wittrock, M. C. (2001), "A taxonomy for learning, teaching, and assessing: A revision of Bloom's taxonomy of educational objectives", White Plains, NY: Longman.

Ariely, D. (2008), "Predictably irrational", New York: HarperCollins.

Beautement, A., Sasse, M. A., & Wonham, M. (2009, August), "The compliance budget: managing security behaviour in organisations", *In Proceedings of the 2008 New Security Paradigms Workshop* (pp. 47-58), ACM.

Becker, I., Parkin, S., & Sasse, M. A. (2017), "Finding security champions in blends of organisational culture", *Proc. USEC*, 11.

Belk, R. W. (1988), "Possessions and the extended self", *Journal of consumer research*, 15(2), 139-168.

Belk, R. W., & Coon, G. S. (1993), "Gift giving as agapic love: An alternative to the exchange paradigm based on dating experiences", *Journal of consumer research*, 20(3), 393-417.

Bloom, B. S., Englehart, M. D., Furst, E. J., Hill, W. H., & Krathwohl, D. R. (1956), "Taxonomy of educational objectives: Handbook I. Cognitive domain", New York: David McKay.

Blythe, J., Koppel, R., & Smith, S. W. (2013), "Circumvention of security: Good users do bad things", *IEEE Security & Privacy*, 11(5), 80-83.

Driscoll, J. W. (1978), "Trust and participation in organizational decision making as predictors of satisfaction", *Academy of management journal*, 21(1), 44-56.

Franke, N., Schreier, M., & Kaiser, U. (2010), "The 'I designed it myself' effect in mass customization", *Management science*, 56(1), 125-140.

Hsu, J. S. C., Shih, S. P., Hung, Y. W., & Lowry, P. B. (2015), "The role of extra-role behaviors and social controls in information security policy effectiveness", *Information Systems Research*, 26(2), 282-300.

Kahneman, D., Knetsch, J. L., & Thaler, R. H. (1990), "Experimental tests of the endowment effect and the Coase theorem", *Journal of political Economy*, 98(6), 1325-1348.

Kahneman, D., Knetsch, J., & Thaler, R. (1991), "Anomalies: The endowment effect, loss aversion, and status quo bias", *Journal of Economic Perspectives*, 5(1), 193-206.

Kirlappos, I., Parkin, S., & Sasse, M. A. (2015), "Shadow security as a tool for the learning organization", *ACM SIGCAS Computers and Society*, 45(1), 29-37.

Krathwohl, D. R. (2002), "A revision of Bloom's taxonomy: An overview. Theory into practice", 41(4), 212-218.

Kruger, J., Wirtz, D., Van Boven, L., & Altermatt, T. W. (2004), "The effort heuristic". *Journal of Experimental Social Psychology*, 40(1), 91-98.

Kruger HA., Drevin, L., Steyn, T. (2006), "A framework for evaluating ICT security awareness". *Proceedings of the 2006 Information Security South Africa Conference*, Sandton, South Africa.

Nkhoma, M., Lam, T., Richardson, J., Kam, B., & Lau, K. H. (2016), "Developing case-based learning activities based on the revised Bloom's Taxonomy", *In InSITE 2016: Informing Science and IT Education Conferences* (pp. 85-93), Informing Science Institute.

Norton, M., Mochon, D., and Ariely, D., "The IKEA Effect: When Labor Leads to Love", *Journal of Consumer Psychology* 22, no. 3 (July 2012): 453–460.

Olivos, O. (2012), "Creating a security culture development plan and a case study", *Proceedings of the sixth international symposium on Human Aspects of Information Security & Assurance HAISA 2012*, Greece.

Pfleeger, S. L., Sasse, M. A., & Furnham, A. (2014), "From weakest link to security hero: Transforming staff security behaviour", *Journal of Homeland Security and Emergency Management*, 11(4), 489-510.

Pierce, J. L., Kostova, T., & Dirks, K. T. (2003), "The state of psychological ownership: Integrating and extending a century of research", *Review of general psychology*, 7(1), 84.

Schlienger, T., Teufel, S. (2003), "Information Security Culture – from Analysis to Change", *Proceedings of the 3rd Annual Information Security South Africa Conference*, Sandton, South Africa.

Straus, L., Robbert, T., & Roth, S. (2016), "Customer Participation in the Customization of Services–Effects on Satisfaction and Behavioral Intentions", *Journal of Business Market Management*, 9(1), 498-517.

Van Niekerk, J., Von Solms, R. (2006), "Understanding information security culture: A conceptual framework", *Information Security South Africa (ISSA)*, Johannesburg, South Africa.

Van Niekerk, J., Von Solms, R. (2008), "Bloom's taxonomy for information security education", *Information Security South Africa (ISSA)*, Johannesburg, South Africa.

Yates, G. C., & Hattie, J. (2013), "Visible learning and the science of how we learn", Routledge.

Yuan, X., Jiang, K., Murthy, S., Jones, J., & Yu, H. (2010), "Teaching security management with case studies: experiences and evaluation", *Journal on Education, Informatics and Cybernetics (JEIC)*, 2(2), 25-30.

Yuan, X., Murthy, S., Xu, J., & Yu, H. (2010, October), "Case studies for teaching physical security and security policy", *In 2010 Information Security Curriculum Development Conference* (pp. 21-26). ACM.