Poster: Designing a Persuasive Application to Improve Organizational Information Security Policy Awareness, Attitudes and Behavior

Marc Busch[1], Peter Wolkerstorfer[1], Christina Hochleitner[1], Georg Regal[1], Manfred Tscheligi[1,2]

[1]AIT – Austrian Institute of Technology GmbH
Modecenterstrasse 17/Objekt 2
1110 Vienna, Austria
FirstName.LastName@ait.ac.at

[2]University of Salzburg
Sigmund-Haffner-Gasse 18
5020 Salzburg, Austria
manfred.tscheligi@sbg.ac.at

1. INTRODUCTION

Employees in organizations frequently violate information security policies. According to a survey by PWC [8], 93% of large and 87% of small organizations had a breach in information security in 2013; 36% of the security breaches are caused by the organizations' employees. Approaches to increase information security policy compliance, such as access control management systems patronize users and may provoke resistance or negative attitudes towards organizational information security. Other approaches (such as trainings and awareness programs) have an influence on awareness and attitudes, but are obtrusive, time-consuming, and expensive and must be administered several times to have a long-term effect.

To overcome these limitations of classical measures, we designed an application to increase information security policy compliance by promoting awareness, positive attitudes and behavior regarding information security by using persuasive strategies. Persuasive strategies have been used only rarely in the field of information security [7] and not in a focused way to increase information security policy compliance.

2. DESIGN OF THE APPLICATION

2.1 Theoretical Background

The design of the application relies on three scientific foundations for understanding and changing human attitudes and behavior: First, on the *Theory of Reasoned Action (TRA)* [3]. This theory states that an actual behavior is influenced by an intention to perform that behavior, which is in return influenced by the attitude towards that behavior and the belief what others might think about that behavior. An advancement of *TRA* is the *Theory of Planned Behavior (TPB)* [1]. *TPB* adds perceived behavioral control as a direct influence on the intention to perform a behavior and the behavior itself. Second, we rely on the design rationale of a recent meta-study of important factors for predicting information security policy compliance [6]. This study confirmed (according to *TRA* and *TPB*) that attitudes, perceived behavioral control and subjective norms – as well as awareness – are among of the most important factors for determining compliance towards organizational information security. Third, we use the framework of persuasive strategies collected by [5]. Persuasive strategies are strategies that aim at changing human attitudes and behaviors and therefore build on *TRA* and *TPB*. From these strategies, two HCISec experts chose 8 that seemed most promising in the field of organizational information security: *Rewards*, *personalization*, *social comparison*, *suggestions*, *self-monitoring*, *cooperation*, *competition* and *simulation*.

2.2 Persuasive Elements

A medium-fidelity prototype of the application was designed for Android tablets. The main goal of the application is an increase of information security policy compliance by increasing awareness for information security and by changing employees' attitudes and behavior regarding information security in a more positive way. The application has 7 main features/tabs: "Login", "My Security Policies", "Security Points", "Personalization, "Security Quiz", "Challenges" and "Statistics" (see Figure 1 – left side). As basic functionalities (without intended persuasive effect) users can "Login" and see which security policies apply to him/her ("My Security Policies"). We now describe how the persuasive strategies are integrated into the application. See Figure 1 for a screenshot of the application.

Persuasive strategy *rewards:* Virtual "Security Points" can be collected in the application. The users can earn security points by taking a "Security Quiz", by committing and succeeding at special "Challenges" and by filling in the "Personalisation" questionnaire. However, they can also loose security points by causing incidents in information security (e.g. data loss as a consequence of insecure document handling). Depending on the number of security points, users get so-called *Security Badges* (Beginner, Intermediate, Expert, Professional, Master) – see lower left corner in Figure 1.

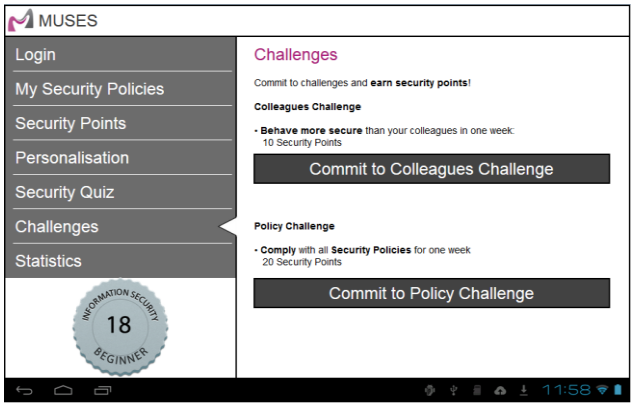

Figure 1. Low-fidelity prototype of the tablet application (with the tab "Challenges" opened)

Persuasive strategy *personalization*: To let users *personalize* the application, they can fill in a questionnaire, which determines their persuadability for each of the implemented strategies (*rewards, personalization, social comparison, suggestions, self-monitoring, cooperation, competition and simulation*). Persuadability is the individual susceptibility to persuasive strategies and builds on the work of [4], which was extended by [2]. The questionnaire builds on a list of statements related to the persuasive strategies (e.g. "*I like to compete against others"* related to the strategy *competition*), which have to be rated on a likert-scale. Based on the results of the persuadability questionnaire, the application makes personalized *suggestions* for specific activities, e.g. to look at the "Statistics" of co-workers when the user is especially susceptible to the persuasive strategy *social comparison.* This ensures that the persuasive approach will not be the same for all employees, but tailored to individual differences in persuadability, which makes it more effective.

Persuasive strategies *social comparison/self-monitoring:* The *social comparison* and *self-monitoring* is integrated in the "Statistics" tab of the application and shows the number of security policy violations per week for the single employee as well as for the average employee (see Figure 2 for an example). The employee is presented her/his security compliance history in a visualized way and can compare her-/himself with other employees.

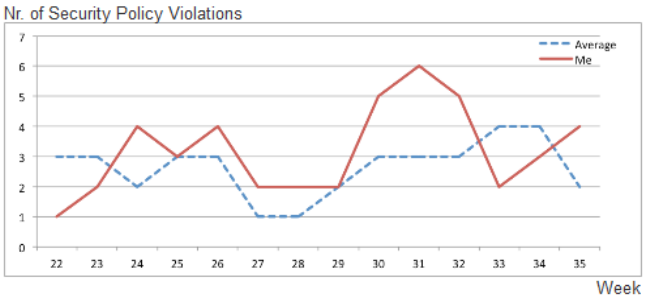

Figure 2. An example for security policy statistics, which compares individual employees to the average employee

Persuasive strategies *cooperation/competition*: Cooperation and *competition* is facilitated through "Challenges" (see again Figure 1). Users can commit to specific challenges that are either competitive (e.g. "Behave more secure than your colleagues for one week") or cooperative (e.g. "Build a team of three colleagues and comply with all security policies for one week"). Users can earn security points by fulfilling these challenges either alone or in a team.

Persuasive strategy *simulation:* This is integrated into the risk communication outside the main application. When a user acts on a primary task (e.g. user wants to open a document) and an information security breach is about to happen (e.g. user wants to open a sensitive document within an un-secured network), the application simulates what will happen to the user's security points if he continues with his action and a security incident is caused by her/his behavior (e.g. loss of document). A pop-up (see Figure 3) simulates the consequences for the user. The user is then self-responsive and can either decide to select ("I Still Want to Continue") or to "Cancel" the action.

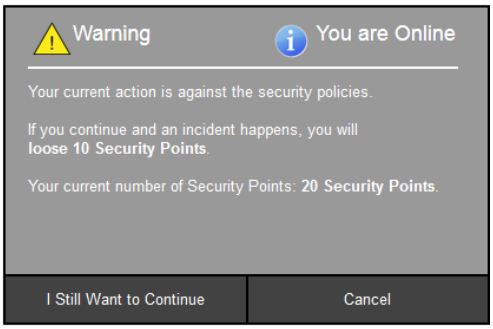

Figure 3. Risk-communication when an information security breach is about to happen (pop-up)

3. SUMMARY AND CONCLUSION

We have presented the design of a prototypical application that integrates persuasive strategies to increase organizational information security policy compliance by improving attitudes and behaviour and by raising awareness. These persuasive strategies rely on theories on how to change attitudes and behaviour (*TRA* and *TPB*). We believe that through the combination of the persuasive strategies the application will engage and motivate employees in information security.

4. ACKNOWLEDGEMENTS

This work was partially funded by the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement 318508 (MUSES – Multiplatform Usable Endpoint Security).

5. REFERENCES

1. Ajzen, I. The theory of planned behavior. *Organizational Behavior and Human Decision Processes 50*, 2 (1991), 179–211.
2. Busch, M., Schrammel, J., and Tscheligi, M. Personalized Persuasive Technology – Development and Validation of Scales for Measuring Persuadability. In *Persuasive Technology*. Springer Berlin Heidelberg, 2013, 33–38.
3. Fishbein, M. and Ajzen, I. Belief, attitude, intention and behavior: an introduction to theory and research. (1975).
4. Kaptein, M.C. Personalized persuasion in Ambient Intelligence. *Journal of Ambient Intelligence and Smart Environments*, (2012).
5. Oinas-Kukkonen, H. and Harjumaa, M. A systematic framework for designing and evaluating persuasive systems. *Persuasive Technology*, (2008).
6. Sommestad, T., Hallberg, J., Lundholm, K., and Bengtsson, J. Variables influencing information security policy compliance: A systematic review of quantitative studies. *Information Management & Computer Security 22*, 1 (2014), 42–75.
7. Yeo, A., Rahim, M., and Ren, Y. Use of Persuasive technology to change end user's IT security aware behavior: a pilot study. *International Journal of Human and Social Sciences*, (2009), 673–679.
8. http://www.pwc.co.uk/assets/pdf/cyber-security-2013-exec-summary.pdf