Empowering Information Security Managers: tailored information security policy design with POLCO software

Elham Rostami
CERIS, Informatics, Örebro University
Örebro, Sweden elham.rostami@oru.se

Abstract

Information security is crucial for protecting an organization's information assets, and information security policies (ISPs) are formal controls that provide guidance in this regard. However, employees' non-compliance with ISPs is a persistent issue, and the design of ISPs can contribute to this problem. Tailored ISP design theory, which includes four design principles and a conceptual model, offers a solution by allowing information security managers to create ISPs that are relevant for different groups of employees. This research introduces POLCO, a software developed based on tailored ISP design theory, to systematically tailor ISPs. The evaluation of functionality of POLCO as a proof of concept was conducted with master students in an information security management program, and the results showed that POLCO fulfils the design principles, making it a potential tool for reducing employee non-compliance with ISPs.

Keywords: policy component, tailored ISP design theory, POLCO

1. Introduction

Information security is paramount in safeguarding an organization's information assets, and relying solely on technical solutions is inadequate. Information security policies (ISPs), as crucial formal controls, are instrumental in safeguarding an organization's information assets. [1]. Hence, it is imperative that employees not only read ISPs but also comply with them. However, non-compliance with ISPs among employees persists as a persistent issue [2]. [3] has argued that ISP non-compliance may stem from two sources: employee behaviour and ISP design. As such, employees should not be solely blamed for non-compliance, as the design of ISPs can also pose challenges to compliance. ISPs can be cumbersome and demotivating, making the design of high-quality ISPs that facilitate informed decision-making critical. One approach to improving ISP quality is the design of tailored ISPs, for different employee groups based on their needs. However, designing such tailored ISPs presents challenges for information security managers and may add to their workload. Therefore, there is a pressing need to provide support to information security managers in the design of tailored ISPs. Despite this need, current research lacks comprehensive guidelines for information security managers on how to design tailored ISPs, with the few available guidelines offering manual support. One exception is tailored ISP design theory [3] that provide a set of design principles and a conceptual model to develop a software to design tailored ISPs. Applying tailored ISP design theory, this research, introduce a software called POLCO for information security managers to systematically tailor ISPs. This software has the potential to enhance the relevance of ISPs for employees, and consequently, may prove effective in mitigating non-compliant behaviours among employees. Furthermore, the software facilitates the provision of support to information security managers, thereby enabling efficient ISP management.

2. Related Research

Despite existing literature on ISP management, research on software to aid in this type of management is limited. Some of the existing software tools include features such as monitoring and measuring employees' compliance with ISP [4], or automated control of employees' awareness of ISPs [5]. Some tools [e.g., 6] also provide tailoring approaches by selecting relevant controls based on an organization's information security

requirements. However, the extent of tailoring to different target groups or individual employees' work situations is unclear in these cases. Overall, there is a scarcity of research on software for ISP management and further investigation into tailored ISP management tools is needed.

3. Tailored ISP Design Theory

Tailored ISP design theory [3] consists of four design principles (DP) and a conceptual model. The design principles are: DP1) Use internally consistent and coherent ISP modules because they enable a systematic decomposition of the ISP content, DP2) Use self-contained ISP modules because they are free-standing and reusable across multiple ISPs, DP3) Store ISP modules in a repository, because it makes them retrievable for reuse across multiple tailored ISPs, and DP4) Select ISP modules based on work tasks and assemble them to a tailored ISP because work tasks differ between roles and are means for tailoring. The design principles refer to the ISP module, which has been proposed as a conceptual model known as the "policy component model." This model encompasses a collection of Unified Modelling Language classes that represent various concepts: actor, role, information security policy, policy component, policy statement (actionable advice, educational content, general content), consequence, concept, goal, supplementary source, and structure. The classes are associated with each other through several named associations.

4. Research Method

The aim of developing the POLCO software was to solve a practical problem: the lack of effective tools that support information security managers' tailoring ISPs to different target groups in an organisation. Employing design science research process model by [7] with the third entry point (Design & Development Centered Initiation), POLCO was created using Visual Studio, C#, HTML, CSS, JavaScript, and Microsoft SQL Server, grounded in tailored ISP design theory. POLCO represents the initial version of the software, with emphasis placed on adhering to the design principles. These principles were operationalized into design goals, including the ability for users to: a) create self-contained policy components, b) save policy components, c) develop tailored ISPs utilizing policy components, and d) reuse policy components in different tailored ISPs. Throughout the design and development process, a database containing 159 ISPs from public agencies in Sweden was utilized as test data, enabling continuous testing and refinement of the software.

The functionality of POLCO as a proof of concept, was evaluated by master students in Information security management program, at Örebro university, Sweden. Evaluating the functionality of POLCO as a proof of concept was needed, in this stage. According to Nunamaker and Briggs [8] studies that focus on evaluating the proof of concept can produce valuable insights about possible solutions to important practical problems. They also added that this type of studies is done at the universities, typically with student subjects. This point is more valid, when we know that as the very first version of the software, design flaws are expected, which makes it unsuitable to test the software as a proof of value or proof of use (e.g., in an organization)

Thus, two groups, each consisted of 3 students re-designed an existing monolithic ISP to tailored ISPs using POLCO. When the evaluation was done, students were interviewed separately through a Zoom meeting to understand if POLCO fulfils the design principles. Each interview took approximately one hour. First students presented their tailored ISPs for each target group that they identified in the monolithic ISP. Then, I asked them questions related to the design goals. The questions were: 1) could you develop a self-contained ISP component? 2) could you save the developed ISP in POLCO? 3) could you develop a tailored ISP by using the policy component? and 4) could you re-use policy components in different tailored ISPs? During the interview, students had the opportunity to provide their suggestions in relation to each question. The interview sessions were video recorded. I analysed the students interview by identifying problems and suggestions expressed by the students and associated them with the design principles. Part of the result

of analysis is presented in Section 6.

5. POLCO

This section describes POLCO briefly. Fig. 1 shows the interface with the functionality to add and remove policy components to a tailored ISP. The interface is vertically divided into two sections. The left section contains a menu to access the main functionality, and the right section contains the information security manager's work area. Consequently, the content of this area changes depending on the menu selection. The functionality for adding or removing a policy component is shown in Fig. 1. The main menu items are Policy, Policy Component, Role, and Actor. Each of these menu items has sub-items, making it possible to work with content such as creating new policy components (see (1) in Fig. 1), and accessing, editing, and removing existing policy components (see (2) in Fig.1.)

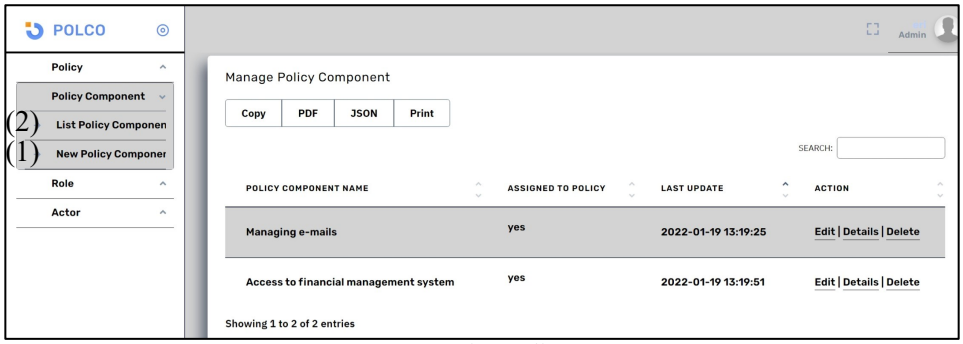

Fig. 1. Managing policy components

The development of a tailored ISP in POLCO entails the following procedural steps. Firstly, a new policy component is generated for a specific task and stored in the software. Next, a tailored ISP is created and saved, serving as a designated container for policy components. Subsequently, information security managers can populate the tailored ISP with pertinent policy components. Lastly, the assignment of each tailored ISP to a role, responsible for executing designated tasks, is undertaken. One notable advantage of POLCO is its flexibility in accommodating user preferences, enabling the execution of the aforementioned steps in varying orders.

6. Evaluation

In this section, I present lesson learned from evaluating POLCO by students. As discussed in the Research Method section, my intention was to develop a software that fulfils the design goals. Therefore, the evaluation below is structured using these goals.

Design goal 1- Creating self-contained policy component using POLCO. Students in both groups said that they could develop policy components using the software. Students in group 1 said: "*Generally, it was very simple and smooth creating policy component.*" Although developing the policy component in POLCO was doable and easy, students in group 2 said that for some policy components they faced some challenges, since the original ISP that they received was not very well-designed. For example, they couldn't find different roles easily. Thus, this problem was not related to the software as such.

Design goal 2 - Saving the policy component in POLCO. After creating the policy component, students could save it in POLCO. However, they found some issues. One of the concerns was about the ability to save multiple policy components with identical names in POLCO. In relation to that Group 1 said: "*POLCO lets you to create policy components (and tailored policies) with the same name. But you should not be able to do that.*" To address this issue, students suggested having a warning system that alerts users when they attempt to save a policy component with a name that already exists in the system, or when they try to save a name for a policy component that is already taken.

Design goal 3 - Developing a tailored ISP by using a policy component. Students said that they were able to develop tailored ISPs by using the policy components that they developed and saved, however they faced some challenges. One of the challenges was related to the lack of traceability in POLCO. Group 2 students mentioned that they faced

difficulties in identifying which policy component was assigned to a specific tailored ISP. Similarly, Group 1 students noted that there was no confirmation message when a policy component was added to a tailored ISP. To address this issue, Group 1 suggested the implementation of a graph that visually represents the current state of tailored ISPs and policy components.

Design goal 4 - Re-using policy components in different tailored ISPs. The analysis of student feedback revealed that students from both Group 1 and Group 2 confirmed that it is possible to assign one policy component to different tailored ISPs in POLCO. However, Group 2 students identified an issue where POLCO allowed users to add the same policy component multiple times to the same tailored ISP. This duplication of policy components in tailored ISPs was recognized as a difficulty by the students. To address this issue, Group 2 students suggested implementing a solution that prevents users from adding the same policy component to a tailored ISP more than once.

7. Discussion and conclusion

POLCO is the first software that is built based on tailored ISP design theory and as an artefactual contribution [9] has several implications for research and practice. In research, it allows researchers to investigate the extent to which this type of software can support information security managers and impact their workload. For example, the time and effort put into designing and updating ISPs can be investigated compared to previous ways of working. POLCO can also be used as a future research tool to explore whether tailored ISPs designed by this software are more accessible to employees. This type of research are in line with previous research that assert accessibility of ISPs has impact on employee's ISP compliance behaviour [10]. Naturally, as the initial iteration of POLCO, further refinement is warranted considering feedback from students. Nonetheless, a more advanced version of POLCO has the potential to be implemented within organizational for the purpose of designing tailored ISPs or re-design available ISPs to suit diverse employee group's needs.

One of the limitations of this research is that POLCO has been evaluated as a proof of concept. Practitioners and researchers should be aware that the need for further validation might reveal additional design limitations by evaluating proof of value and proof of use when information security managers use POLCO to tailor ISPs.

References

1. Whitman, M., *Security policy: From design to maintenance. In Information security: Policy, processes, and practices (Straub DW, Goodman SE and Baskerville R, Eds), pp 123–151, M. E. Sharpe, New York.* 2008.
2. Chowdhury, N.H., M.T. Adam, and G. Skinner, *The impact of time pressure on cybersecurity behaviour: a systematic literature review.* Behaviour & Information Technology, 2019. **38**(12): p. 1290-1308.
3. Rostami, E., *Tailoring information security policies–a computerized tool and a design theory*, 2023, Örebro universitet.
4. Alotaibi, M.J., S. Furnell, and N. Clarke, *A framework for reporting and dealing with end-user security policy compliance.* Information & Computer Security, 2019.
5. Brunner, M., C. Sillaber, and R. Breu. *Towards automation in information security management systems*. in *2017 IEEE International Conference on Software Quality, Reliability and Security (QRS)*. 2017. IEEE.
6. Coertze, J. and R. von Solms, *A software gateway to affordable and effective Information Security Governance in SMMEs. In 2013 Information Security for South Africa (pp. 1-8). IEEE.* 2013.
7. Peffers, K., et al., *A design science research methodology for information systems research.* . Journal of Management Information Systems, 24, 45-77., 2007.
8. Nunamaker, J., Jay F and R.O. Briggs, *Toward a broader vision for information systems.* ACM Transactions on Management Information Systems (TMIS), 2012. **2**(4): p. 1-12.
9. Ågerfalk, P.J. and F. Karlsson, *Artefactual and empirical contributions in information systems research.* 2020.
10. Weidman, J. and J. Grossklags, *What's in your policy? An analysis of the current state of information security policies in academic institutions.* 2018.