Enhancing information security awareness programs through collaborative learning

Adam P. Filippidis[1], Thomas Lagkas[1], Haralambos Mouratidis[2], Sokratis Nifakos[3], Elisavet Grigoriou[4], Panagiotis Sarigiannidis[5]

[1] Department of Computer Science, International Hellenic University, Kavala Campus, Greece

[2] Massive Dynamic Sweden

[3] Department of Computer and Systems Sciences, Stockholm University, Sweden

[4] Sidroco Holdings Ltd., Nicosia, Cyprus

[5] Department of Electrical and Computer Engineering, University of Western Macedonia, Kozani, Greece

adamfilippidis@gmail.com
tlagkas@cs.ihu.gr
haralambos@dsv.su.se
sokratis@massivedynamic.se
egrigoriou@sidroco.com
psarigiannidis@uowm.gr

Abstract: Information security attacks targeting human nature, such as phishing, are rising rapidly. Information security Awareness (ISA) programs have been proven to be valuable proactive measures that increase Return On Investment (ROI) regarding information security enhancement. These programs tend to focus on concepts and technical aspects. Although these customary instruction methodologies have their preferences, trainees can additionally take advantage of educational techniques that are more intuitive and situation driven. This study aims to increase the efficiency of learning in such programmes by using design science to create an artefact for learning and then testing the acquired knowledge. Design science will be used as a research method. The creative method, a brainstorming technique, and five steps in design science are performed: explicate the problem, define requirements, design and develop artefact, demonstrate artefact, and evaluate artefact to develop a process framework to respond to this problem. The problem is explicated with a literature review and the requirements to be met by Game-Based Learning (GBL) are set. The first artefact, which is an interactive book support quizzes, crossword puzzles, multimedia such as video, and "complete the word" simple games that enhance the learning process. The second artefact is a printed board game with hackers and cards with the goal to support the learning process and assess the ability of the participants to respond and take actions based on this new knowledge. At last, limitations that exist in security education such as lack of user-centered modules and limited guidelines from learning theories are elaborated and future work is also presented.

Keywords: Information security awareness, security assessment, computer security, Game-Based Learning, Collaborative Learning, Serious Games, Multi-player Games

1. Introduction

Information security attacks targeting human nature, such as phishing, are rising rapidly. As systems are becoming more complex for attackers to exploit, the human factor becomes a target of high interest. The organization's risk of threats increases when users of ICT systems are unaware of cybersecurity (Filippidis, et al., 2018). Current awareness training methods lack effectiveness, but gamification shows promising results due to its ability to counter several weaknesses of existing training, by stimulating motivation and engagement of participants (Ng Jia Jian & Intan Farahana Binti Kamsin, 2018).

The problem that this research tries to solve is the lack of efficiency of ISA training in educational institutions. This study aims to increase the efficiency of ISA training in the field of higher education and more specifically among teachers and students. Design science is used to create a cybersecurity interactive book artefact for learning and then testing the acquired knowledge with a second artefact which is a board game. This approach enables teachers and students of higher education to learn and test their security knowledge in an interesting and fun way that interactively encourages knowledge acquisition with the goal to play and win over their opponents. This activity engages the players in fun but also motivates practice and learning effectively.

This research aims to answer the following research questions:

- How can an interactive book artefact help to improve ISA learning for teachers and students?
- How can gamification be applied to educational ISA training in order to improve it?

The game is an interactive board game which supports practicing knowledge in cybersecurity through a variety of questions designed to measure understanding of the subject. Players have personality cards that are representing the different personality styles of hackers. The game starts with the player with the higher number of dice and continues clockwise. Players have to draw a question card and answer them correctly. Also, the game includes fun unexpected events like a duel box, where a player can challenge another player as an opponent. The player that answers first and correctly takes the other player's position on the board.

This paper is structured as follows. The next session presents background on ISA and gamification. Then, follow the methodology and the presentation of the artefact. Limitation of the research, conclusion and future research concludes our paper.

2. Background

This section presents literature on similar approaches to the problem and proposed solutions. Then, we study knowledge creation and different methods in order to elicit the content that will be used for the training from information security books and develop the interactive book and the game artefacts in an accurate way. Through this section challenges and approaches to the problem will be presented.

3. Relevant research

Gjertsen, et al. (2017), used design science to produce an artefact that would result in increased motivation and learning outcomes. A gamified interactive prototype application was developed based on interviews with security experts and a workshop with regular employees at two companies. Then the artefact was evaluated by employees in a second workshop. Their results indicate that gamification has the potential to increase behaviour. They created a prototype that has the goal to improve the knowledge of the trainees on information security, but they were not evaluating the change in behavior which is a significant pitfall that should be avoided when designing such applications because artefact evaluation is a critical stage of the design science process.
“Cyber hygiene”, is a term that exists and is commonly used by the time this paper is published, which refers to the behavior development of the users. This means that the literature study was not complete for the specific problem that was described, and this leads to a limited scope and a weak artefact that does not effectively solve the problem. Below, Figure 1 shows the behavior models to position cyber hygiene.

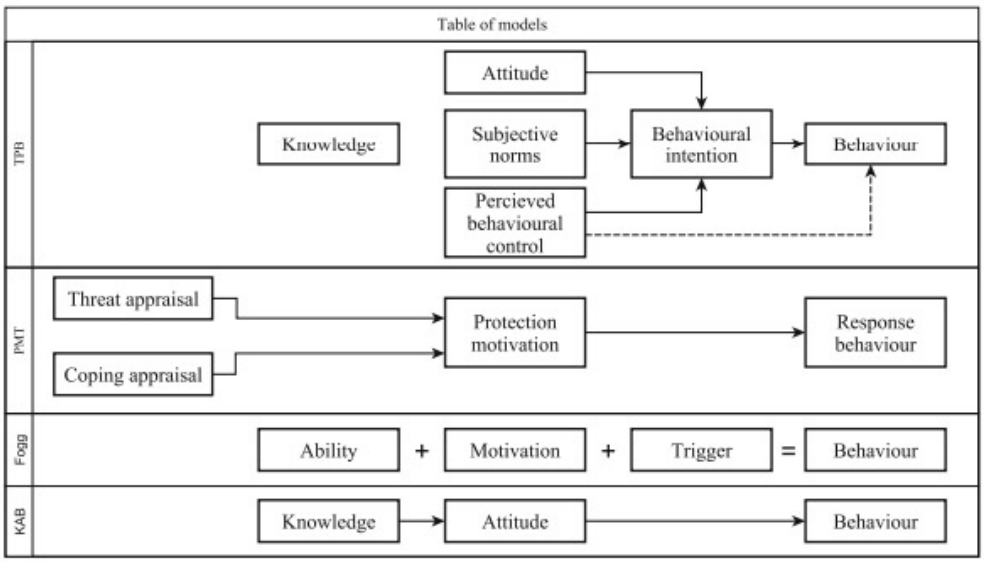

Figure 1: Behavior model to position cyber hygiene, (Maennel, et al., 2018)

Scrimgeour & Ophoff (2019) used a design science research approach with several iteration cycles to create a practical method to implement an information security awareness campaign (ISAC) within an organization. Then, the campaign was evaluated based on the impact, effectiveness and results of each step, as well as the feedback from the participants. The results of the study show a valid method for implementing an ISAC. Although the

limitation of statistical generalization exists within a single case study, researchers propose that analytic generalization is possible. Another limitation is that certain steps within the method proved time-consuming and confusing to some participants.

Rieff (2018), in order to improve information security awareness training effectiveness, used Hevner's seven guidelines (Hevner, et al., 2004) concerning design science to develop a framework. The framework is designed to guide developers in gamifying cybersecurity awareness programs. An empirical case study proved the usability of the framework through gamification of an existing program and compared participant experiences between the existing training and the gamified one. First, a literature study was made to study the contructs of cybersecurity awareness which led to a newly developed model. Then, gamification mechanics were applied to cybersecurity awareness training and a framework was designed. The framework aligned and applied within the organization. Following, the artefact was evaluated by performing observed expert interviews and research contributions such as the artefact and cybersecurity awareness construct models were discussed. After that, literature studies concerning cybersecurity awareness and gamification were performed to construct the framework. The research was conducted iteratively and the initial framework design is followed by expert interviews and a case study. As the last step, the research is communicated and presented through a framework with two layers of abstraction. The study results show a higher perceived increase in cybersecurity awareness in the gamified training when compared to existing training, although not significantly higher.

Silic & Lowry (2020) used a mix of design science research, kernel theory and hedonic-motivation system adoption model (HMSAM) to increase the efficacy of information security training. A study with 420 participants shows that fulfilling users' motivations and coping needs through gamified security training can result in statistically significant positive behavioral changes. A long-term field experiment showed that gamification can be used to foster training systems that are less invasive of employees' everyday work routines, that provide intrinsic motivation to learn and comply with security efforts, and that provide the efficacy necessary so that employees will comply.

4. Knowledge Creation

Knowledge creation in information security is still lacking clarity. Creation of IS security knowledge remains an ad hoc process (Belsis & Kokolakis, 2005). This situation prevents the organization from creating security knowledge.

The organization cannot create knowledge on its own, but by the actions of the human capital and the interaction that takes place within the group. This interaction between tacit and explicit knowledge is called knowledge creation (Nonaka & Takeuchi, 1995).

Nonaka (1991) created the SECI model which is the acronym for the four dimensions of knowledge: Socialization, externalization, combination and internalization. The interaction between tacit and explicit knowledge based on the SECI model creates four basic patterns for creating knowledge in any organization (see also Figure 2):

1) **From Tacit to Tacit**: one shares tacit knowledge directly to another (**Socializing**).
2) **Explicit to Explicit**: when combining discrete pieces of explicit knowledge into a new whole (**Combination**).
3) **Tacit to Explicit**: when one articulates the foundations of the tacit knowledge acquired and converts it to explicit knowledge that permits sharing with the team (**Externalization**).
4) **Explicit to Tacit**: when a new explicit knowledge is shared and others begin to internalize it like extend and reframe their own tacit knowledge (**Internalization**).

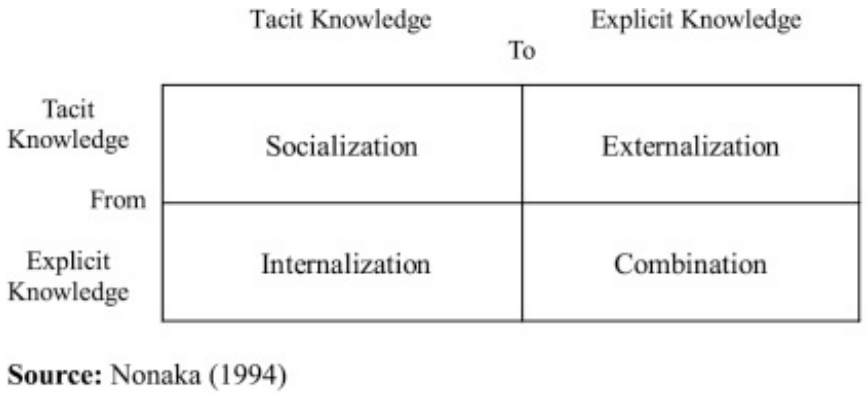

Figure 2: Knowledge creation types

SECI model introduces a kind of spiral knowledge. One first learns tacit knowledge (socialization). Then, translates this into explicit knowledge (articulation). Then, the knowledge is combined (combination). Finally, through the experience of creating something new they enrich their tacit knowledge base (internalization). At last, the same procedure starts again at a higher level (spiral) (see Figure 3).

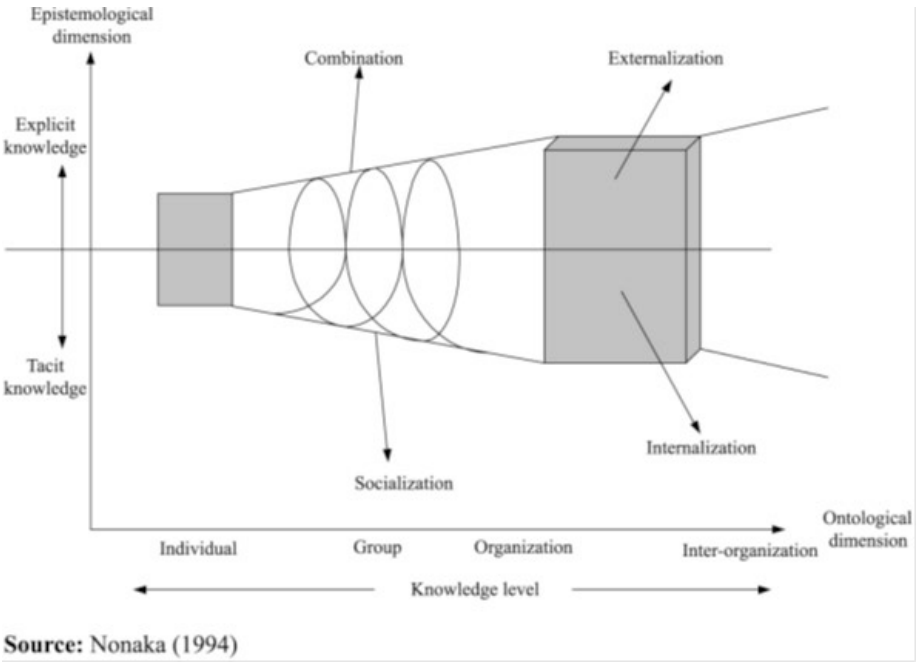

Figure 3: The knowledge spiral

5. Methodology

Design science framework by Johannesson and Perjons (2014) consists of five steps: explicate the problem, define requirements, design and develop artefact, demonstrate artefact, and evaluate artefact.

For the first activity, explicate the problem resources from the literature that are used as described in Johannesson and Perjons (Johannesson & Perjons, 2014, p. 92). For defining the requirements activity, a literature study alongside the specific domain constraints were considered. The following proposed tasks were set based on the literature:

1. **Define project scope:** clear definition of the context which will define the education material properly.
2. **Define stakeholders:** educational employees, students, and visitors to the universities.
3. **Define learning objectives:** what we want the trainees to be able to do after the training. This includes the ability to demonstrate basic understanding of the information security threats and vulnerabilities, the ability to identify risks and perils of common information security threats associated with e-learning activities, to become aware of the significance of adopting preventive habits to enhance cyber hygiene

behavior, to become aware of the most common information security techniques and best practices and to know when risky behavior from their side can potentially impact the equivalent organization.

4. **Extract categories, key elements, and knowledge:** categories that are useful to the learning actors, key elements like terms and transformation of information found in the literature to knowledge as suggested by Nonaka & Takeuchi (1995).
5. **Define book and application requirements:** different requirements for the interactive book that will enhance the learning process and the board game created to assess knowledge acquisition were defined.

Data collection uses a literature review for the categories, key elements and knowledge extraction. As artefact, an interactive book that supports video, puzzles, crosswords, word completion and interaction with the user was selected for the learning part. A second artefact, a board game based on quizzes was selected for the assessment part of the process. For the development of both artefacts the creative method which is a brainstorming technique to collect ideas was used. For demonstration and evaluation of the interactive book a second iteration was performed and a prototype of the artefact was demonstrated to all project team members for evaluation and improvement suggestions. The board game was evaluated on dozens different iterations by playing, and feedback was used to improve it. Figure 4 presents the methodologies that used for each step of the design science process.

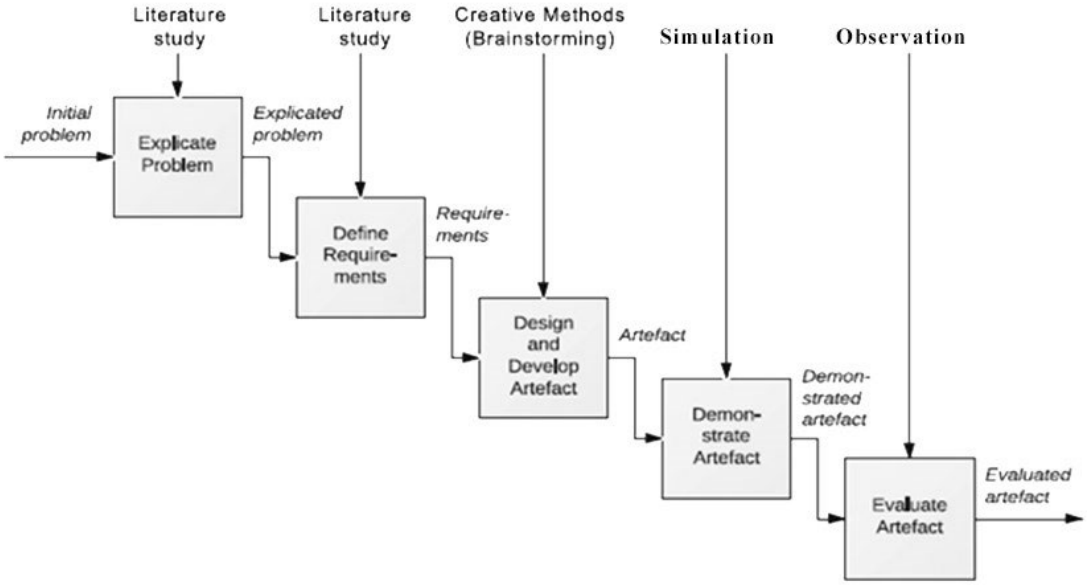

Figure 4: Steps of Design Science method (Johannesson & Perjons, 2014, p. 78)

6. Artefact presentation

The first artefact, is an interactive book, which supports quizzes, crossword puzzles, multimedia such as video, and complete the word simple games that enhance the learning process.

For the interactive book, the moodle platform and h5p moodle plugin was selected. Six categories were elicited from the literature with their key elements and a hundred multiple-choice questions were developed. Next, 63 images were designed in total and mapped with the questions. The learning categories are backup, remote access, data security, password security and management, social engineering (phishing, pharming, etc.), and software attacks (viruses, worms, denial of service). Each question is written simply and educationally so the trainee can have a good explanation of each answer. Playability of learning and assessment of the web and mobile version of the app was performed. At last, User Interface and User experience were assessed. Figure 5 shows a screenshot of the interactive book which is the learning part of the Cyber Hygiene Game App.

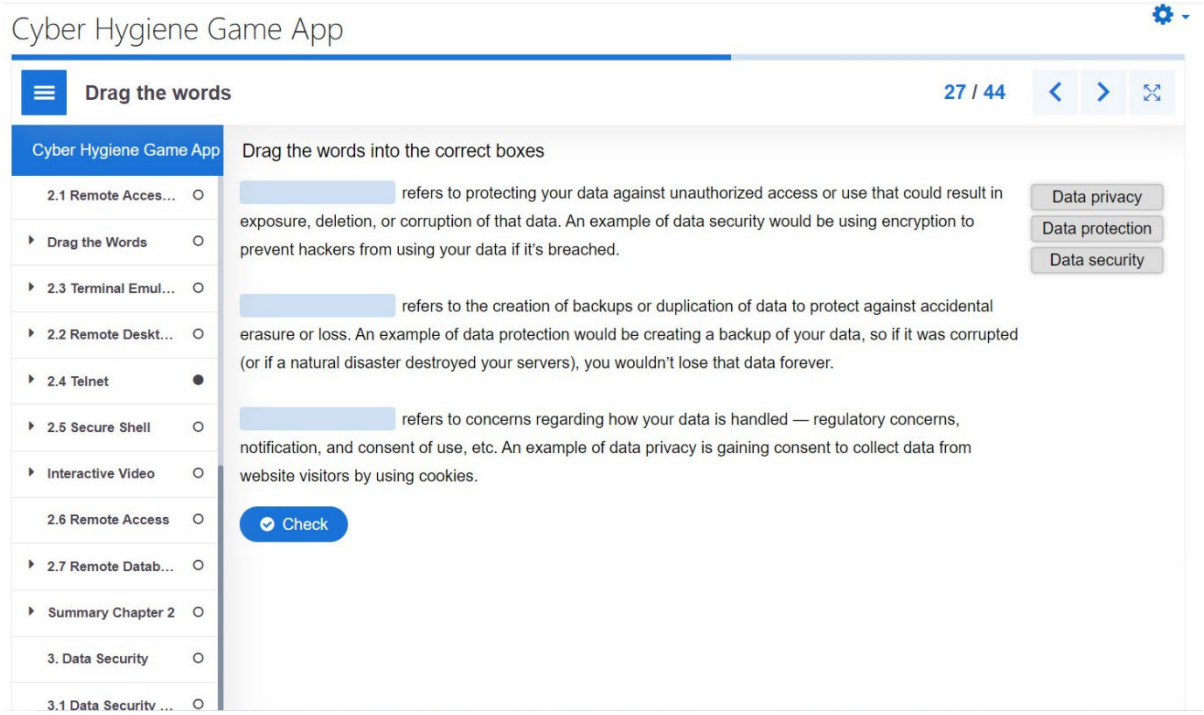

Figure 5: Cyber Hygiene Interactive book.

The second artefact is a printed board game with hackers and cards with the goal to support the learning process and evaluate the change in the ability of the participants to respond and take actions.

Purpose of the game is to practice cybersecurity knowledge by answering questions (trivial game) which are carefully designed in order to boost understanding of the subject. The game starts with the player with the highest number of dice and continues clockwise. If the players answer correctly, move forward in the board the steps written on the card depending on its degree of difficulty, unless a hidden hacker card or source code card tells them otherwise. If they answer incorrectly, then the next player takes turn. There are six personality cards and depending on how many players there are, they take a card at random and place it closed in front of them. Each personality gives the player a unique attribute, however, they can only use it once and will have to reveal their card to the other players. Question cards include questions that players are asked to answer and have graded difficulty (Easy = 1 step, Medium = 2 steps, Difficult = 3 steps). When a player falls on one of the 3 duel boxes (boxes with swords), they can choose another player as an opponent. A third player will take 3 question cards in their hand and ask the questions one by one. Whichever player answers first correctly and faster that the other wins the duel. Hacker cards are cards that have a hacker on the back. When a player falls on these boxes, they draw a card and read the command given to them without the other players seeing what is written on it. They can use it in that round, but they can also keep it turned upside down in front of them. The same goes for source code cards. The winner is the player who manages to complete the entire round of the board by answering the questions correctly and thus gaining steps to move forward. Figure 6 shows a presentation of the board and the back side of the cards of the game.

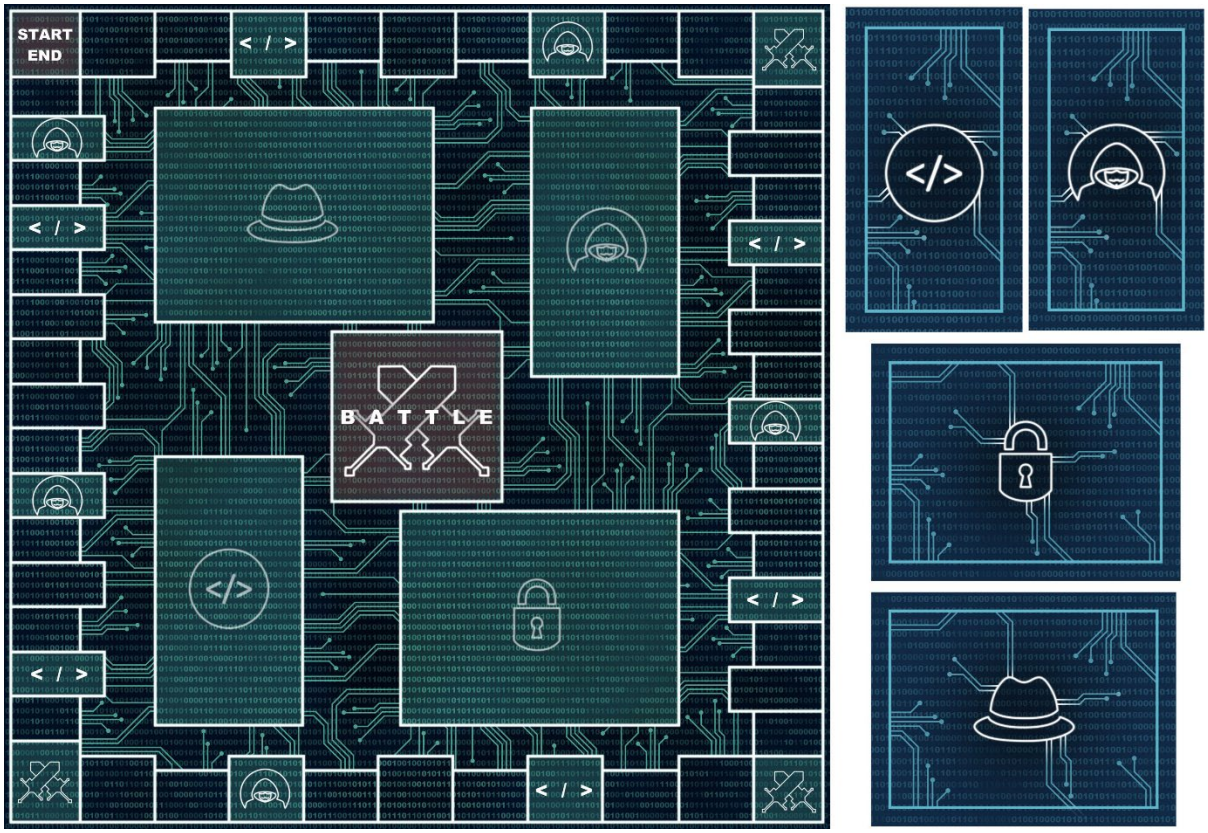

Figure 6: Presentation of the board game

7. Limitations

This research tries to treat the problem of effectiveness in information security awareness training although limitations apply. First of all, this research is limited by key actors who are university teachers and students. Next, the research is limited by its specific context which applies to users that have no technical background and the use of systems is very specific. Generalization of this research is still possible but is something that needs verification. Research scope definition, key actors, learning objectives, categories, key elements, and knowledge extraction for information security awareness from literature was performed carefully, but still further verification with actual deployment of the results on a real case is needed. Game design and game engine creation was tested repeatedly, but still more cases are needed for feedback and improvements.

8. Conclusions

In this study, we used design science to create artefacts in order to improve efficiency of information security awareness training. The study starts with introduction and motivation of the problem which is the lack of efficiency of ISA training in educational institutions. This research aims to improve learning by an interactive book artefact for knowledge acquisition and a board game used to boost learning and assess the acquired knowledge. At first, participants were separated in two groups. The first group took a simple quiz in order to assess their current knowledge and then they asked to read a textbook. Some days later, they took the quiz again to assess knowledge acquisition. Another group of participants took the quiz and then asked to use the interactive book for learning and then play the board game. A few days later, the second group also took the quiz. Results show better understanding for the group that played the game, but a broader sample is needed for more accurate results. Studying literature on the subject equipped us with a good starting point and foundations on how to treat the problem. Knowledge creation process helped us to transform information into knowledge chucks, and to choose a proper game type and style for this kind of information. The presented artefacts are improvements to flat information learning and provide an alternative way for information security awareness training in a fun and educational way. Design science by Johannesson and Perjons (2014) and its five steps provide a clear forward method for artefact design and development.

9. Future work

As future work, multiple game scenarios will ensure the evaluation, and the educational value will be measured more accurately. This includes different types of scenarios, for example by scenario-based story telling. Next, technological developments to improve student engagement and learning effectiveness, such as virtual reality, web virtual world technologies, 3D in a game-like setting are considered an effective next step for user engagement on the gamification part of the study. In the methodology part, the study of frameworks that provide educational guidelines for further improvement of the content and the game are also in our future plans.

Acknowledgement. This paper has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101021936 and it was supported by the Erasmus+ Programme of the European Union [grant number 2020-1-SE01-KA226-HE-092518].

References

Belsis, P. & Kokolakis, S., 2005. Information systems security from a knowledge management perspective. Information Management & Computer Security, pp. 189-202.

Brocke, J. v. & Lippe, S., 2010. Taking a Project Management Perspective on Design Science Research. Global Perspectives on Design Science Research, pp. 31-44.

Filippidis, A. P., Hilas, C. S., Filippidis, G. & Politis, A., 2018. Information Security Awareness of Greek Higher Education Students - Preliminary Findings. Thessaloniki: IEEE., 7th International Conference on Modern Circuits and Systems Technologies (MOCAST).

Gjertsen, E., Gjære, E., Bartnes, M. & Flores, W., 2017. Gamification of Information Security Awareness and Training.. s.l., Proceedings of the 3rd International Conference on Information Systems Security and Privacy.

Johannesson, P. & Perjons, E., 2014. An Introduction to Design Science. London: Springer.

Leymann, F. & Altenhuber, W., 1994. Managing business process as an information resource. IBM Systems, pp. 326-348.

Maennel, K., Mases, S. & Maennel, O., 2018. Cyber Hygiene: The Big Picture. Computer Science, pp. 291-305.

Ng Jia Jian & Intan Farahana Binti Kamsin, 2018. Cybersecurity Awareness Among the Youngs in Malaysia by Gamification. s.l., s.n.

Nonaka, I., 1991. The knowledge creating company. Harvard Business Review.

Nonaka, I. & Takeuchi, H., 1995. The knowledge creating company: how Japanese companies create the dynamics of innovation. Oxford: Oxford University Press.

PMP, 2017. A Guide to the Project Management Body of Knowledge (PMBOK® Guide)–Sixth Edition. Newtown Square, Pennsylvania: Project Management Institute, Inc.

Rieff, I., 2018. Systematically Applying Gamification to Cyber Security Awareness Trainings: A framework and case study approach. Computer Science.

Scrimgeour, J.-M. & Ophoff, J., 2019. Lessons Learned from an Organizational Information Security Awareness Campaign.. IFIP Advances in Information and Communication Technology, p. 129–142.

Silic, M. & Lowry, P. B., 2020. Using Design-Science Based Gamification to Improve Organizational Security Training and Compliance.. Journal of Management Information Systems , 37(1), p. 129–161.

.