The Sixth International Conference on Design Creativity (ICDC2020)
Oulu, Finland, August 26th – 28th 2020
https://doi.org/10.35199/ICDC.2020.30

On the design of playful training material for information security awareness

Johan Lugnet, Åsa Ericson, Martin Lundgren and Johan Wenngren

Information Systems, Luleå University of Technology, Sweden

Abstract: This paper presents the rationale for the design of a card deck game sustaining information security training. The efforts have followed design thinking, been inspired by an approach for problem-based learning, and used gamification. The card deck game primarily aims to support entrepreneurs in small and medium-sized manufacturing companies, heading towards the introduction of digital services, yet is also useful for anyone to practice risk awareness. Information security, here in short representing the efforts to protect information and mitigate risks to uphold confidentiality, integrity and availability, is by SMEs often seen as a technical problem, but is depending on human behaviour. Literature on security training, emphasises the relevance of interpersonal dialogues and reflection, such reflection is not supported by traditional education, as for instance reading theory and answering questions. The application of gamification has shown to increase awareness, where the play becomes an eye-opener to progress focused dialogues and learning.

Keywords: *Serious play, Gamification, Design thinking, Educational games, Digital service innovation.*

1. Introduction

Digitalization drives new solutions based on information and communication technologies (ICT) in business and everyday life. Many innovative digital services that make interactions with organisations efficient have been introduced, for instance e-ID, e-invoice, and e-signature. Adding to that, services like Uber and Airbnb, but also applications for medical care and labour services have been introduced, and connect companies with their customers via digital platforms. These new businesses are often a result of creative service innovations, and some even disrupts established markets in radical ways. The disruptive ones often come from agile entrants rather than from large incumbents (Christensen, et al., 2015). The interconnectedness and swift use and sharing of information benefits society in several ways, and companies in particular. Yet, benefits become a weakness if not secured against attacks. For example, enterprise ransomware breaches have increased 12%, while overall ransomware activities have dropped with 20%, and supply chain attacks has increased with 78%. These attacks have during the latest years become more ambitious and stealthier (Symantec, 2019). Accordingly, trends show that targeted attacks have companies in the riflescope, and many of the companies are unaware that they are under attack until they suffer from the effects. Low awareness of threats and risks, and how they can be mitigated proactively is a barrier for small- and medium sized companies (SMEs) to develop and introduce safe digital services. Yet they are, more or less, forced to increase digital solutions to stay competitive in their business environment. This makes it important to train a risk aware and mitigation

mindset, consequently internalise information security risk management into everyday activities, and in particular in parallel with the early phases of digital service innovations.

Information security is a term that is commonly used to describe the activities of protecting information from e.g., unauthorized, inappropriate access, use, and modification, thus includes also risk management. Risk management focuses threats, vulnerability and consequences by addressing policies, procedures and technologies to prevent or reduce risks. The similarities and differences between information security and cyber security have been discussed in academia (e.g., von Solms and van Niekerk, 2013). It has been found that information security often assumes information to be an organisational asset which can be managed by applying the CIA triad of Confidentiality, Integrity and Availability (Whitman and Mattord, 2014), while cyber security may include to protect humans, and any of their assets that can be accessed via digital channels. Thus, cyber bullying, home automation and digital media will be included (von Solms and van Niekerk, 2013). Nevertheless, the use of ICT is a key similarity between the two concepts. Traditionally, ICT security is known by its technical aspects, e.g., firewalls, encryption and anti-virus software, which ensure reliability of networks and infrastructures.

New types of cyber criminality provide a lucrative underground economics based on, e.g., social engineering. In the context of information security, social engineering means that criminals apply psychological manipulation of people to make them take actions which open up for attacks or frauds, e.g., clicking a link with malware in the belief that they have a possibility to win something. 'Phishing' and similar sophisticated ways of accessing accounts and data are common. These rely upon social principles mainly from marketing theory, e.g., people tend to take actions quickly if the offer seems to be limited in time or number (scarcity), or by using popups when closing down a site that indicate a loss if not signing up now (commitment). The human non-reflective actions are the significant reasons for these categories of intrusions to be so successful (Korovessis, et al., 2017). Thus, threats are hence becoming more related to the human behaviour, and they are taking new forms in a fast pace.

Material, or tools, for practical information security training are recommended to promote continuous reflections and dialogues. If so, the awareness will have an effect on daily routines, since people starts to observe and reflect upon their actions (Puhakainen and Siponen, 2010). Those interpersonal dialogues and reflections are not supported by education material based on reading and writing, thus the material has to sustain interactions and knowledge sharing among a group of people. Crossler, et al. (2013) concluded that security training has to go beyond educational standards, and integrate dynamic influences among people which, in turn, shape their everyday experiences.

Embarking from this challenge and background, interactive material was going to be developed to train SMEs, mainly novices in information security, but skilled in using ICT for their ordinary products. Having a long background in teaching and applying design thinking (e.g., Brown and Katz, 2008) for better teamwork and co-creation (e.g., Ericson, et al., 2007), we found this doable as a design methodology for the task. Also, we found that Problem-based learning (PBL) would be a sound inspiration for the support tool as such, since PBL uses trigger material and open-ended problems, to sustain critical evaluation, self-directed learning, but also listening and respect for other's views (Wood, 2003). Adding to this, serious play (Schrage, 1999) which is well in line with design thinking led us into gamification (e.g., Narayanan, 2014). The purpose of this paper is hence to present the rationale and methodology for the design of playful training material for information security awareness. This is done in order to elaborate on the topic of creative design in relation to knowledge dissemination to entrepreneurs in small and medium sized firms.

2. Awareness training in information security

Earlier studies on information security training have received some criticism of being too focused on reading and tests (e.g., Lacey, 2010), hence misses the importance of creating and maintaining awareness and critical thinking. Such criticism is still presented (Ghazvini, A. and Shukur, Z. 2017). Puhakainen and Siponen (2010) emphasized the importance of applying learning tasks that are active, and motivate the people's cognitive processing, e.g., reflecting and discussing the relevance of the tasks at hand. They also conclude on the importance to relate such training activities to the employees' daily routine work. The employees' behaviours are formed, when they analyse and reflect on real-life

scenarios. Training produces skills and competences among learners, while attention on identifying security concerns and thinking out how to act on them is related to awareness (Wilson and Hash, 2003). Attention and focus are related to awareness, and are identified as a core skill for the future (Eyal, 2019). Korovessis, et al. (2017) explain awareness as having knowledge of a situation or fact. However, they also present Nonaka's and Takeuchi's SECI model for knowledge creation which, as a consequence, makes their explanation too simple. Nonaka, et al., (2000) describes organizational knowledge creation as a dynamic process generated in social interactions, in which the relative, dynamic and humanistic perspectives are fundamental. So, to supplement the SECI model consisting of four modes, i.e., socialization, externalization, combination and internalization in which tacit knowledge is transformed into explicit, Nonaka, et al. (2000) adds a platform for knowledge conversion and self-transcendence, i.e., *Ba*. Thereby they introduce the importance of the progress of a shared context. *Ba* enables individuals to create knowledge in a specific time and space context which unifies physical (like an office), virtual (like digital tools) and mental (like shared ideals) dimensions. Or, simplified, *Ba* is where information is interpreted, agreed upon and turned into knowledge (Nonaka, et al., 2000). The knowledge creation, and thus also awareness, happens in an interplay between humans, but perhaps only if some kind of a *Ba* manifestation supports the process. Having this view in mind, software tools may manifest *Ba* and enable self-paced awareness training, as suggested by Furnell, et al. (2002) and Korovessis, et al. (2017).

Other studies have developed tools for information security awareness including analysing risk events, discussion forums, newsletters etc. (e.g., Chen et al., 2006). Kruger and Kearney (2006) propose a tool to measure and evaluate awareness successes in an organization or company. The tool consists of three dimensions of measures, i.e., knowledge–what the person knows; attitude–what the person thinks; and behavior–what the person does. The tests and evaluations of knowledge, or awareness, are based on a questionnaire which provide visual graphics of the awareness level in the company. Thus, providing an instrument for the board of directors, to monitor and control the company status. Yet, may lack in empowering employees to train information security more practically. Kruger and Kearney (2006) highlights themselves that finding the right questions are important, but not straightforward.

The concept of SETA programs – Security Education, Training, and Awareness, have been introduced in larger organisation to enhance security by increasing knowledge and developing skills so that employees perform their jobs more securely (Whitman and Mattord, 2014). A supplement to those technical-oriented initiatives are general education and training approaches to motivate and increase awareness in an organisation. Researchers argued that games and the concept of gamification could be an effective way of training cyber security (Alotaibi, et al., 2016). When reviewing literature on information security awareness, we found that during the last years a number of training tools addressing different applications areas have been developed and proposed (an encompassing list of sources can be found in Korovessis, et al., 2017). However, we have also found that many efforts are based on quantitative measures, which make important contributions in their own right, but as is also shown in other studies, not sufficient to solely support awareness training. Awareness is also an interest in other fields, for instance creativity, innovation and design, and recent studies in those fields motivate game and play to be included in the efforts of information security training.

3. Serious games and gamification: an active learning approach

Serious games, which are different from playing with prototypes for design purposes, is used to facilitate active learning, meaning that players learn by the interactions between a game and peers. The fun of playing makes people committed. And, the game trains cognitive skills, as for instance context awareness, attitude, problem-solving, and communication (Mettler and Pinto, 2015). It has been found that adult learners/professionals prefer actions rather than explanations, and the possibility to apply more than one learning style (Mettler and Pinto, 2015). Educational games, in opposite to leisure games, are designed to meet specific learning objectives, and often have a defined mission to complete, and learn from. The interactive and mission-oriented approach of educational games is found suitable for training safety issues (Martínez-Durá et al., 2011). Guidelines for designing educational games suggest, for example visual representations and symbols that are easy to understand, supportive instructions and help manuals (Pinell, et al., 2008). Playing an educational game gives enjoyment, in turn makes learners

play, i.e., practice, more. It must be noted that playing and learning is not a one to one match, but research on the psychological aspects concludes that humans want to accomplish missions they have started, and that a mix of learning and performing goals are beneficial for that (Landers and Callan, 2011). Active adult learning must be built, not only on content and formal knowledge, but also on experience and applying skills. Thus, the hands-on experiences, problem-based training, and experimenting when using educational games bring the principles of reflection, peer dialogues and on-the-job learning to life (Kang, 2019).

Gamification, and how to define it, has been a subject for debates, where some advocates a wider view and some advocates a strict view on what it is, and what it is not. For example, serious game and educational games were considered as not gamification by those advocating a strict definition (e.g., summarized in Chou, 2014). Chou (2014) describes gamification as *"…the craft of deriving fun and engaging elements found typically in games and thoughtfully applying them to real-world or productive activities"* (p.8). By that he stresses a human-focused design rather than a function-focused design, and conclude that the gaming industry was pioneers in applying a human focus in the design of their solutions, i.e., that is why the term gamification is used. The missions in games, e.g., killing the dragon or saving the princess, are means to keep the player entertained and make them committed to the game (Chou, 2014). Thus, the creation of purposeful missions is an important design activity in gamification. The models suggested by Nonaka, et al. (2000) stated that it is in the actions and interactions between; chaos-order, tacit-explicit, micro-macro, body-mind, emotion-logic, and action-cognition, that knowledge is created. Quick and continuous changes between some of those opposites, would in a real world be frantic, but put into a game it would be a base for pleasure. Gamification, as commonly applied in non-gaming contexts, achieves a change in behavior and/or attitude, and it increases motivation and engagement (Ma, et al., 2011). Chou (2014) has categorized eight dimensions which drives motivation and engagement, and could be used as a design framework. The dimensions are (p.24); meaning, empowerment, social influence, unpredictability, avoidance, scarcity, ownership, and accomplishment. The dimensions stimulate both the analytical and the creative senses of the players. A number of game elements are then connected to each of the dimensions, e.g., leaderboards, points, badges (what is often named as gamification, or game mechanics).

4. Serious play and design thinking: a creative design perspective

Serious play (Schrage, 1999) is presented as serious design and development work based on rapid prototyping. All types of prototypes are recommended, from the simplest simulations like gestures and skits to more sophisticated and built, but still those prototypes should be created rapidly enough to progress learning and communication. Serious play is not only learning by prototyping, but changes the organisational culture from a show-and-tell to a formative one, i.e., show-and-ask (Schrage, 1999). Boundary objects, like prototypes, become an interface which enables shared culture and values (Subrahmanian, et al., 2003). Schrage, already in 1999, concluded that culture will have an ever-more-prominent role in organisational value creation. The discussions today about coming demands from future and modern employees indicate that organisational culture based on new value words, as for example, open, collaborative, and non-hierarchical, is important. What are motivating modern employees also become different since they are brought up in the era of digitalization. They are motivated by, e.g., empowerment, trust, instant feedback, and flexibility. In line with this, it is suggested that businesses must develop a proactive and creative strategy for learning at the workplace (Kang, 2019).

Design thinking, in recent time, is related to the work at Stanford Design School, and has been formed as the IDEO way to innovation (Kelley, 2001). This approach seems unstructured, i.e., not process-like, or as Leifer and Steinert (2011) describe it – 'a rather loosely labelled box'. In fact, the box contains numerous of tools for innovation and design. So, design thinking is a well-developed and continuously refined methodology to guide teamwork. Kelley (2001) stresses that the basics of the methodology is interpreted differently according to the task at hand and the context in which the design problem is situated.

The IDEO way suggests the interactive activities of:

- Observation to understand users, i.e., learn from, not fixing people.

- Brainstorming to generate ideas, i.e., connect user data to the task.
- Rapid prototyping to visualize possible solutions, i.e., speed up decision-making and innovation.
- Refining to narrow down choices, i.e., create agreement from stakeholders based on a few alternatives.
- Implementation, i.e., a cross-functional team package a desirable, valuable and feasible solution.

Quick iterations between the activities are emphasized, as is also visualising ideas. Conformity is not a goal of the activities, rather diversity is targeted. Ambiguity is a source for creativity, and anyone practicing design thinking should develop an *"ability to let change occur rather than managing it"* (Leifer and Steinert, 2011, p.160). Design thinking recommends a questions-driven approach where communicative prototyping enables learning loops (Leifer and Steinert, 2011), serious play promotes a show-and-ask culture (Schrage, 1999), playing with scarcity, i.e., low-fidelity prototypes evokes creative improvisation (Naranayan, 2014), and working in heterogeneous teams increases learning (Dym, et al., 2005). An informal milieu is essential to make people more open to share ideas and thoughts, and gives confidence as well as commitment to jointly explore a situation.

We had, as introduced in the beginning of this paper, identified how firms are challenged by information security risks in the strive to develop and offer new digital services. From that insight, we decided to develop training material to increase basic understanding of information security risks. From reviewing literature on awareness training in information security we could conclude, on the one side, that tools exist. And, on the other side, we could conclude that tools that would engage and motivate interpersonal reflections and dialogues were limited, as was also suggested by previous research. In parallel, our empirical studies among SME firms aligned with the view that traditional training material was found 'time consuming', 'boring' and 'non-productive', thus did not engage learners. Also, it was expressed that traditional material was directed towards an organizational level, and did not address the individual employee level. An active learner approach, based on inspiration from PBL led us to serious games and gamification, this was combined with our background in serious play and design thinking, as presented above. This rationale encouraged the methodology for the design of a card deck game for information security awareness.

5. Card deck game design

The idea of designing a physical card deck game derived from PBL principles of using a trigger material, but is also grounded in our experiences of using physical prototypes to motivate communication in a team (c.f. design thinking and serious play). Also, our previous observations of innovative teamwork indicated that a shared 'object on the table', which all members in the team have the possibility to interact with, stimulate focused dialogues and creative thinking (Ericson, et al., 2016). Further, to understand the targeted users' maturity level on information security, informal talks have been done, e.g., 'Tell us about your view? How do you deal with it?'. Adding to this, teaching and course development in basic information security subjects have provided insights to understand, not only students as novices, but also the level of people being novice employees in firms. In this first phase, we found that the starting point for the training package we planned to deliver in the project, could be, in our view, very basic, i.e., to get into the context and learn the vocabulary. Thereby, we also decided that the game should not require any pre-knowledge about information security, but that was the core goal of the game. This resulted in a design brief describing the needs, and an initial idea for a solution, i.e., a physical game nudging dialogues between the players about information security risks and countermeasures for a company.

The brainstorming phase did also include benchmarking, testing and evaluation of different board games. Since the variety of games is huge, the focus for the benchmarking was on pro and cons between different types, size, easy to use, game elements etc. Here we also invited an expert, a game passionate person developing, testing and selling board games. He facilitated the idea generation by asking, to us, new questions about the intended users, e.g., 'Will they play in solitude, and compete against their own results? Will they play in teams, collaborating to win? Or will they play as competitors, the best person will win everything?". This rendered up in a second iteration evaluating the benchmarked material

again, and connecting it closer to the intended users. In the end, the benchmarking refined the design brief by adding that the game should be a deck of cards, the game should be played in competition, and one player should be the winner, also the time to play should not be long. It would be better if each game round takes, approximately 15-20 minutes. If so, the game can be played several times, giving the 'loser' of the first round a second chance, i.e., repeating the training/playing the game should be motivated.

The following phases, rapid prototyping and refining were first started by seeking more detailed information on game development. The MDA framework, stands for Mechanics, Dynamics and Aesthetics (e.g., Kritz, et al., 2017) gave rise to constraints for the evaluation of the prototypes that were developed. That is, we did not use the framework as intended, but adapted the dimensions to better evaluate our prototypes. The MDA framework is suggested to be used for *"decomposition of games into coherent and understandable parts"* (Kritz, et al., 2017, p.182). So, in retrospective, MDA would perhaps also been supportive in the analysis and comparison between certain game types. Nevertheless, we applied MDA more superficial, but it facilitated the outline of a refined prototype. The prototype has been tested and evaluated in several iterations with different users/players, e.g., colleagues, friends, students, and company representatives. Mechanics was, as Kritz, et al. (2017) also conclude, observable only from the developers' side, i.e., we could relate actions to a certain item/element, as for example a symbol representing trading of cards. Dynamics was used to observe how the players interacted with the game, and aesthetics was used to observe emotional expressions, e.g., laughter, persistence, strategical wickedness. During the prototyping tests some of the players altered the competitive components of the game, and started to collaborate even though only one person could win the game. When we asked why, the answer was "*I can win the next round!",* thus indicating both being amused by the game, and finding the time spent on it worthwhile.

After prototyping, testing and deciding the design of the game and the contents on the cards, the appearance of each card was assigned to a skilled graphical designer. The owner of a business for playing cards and board games was invited to provide feedback based on his expert knowledge regarding game logic used for the training material developed in the project. The training tool, i.e., the card deck game, consists of 68 cards in different categorize of cards, see figure 1.

Figure 1. Some example cards from the game.

First the category of cards indicating five different roles in an organization, the second category (see cards with lightbulb in left corner in figure 1) contains of five countermeasures. The third type of card is information security threats (see the red card in figure 1), last category represents five different strategy cards (grey cards). The idea of the game is that the players collect cards, the one that first have 4 different roles, which are not subject of vulnerability attacks or threats played by the other players will win. The players can protect their organization by playing a countermeasure on their own role. The green card in figure 1 shows one role, namely The IT guy; The one responsible for IT and digital professional services at the organization. A free translation from of the description on the card from Swedish; *"The IT technician is a role that takes care of different technical problems. Expert on most things. They speak their own language and fix your problems."* The game is available in Swedish and Finnish, the native language of partners in the research project that game has been developed the game.

6. Concluding discussion

This paper set of to present the rationale and methodology for the design of playful training material for information security awareness. We took up this as a means to elaborate on the topic of creative design in relation to knowledge dissemination to entrepreneurs in small and medium sized firms. The rationale for designing a card game emerged from ideas based on educational games and gamification, and the design methodology was based on design thinking and serious play. In the latter, understanding users, prototyping and iterations forms the path. Gamification was suggested as human-focused design (Chou, 2014) which supported the combination with design thinking as a methodology. Grounding the training material in real needs extracted from company representatives was, to our understanding, a key to successful implementation. Time, for example, is a limited resource for small companies, which also had an impact on the instructions with rules that we developed for the game. It turned out that those were perceived as taking too long time to read trough, despite doing several iterations to shorten the text to its utmost minimum. Instead a short video describing how to *start* playing was filmed, and can be accessed through a QR-code on the card package. The approach of the players to just start playing the game, also indicated that the game would be even more intuitive if symbols were improved. Yet, the game inspires dialogues among the players about risks and countermeasures, e.g., if the risk is to be hacked, what can be done to proactively prevent that. The interactions in-between players and the game are activating terms and concepts into their own discourses, and relating them to their own company contexts. Thus, creating awareness—attention and focus—on potential scenarios of information security risks that individuals may encounter, however more studies evaluating the game approach is encouraged.

Acknowledgements

Financing for the CYNIC project (20201650) from the EU program INTERREG North 2014-2020 which supports cross-border collaboration to strengthen competitiveness and attractiveness in and between northern Sweden, northern Finland, northern Norway and Sápmi, and Region Norrbotten and Lapin Liitto are gratefully acknowledged.

References

Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2016). A review of using gaming technology for cyber-security awareness. *International Journal for Information Security Research*, 6(2), 660-666.

Brown, T., & Katz, B. (2009). Change by Design, How Design Thinking Transforms Organizations and Inspires Innovation. Harper Collins, USA.

Chen, C. C., Shaw, R., & Yang, S. C. (2006). Mitigating Information Security Risks by Increasing User Security Awareness: A Case Study of an Information Security Awareness System. *Information Technology, Learning, and Performance Journal*, 24(1), 1.

Chou, Y. (2014). Actionable gamification: beyond points, badges, and leaderboards. https://yukaichou.com/gamification-book/

Christensen, C.M., Raynor, M.E., & McDonald, R. (2015). What is distuptive innovation? *Harvard Business Review*, December 2015, 44-53.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future Directions for Behavioral Information Security Research. *Computers & security* (32), pp. 90-101.

Dym, C. L., Agogino, A. M., Eris, O., Frey, D. D., & Leifer, L. J. (2005). Engineering design thinking, teaching, and learning. *Journal of Engineering Education*, 94(1), 103–120.

Ericson, Å., Larsson.A., Larsson, T., Larsson, M. (2007). Need driven product development in team based projects, *In proceedings of International Conference on Engineering Design (ICED)*, 28-31 August 2007, Paris, France.

Ericson, Å., Wenngren, J., Holmqvist, J., Hammarberg, K. (2016). The case of an innovation contest: participatory design in a social context, *In proceedings of the DESIGN 2016 14th International Design Conference*, 16-19 May, Dubrovnik, Croatia.

Eyal, N. (2019). Stanford psychology expert: This is the No. 1 skill of the future–but most fail to realize it. Published 2019-10-09.

Furnell, S., Gennatou, M., & Dowland, P. (2002). A Prototype Tool for Information Security Awareness and Training. *Logistics Information Management*, 15(5/6), 352-357.

Ghazvini, A., & Shukur, Z. (2017). Review of information security guidelines for awareness training program in healthcare industry. *In proceedings of the 2017 6th International Conference on Electrical Engineering and Informatics* (ICEEI), Langkawi, pp. 1-6.

Kang, S-Y. (2019). To build the workforce of the future, we need to revolutionize how we learn. *World Economic Forum*, https://www.weforum.org/. Accessed 2020-01-01.

Kelley, T. (2001). The art of Innovation. Lessons in Creativity from IDEO, America's Leading Design Firm, Currency and Doubleday, USA.

Korovessis, P., Furnell. S., Papadaki, M., & Haskell-Dowland, P. (2017). A toolkit approach to information security awareness and education. *Journal of Cybersecurity Education, Research and Practice*, Vol. 2017, 2, Article 5.

Kritz, J., Mangeli, E., & Xexéo, G. (2017). Buildning an ontology of boardgame mechanics based on the BoardGameGeek Databas and the MDA framework. *In proceedings of SBGames 2017*, November 2-4, Brazil.

Kruger, H. A., & Kearney, W. D. (2006). A Prototype for Assessing Information Security Awareness. *Computers & security*, 25(4), 289-296.

Lacey, D. (2010). Understanding and Transforming Organizational Security Culture. *Information Management & Computer Security*, 18(1), 4-13.

Landers, R. N., & Callan, R. C. (2011). Casual social games as serious games: The psychology of gamification in undergraduate education and employee training. *In Serious games and edutainment applications* (pp. 399-423). New York: Springer.

Leifer, L., & Steinert, M. (2011). Dancing with ambiguity: Causality behavior, desgin thinking, and triple-loop-learning. *Inforamtion Knowledge Systems Management*, 10, 151-173.

Ma, M., Oikonomou, A., & Jain, L. C. (2011). Serious games and edutainment applications. New York: Springer.

Martínez-Durá, R. J., Arevalillo-Herráez, M., García-Fernández, I., Gamón-Giménez, M. A., & Rodríguez-Cerro, A. (2011). Serious games for health and safety training. *In Serious Games and Edutainment Applications* (pp. 107-124). New York: Springer.

Mettler, T., & Pinto, R. (2015). Serious games as a means for scientific knowledge transfer—A case from engineering management education. *IEEE Transactions on Engineering Management*, *62*(2), 256-265.

Narayanan, A. (2014). Gamification for employee engagement. eBook, Impackt Publishing, Birmingham, UK.

Nonaka, I., Toyama, R., & Konno, N. (2000). SECI, Ba and leadership: a unified model of dynamic knowledge creation. *Long Range Planning*, 33, 5-34.

Puhakainen, P., & Siponen, M. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly*, 34(4), 757-778.

Schrage, M. (1999). Serious play: how the world's best companies simulate to innovate. Library of Congress Cataloging-in-publication data, US.

Subrahmanian, E., Monarch, I., Konda, S., Granger, H., Milliken, R., Westerberg, A., & The N-DIM group (2003). Boundary objects and prototypes at the interfaces of engineering design. *Computer Supported Cooperative Work*, 12, 185-203.

Symantec (2019). ISTR Internet Security Threat Report, Vol 24, February 2019.

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97-102.

Whitman, M. E., & Mattord, H. J. (2014). Principles of Information Security, Fifth ed. Cengage Learning.

Wilson, M., & Hash, J. (2003). Building an information technology security awareness and training program. *NIST Special publication*, *800*(50), 1-39.

Wood, D.F. (2003). ABC of lerning and teaching in medicine. *Problem based learning*. BMJ 2003, 326-328.