University of Piraeus

Department of Digital Systems

MSc in e-Learning

Master Thesis

Simulation based learning in critical infrastructure security awareness:

An empirical study

Elisavet Maria Katsika

MHM1709

Piraeus, 31/01/2020

SUPERVISOR

Assoc. Prof. Fotini Paraskeva

University of Piraeus

Abstract

The digital transformation process that is currently underway is not only associated with benefits; among its downsides, increased cyber risk is mentioned more often than not. Most cyber security breaches are attributed to the human factor, and erring in turn is, more often than not, attributed to lack of awareness and proper training. The problem in fact is that humans lack security awareness, even though they may have been exposed to security related knowledge during their studies or otherwise. This gap between learning in theory and practically applying knowledge can be bridged using simulations. Simulation training is broadly used in a variety of scientific and professional domains such as health, the military or the navy and air forces (pilot simulators). As cybersecurity is an abstract concept, a simulation-based learning process targeting cybersecurity would be more challenging than in the case of other fields of knowledge, because a simulation for cybersecurity training should not only be about executing commands and following standard procedures, but also about making decisions and implementing risk management strategies and scenarios. This thesis investigates how simulation-based learning affects the knowledge of cybersecurity risk management. To this end, an experiment was set up, leveraging the simulation game CyberCIEGE. Thirteen undergraduate IT students were involved in the experiment and took part in the simulation game, by completing two questionnaires, one prior to playing the game and one after having played it. The purpose of the questionnaire was to define how the students self-assess their cybersecurity awareness and if this assessment is in fact reflected in their true knowledge. To do so, the questionnaire did not rely only on oneself's opinion, but it included technical questions as well. Even though the study we conducted provided preliminary results which, due to limitations, cannot be considered representative of a large population, it can prepare the ground for a longer, tailor-made, structured and well-designed intervention to take place in a larger scale, with more learners participating, more resources and data collection tools and with no time restrictions. The methodology and design employed for the thesis' purposes can be adapted and used in a larger scale study; given that the intervention was designed to be able to be re-used (be as sustainable as possible for further use), researchers and instructors can implement it to a program to explore the field of cybersecurity education which is currently advancing, and is in need of new challenges and systematic analysis.

Acknowledgements

Firstly, I would like to express my sincere gratitude to my supervisor Assoc. Prof. Fotini Paraskeva for supporting me throughout my MSc study and related research, for her patience, and the guidance and knowledge she always provided me with, when I most needed it. Her advice helped me throughout the time of researching and writing of this thesis. I am truly grateful for having this opportunity to have her as my supervisor and mentor during this last year.

Moreover, I would like to thank our MSc's professors, for the knowledge and support they provided me with during the first two semesters of the Master's program. Without them, I would not have been able to broaden my horizons and always opt for the acquisition of concrete, long-term knowledge.

Furthermore, this thesis would not have been completed without the help of Prof. Kostas Lambrinoudakis, who gladly gave us permission to host our intervention in one of his labs, in the context of his *Information Systems Security* class. My special thanks also to Christos Lyvas, who assisted before and during the intervention. With his technical expertise and overall support, the experiment was conducted with no implications. It goes without saying that I am most thankful for our university's students who agreed to participate in our intervention for this thesis's needs. I would also like to thank our department's PhD student, Vicky Karampa, for her precious assistance and support during the latest phases of this journey. Her valuable insight, advice and her overall attitude were of utmost help for me, and for those I am most grateful.

My sincere thanks go to my family, and especially to my father, whose contribution to this Master thesis is most valuable. Not only did he support me throughout the whole duration of the MSc, but he also assisted and provided guidance whenever it was needed for the thesis's purposes, in terms of technical inquiries or cybersecurity concepts' clarifications.

Last but not least, I would like to thank my friends and my fellow classmates, for their constant feedback and the patience they have shown towards me during this last year. Their consultation in times of need has been remarkably helpful and sincerely appreciated.

Table of Contents

Table of figures

List of tables

Chapter 1 - Introduction

In a world characterized by digital innovations and tremendous changes in the way computers function, we are more than ever in need of cybersecurity education. Nowadays, most of us have basic or advanced computer skills, however, skills are not enough to protect ourselves, our digital systems and important assets from potential cyber threats. Most data incidents occur because of human error, and erring is, more often than not, attributed to lack of awareness and proper training. In fact, IBM observed that 95% of all security incidents involve some kind of human error (IBM, 2014).

Apart from common mistakes such as weak passwords, people keep uploading and sharing tons of personal data to third parties without thinking who might end up collecting that information and how it can potentially be used against them. The lack of sufficient security awareness is one of the top vulnerabilities associated with employees. Humans do not act securely by nature, and secure behavior erodes with time, especially when there is a lack of underlying security awareness. This makes everything easier for any malicious party; there is no need to hack the system if you can compromise the human.

A recent example of a cybersecurity incident that affected critical infrastructure, particularly the healthcare infrastructure, is the ransomware WannaCry attack, which was launched at a worldwide scale. In the UK, the attack probably began when an NHS employee clicked on a malicious link (phishing attack). Thereon, the attack spread easily since large numbers of NHS organizations failed to act on a critical notice from Microsoft two months before the attack - a software patch which, had it been installed, would have prevented the attack. There is no doubt that the impact of WannaCry would have been much smaller or could have even been avoided if NHS employees had been properly prepared (Michalas, 2017).

But why are employees often unaware of issues related to cybersecurity? A main reason is the cost/benefit ratio: it's easy to articulate to decision makers the exact cost of equipment, why spending on it is needed and what will happen if they do not, but when it comes to enhancing user security awareness, things become much more complicated. Trying to calculate return on investment for these activities can be difficult, especially if the organization has never experienced an incident that can be directly attributed to lack of security awareness. Thus, there are no obvious tangible gains from investing in cybersecurity measures (Wright, 2015).

The complication starts already from university, where students take cybersecurity classes but, in reality, they are unaware of threats and how to prevent them, whilst they feel confident of the opposite (Gkioulos, 2017). Students tend to rely on their theoretical knowledge and feel capable of applying it to practical situations even if they have never experienced such. For example, a computer science student acknowledges that it is not wise to give access to personal data to whichever website, however they might disregard that if it is the only way to watch their favorite

show or buy something they are unable to find elsewhere. We are all, more or less, victims of this behavior, regardless of our educational background. One way to address this and to help students create associations between theory and practice is use a cybersecurity simulation tool for training groups of students. This could have a high cost, if simulation games that can be used for free in educational environments were not available. One such simulation game is CyberCIEGE, which was used to help us conduct the pilot study for the purposes of this master thesis and it will be further analyzed in the next chapters.

1.1 Cyber-security risk management

The rate at which technological development is advancing is introducing a constantly changing set of new challenges to the cybersecurity field. A growing range of cyber threats and vulnerabilities in critical infrastructures requires more than ever secure and resilient digital systems, in order to protect organizational and personal data from the aforementioned dangers.

As mentioned before, many security failures involve human error, which is most likely to occur when the human factor is not being taken into consideration. Therefore, given its multidisciplinary nature, cybersecurity could and should be researched by scientists of numerous scientific fields collaborating altogether to address the matter from numerous, different perspectives, including IT professionals, researchers, mathematicians, engineers, social scientists and psychologists.

Cyberspace is a vast, enormous territory which crosses geographical and governance boundaries, therefore, governments, as well as industry and academia, play individual and interdependent roles in protecting the privacy and security of data and networks in general. In order to ensure cybersecurity awareness, all the aforementioned parties need to make efforts by implementing best practices and policy frameworks. Risk assessment methods can be used to calculate risk against the value of the assets that need to be protected, and to measure the level of protection required. Such methods include strong passwords, two-factor authentication, biometrics, encryption, firewalls, penetration testing and others (Gagliardi, 2016).

Businesses worldwide are already developing information security risk management strategies, enabling them to take a systematic approach to risk management. This approach reduces the associated risks to sensitive information assets and protects them from cyber threats. Specialized training and expertise are needed during university studies, in order for the future employees to be adequately skilled for implementing such approaches in their workspace. However, it is not easy to teach such complex notions without using any practical, hands-on means.

From an educational aspect, an adequate method to be used for this kind of training, which could result in efficient learning outcomes for the trainees, could be integrating programs containing simulation interventions based on the simulation-based learning model which has its roots in

constructivism and constructionism, and encourages -among others- critical and proactive thinking, decision-making, problem solving and risk analysis skills.

1.2 The research problem

Simulation training is broadly used in a variety of scientific and professional domains such as health, the military or the navy and air forces (pilot simulators). Simulation-based learning should not replace real learning but enhance the learning experience for the users by actively motivating them to take actions, such as decision making, problem solving and managing risk. Moreover, it is more likely for learners to retain information when actively taking action, compared to when they hear or read new information. It has been proven that simulation increases engagement, by allowing interaction, critical thinking and experiential learning which is based on constructivism learning theories, known to motivate and activate learners towards creating knowledge themselves (Magennis, 2005). A key term to understand the reasons why simulation games have significant effects in learning is student-centered learning. By performing acts in a specifically defined context, learners are most probably motivated, thus engaged, and ultimately it is more likely that the intended learning outcomes are achieved (Arnett, 2017).

As far as cybersecurity is concerned, a simulation-based learning process would be more challenging, given that cybersecurity is an abstract concept. The difference from previously mentioned fields (such as health or air forces) is that a simulation for cybersecurity training should not only be about executing commands and following standard procedures but also about making decisions and implementing risk management strategies and scenarios. For example, what would an employee in a multinational company do if they accidentally opened a malicious attachment? How could that action be prevented, provided that the company cannot invest a large amount on cyber defense? These questions demand decision making and risk management skills to be answered, and sometimes there are multiple answers to each question, depending on the individual's background, prior knowledge and ethics.

The problem in fact is that students and employees lack security awareness even though they may have taken security classes during their studies or training programs. This gap between learning in theory and practically applying knowledge can be bridged using simulation-based learning. Yet, in what context can this lack of security awareness be addressed and what measures should be taken towards its elimination? One way would be training employees on site, according to each workplace's needs. A more efficient and proactive way though, would be raising awareness in a practical way through training, starting from university. IT and cybersecurity departments offer various security courses that do help students build basic knowledge about security which could however become concrete if applied in a real or real-like environment.

Supporting and facilitating security courses via a simulation training game such as CyberCIEGE could hence result in applying and contextualizing concepts that students have previously learned; helping them form a structured and practical mindset through decision making; engaging them to actively learn new concepts and useful information; and preparing them hands-on for a possible cyber threat or attack at their future workplace.

1.3 Aim and Objectives

This thesis' overarching aim was to investigate how simulation-based learning affects the knowledge of cybersecurity risk management. This breaks down in three sub-objectives:

i) to examine the educational potential & affordances of the serious game CyberCIEGE,
ii) to investigate how the integration of a serious simulation cybersecurity game in the learning process affects user behavior, technical knowledge and skills, and engagement of undergraduate IT students, and
iii) to determine whether the simulation-based learning theory's components can be implemented in a pedagogical instructional design's phases by the same theory, utilizing the serious game CyberCIEGE in a workshop.

By examining the efficiency of the game CyberCIEGE we were able to determine whether simulation-based learning is an adequate method for ensuring this knowledge and therefore diminishing the risk of malicious attacks in the future, by helping students apply their theoretical knowledge and giving them the chance to be skillful in a high risk situation. This will not only provide them with cybersecurity risk management knowledge but will also prepare them for a potential threat in their working field in the future.

1.4 Research questions

Our hypothesis is that simulation-based learning with the use of a simulation game will help raise cybersecurity awareness of undergraduate IT students. In order to examine if this hypothesis is true, we need to reflect on the following research questions:

- RQ1: What is the educational potential & affordances of the serious game CyberCIEGE?

- RQ2: Can the instructional design workflow based on the SBL enhance

  RQ2a: users' behavior
  RQ2b: technical knowledge and skills
  RQ2c: user engagement

- RQ3: Can the SBL theory components be implemented in a pedagogical instructional design's phases by the SBL theory, utilizing the serious game CyberCIEGE in a workshop?

Regarding the following:

RQ3a: activation of prior knowledge/experience (Introduction)
RQ3b-i: familiarization with the environment, the case, and the roles (Briefing)
RQ3b-ii: setting individual roles (Briefing)
RQ3c-i: participation in the simulation (Scenarios)
RQ3c-ii: practice of knowledge and skills (Scenarios)
RQ3d-i: comprehensive evaluation (Debriefing)
RQ3d-ii: reflection and critical analysis of the learning process (Debriefing)
RQ3d-iii: the knowledge and the learning environment (Debriefing)
RQ3d-iv: setting new learning goals (Debriefing)

1.5 Results and contribution

This Master thesis' aim was to is to investigate how simulation-based learning affects the knowledge of cybersecurity risk management. By examining the efficiency of the game CyberCIEGE we were able to determine whether and to what extent simulation-based learning could be an adequate method for ensuring this knowledge and therefore diminishing the risk of malicious attacks in the future, by helping students apply their theoretical knowledge and giving them the chance to be skillful in a high risk situation.

More and more cybersecurity projects, programs, campaigns and attempts to raise cybersecurity awareness and provide safer, fraudulent-free and harder to compromise environments are being developed and funded by international carriers, such as the ECHO project (European network of Cybersecurity centers and competence Hub for innovation and Operations) which is one of four Pilot projects, launched by the European Commission, to establish and operate a Cybersecurity Competence Network, the ECSC, an initiative of multiple European countries supported by the European Union Agency for Network and Information Security (ENISA), the STOP. THINK. CONNECT.™ public-awareness campaign proposed by APWG in 2009, a coordinated cybersecurity campaign aiming to raise public awareness and many more.

That is why it is becoming necessary to explore the field from and interdisciplinary aspect, emphasizing in the best possible ways to train internet users and to help raise cybersecurity awareness, implementing theoretical backgrounds and best practices into the training process and designing appropriate learning paths to provide efficiency, accuracy and engagement.

Chapter 2 – Literature review

In this chapter, we will provide a literature review analysis, to describe the learning theory behind our thesis' structure and research design, we will present the instructional model of simulation-based learning and its components and explain the instructional design we employed further on (ASSURE model). Moreover, what follows is a review on the state of the art of the concepts of: cybersecurity education, simulation-based learning in the learning process and engagement in serious games.

2.1 Learning Theory: Constructivism

As learning theories and technology have advanced, and educators have become more and more familiar with multimedia tools and integrate them into the learning process, there has been a focus to constructivist views and instructional designs, instead of behavioral ones. Many researchers have emphasized on the importance of open-ended, exploratory and authentic learning which can develop concrete and meaningful knowledge, and can be achieved through the implementation of constructivist theories into the learning process (Harper, 2000).

Constructivism focuses on the notion that knowledge is constructed through experience by the learner, during the learning process, which, according to this theory, is always an active process. According to A. Woolfolk (1980), (Woolfolk, 1980): "The key idea is that students actively construct their own knowledge: the mind of the student mediates input from the outside world to determine what the student will learn. Learning is active mental work, not passive reception of teaching" (p.485). According to E. Bredo (1997), learners do not just acquire knowledge through interacting with objects and situations, but actively construct it (Bredo, 1997).

Kolb's learning cycle is practically the basis of experiential learning. It consists of four stages: 1. Concrete experience, 2. Reflective observation, 3. Abstract conceptualization, 4. Active experimentation. Designing higher education classes in accordance with Kolb's cycle can be efficient, since, given that its basis is the theory of constructivism, it activates prior knowledge and introduces new situations (real-life ones), which lead to formulating new knowledge by associating already acquired concepts with the aforementioned newly introduced ones. It can increase cognitive curiosity and learner motivation as it establishes a deep approach to studying and learning (Wach-Kakolewicz, 2016).

Simulation-based learning is based on constructivist theories of learning. As simulation design and use have developed over the years, Bliss and Ogborn (Bliss, 1989) describe computer based simulations as "programs in which the computer acts as an exploratory tool, supporting a real world activity while facilitating user understanding of the processes, which may be otherwise inaccessible, in complex dynamic systems" (Harper, 2000, p. 119). This viewpoint is accordant

with the constructivist learning theories. Experiential simulations focus on immersing learners into a real-life situation where they have defined roles and goals. Their components follow as described by Gredler: "(a) a scenario of a complex task or problem that unfolds in part in response to learner actions, (b) a serious role taken by the learner in which he or she executes the responsibilities of the position, (c) multiple plausible paths through the experience, and (d) learner control of decision making" (Gredler M. E., Educational games and simulations, 1996, p. 523).

As mentioned in previous chapters, serious games hold an important role in engaging and motivating learners with regard to the learning process, and are becoming an aiding tool for many educators who wish to upgrade their educational program and involve students with active, exploratory and experimental learning, trial-and-error and problem-solving techniques which in turn will help them develop respective skills and enrich their knowledge (by also helping them learn *how* to acquire knowledge/new concepts). Research shows that game-based learning is more effective than traditional, passive learning, in communicating concepts and allowing exploratory skills to emerge (Kafai, 2006), (Papert, 1991).

In this multifaceted context, it can be overwhelming for educators to make use of digital games in the learning process. It is thus, critical, to consider the core characteristics of games and how these can be employed to design a learning experience for 21st century learners, already familiar with interactive technologies and gaming for entertainment purposes. In games, players interact with a contextualized, constructivist environment where their decisions and actions have a direct impact on the game's progress and outcome (Marone, 2016). Within this scope, situated cognition claims that both thinking and learning are the consequence of the interaction between an individual and their environment or social setting (Anderson, 1996). Further to this notion, declarative and procedural knowledge are interconnected (knowing *that* and knowing *how*), as knowledge is constructed through meaningful practices in a situated context (Lave, 1991).

2.2 Instructional Model: Simulation-based learning

The instructional model which was chosen for this thesis is that of the simulation-based learning, whose phases are presented below, as suggested by Joyce et al's *Learning through Simulation model*:

1. **Introduction:** During this phase, the most important concepts and course topics are presented, and the simulation is explained to the students. It includes explanations of the course's organization and the conceptual framework is also introduced.

   Components: activation of prior knowledge/experience

2. **Simulator briefing:** During this second phase, the instructor explains the scenarios (goals, roles, rules, elements, procedures): students are informed about what is expected of them. Examples and presentations by the researcher are useful during this phase.

   Components:

   i) familiarization with the environment, the case, and their roles
   ii) setting individual roles

3. **Scenarios:** Participation in the simulation scenarios. The researcher monitors, facilitates the procedure, and guides the students through it. Students practice their skills and knowledge by engaging in a hands-on experience.

   Components:

   i) participation in the simulation
   ii) practice of knowledge and skills

4. **Debriefing:** Evaluation and analysis of the learning process, the knowledge and the learning environment. Feedback from the students' end with regard to their own learning and possible setting of new learning goals.

   Components:

   i) comprehensive evaluation
   ii) reflection and critical analysis of the learning process
   iii) the knowledge and the learning environment
   iv) setting new learning goals

2.3 Instructional design: ASSURE model

The ASSURE model consists of 6 stages: **A**nalyze learners, **S**tate objectives, **S**elect media & materials, **U**tilize media & materials, **R**equire learner participation, **E**valuate & revise(Figure 1).

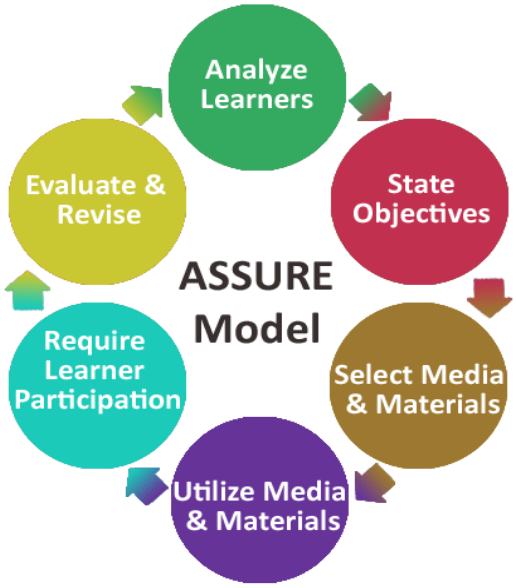


Figure 1. Instructional design: ASSURE model stages

It was selected to be the instructional design according to which we planned our intervention, as it was deemed adequate to assist us in designing and developing an appropriate training session according to our needs and the intervention's structure. Each of the model's stages breaks down to sub-stages, which we'll analyze and associate with our own actions and the workflow's process in Chapter 3. The stages and sub-stages of the model can be viewed below:

- **Stage 1: Analyze learners**

A1. Determine learners' attributes (age, abilities, gender)

A2. Determine learners' prior competencies

- **Stage 2: State objectives**

S1. State learning objectives

- **Stage 3: Select media & materials**

S1. Pick strategy, technology and tools based on the objectives set previously

- **Stage 4: Utilize media & materials**

U1. Prepare technology/media/materials

U2. Prepare environment

U3. Prepare learners

U4. Provide learning experience

- **Stage 5: Require learner participation**

R1. Actively engage students in the learning process

R2. Ensure active participation

- **Stage 6: Evaluate & revise**

E1. Data collection

E2. Data analysis

E3. Results & Summary

2.4 Cybersecurity Education

As already mentioned, the cybersecurity field is becoming more and more popular and acclaimed, thus the need to extend research and promote cybersecurity education from an early age. Steps are being taken towards this initiative all around the world by many professionals of the field. Initiatives such as case studies employing serious games, gamification and simulations have emerged and increased rapidly in the last few years.

Confucius' quote: "I hear, and I forget. I see and I remember. I do and I understand." seems more accurate than ever now that we're constantly bombarded with new knowledge and information

for which, in order to be retained, practical involvement is deemed -if not imperative- undoubtedly helpful for any learner.

This is the reason why many cybersecurity educators and researchers nowadays select gaming and simulations as a means to enhance their learners' knowledge acquisition and to help them achieve their learning objectives on a more holistic level. Whilst most training interventions focus on physical security, steps have been taken recently to give importance to computer infrastructure security, on which many important sectors rely, such as air traffic or banking traffic. With malicious attacks occurring more often than not in the last years, and with the number of security breaches constantly increasing (by 11% since 2018), more and more companies invest in digital training for their employees. Let's admit it; it's easier, time-efficient, engaging and relevant to make someone a cybersecurity expert using technology, given the field's digital nature in the first place.

Over the last decade, the number of computer games has increased and, more specifically, serious games are becoming more and more popular in association with cybersecurity training. One very interesting research was conducted by Hendrix et al (Hendrix, 2016): the researchers identified 28 papers and conducted an analysis of cybersecurity training games employed by the authors of these papers. Most games were used to raise cybersecurity awareness within the general public. Findings showed that the trainees' assessment with clearly described methods and outcomes was only conducted in 11/28 studies. These games were: Anti Phishing Phil, 'Security games by Next Generation Security (NGSEC)', CyberCIEGE, PicoCTF, Control-Alt-Hack, and 'A series of interactive visualisations', and these studies reported positive results, i.e. proving a contribution to training or raising cybersecurity awareness.
Surprisingly, 6/28 did not use any evaluation method and a further 6 involved an evaluation which was superficial method-wise or results-wise.

While these studies indicate how serious games can be effective training tools, they also prove how immature the field is, in need for more innovative solutions and interventions, as well as meticulous evaluation and assessment to determine the learning outcome, ascertain any challenges and limitations and address them in order to eliminate them in the future. It is clear that more prosperous studies are needed, including a sizeable number of trainees and long-term interventions which can provide measurable outcomes and tangible results. What should be noted here is that, according to that same research, CyberCIEGE was the only game which appears in both academic studies and product-related searches.

Another study, focusing on US demand, describes how the National Science Foundation (based in the US) has established grants to reward projects promoting cybersecurity education (Li, 2016). The paper describes the idea of CTF (Capture-the-Flag) events, to increase awareness – especially that of the upcoming generation. These events are practically competitions held worldwide, which bring together various teams of young researchers who compete against each other in cybersecurity-related challenges. The participants are mainly trained to protect their systems from malicious attacks.

2.5 Simulation Based Learning - State of the Art

There are certain causes for the massive increase in information technology security incidents, and these are the growing numbers of electronic data, smart mobile devices, organized cybercrime groups, intelligent external and internal security threats, difficulty in tracing attackers and little cybersecurity knowledge among users (Aloul, 2012).

Even though governments have introduced laws to fight against cybercrime, which have been implemented by many countries in Europe, Asia and North America, incidents still occur, mainly because of user mistakes, which are considered one of the top threats regarding cybersecurity in organizations globally, as mentioned in Chapter 1.

Traditional learning methods are beginning to fade nowadays, with the students being more and more up to date and, more often than not, more technologically advanced than their instructors. The intrusion of technology in our lifestyles has begun to have an impact in the way we learn, since both students and educators demand more intriguing and more interesting ways of receiving and transmitting knowledge, respectively. A three-hour lecture is considered outdated, even with the use of vivid presentations or activities involving a computer.

This rapid technological advance is leading educators to use alternative pedagogical approaches in their classrooms, and to reach out to more interactive and intrinsic methods of teaching, in order to maintain motivation and increase quality, by providing meaningful and lasting learning. As referred in the study of Corinne Auman, the author decided to alter her way of teaching from lecturing to using simulation games due to the fact that the feedback she received from her students on the lectures was not ideal (Auman, 2011).

According to the same study, Lean, Moizer, Towler, Abbey, identified the three obstacles that educators come across when trying to implement new pedagogies: suitability, resources and risk. Suitability is defined by the effectiveness of the teaching pedagogy in achieving the intended learning objectives and the availability of materials for such a pedagogy. Resources are about planning and implementing the pedagogy, as well as available tangible (material, infrastructure, budget) and not tangible (creativity) resources available. Finally, risk means estimating the variables of the new teaching method such as lack of control or student reactions.

One main reason for educators to try changing their teaching methods is uninterested students who show no will to engage and participate to the learning procedure. This stagnancy normally alerts educators, who then try to find alternative ways of teaching. According to the book *The Power of Mindful Learning* (Langer, 1997) learners are attracted to novelty, therefore pay active attention to novel situations, something that increases both performance and retention of information, thus leading to more effective learning.

According to R. Dorner et al. (Dorner, 2015), simulation-based learning, which owes much to historical military training practices, started being considered as a necessity in the 1950s, when

organizations began adopting simulation-based practices, given the fact that they could easily be used to accurately reflect real-world social, economic and political situations. Dorner et al. give an interesting insight regarding the evaluation of serious games, which they consider the offspring of simulations: from physiological measurements to audiovisual technologies, in-game assessments such as game analytics, or specific evaluation methods focused on player experience such as the Gameplay Experience Questionnaire (GEQ). Moreover, a combination of methods can be used, such as combining qualitative observations and self-reports. Another example of evaluating a serious game is comparing an educational game to traditional instructional methods.

Simulation-based learning has been popular in many fields such as health, chemistry or engineering. Several studies have been conducted measuring the effectiveness of simulations in the respective fields. For example, a comparative study conducted at DeVry University in Illinois explored the impact of the use of computer simulation design methods on students' problem-solving skills for circuit construction in an undergraduate ECET (Electronic Computer Engineering Technology) course (Taher, 2014).

In order to address the growing industry demands, new tools and modern methods need to be integrated into the engineering curricula, which can be a challenge for most educational faculties since the equipment needed would require a considerable amount of time and financial resources to be effectively incorporated in the labs. Therefore, according to the aforementioned study, simulations and virtual experiments could offer a cost-saving, facilitating solution, along with multiple other advantages.

Furthermore, another scientific field where simulations have been vastly used and their application has been examined and has proven to be effective, is health. Many studies have been conducted in order to further research and examine the learning outcomes of simulation based learning in medicine, such as several case studies in the Nordic countries, which have reached conclusions regarding technical and non-technical skills as well as the educational aspects of this method being used in the health field (Husebø, 2018).

The results have in fact demonstrated that skills can be improved by computer-based simulations. In these studies, the process of learning technical skills through simulation was researched in various contexts to measure and evaluate skills, educational methods, and safety as well as quality of service.

Whilst simulations have been used effectively in the aforementioned scientific fields, they have not been yet introduced widely as a means to enhance cybersecurity knowledge. Simulators and simulation games about cybersecurity have been around for years, however, they have not been used by a large majority of instructors and educators, nor has there been further research as per their effectiveness in cybersecurity education. For example, simulators such as CyberProtect, MAADNET, CyberCIEGE, DETERlab, S-vlab and others, have been used effectively and comprise clear learning objectives. Even though these numerous tools could be qualified to be used in an

experiment such as the one presented in this thesis, we have opted for CyberCIEGE, which we will further analyze below.

What is more, in a research using an AR serious game to raise cybersecurity self-awareness in high-school students which was conducted, the goal of the game is to defend the victims (classmates) of the security threats that "rain upon" them (identity theft, over-sharing, malware) by using shields which represent the countermeasures (robust passwords, multilevel security, healthy skepticism) to block each threat with the right shield. A survey was completed by the students after the presentation to evaluate its results; the questions they had to answer were about the knowledge they gained, how vulnerable they are to the threats explained, how capable they are to defend themselves and their confidence in technology. The use of the serious game did not have a significant influence on the acquisition of knowledge since there were not any new concepts introduced, but it did indeed affect the students' self-awareness and decreased their confidence in technology, which was an intended result (Salazar, 2013).

Another very interesting approach was conducted by Valdemar Švábenský et al; the undergraduate students who participated created a serious cybersecurity game deployed at a cyber range, which allowed emulating real threats and attacks in a controlled environment. Then their peers played the game and the overview was presented during an open day event of the faculty. The concept focused on inducing adversary thinking, a crucial skill for cybersecurity experts who need to be proactive and able to think like an attacker to set up effective countermeasures. The sessions included a combination of lectures, student hands-on practice, and group work. By integrating labs with lectures, using cooperative learning and project-based learning, the students were able to have an authentic experience by exercising adversary thinking in real-world settings. One major advantage is that they could see the practical results of their work during the semester and also at the end, when presenting their game to their peers. Feedback from attendees of the Open Day event which took place after the finalization of the project showed that it even attracted some of them to the cybersecurity field (Švábenský, 2018).

Kavak et al (Kavak, 2016)conducted a study to characterize and analyze simulation tools used in the cybersecurity field. In the context of cybersecurity simulation, a scenario is the description of an actual or potential cyber incident (e.g. a cyber-attack). They use the example of the attack against the company RSA (in 2011) to explain how an actual incident can provide useful and adaptable scenario elements: "The attacker sent two different phishing emails over a two-day period…to two small groups of employees… The email subject line read '2011 Recruitment Plan'. This was intriguing enough for one of the employees to actually pull the email out of their Junk Box and double-click on the email attachment… The [attached] spreadsheet contained a zero-day exploit that installs a backdoor through Adobe Flash vulnerability (CVE-2011-0609)… The attacker first harvested access credentials from the compromised users … performed privilege escalation on non-administrative users in the targeted systems, and then moved on to gain access to key high value targets, which included process experts and IT and Non-IT specific server administrators… The attacker then used FTP to transfer many password protected RAR files from the RSA file server to an outside staging server… RSA detected this attack in progress" (Kavak, 2016). Some scenario elements can be extracted, such as:

- Attacker
- Users-target of the attacker
- System and data-target of the attacker
- Interactions between the attacker, the users and the employees
- A network infrastructure that interconnects the system and humans

These elements can be further categorized into two groups: cyber systems and actors. One of the simulators analyzed in the same study is OMNET++, which models networks used to test distributed denial of service (DDoS) attack and defense mechanisms based on a multi-agent structure. It is actually becoming one of the most popular ones as it's able to manage several scenarios at once, plus, it offers a large number of frameworks (e.g. INET, MIXIM). A case study which was conducted using this particular simulator, proposed NETA, a novel framework that was used to simulate implementing cyber-attacks (Sanchez Casado, 2013).

Another simulator tool that has been used broadly and effectively in cybersecurity training projects is DeterLab: The DETER project's goal is to improve and advance cybersecurity research and education. For this purpose, educators worldwide use DeterLab, which is public, free experimental facility which provides tools and capabilities using built-in scenarios and data collection mechanisms (Benzel, 2011).

Cognitive and behavioral modeling can be embedded in cybersecurity education, namely cognitive models such as network users, defenders and attackers that interact with the same software that actual humans interact with, and can explain or even predict cyber user behavior (Veksler, 2018). This type of simulations requires generic knowledge, as well as basic cybersecurity procedures knowledge, and cognitive processes; cognitive architectures vary in capabilities, implementation of cognitive processes, modeling languages etc. This is the reason why some are preferable to others, for example, both Soar and ACT-R architectures employ reward-based learning. Other models simulating user behavior are developed models that predict how a user will behave in a web browser based on current goals. There are models which focus on social network use, chat behavior, team performance and email activity. The aforementioned models are more likely to be efficient when tailored according to the subpopulation being modeled: it is best to employ the target group's information such as age, gender, education to set up relatable models.

Simulation-based learning has proven to be effective with students and professionals as it is highly based on trial and error within a safe environment which allows learners to make decisions and understand their consequences. It is also motivating and engaging because it promotes learning by doing, thus actively participating in a certain cause. It is very important to highlight the multidisciplinary nature of the cybersecurity field, in order to understand why it is difficult to provide a holistic simulation training and retrieve measurable and significant data of the process: by the term *cybersecurity* one does not simply refer to the security of data or systems involved, alone. In addition to that, it is about concepts, policies, risk management approaches that help

ensure data and involved parties' protection (thus humans) from any harm that can occur from a security breach (Veksler, 2018). Given this fact, we can only conclude that the human factor is and will be at risk, for as long as it remains a risk factor; and one way of altering this is to raise awareness. Interestingly enough, although simulations have been used for various purposes and in various fields, measurable indicators to determine what effect they have concerning critical infrastructure cybersecurity awareness are not available.

2.6 Engagement in Serious Games – State of the Art

Learning through playing is proving to be an efficient method for training not only children, but adults in need of training of all sorts. By combining fun and learning via the use of a serious game in education and/or in corporations where employees need to be trained adequately to perform in their work environment, it becomes easier to conceptualize specific notions and increase productivity. Moreover, since they are visually pleasing, they ensure the user's attention and thus enhance knowledge retention.

According to the eLearning industry website (Hughes, 2019), a serious game needs to have clear and concrete learning goals which should be communicated with the players to help clarify what it is they will learn and which areas they need to improve in. Also, it needs to have sets of rules, to make sure users will not get lost or that the game does not become too easy for them. This could result in a negative experience and no information retention. A third aspect to consider is implementing a feedback system: feedback needs to be relevant to the users' previous actions and thoroughly explain why each action is correct or wrong to promote problem-solving skills in real-life situations. Making sure that the users' engagement is present is key, and the real challenge is keeping the game difficult enough for them to be curious and excited to finish it, but at the same time ensuring it is not so overwhelming that they have serious difficulty in completing it. In relation to this, the information provided in the game should be relatable, to ensure that players will reproduce and use the skills they learnt in their everyday job, in real life. What is more, a serious game needs to have a flow, be designed to be adaptive and flexible, in case changes are needed at some point in the future. Last but not least, a very important game element that should be implemented is public recognition: if the game's successful completion provides a reward (not only a virtual one, but a compensation for the best player's performance - for example a trophy), and this is known beforehand, it should increase their motivation and boost their confidence.

In virtual games' research, concepts related to the idea of player engagement are immersion, involvement, presence and flow. The notion of engaged behaviors is also used to help teachers in assessing learners' engagement, however their nature or scope remain unclear. According to Jari Takatalo et al., "In learning or entertainment games, continuously identifying and analyzing learners' or players' engagement (i.e., session after session) and under ecologically valid

conditions (i.e., the activity is performed in its natural environment and in authentic conditions) is crucial (Takatalo, 2011)." In the education field, engagement can be considered as the "behavioral intensity and emotional quality of a person's active involvement during a task" (Reeve, 2004).

Perski et al., defined engagement as: the extent of the learner's involvement, and a subjective experience characterized by affect, attention and interest (Perski, 2017). When assessing the effectiveness of a serious game in education, engagement is a major factor to consider, as, along with realism, it is one of the challenges in serious games. It can be measured using real-time observation, interviews and questionnaires. According to Mihaly Csikszentmihalyi (Csikszentmihalyi, 1990), engagement is what makes learning fun, as it refers to one's emotional state in which continuation of playing does not enforce any effort. Two dependent factors for engagement are: user characteristics and environmental factors. The first one depends on individual notions (e.g. previous experience, background, personality, demographics), whereas the latter has to do with the setting where the game is played and the game elements.

According to Ellen Schuurink (Schuurink, 2008, p. 3): "Dickey (Dickey, 2005) explains how to design a game for instructional learning that engages users, identifying the following criteria: focused goals, clear and compelling standards, protection from adverse consequences from initial failures, affirmation of performance, affiliation with others, novelty and variety, choice and authenticity. In a study of student engagement on simulations, Davies (Davies, 2002) identifies the complexity of the simulation, the learning environment as a whole, and overcoming the 'barrier' of navigational opacity as important factors, in addition to sufficient time to get engaged."

The same study claims that, apart from the game elements above, which are considered critical requirements for engagement, specific characteristics of the game environment such as sound and dynamic elements can also contribute to the game experience and thus to the engagement of the user. Sound can determine perceived realism, foster attention and recognition, create a sense of place, increase enjoyment, and improve the sense of presence, performance and memory in virtual environments. However, sound can have a negative influence on performance. It has been also shown that visual dynamic elements are important factors for the external, ecological and incremental validity of the environment. Even though the study found that sound and dynamic elements do not directly trigger engagement, when compared to other elements such as challenge, discovery, feedback, and control, they do support the user's navigation.

Another systematic review (Maheu, 2018), collected evidence regarding the effectiveness of serious games and the impact of design elements (DEs e.g. points, difficulty adaptation, storyline) on engagements and learning outcomes of healthcare professionals and students. While it is believed that engaging in a gameplay will urge the learner to become involved and complete the in-game challenges, thus, improve their educational outcomes, there are concerns that DEs can be distracting and negatively affect the learning outcomes of the game. What is interesting is that the optimal DEs' integration in serious games remains unknown. Given that a study on the impact of DEs of serious games on engagement and educational outcomes has not been

conducted yet, this review's objectives were the following: to identify and analyze the best available evidence on the effectiveness of serious games on both engagement and learning outcomes of healthcare professionals and students, and to demonstrate which DEs have been implemented in serious games designed for this purpose, as well as their impact on engagement and learning outcomes.

According to a study conducted to measure engagement in manufacturing and engineering (36 engineers and project managers of the Carel Company participated), traditional learning methods are ineffective compared to applying advanced learning technologies to train employees. The results of the study showed a higher level of engagement when the employees played the serious game SBCE (Set-Based Concurrent Engineering), (Pourabdollahiana, 2012).

Generally, in research related to serious games and user engagement, the latter is mostly measured via qualitative feedback data through questionnaires, either during classroom time or during intervals. There is one project, though, which used IoT (Internet of Things) to introduce attendance as a measure, achieved through a hybrid sensor network: the project suggests a computer algorithm via which user behavior and judgement can be monitored in a non-intrusive way using network distributed sensors and put into a serious game (Henry, 2017). This data algorithm can be embedded in serious games as it uses a game's points system to portray results (by monitoring attendance and punctuality using IoT, it turns this data into a score, where a high value means high engagement levels). This study was not validated using real students but a simulation with personae and spreadsheet software was conducted, thus the results are preliminary. However, such an implementation is promising and constitutes a contemporary approach to measuring and encouraging student engagement via serious games and IoT.

When assessing the effectiveness of serious games, identifying the levels of engagement is an important factor. A proposed approach to transforming low-level behaviors (such as mouse clicks) into contextualized high-level behaviors was applied in a study employing a serious game for training purposes within the health sector. As described in the study, interaction traces (e.g. mouse clicks) turn into meaningful data corresponding in high-level traces (e.g. activities). These high-level traces correspond to engaged behaviors. Therefore, a behavior corresponds to a chain of actions performed by the user. In the study, this approach was used to identify engagement in a serious game related to clinical education: the sepsis fast track serious game. The game is characterized as a point-and-click one, i.e. all game interactions are performed by combining clicks in game objects (e.g. nurse, patient). An example of the the game's flow is the following: the actor (physician) needs to perform certain actions (ask the patient about their symptoms, run tests) to confirm that the patient has sepsis. These actions are reflected in the game by sequences of clicks, moves and decisions (game actions). For these primary actions to be transformed to important actions there are several rules of transformation. This work can potentially provide an idea on the player's commitment and engagement levels in gameplay during the learning process (Ribeiro, 2014).

Regarding engagement in cybersecurity serious games in particular, participants of a study for the purposes of a MSc thesis rated the game *ThreatBattle* below average on engagement

(responding to GEQ questions), even though the study concluded that the game positively influenced their attitude and behavior (Grevelink, 2015). It is not surprising that more and more institutions and companies choose gamification and serious games in their trainings, since game elements are more likely to provide a fun, immersive learning experience, far more engaging than traditional methods.

2.7 Summary

Summarizing, it is clear that the field of cybersecurity education is a fast evolving one, in constant need for research and application of best practices to ensure it can be robust in the near future. It is common to use simulations to train Internet users (regardless if they are IT experts or not), as there are many simulation tools available for this purpose even free of cost. Serious games can also be used adequately, but the concept of engagement in serious games used to raise cybersecurity awareness has not yet been vastly explored. It is safe to say that the research gap remains regarding cybersecurity education as a whole. In the next chapter, we shall provide a thorough analysis of our case study, in relation with this thesis' aim and objectives, and the research questions we have mentioned already in Chapter 1.

Chapter 3 – Methodology: An empirical study

In Chapter 3, we will firstly clarify our aim, our research questions and the methodology we selected to deliver our project. Moreover, we will provide a descriptive analysis of the research design, the educational design (workflow processing), the research and data collection tools used, as well as a description of the sample. An analysis of the simulation tool CyberCIEGE (which we used during our experiment phase) is also included in this chapter.

3.1 Aim and Objectives

This thesis' overarching aim was to investigate how simulation-based learning affects the knowledge of cybersecurity risk management. This breaks down in three sub-objectives:

i) to examine the educational potential & affordances of the serious game CyberCIEGE,
ii) to investigate how the integration of a serious simulation cybersecurity game in the learning process affects user behavior, technical knowledge and skills, and engagement of undergraduate IT students, and
iii) to determine whether the simulation-based learning theory's components can be implemented in a pedagogical instructional design's phases by the same theory, utilizing the serious game CyberCIEGE in a workshop.

Following the thesis' objective (and sub-objectives), we shall proceed to the description of our research questions, which emerged from the objectives described above.

3.2 Research questions

Our hypothesis is that simulation-based learning with the use of a simulation game will help raise cybersecurity awareness for undergraduate IT students. In order to examine if this hypothesis is true, we need to reflect on the following research questions:

- **RQ1:** What is the educational potential & affordances of the serious game CyberCIEGE?

- **RQ2:** Can the instructional design workflow based on the SBL enhance
  - **RQ2a:** users' behavior
  - **RQ2b:** technical knowledge and skills
  - **RQ2c:** user engagement

- **RQ3:** Can the SBL theory components be implemented in a pedagogical instructional design's phases by the SBL theory, utilizing the serious game CyberCIEGE in a workshop?

Regarding the following:

- **RQ3a:** activation of prior knowledge/experience (Introduction)
- **RQ3b-i:** familiarization with the environment, the case, and the roles (Briefing)
- **RQ3b-ii:** setting individual roles (Briefing)
- **RQ3c-i:** participation in the simulation (Scenarios)
- **RQ3c-ii:** practice of knowledge and skills (Scenarios)
- **RQ3d-i:** comprehensive evaluation (Debriefing)
- **RQ3d-ii:** reflection and critical analysis of the learning process (Debriefing)
- **RQ3d-iii:** the knowledge and the learning environment (Debriefing)
- **RQ3d-iv:** setting new learning goals (Debriefing)

3.3 Methodology

Quantitative experimental research was used as our research methodology. The definition of this type of research, is one or more variables are manipulated to determine their effect on a dependent variable. There is a cause and effect relationship between the variables, this is the reason why it is important for experimental research to define that the results (effects) observed from an experiment are due to the cause. It is also important to always know which variables are to be measured. In our case, we used a quasi-experiment, where the researcher influences something (i.e. implements a simulation game into the traditional learning process) to measure the consequences of this action (i.e. the effect of this intervention in different aspects).

Quantitative research is used to reach conclusions based on statistical analysis of collected data through several means such as questionnaires, surveys etc. Its main objective is to prove the relationship between a variable and another within a population. There are two types of quantitative research design, descriptive and experimental. We chose the latter for our methodology, given the need to establish causality between two variables. As mentioned previously, there is a cause and effect relationship between the variables, that is the reason why it is important for experimental research to define that the results (effects) observed from an experiment are due to the cause. This methodology has been chosen by various researchers who have conducted similar studies, in the cybersecurity field and, in general, it is common when simulation-based learning is employed.

In *Experimental Research Methods* (Ross, 2003), Ross and Morrison describe the steps of conducting experimental studies in educational technology:

Step 1: Selecting a topic:

Choosing a general area of interest and finding a researchable problem to focus on.

Our case:

The general area of personal interest chosen was cybersecurity education, due to the researcher's personal interest, as well as the eminent need for more research to be made in the field.

Step 2: Identifying the research problem:

The problem needs to be of importance to the scientific field. Research and literature review are necessary for the research problem to be properly defined during this step.

Our case:

The research problem was already known, since there has been an eminent need of raising cybersecurity awareness, as described in Chapter 1.

Step 3: Conducting a literature search

During this step, more thorough literature research is required to find state of the art studies, focus on their design, methods, procedures and findings, to construct a study according to best practices.

Our case:

Our literature search revolved mainly around cybersecurity education, simulation-based learning in cybersecurity and serious games used in cybersecurity education, taking into consideration the theoretical background of the simulation based learning theory, the constructivist theory of learning and the serious games' integration in the learning process as described in previous studies.

Step 4: State the research questions

The most critical step, where the researcher needs to decide which questions they want to be answered. The research questions will define the research design and methodology, the procedure to be followed and the objectives to be set. They are key to the research itself as they need to be answered by the end of the study.

Our case:

Our research questions emerged from the research problem, therefore, after careful literature research and consideration of the scientific field's current needs and research gaps, it was decided that three main questions will need to be answered for the purposes of this study:

- **RQ1:** What is the educational potential & affordances of the serious game CyberCIEGE?

- **RQ2:** Can the instructional design workflow based on the SBL enhance
  - **RQ2a:** users' behavior
  - **RQ2b:** technical knowledge and skills
  - **RQ2c:** user engagement
- **RQ3:** Can the SBL theory components be implemented in a pedagogical instructional design's phases by the SBL theory, utilizing the serious game CyberCIEGE in a workshop?

Regarding the following:

- **RQ3a:** activation of prior knowledge/experience (Introduction)
- **RQ3b-i:** familiarization with the environment, the case, and the roles (Briefing)
- **RQ3b-ii:** setting individual roles (Briefing)
- **RQ3c-i:** participation in the simulation (Scenarios)
- **RQ3c-ii:** practice of knowledge and skills (Scenarios)
- **RQ3d-i:** comprehensive evaluation (Debriefing)
- **RQ3d-ii:** reflection and critical analysis of the learning process (Debriefing)
- **RQ3d-iii:** the knowledge and the learning environment (Debriefing)
- **RQ3d-iv:** setting new learning goals (Debriefing)

Step 5: Determine the research design

The stage where an adequate research design and methodology need to be determined for the study to be completed with a scientific value. The research design will be decided based on the type of study and on the results that we want to have.

Our case:

Quantitative experimental research was decided as our research methodology due to the fact that we conducted an experiment and there was the need to establish a cause-effect relationship between variables. More information regarding the Methodology can be found in Chapter 3.

Step 6: Determine methods

Determining subjects/participants, materials/resources, data collection instruments, procedures.

Our case:

Our study sample were 13 undergraduate IT students, the resource employed was the serious game CyberCIEGE, and the experiment was conducted in a computer lab, embedded in a workshop of a cybersecurity curriculum course. The instructional design was decided to be as per the ASSURE model's guidelines. For our data collection we used live observation and pre-survey/post-survey questionnaires. Data was analyzed using IBM's SPSS to find means and reach conclusions accordingly.

Step 7: Determine Data Analysis techniques

Statistical analysis procedures vary depending on the research questions and the type of data. Clearly defined research questions are needed to choose adequate analysis methods.

Our case:

Due to our sample being small, most data analyses were based on means and frequencies (answers' distribution). Observation data were also used as additional aid.

For our specific needs, we performed a quasi-experiment, i.e. we influenced something (integrated a simulation game into the traditional learning process) to measure the consequences of this action in correlation with three metrics: user behavior, technical knowledge/skills and engagement.

For our research questions to be answered, we had a sample of 13 undergraduate IT students. They were involved in the experiment and took part in the simulation game, by completing two questionnaires, one prior to playing the game and one after having played it.

The pre-survey questionnaire was distributed and completed by each student individually, before conducting the experiment. The purpose of the questionnaire was to define how the students self-assess their cybersecurity awareness and if this assessment is in fact reflected in their true knowledge. To do so, the questionnaire did not rely only on oneself's opinion, but it included technical questions as well. By analyzing these data, we were then be able to conclude if the students were cybersecurity aware prior to playing a related game. Indeed, they were, as analyzed in Chapter 4, which was expected given the fact that they are all IT students and already have knowledge of basic cybersecurity concepts from personal experience and previous semesters.

CyberCIEGE was selected to be used in our experiment to test (among others) whether cybersecurity's risk management knowledge and engagement can be raised via a simulation game. The game was played by the students individually in a computer lab, in order to avoid distractions.

Lastly, the results were measured using the post-survey questionnaire which defined how our research questions are answered. In relation to awareness being raised or not, another important aspect we wanted to examine is whether the students are the levels of users' engagement with the game and thus, the cybersecurity field. In order for us to measure engagement, the students also completed a GEQ (Game Engagement Questionnaire) which was embedded in the post-survey questionnaire as a different section.

3.4 Descriptive flow of the research design approach

In this chapter, we will explain how the intervention was designed (from a research and an educational aspect) and the steps of how it was implemented in the learning process as an empirical study.

3.4.1. Research design

According to the proposed methodology, and in order to investigate the research questions, a research project was designed, i.e. the intervention we implemented in the learning process for the needs of this Master thesis. The research design included the following three distinct phases:

Phase1: Preparation

- Researcher: Establishing the problem, setting the goals, selecting the tools, collecting learner characteristics (e.g. demographics), defining learners' prior knowledge.
- Learners: Completing the pre-survey questionnaire (each student individually).

Phase2: Intervention

- Researcher: Preparing the lab, presenting the project to learners, observing, providing assistance, guidance and facilitating the process.
- Learners: Participating in the experiment using the serious game CyberCIEGE by playing live for 1:30 hours.

Phase3: Evaluation

- Researcher: Collecting data, analyzing data, providing results.
- Learners: Completing the post-survey questionnaire (each student individually).

The figure below presents the phases of the research design, as described above (Figure 2):

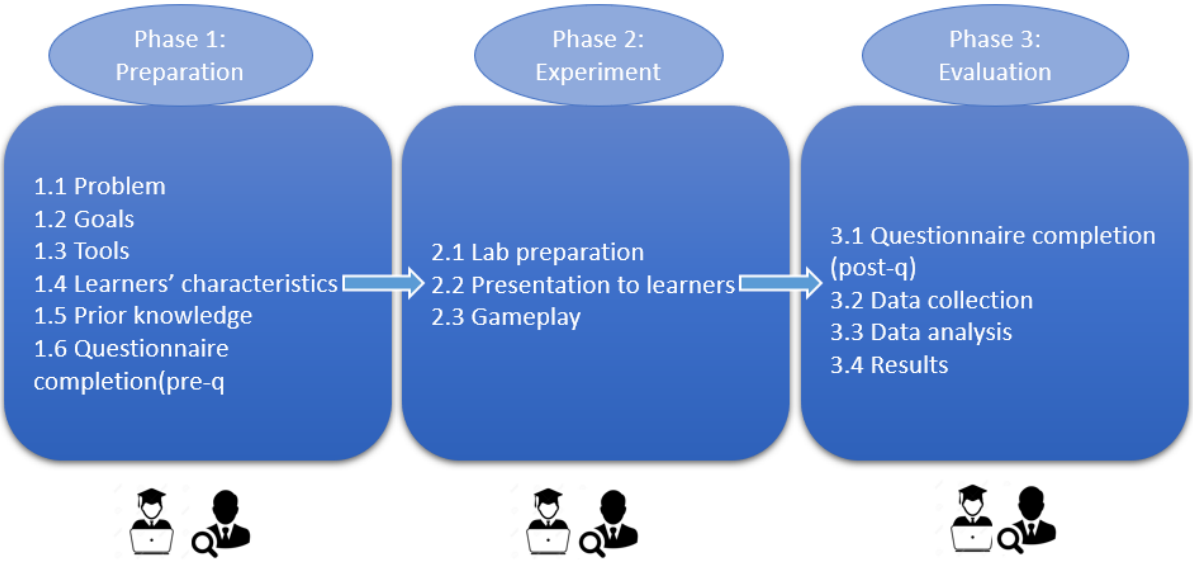


Figure 2. Research design phases

Having described the educational phases, we continue to chapter 3.4.2, where we will further analyze how the instructional ASSURE model was employed and implemented in the research design.

3.4.2. The application of the ASSURE model to the research design

With the help of the ASSURE model we divided our approach into 3 phases and matched them with the model's stages and substages. For each stage we determined separate research procedures in accordance with the substages. In particular, the first phase of the research design (**Preparation**) comports with the stage **A (Analyze learners), S (State objectives)** and **S (Select media and materials)**. The following table (Table 1) presents this matching in detail:

Table 1. The Assure Model matched with the Research Design and Research Procedure (1)

Research Design	Assure Stage	Assure Substage	Research Procedure
Phase 1: Preparation	**Analyze learners**	A1. Determine learners' attributes (age, abilities, gender)	A1. Our learners are undergraduate IT students in the department of Digital Systems at the University of Piraeus, 20-25 years old, males (12) and females (1).
		A2. Determine learners' prior competencies	A2. Attendance in one cybersecurity course during the previous semester, general cybersecurity basic concepts' knowledge.
	State objectives	S1. State learning objectives	S1.1. Familiarization with basic cybersecurity concepts and procedural policies: e.g. passwords, firewall, networks. S1.2 Understanding the importance of physical security and how to establish it. S1.3 Understanding the importance of patches and how to apply them.
	Select media & materials	S1. Pick strategy, technology and tools based on the objectives set previously.	S1. CyberCIEGE game, SPSS, Pre-Q, Post-Q, Observation

At the same time, this matching could be imprinted clearly in the figure below (Figure 3):

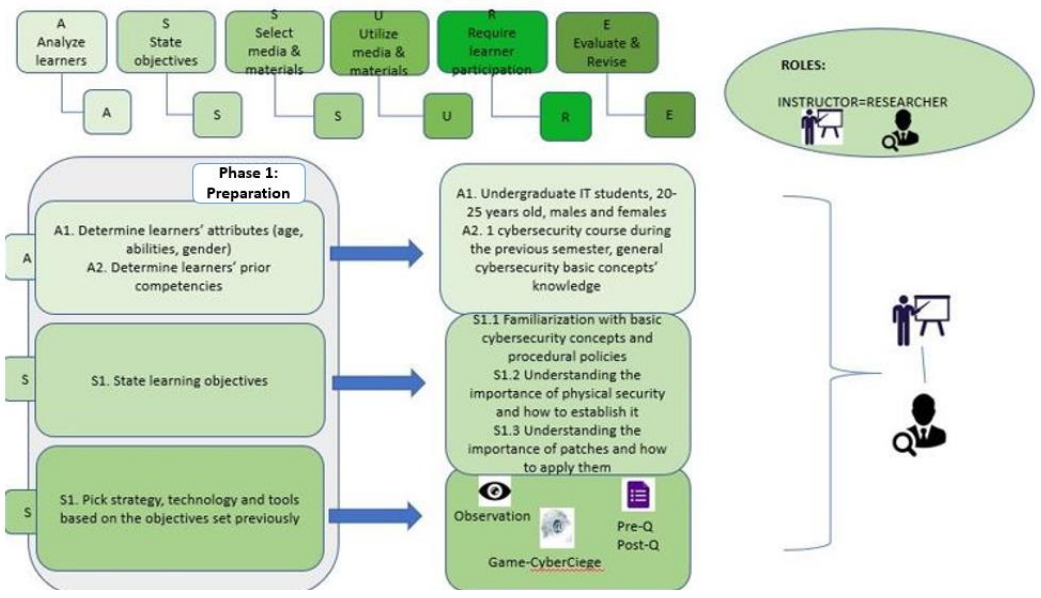


Figure 3. Phase 1: Preparation – Stages A, S, S of the Assure Model

Similarly, the second phase of the research design (**Intervention**) comports with the stage **U (Utilize media & materials)** and **R (Require learner participation)**. The following table (Table 2) presents this matching in detail:

Table 2. The Assure Model matched with the Research Design and Research Procedure (2)

Research Design	Assure Stage	Assure Substage	Research Procedure
Phase 2: Intervention	**Utilize media & materials**	U1. Prepare technology/media/materials	U1.1 Install CyberCIEGE on the learners' PCs and test it. U1.2 Share pre and post questionnaires with the learners (Google forms).
		U2. Prepare environment	U2.1 Ensure there is no noise. U2.2 Ensure there are enough desks and computers.
		U3. Prepare learners	U3. Start the PowerPoint presentation to introduce the learning objectives and the learning procedure
		U4. Provide learning experience	U4. Carry out the workshop.
	Require learner participation	R1. Actively engage students in the learning process	R1. Encourage learners to ask questions, to recall prior knowledge, to use the internet, to provide feedback.
		R2. Ensure active participation	R2. The researcher needs to be alert and available and provide help when needed.

At the same time, this matching could be imprinted clearly in the figure below (Figure 4):

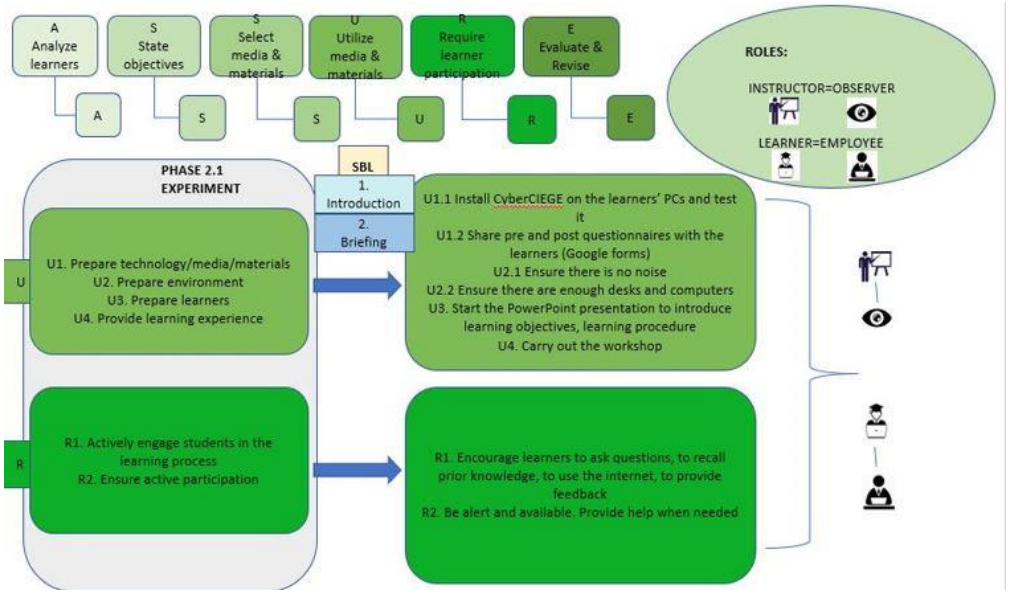


Figure 4. Phase 2: Intervention – Stages U, R of the Assure Model

Finally, the third phase of the research design (**Evaluation**) comports with the stage **E (Evaluation and Revise)** presented in detail at the following table (Table 3):

Table 3. The Assure Model matched with the Research Design and Research Procedure (3)

Research Design	Assure Stage	Assure Substage	Research Procedure
Phase 3: Evaluation	**Evaluate & revise**	E1. Data collection	E1. Pre-Q, Post-Q, Observation notes.
		E2. Data analysis	E2. SPSS statistical analysis, observation notes' analysis.
		E3. Results & Summary	E3. Analyzed data accumulation and conclusions.

At the same time, this matching could be imprinted clearly in the figure below (Figure 5):

Figure 5

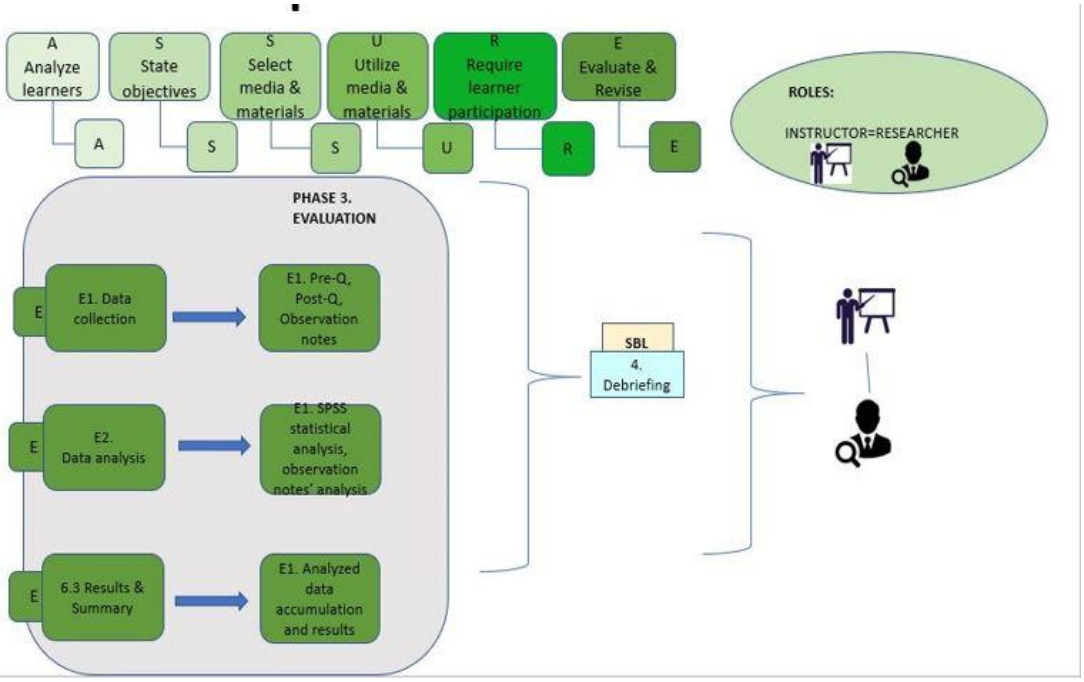


Figure 5. Phase 2: Intervention – Stage E of the Assure Model

In the paragraphs that follow we will describe the conceptual framework, the educational process of the workshop in detail.

3.4.3. The conceptual framework

A conceptual framework is essential to direct and carry out a research project. Before planning and executing one's own research study or project, they need to take into consideration previous research, theories and findings regarding the research question(s), therefore it is much more than a literature review, as it should facilitate the researcher's work with regard to setting parameters, goals, identifying the research gap and raising adequate research questions, and thereon combining multidisciplinary information and practices to synthesize their project via a holistic approach.

The educational process of the workshop is analyzed below in detail: we will explain how the SBL model's phases were employed and matched with the project's educational phases, and we will provide a thorough description of each of the simulation tool's use cases that were used during the intervention.

3.4.3.1. The educational process of the workshop

According to the SBL model there are four phases, on which the educational scenario (macro-script) was adapted. These phases are:

1. Introduction
2. Briefing
3. Scenarios
4. Debriefing

Each one (or more) of these phases corresponds to a respective phase of our research design flow.

More specifically, during the SBL's **"Introduction"** phase **(Phase 1: Preparation)**, the learners' prior knowledge is activated. This is achieved by a brief presentation of the project that is about to take place and by completing the pre-survey questionnaire.

During the **"Briefing"** phase **(Phase 2: Experiment)**, the participants are getting familiar with the environment, the use cases, their roles and their objectives. They are asked to play 3 different scenarios (use cases) integrated in the CyberCIEGE game, all based on cybersecurity risk management. All three scenarios take place in an office environment. Secrecy is required in order to protect important company assets. Each scenario provides users with a description of the threat/problem, a description of the setting, an introduction to the scenario's flow (Figure 6) and a definition of the scenario's objectives:

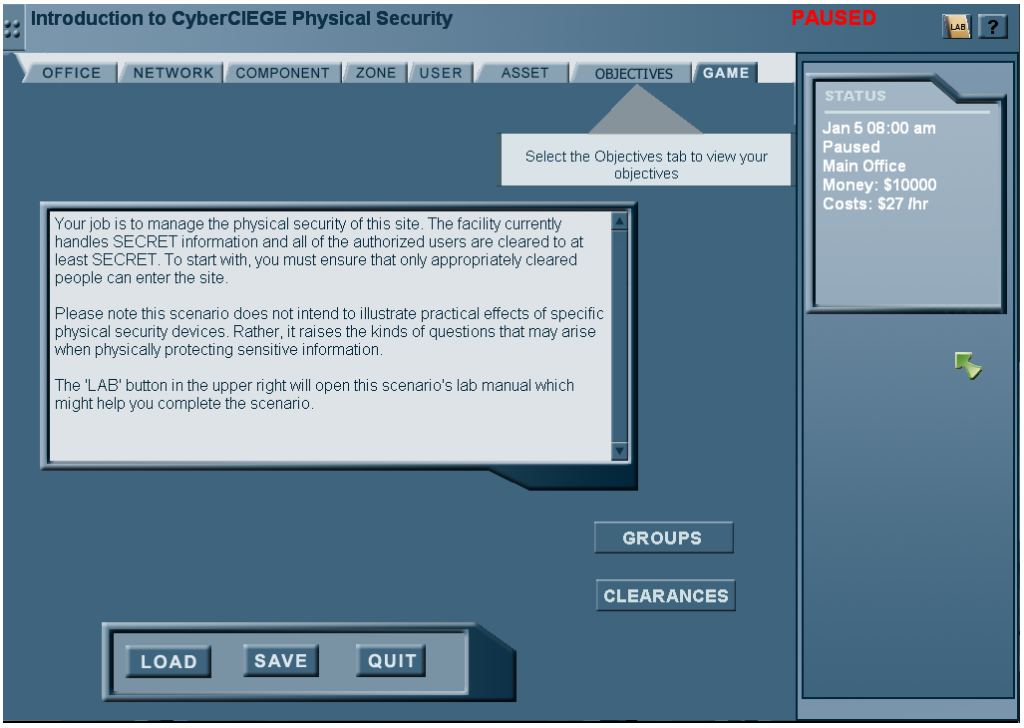


Figure 6. CyberCIEGE Introduction to the Physical Security scenario

During the phase of **"Scenarios" (Phase 2: Experiment)**, three different scenarios corresponding to three use cases were given to the participants. Each use case serves different objectives and corresponds to the micro-script of the educational process. A description of the three CyberCIEGE game use cases and each use case's learning outcomes follow, as retrieved from the NPS website's respective articles (NPS, Introduction Scenario, 2006), (NPS, Physical Security, 2006), (NPS, Patches, 2011).

Scenario 1 (Use Case 1): Introduction

The first of the three scenarios the learners were asked to complete during the intervention process. A table containing more detailed information on the Introduction scenario can be found below (Table 4):

Table 4. CyberCIEGE UseCases (1)

UseCase 1: Introduction Scenario			
Scope: A basic tutorial use case that walks the player through the mechanics of the game and introduces them to some of the CyberCIEGE security concepts and game components. It helps users get familiar with concepts such as objectives, assets, networks, passwords, malicious attachments etc.	Description: The CyberCIEGE "Introduction" use case is a simple one that provides new players with an introduction to CyberCIEGE, along with some game interfaces and features. Players will need to purchase computers and technological equipment and connect them to networks. Players will also train their users, configure user workstations and establish physical security. As with all CyberCIEGE use cases, students are prompted to explore the consequences of "wrong" choices as well as trying to make the right decisions. It is advised to play the the introduction use case several times so that users can experiment with regard to what they believe are the correct choices.	Concepts: This use case explores the following CyberCIEGE concepts: • Purchasing workstations and placing them on user's desks • Connecting workstations to an existing LAN • Hiring support staff to help manage the information technology resources • Establishing simple procedural settings to manage user behavior (e.g., beware of email attachments) • Buy user training so that they better understand the procedural policies • Set physical zone security to protect against equipment theft. • Configure workstations to automatically logoff after a period of inactivity.	Learning outcomes: This use case proposes the following learning outcomes: • Establishing the initial network • Establishing Procedural Security and User Training • Establishing Physical Security and Individual Accountability

Briefly, the micro-script is imprinted through the game flow, to the figure below (Figure 7):

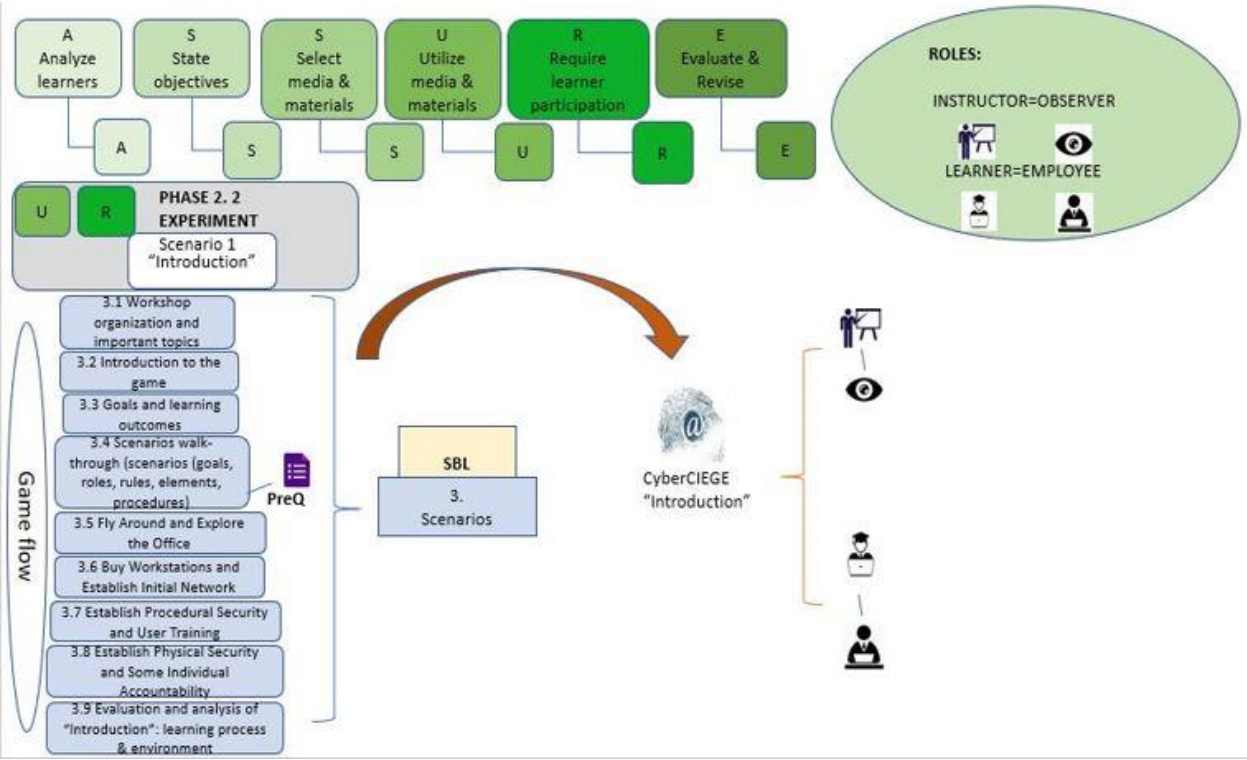


Figure 7. The 2nd Phase "Scenarios" – Scenario 1: "Introduction"

As it can also be viewed from Figure 7 above, there is a correlation between each CyberCIEGE's scenario's (use case's) learning goals and the activities provided in the respective use case that the user has to complete in order to achieve them. In the current chapter we will match each use case's goals with the respective activities and we will indicate the roles of the participants in the workflow, as well as the way they are assessed during gameplay.

The micro-script encompasses the following:

Learning goals:

LG1.1 Establishing the initial network
LG1.2 Establishing Procedural Security and User Training
LG1.3 Establishing Physical Security and Individual Accountability

Activities:
A1.1 Purchasing workstations and placing them on user's desks
A1.2 Connecting workstations to an existing LAN
A1.3 Hiring support staff to help manage the information technology resources

A1.4 Establishing simple procedural settings to manage user behavior (e.g., beware of email attachments)
A1.5 Buy user training so that they better understand the procedural policies
A1.6 Set physical zone security to protect against equipment theft.
A1.7 Configure workstations to automatically logoff after a period of inactivity.

Roles:

R1.1 Company's employee-IT expert (students)
R1.2 Moderator-facilitator-observer (researcher)

Assessment

A.1 Successful completion of the use case → users have reached the game's objectives

Scenario 2 (Use Case 2): Physical security

The second of the three scenarios the learners were asked to complete during the intervention process is exploring the concepts of physical security. A table containing more detailed information on the Physical security scenario can be found below (Table 5):

Table 5. CyberCIEGE UseCases (2)

UseCase 2: Physical Security			
Scope: Introduces CyberCIEGE zones and methods of physically protecting assets.	Description: The CyberCIEGE "Physical Security" use case introduces players to CyberCIEGE zones and methods of physically protecting assets. It introduces players to assets having a high attacker motive. As with all CyberCIEGE use cases, students are encouraged to explore the effects of "wrong" choices as well as trying to select the correct choices.	Concepts: This use case explores the following CyberCIEGE concepts: • Understanding the meaning of security labels (e.g., "SECRET") in terms of the value of the asset to the enterprise and the value of the asset to attackers. • Ensuring suitable policies and protection mechanisms are in place	Learning outcomes: This use case proposes the following learning outcomes: • Establishing Physical Security to protect SECRET assets • Establishing Physical Security to protect TOP SECRET assets

		before going operational (i.e., before pressing the play button). • Physically limiting access to assets to those users who are cleared to access the asset based on its security label. • Enforcing physical access limitations using mechanisms having a strength that is consistent with the asset attacker motive. • Within some environments, not all users are cleared to access all assets, and within such environments, steps should be taken to protect assets from insufficiently cleared users. • There are zones that are within the entire site. These zones can have stricter access restrictions than the site.	

Briefly, the micro-script is imprinted through the game flow, to the figure below (Figure 8):

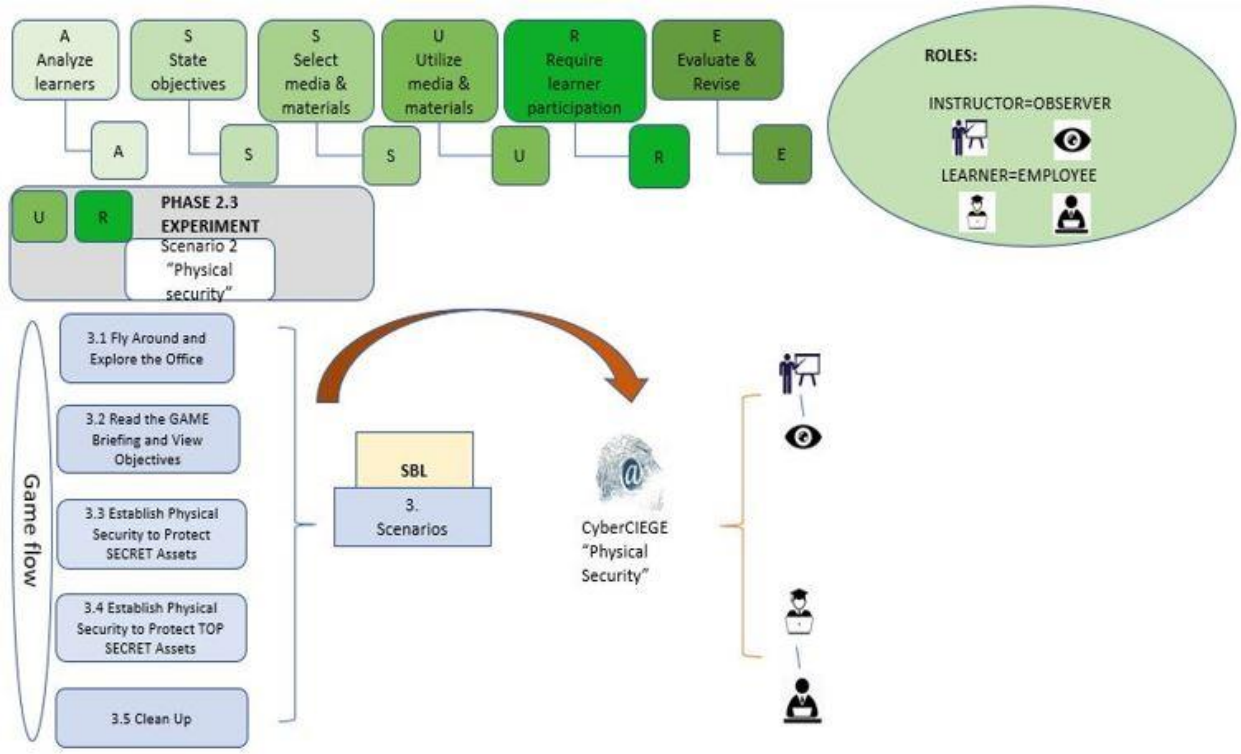


Figure 8. The 2nd Phase "Scenarios" – Scenario 2: "Physical Security"

The micro-script encompasses the following:

Learning goals:

LG2.1 Establishing Physical Security to protect SECRET assets
LG2.2 Establishing Physical Security to protect TOP SECRET assets

Activities:

A2.1 Ensuring suitable policies and protection mechanisms are in place before going operational (i.e., before pressing the play button).
A2.2 Physically limiting access to assets to those users who are cleared to access the asset based on its security label.
A2.3Enforcing physical access limitations using mechanisms having a strength that is consistent with the asset attacker motive.
A2.4 Within some environments, not all users are cleared to access all assets, and within such environments, steps should be taken to protect assets from insufficiently cleared users.
A2.5There are zones that are within the entire site. These zones can have stricter access restrictions than the site.

Roles:

R2.1 Company's employee-IT expert (students)
R2.2 Moderator-facilitator-observer (researcher)

Assessment

A.2 Successful completion of the use case → users have reached the game's objectives

Scenario 3 (Use Case 3): Patches

The third and last of the scenarios the learners were asked to complete during the intervention process is exploring the concept of patches and the importance of training employees on application patching. A table containing more detailed information on the Patches scenario can be found below (Table 6):

Table 6. CyberCIEGE UseCases (3)

Scenario 3 (Use Case 3): Patches			
Scope: The CyberCIEGE patches use case explores the need to apply software patches to applications and operating systems.	Description: Application software and operating systems have flaws that attackers can exploit to compromise systems. When flaws are discovered, the vendor often issues a patch that repairs the flaw. CyberCIEGE provides two methods for managing the patches on a given computer. Configuration settings can direct IT support staff to perform selected patch management functions (though this requires that you have suitable IT staff support). Alternately, individual users can be directed to manage the patches on their workstations via procedural settings (though users must be suitably trained, or they will ignore the	Concepts: This use case explores the following concepts, as described in the NPS university's website: Many applications and operating systems have flaws that can be exploited by attackers to compromise computers and/or assets stored on those computers; • After specific flaws become publicly known, there are often a lot of attacks mounted against systems that contain those flaws. • Sometimes an enterprise's use of unpatched software is visible from the Internet via a network	Learning outcomes: This use case proposes the following learning outcomes: • Patch web application server via configural settings • Ensure user procedural security via procedural settings • Test the effectiveness of patches of applications before they are applied

	procedures). CyberCIEGE software patch requirements vary depending on the software. For server-based applications (e.g., web server applications), you can sometimes assess software patch requirements by running a "scan".	"scan". • Software patches that are only intended to address security flaws will sometimes have unexpected effects on the behavior of applications. It is advantageous to establish a regime to test new patches before applying them to operational systems. • Procedures and responsibilities for managing patches must be consistent with available resources. In some environments, individual users must manage and apply patches to their own systems. In these environments, user training is often necessary.	

Briefly, the micro-script is imprinted through the game flow, to the figure below (Figure 9):

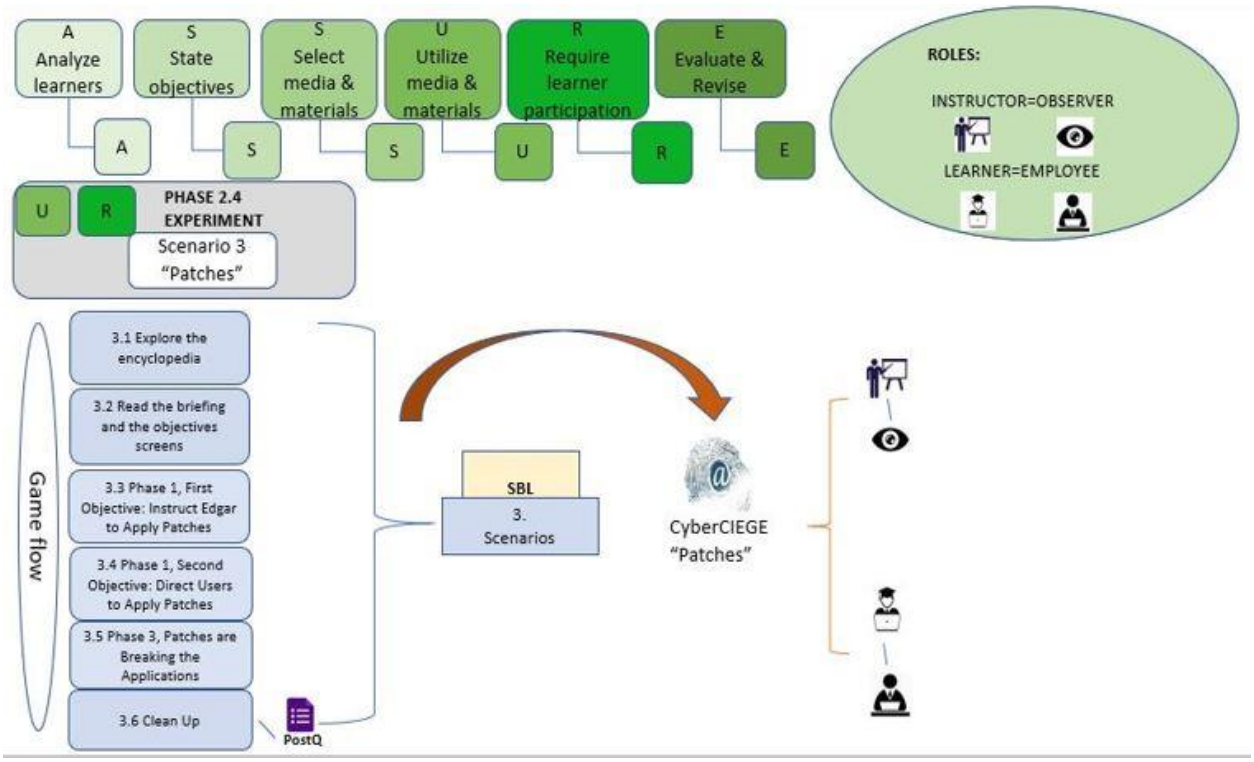


Figure 9. The 2nd Phase "Scenarios" – Scenario 3: "Patches"

The micro-script encompasses the following:

Learning goals:

LG3.1 Patch web application server via configural settings
LG3.2 Ensure user procedural security via procedural settings
LG3.3 Test the effectiveness of patches of applications before they are applied

Activities:

A3.1 Patching web application server via configural settings
A3.2 Ensure user procedural security via procedural settings
A3.3 Test the effectiveness of patches for applications before they are applied

Roles:

R3.1 Company's employee-IT expert (students)
R3.2 Moderator-facilitator-observer (researcher)

Assessment

A.3 Successful completion of the use case → users have reached the game's objectives.

During the **"Debriefing"** phase **(Phase 3: Evaluation)**, a comprehensive evaluation takes place. The learners provide their feedback and complete the post-survey questionnaire. A first analysis of the learning process, of the learning environment and the learners' acquired knowledge is made by the researcher. Setting new goals is the last step (but not least). Further analysis of the above can be found in Chapter 4. Limitations we encountered did not allow us to set new goals (i.e. the intervention was not to be repeated).

3.4.3.2. Tools

Technological Tools:

- CyberCIEGE is a serious game, which is more explicitly described in Chapter 3.4.3.2.1, *Describing the simulation tool: CyberCIEGE*. It is a simulation game designed for training purposes, and it is used for learners to familiarize with cybersecurity concepts.

Tools for data collection and analysis:

- Observation: Live observation of the sample by the researcher throughout the whole process of the intervention (an observation checklist is available in the Appendix).
- Survey: Google Forms questionnaires (pre and post intervention).
- Software used for statistical analysis: IBM SPSS.

3.4.3.2.1 Describing the simulation tool: CyberCIEGE

CyberCIEGE, an interactive cybersecurity game simulator created by the American Naval Postgraduate School (NPS) and Rivermind, is created to train employees and IT students. The project has been distributed to thousands of users in the US Government and is available for distribution to commercial and educational institutions as well as government agencies outside the US.

According to the game's description on the NPS website: "CyberCIEGE enhances information assurance and cybersecurity education and training through the use of computer gaming techniques such as those employed in SimCity™. In the CyberCIEGE virtual world, users spend virtual money to operate and defend their networks, and can watch the consequences of their

choices while under attack" (NPS, CyberCIEGE, n.d.). The CyberCIEGE simulation can be either used for training or for assessing students' risk management ability and cybersecurity knowledge.

The game has its own language, and scenarios are created using this language [Scenario Development Tool (SDT)]; it graphically represents the scenarios and also allows designers to create their own by using re-usable scenario elements from the existing ones. There are nearly 20 scenarios, each about different concepts of cybersecurity. The game's interface is a 3D office environment containing users (employees) and network systems, server rooms etc. It is played in real-time, much like Sims™, and contains game elements such as the following:

- Assets: Important confidential information of the company that needs to be secured and protected
- Asset goal: Specific goal to reach regarding the asset.
- Users: Scenarios include several virtual users/characters (employees of the company).
- Zones: Several physical zones are included; some of them have restricted access to some users only.
- Objectives and phases: More complex scenarios are divided to two or more phases, each consisting of one or more objectives (Raman, 2014).

CyberCIEGE has been incorporated into a range of different curricula at different levels of education. For example, campuses include the game in their Security and Risk Analysis courses (Virginia Tech Pamplin College of Business, Penn State University, National Defense University of Taiwan). It is used by several online universities, due in part to providing hands-on exercises without requiring access to lab systems (e.g. TUI University). Technical and vocational schools such as the ITT Technical Institute have used the game as part of network security training.

As far as research is concerned, two limited studies of the effectiveness of CyberCIEGE have been carried out; Jones, et al. (Jones, 2010) compared CyberCIEGE with a DoD information assurance awareness video in an undergraduate computer security course at North Carolina A&T State University. They found that the students who played the game were more enthusiastic about the game than the other group was about the video, and they also found that the game group gave more detailed answers to test questions, though that may have been caused due to the game group devoting more time to it than did the video group. Fung et al. (Fung, 2008) carried out a pilot study on the use of CyberCIEGE for raising awareness and knowledge on information security among a group of students, comparing it with a traditional classroom lecture. Both studies were encouraging, though not conclusive, due to small sample sizes (Thompson, 2011).

Another study which was conducted to implement game-based scenarios into cybersecurity education and to analyze the effectiveness of this method, used two groups of engineering students; the first group completed questionnaires with multiple choice questions based on the game scenarios, prior to playing. The second group played the game and replied to the same questionnaires afterwards. Results showed a significant statistical deviation between the two groups, implying that the second group, which was assessed after playing showed better learning

outcomes than the first one (Raman, 2014).

T. Tiat Leng gives a thorough description of the game in *Scenario Selection and Student Assessment Modules for CyberCIEGE*: "CyberCIEGE simulates a range of scenarios involving networked computer systems with the player defender role and the computer assuming the attacker role. The player needs to construct computer networks with components such as servers and workstations and apply appropriate security measures to ensure that the system's security posture is able to meet the organizational goals. The game lies in the tension created by the competing goals of efficient and affordable access to assets and protection of assets from unauthorized disclosures or modification. This is a significant improvement over that of CyberProtect which had only considered the application of protection mechanisms without clearly articulating the organization goals. CyberCIEGE has a wider range of options, allowing the player to construct, interconnect and apply protection of the network as well. The player will make decisions that affect the behavior of a set of virtual user characters. Hostile game characters may develop and attack the system, ranging from vandals, disgruntled insiders, incompetent users, to professional attackers. In CyberCIEGE, the player starts the game with a finite budget and has to perform resource management to establish an ever-growing enterprise, reaping the benefit of productive users while balancing benefits of protecting their assets against attackers." (Leng, 2003, p. 17).

Therefore, we consider CyberCIEGE a technological innovation, because without the simulation software we would not be able to run a case study, let alone having measurable data to work with. Hence, it all starts from understanding that cybersecurity is an area that needs to be studied also from an educational viewpoint and not only from a technical one, as it is an interdisciplinary field. Our aim was not only to provide and analyze data, but also to use them in favor of cybersecurity awareness, to help increase it and implement it in education, not only in higher education, but in a holistic way, as it is nowadays a matter that should concern us all.

Below, we will describe the game's internal tools (components), such as assets, networks goals and objectives etc.

- **Assets**

Assets represent various information resources. The more negative the impact of an unauthorized modification or lack of availability of the asset, the more valuable it is for the company (thus the classification in SECRET and TOP SECRET).

- **Components**

Components such as networks, servers, firewalls are used in the game, and assets can be found in workstations or servers. Routers can connect two or more workstations and can block or permit services between networks.

- **Networks**

Local networks (LANs) allow for components to be interconnected and communicate Networks can be internal and/or external (connected to the Internet), and this can be customizable in the scenarios depending on the immersion in security concepts the instructor wants to achieve.

- **Users & Goals**

Users are employees of a company, meant to provide revenue for the company's benefits. The productivity and happiness of employees depends on their goals: when they're met, happiness and productivity are high. When they fail, both of them decrease. If the user makes the appropriate choices to complete the scenario's objectives, and the objective is complete, the respective user in the game will be productive and happy due to this event.

- **Objectives and phases**

Each scenario consists of phases and objectives that need to be fulfilled in each phase by the users for a successful scenario completion (Figure 10). Difficulty increases as the scenarios advance (e.g. Patches is more difficult than the Introduction scenario) and the purpose of this structure is to guide users to perform certain actions to reach a certain outcome.

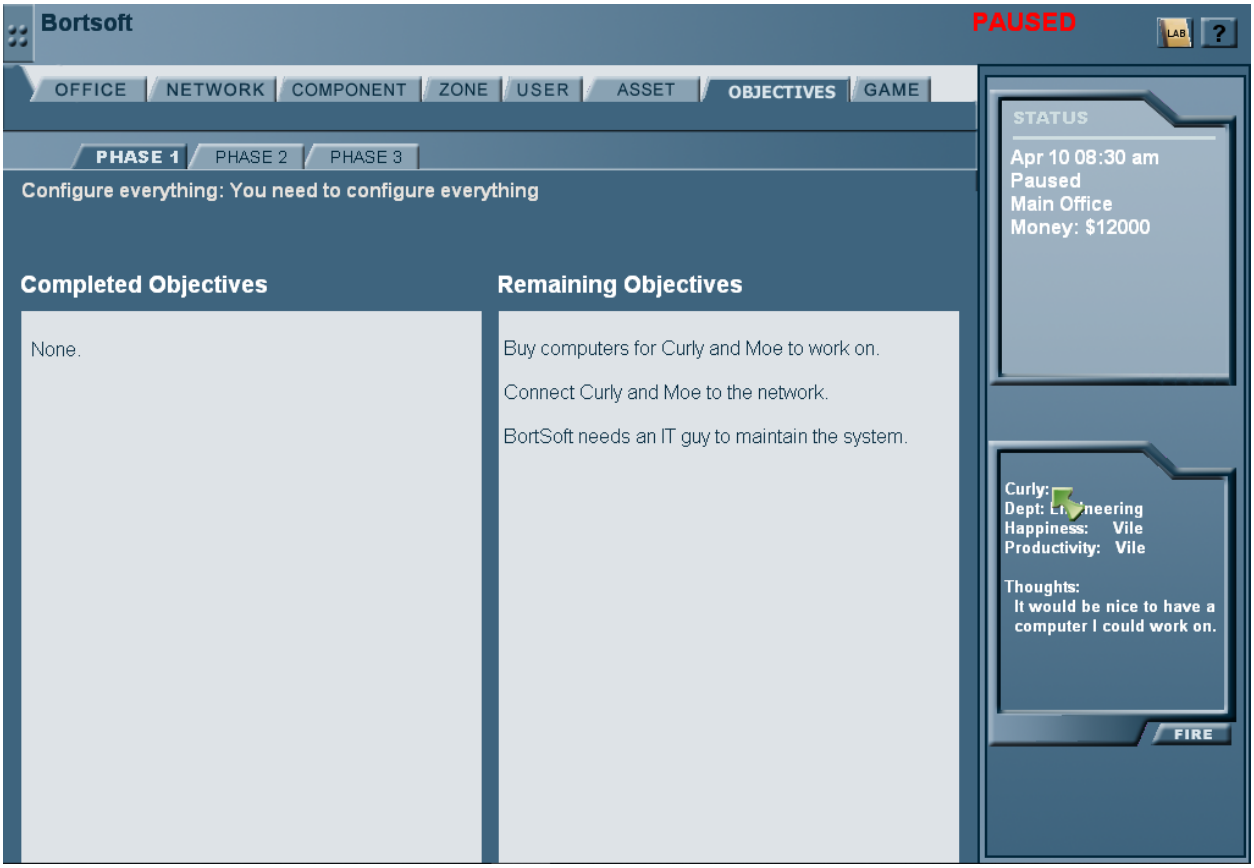


Figure 10. CyberCIEGE scenario objectives example

We decided to use CyberCIEGE after comparing it with similar simulation software. For this purpose, we consulted the table of didactical capabilities of several simulation tools as described by Pastor, Diaz and Castro (Pastor, 2010, pp. 1914-15), (see Table 7, Table 8).

Table 7. Cybersecurity training games: Didactical capabilities

Simulator name	Target audience	Teaching objectives	Learning curve
CyberProtect	Novice network security professionals	Generic information security training	Fast
MAADNET	US military academy cadets	Generic information security training	Fast
CyberOps: NetWarrior	Information Assurance students	Generic information security training	Fast
DETERlab	Academic and industrial cybersecurity researchers	Teaching is not the main target. It has been used as a laboratory by university level cybersecurity classes	Slow
CyberCIEGE	Information assurance students	Information Assurance basics. Risk management. Resource management	Fast
NIIST	Researchers of new and existing internet security technology, protocols protocol mechanisms	Research and evaluate the dynamic behavior of an interactive suite of security protocols in large scale VPNs	
RINSE	Experienced network security professionals	Large scale, real-time cybersecurity training and exercises	Unclear

RCEL	Information Assurance students with a profound technical background	Support of an information assurance education program	Moderate
Tele-Lab: "IT Security"	Information Assurance students with minimum previous knowledge	Many different subjects. Basic level	Moderate
NeSSi2	Computer science students and professionals	Detailed examination and testing of security-related network algorithms, detection units and frameworks	Moderate
S-vLab	Students of 4 degree course in a 5 years degree	Java Security	Fast
AWARE	Windows XP users	Detect potential attacks and remediate the effects using Windows XP built-in tools	Fast
RADICL	Information Assurance and Computer Engineering students	Understanding attack scripts and other malware	Moderate

Table 8. Cybersecurity training games: Didactical capabilities (continued)

Simulator name	Usability	Level of detail
CyberProtect	Very Good	Fair
MAADNET	Very Good	Fair
CyberOPS: NetWarrior	Excellent	Good
DETERlab	Good	Excellent
CyberCIEGE	Excellent	Good
NIIST	Fair	Very Good
RINSE	Good	Good
RCEL	Good	Excellent
Tele-Lab "IT Security"	Good	Unclear
NeSSi2	Very Good	Excellent
S-vLab	Good	Fair
AWARE	Very Good	Fair
RADICL	Good	Very good

3.4.3.2.2. Research Tools

Assessment and evaluation:

Questionnaires (pre and post-survey), observation and data analysis:

Questionnaires were used prior and after the game had been played by the students: the first one contained 11 questions, combined to test user characteristics: behavior and technical cybersecurity knowledge. The second one contained the same questions plus 14 more included to measure engagement, using the GEQ questionnaire's questions.

Naturalistic observation was also employed to determine user behavior toward the game itself, to define the emotional state of the users whilst playing and the overall response towards it, as well as the experiment as a whole.

- **Data analysis tool:**

IBM SPSS:

SPPS was used for statistical data analysis as it was deemed adequate for reaching conclusions and exporting results exploited to prove if our objectives were met or not.

- **Metrics:**

User behavior, technical knowledge and skills, engagement:

Our RQ2 revolves around these three concepts. Therefore, our intention and objective are to measure any change in them after having implemented the simulation game in the students' learning process, by comparing the pre-survey questionnaire to the post-survey one and analyzing the data.

3.4.3.2.3 Data collection tools

- Observation: Live observation of the sample by the researcher throughout the whole process of the intervention.

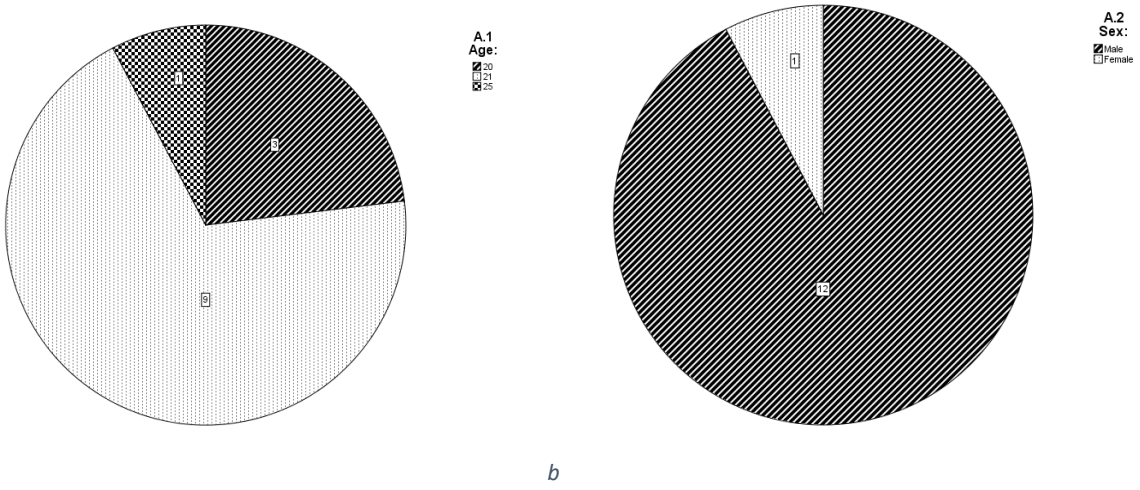
- Survey: Google Forms questionnaires (pre and post intervention).

3.4.3.2.4 The sample

Within an experimental group design, we used pre and post measurements (survey questionnaires answered by our sample). One group of 13 undergraduate students participated as volunteers. The research phases are completed in the following steps:

The pre-survey questionnaire consists of one section (11 questions). The post-survey questionnaire consists of two sections: the same section as the pre-survey one and one section which is the GEQ (containing 14 questions), used to measure the engagement levels of the students.

The participants are 13 undergraduate students at the University of Piraeus, in the Digital Systems Department, aged 20-25, 12 males and 1 female (Figure 11):



a *b*

Figure 11.a. Age distribution, b. Sex distribution

This specific sample was chosen for the following reasons: it is easily accessible and compatible with the kind of study we want to conduct, since our target is to measure the cybersecurity risk management knowledge of IT undergraduate students via a simulation-based learning serious game. The pilot study was conducted using several instruments and tools such as: questionnaires, computer lab and scenarios of the serious game CyberCIEGE. Our instructional design is based on the simulation-based learning educational method, which was chosen due to its relevance with this specific simulation game which was used for our experiment, and it also serves our objective and research questions.

The first phase of the study includes the completion of the pre-survey questionnaire. The questionnaire consists of 11 questions meant for self-assessing cybersecurity risk management knowledge. The questionnaire is completed by each student individually.

During the last phase of our intervention, all participants completed the post-survey questionnaire. This questionnaire consists of a general section which assessed anew the participants' cybersecurity risk management knowledge (it contains the same questions as the pre-survey questionnaire), and of a section which measures the engagement levels after having played the simulation game. All data from both questionnaires were collected and analyzed using the IBM SPSS Statistics software. This analysis is thoroughly described in Chapter 4.

Lastly, as far as ethical issues are concerned, all participants were thoroughly informed about the study beforehand, and were asked to give their written consent which could be cancelled anytime during the study (the consent form can be found in the Appendix). Concerning data privacy, all requirements of GDPR were respected.

3.5 Summary

Summarizing, in this chapter we have presented the process of our research design and workflow (educational design), and have explained how we implemented the components and phases of the SBL and the ASSURE model into it. The workflow process of the intervention can be viewed schematically below (Figure 12):

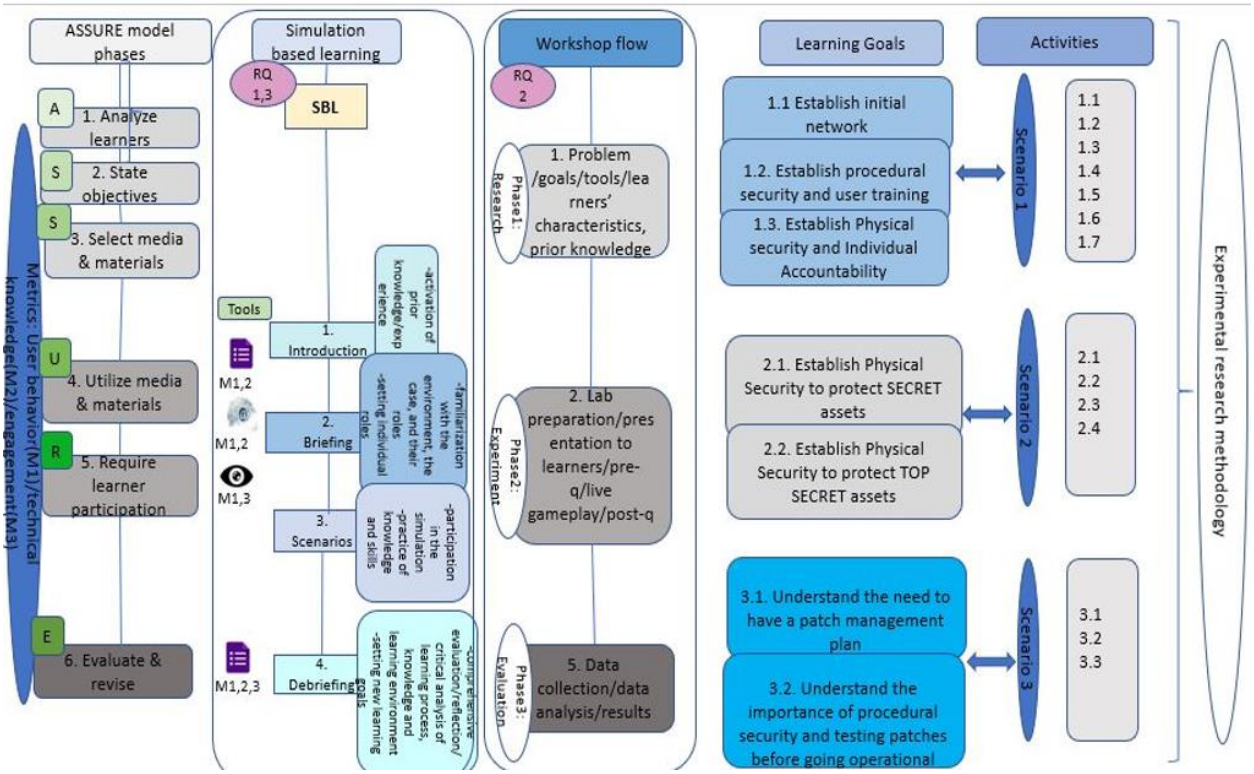


Figure 12. Workflow process

We also described the technological tool that was used (the simulation game CyberCIEGE) and explained the learners' interaction with it during the experiment phase. In the next chapter, we shall provide an analysis of the data gathered through this process and the results.

Chapter 4 – Results

4.1 Objective of the research

This thesis' overarching objective is to investigate how simulation-based learning affects the knowledge of cybersecurity risk management. This breaks down in three sub-objectives: to examine the educational potential & affordances of the serious game CyberCIEGE, to investigate how the integration of a serious simulation cybersecurity game in the learning process affects user behavior, technical knowledge and skills, and engagement of undergraduate IT students, and to determine whether the simulation-based learning theory's components can be implemented in a pedagogical instructional design's phases by the same theory, utilizing the serious game CyberCIEGE in a workshop. By examining the efficiency of the game CyberCIEGE we will be able to determine whether simulation-based learning is an adequate method for ensuring this knowledge and therefore diminishing the risk of malicious attacks in the future, by helping students apply their theoretical knowledge and giving them the chance to be skillful in a high risk situation. This will not only provide them with cybersecurity risk management knowledge but will also prepare them for a potential threat in their working field in the future.

4.2 Methodology

Quantitative experimental research was used as our research methodology. The definition of this type of research, is one or more variables are manipulated to determine their effect on a dependent variable. There is a cause and effect relationship between the variables, this is the reason why it is important for experimental research to define that the results (effects) observed from an experiment are due to the cause. It is also important to always know which variables are to be measured. In our case, we used a quasi-experiment, where the researcher influences something (i.e. implements a simulation game into the traditional learning process) to measure the consequences of this action (i.e. the effect of this intervention in different aspects).

4.2.1 Participants

The participants are 13 undergraduate students at the University of Piraeus, in the Digital Systems Department, aged 20-25, 12 males and 1 female. This specific sample was chosen for the following reasons: easily accessible and compatible with the kind of study we want to conduct, since our target is to measure the cybersecurity risk management knowledge of IT undergraduate students via a simulation-based learning serious game. It should be noted that

the participants are actually undergraduate students, but their defined and assigned role throughout the gameplay was an IT employee in a company, whose actions determine each CyberCIEGE scenario's plot progression.

4.2.2. Means and process of data collection

The experiment can be roughly divided in three phases:

- Phase 1: Completion of pre-survey questionnaire individually by each student. The pre-survey questionnaire consists of one section (11 questions meant for self-assessing cybersecurity users' behavior, as well as risk management skills and technical knowledge). The questionnaire is completed by each student individually.

- Phase 2: Participation in the experiment using the serious game CyberCIEGE by playing live for 1:30 hours. During the second, experiment phase, the participants are asked to play 3 different scenarios integrated in the CyberCIEGE game, all based on cybersecurity risk management. These scenarios are described thoroughly in *Chapter 3.4.3.1. The educational process of the workshop.* Live observation is used as a means of data collection in this phase (i.e. by observing the sample's behavior live, we are able to extract qualitative data on their general attitude towards the intervention and their engagement levels).

- Phase 3: Completion of post-survey questionnaire individually by each student. The post-survey questionnaire consists of two sections: the same section as the pre-survey questionnaire and one section consisting of the GEQ questionnaire (containing 14 questions), used to measure the engagement levels of the students.

4.2.3 Research tools and methods

- Type of instrument/tool: Observation checklist

When the researcher directly observes the intervention and systematically reports the resulting observations. In our experiment, the researcher was present throughout the whole experiment, recording the observation results in paper to use them for further analysis later on. Our observation notes were exploited in order to answer RQ1, RQ2 and RQ3 and can be found in the Appendix.

- Type of instrument/tool: Questionnaires

Instruments used for surveys, consisting of a set of questions, designed to measure a certain item or a set of items. Our pre and post-survey questionnaires were made available to the sample via Google Forms, where each individual submitted their own response, before playing the serious game (answering the pre-survey questionnaire) and after (answering the post-survey one). The analysis of data we collected via the questionnaires was conducted to answer RQ2. Both the pre and post survey questionnaires can be found in the Appendix.

4.2.4 Research questions

Our main goal is to determine if simulation-based learning with the use of a simulation game will help raise cybersecurity awareness for undergraduate IT students. In order to examine if this hypothesis is true, we need to reflect on the following research questions:

- **RQ1:** What is the educational potential & affordances of the serious game CyberCIEGE?

- **RQ2:** Can the instructional design workflow based on the SBL enhance

  RQ2a: users' behavior
  RQ2b: technical knowledge and skills
  RQ2c: user engagement

- **RQ3**: Can the SBL theory components be implemented in a pedagogical instructional design's phases by the SBL theory, utilizing the serious game CyberCIEGE in a workshop?

Regarding the following:

RQ3a: activation of prior knowledge/experience (Introduction)
RQ3b-i: familiarization with the environment, the case, and the roles (Briefing)
RQ3b-ii: setting individual roles (Briefing)
RQ3c-i: participation in the simulation (Scenarios)
RQ3c-ii: practice of knowledge and skills (Scenarios)
RQ3d-i: comprehensive evaluation (Debriefing)
RQ3d-ii: reflection and critical analysis of the learning process (Debriefing)
RQ3d-iii: the knowledge and the learning environment (Debriefing)
RQ3d-iv: setting new learning goals (Debriefing)

4.2.5 Qualitative analysis

In this chapter we will provide a descriptive analysis of the study's results in relation with our research questions, which were presented previously, in *Chapter 4.2.4 Research questions*.

1) **RQ1:** What is the educational potential & affordances of the serious game CyberCIEGE?

An accurate definition of the term 'affordances' is given by Donald Norman, who describes an affordance as a design aspect of an object that suggests how the object should be used: The term affordance refers to the relationship between a physical object and a person (or for that matter, any interacting agent, whether animal or human, or even machines and robots). An affordance is a relationship between the properties of an object and the capabilities of the agent that determine just how the object could possibly be used. A chair affords ("is for") support and, therefore, affords sitting (Norman, 1988, p. 11)."

Further on, we will discuss the educational potential and affordances of the serious game CyberCIEGE. Can it be embedded in a higher education workshop effectively, affecting the students' performance and serving the learning outcomes of a cybersecurity risk management module?

- **Pedagogical uses**

1. **Recording**

Recording user progress and being able to review the learner's actions is possible for the instructor via log files. These can provide important insight on the path the learner followed and can help the instructor better understand and assess their effort. Log files can also assist with reaching conclusions regarding problem-solving skills and critical thinking employed.

2. **First-person view**

The simulation allows learners to access locations otherwise difficult to explore, such as a private company's premises and its offices.

3. Live guidance

Real time supervision and assistance by a researcher/trainer who is familiar with the game is helpful, but not necessary. The game can be played without any intervention, as instructions are provided during gameplay and players can refer to the help articles as well.

4. Feedback

As the scenario evolves, players are provided with feedback, either positive (Figure 13) (when they have reached an objective):

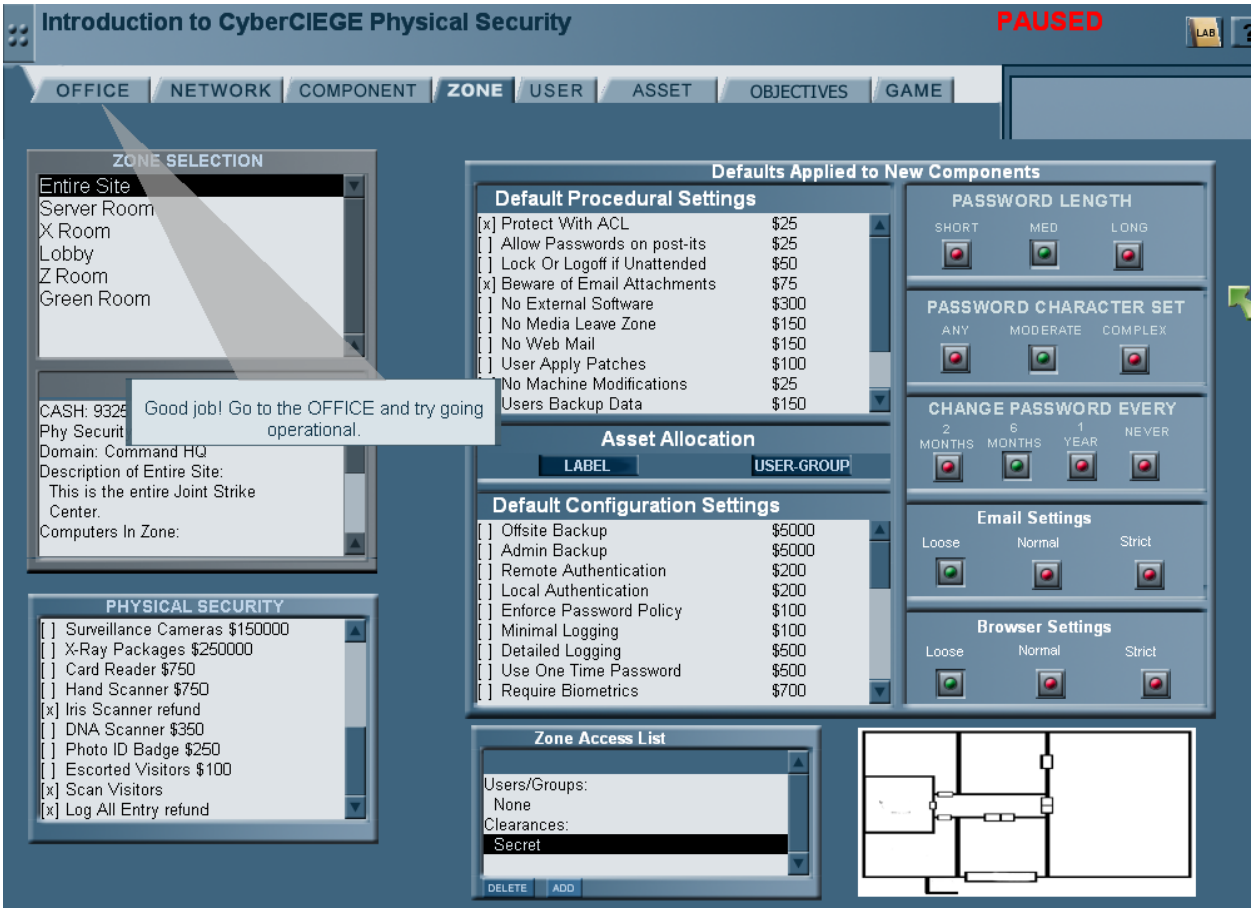


Figure 13. CyberCIEGE Gameplay – Feedback example 1 (positive)

or negative (when something did not go as expected and they need to try again). In the second case, there is also guidance as per the actions that need to be performed by the players to proceed with the scenario and reach its objectives (Figure 14):

Figure 14. CyberCIEGE Gameplay - Feedback example 2 (negative)

5. Customization and flexibility

The game does include a sufficient number of scenarios created for training purposes that can be adequately used in the learning process and integrated in an educational curriculum/program. Apart from the existing ones, however, it is possible to develop new ones, according to the developer's needs, design and learning path, which allows for more flexibility and experimentation. There is a certain scenario flow that should be respected for the users to proceed in the game, meaning that it is best to keep a sequence so that users do not become overwhelmed by suddenly playing a difficult scenario (scaffolding should be employed for this purpose).

6. e-Learning potential

CyberCIEGE, given its nature (simulation game similar to *The Sims*) can be embedded in the learning process and either be played within the premises of a university/organization in a computer lab, or remotely: students simply need to have the game installed in their computers. No internet connection is required. Very much like *The Sims*, there is no need for external guidance, as the game is more intuitive, easy to follow, without complex rules or navigation processes. A potential scenario would be having a sustainable course in an LMS where the game would be embedded and played as part of the learning process. The course could contain other types of resources (always within the cybersecurity context) and could have survey forms embedded as well for the instructor to track the learners' progress and collect data regarding the overall user experience.

- **Educational quality**

7. Engagement

Our experiment's results did not reveal data which would determine increased engagement toward the game, thus toward the cybersecurity field. However, no studies about the game have measured engagement so far, and it would be of great interest to examine this using larger student samples in a more extended intervention (from the aspect of duration and resources).

8. Efficiency

8.1 Active learning

Provided that the game is designed to immerse students in scenarios exploring various cybersecurity concepts, which include many ways to achieve objectives, this leads to experimentation through trial and error by the player. Throughout gameplay, the player becomes a network security analyst and applies concepts learned within one context to reach goals related with some other context. This requires critical and active thinking, which is promoted via the game's techniques and strategies.

8.2 Collaboration

The game is not designed and was not used in collaboration for the purposes of this thesis. However, it did come to our attention that some users were conversing with each other while

playing, asking questions and advice from one another, regarding the gameplay or technical inquiries. In all cases, they were reaching out to the person sitting next to them. This kind of conversation was not impeded, as it seemed to be helping "stuck" users progress and complete the scenarios, and to boost their confidence.

Either in a classroom/lab environment, or in an eLearning one, this kind of collaboration can be promoted and used to increase user engagement and 21st century soft skills which can also be part of the learning process's goals, given their importance nowadays.

- **Logistical and other**

9. No Cost

The game is free of cost and can be distributed by the Naval Postgraduate School for educational purposes, if one requests for it. Also, there is a free sample which is downloadable through their website and can be useful in case someone wants to have a first look at the game or test it out.

10. Support

There is a database available with helpful articles. Instructor tools provided include: a scenario development kit - to customize and create new scenarios, and, a student assessment tool - to track progress and identify potential problem areas. Also, there is a support page where Instructors can reach out to the game's creators for assistance.

11. Time-efficiency

Simulations in general provide virtual experiences which are less time-consuming than real-time experiments. Considering the nature of the subject in discussion here (cybersecurity risk management in critical infrastructures) it would not be possible to conduct a real experiment.

A table can be found below, which contains all the educational affordances of the game, as inferred from our case study and from our literature review regarding CyberCIEGE (Table 9):

Table 9. Summary of CyberCIEGE educational affordances

Educational affordances	Learner's actions	Educational goals
Unconstrained knowledge accession	Play introductory scenarios, Read/watch tutorials to reach higher levels	Construct knowledge, build cognition, and enhance comprehension
Real-time evaluation	Process real-time feedback upon scenario	Evaluate learning outcomes, and improve knowledge

	completion/failure, observe their own behavior during gameplay	cognition
Arbitrary data collection	Collect and interact with virtual objects/gather information during gameplay	Foster data collection ability, build learning basis, develop investigation, and enhance learning cognition
Authentic Context awareness	Retrieve context-aware data, combine scenarios with real world	Enhance trial and error and cause-consequence perception. Engage learning experiences, improve learning effectiveness, and construct authentic knowledge
Vivid Immersion	Combine virtual and real world objects as well as provide spatial, temporal and contextual conceptualization	Improve understanding and enhance learning experiences
Skillful Application	All the above	Foster problem-solving skills, exploring ability, and independent thinking ability

The observation checklist we used to conclude the aforementioned data can be found in the Appendix (3. Observation checklist and notes).

2) **RQ2:** Can the instructional design workflow based on the SBL enhance

- RQ2a: users' behavior?

Users' behavior in relation to the questions asked in the pre-survey questionnaire refer to actions such as logging out of the computer when it's left unattended, checking the anti-virus software for updates, opening attachments from unknown senders and using strong passwords. Related questions were answered by the learners to determine if their user behavior complies with basic cybersecurity guidelines, and how their pre-game behavior compares to their post-game one.

Examining user behavior criteria:

- **Logging out** (B.3 How often do you log out of your computer when you leave the room?)

On a Likert scale from 1 to 5 (1=Never, 2=Rarely, 3=Sometimes, 4=Very often, 5=Always), the most popular response pre-survey was Always (5 out of 13 responses) whereas post survey, 5/13 answered Never and 3/13 answered Always. There is some inconsistency regarding this question, but it is most probably due to the sample being small, thus we cannot make any concrete assumption.

- **Performing anti-virus updates** (B.4 How often do you check the anti-virus software or set it for automatic updates?)

The distribution of responses to this question is similar before and after having played the game: 5: Sometimes, 2: Very often and 3: Always (pre-survey) in comparison to 4: Sometimes, 3: Very often and 3: Always (post-survey). The responses to this question were also expected, given the students' background.

- **Opening incoming attachments** (B.5 How often do you open attachments from incoming emails, from unknown senders?)

The most popular answer pre-survey as well as post-survey was *Never* (8/13 and 9/13 respectively). We can conclude from this question's answers distribution that students are already aware of malicious email attachments and take precautions prior to taking part to our intervention.

- **Understanding the definition of strong passwords** (B.6 Write below an example of a strong password.)

A strong password must contain at least 8 characters, among which: one lowercase character, one uppercase character, one symbol and one number. 3/13 students provided an example which did not contain an uppercase character in both questionnaires. Apart from this, all passwords were long and consisted of symbols and numbers as well. This is expected, provided that the learners are IT students in their 3rd year of undergraduate studies.

- RQ2b: technical knowledge and skills?

Our questions regarding this metric were related to the CyberCIEGE scenarios' concepts that our learners interacted with (physical security examples and importance, patches definition and importance, patch training importance).

Examining technical knowledge and skills criteria:

- **Physical security** (B.7 Write two examples of physical security in a workstation.)

In the pre-survey, the answers given by the students to this question were the following:

1. Security Guards and Personalized ID Cards for staff
2. A strong enough firewall, Combination of biometric and something that only the user knows
3. Firewall, Security officer
4. One-time passwords, Biometric passwords
5. Security cards required to access critical rooms, Bio-metric based access on critical rooms (e.g. server/database room)
6. Eye-recognition pattern
7. Employees with basic security knowledge, managing incoming calls to employees who know security passwords
8. Servers guarded by security guards
9. Security guard
10. Security guard, door with password
11. Security guard

Two answers are missing from the results in the pre-survey questionnaire. Also, some answers are not complete (the students have provided only one example of physical security while they were asked for two). Overall, however, the answers provided are correct.

The answers to the same question in the post-survey questionnaire are as follows:

1. Security Guards, User ID Cards
2. Key lock & iris scanner
3. Patrols on secret rooms, Surveillance cameras
4. Employees with basic security knowledge, managing incoming calls to employees who know security passwords
5. Room with pin door
6. Security guard, pin
7. Security guard, cameras
8. Guard, lock doors, biometrics
9. Firewall, security guard
10. Eye-recognition patterns
11. Hand scanner
12. Guard, Alarm
13. One-time Passwords, Biometric Passwords

During the second CyberCIEGE scenario (Physical Security), users are asked to select the best possible solutions to provide physical security and protect the company's assets. Whilst in the same question prior to playing the game, 11 students replied, all 13 of them replied to this question in the post-survey questionnaire. It is safe to infer that the answers to the post-survey questionnaire reflect the choices of the students in the game. This could have been cross-checked though, had we had access to the logs, to verify if indeed this assumption is true.

- **Importance of physical security** (B.8 How important is it for a company to provide enough physical security to protect its assets?)

Here, the consistency in answers is clear: both in the pre-survey and the post-survey questionnaires, the distribution of answers was the same: 6 "Important", and 6 "Very Important", which allows us to infer that there was no contribution from the game to this particular knowledge, since the students had it already before playing.

- **The term "patches"** (B.9. Are you familiar with the term "patches"?)

The majority of students are familiar with the term *patches* as expected (9/13 pre-survey and 8/13 post-survey), which is the third scenario's topic.

- **Importance of patch management** (B.10 If you chose "Yes" in question 9, write a short definition and explain why patch management is important in your opinion.)

Seven responses were given pre-survey and six post-survey, all of which were relevant and correct. It seems like this scenario did not really affect the users' knowledge, as there's no particular difference in their responses post-survey. According to our observation and the students' feedback, this scenario (Patches) was the most difficult and time-consuming of the three, and many of them were confused as per the actions they had to perform to complete it. This, however, is not relevant to the topic's complexity, rather than the scenario's design and structure. It is possible that learners lost interest during this phase of the intervention due to the aforementioned reason.

- **Importance of application patching training** (B.11 If you chose "Yes" in question 9, select how important it is for a company to train employees for application patching in your opinion.)

The distribution of answers to this question is as follows:

Pre-survey: Moderately important (2), Important (2), Very important (7).

Post-survey: Important (7), Very important (3). It is obvious that students recognize the importance of training for successfully patching applications within a workstation both prior and after the intervention took place.

- RQ2c: user engagement

Examining GEQ questions:

Table 10 shows the mean of 13 answers in each of the GEQ's questions. The Likert scale from 1 to 5 (Strongly disagree to Strongly agree) was used for the purpose of this questionnaire. The distribution of answers ranges on average close to 3.00 (2.91). 3 corresponds to neutral, thus it can be inferred that the game has neither positively nor negatively affected user engagement.

Table 10. GEQ questions average mean score

GEQ	MEAN SCORE
C.1 I felt scared	2.31
C.2 I lost track of where I was	3.00
C.3 Time seemed to stand still and stop	3.00
C.4 I didn't answer when someone talked	2.38
C.5 I couldn't tell I was getting tired	2.92
C.6 I felt like I couldn't stop playing	2.46
C.7 The game felt real	3.15
C.8 Playing seemed automatic	2.92
C.9 I played without thinking how to play	2.85
C.10 Playing made me feel calm	2.46
C.11 My thoughts went fast	3.23
C.12 I wanted to play for longer than I was meant to	3.08
C.13 I lost track of time	3.23
C.14 I really got into the game	3.69

Of all questions, the last one's: *C.14 I really got into the game* mean is the highest (3.69). More specifically, 4 users' answers were "Agree" and 4 were "Strongly agree" (Table 11). Combined

with our observation's conclusions, it would be accurate to assume that users indeed emerged in the game's world (its 3D design contributed to this).

Table 11. GEQ C.14 I really got into the game

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Total
Frequency	1	1	3	4	4	13
Percent	7.7	7.7	23.1	30.8	30.8	100.0

Furthermore, the question: *C.7 The game felt real* can be related to the above, as 38.5% selected "Agree". Positive feedback was also given from the users during gameplay regarding the game's interface, i.e. it felt like a real-world simulation.

For most users, completing the scenarios was a relatively smooth procedure, as there was constant guidance within the game (pop-ups with guiding messages appear during gameplay, so that the user knows where to refer to next in order to solve the problem and reach the goal), as well as supervision and assistance by the researcher, when needed.

It is important to note though that users seemed to have difficulty as the scenarios became more complex: During the last scenario: *Patches,* they needed assistance for the most part and they seemed to get tired and overwhelmed when they couldn't reach their goal, hence the scenario started all over from the beginning. This experience may justify the result in questions *C.6 I felt like I couldn't stop playing* (2.46) and *C.10 Playing made me feel calm* (2.46). In the second question in particular, 6 out of 13 answers (46.2%) were "Disagree", leading us to assume that they were frustrated by the complexity of the last scenario and the fact they had to restart when they failed to reach the scenario's goal**.** As mentioned previously, when we examined questions B.9 and B.10, the students are aware of the term *Patches,* therefore we can infer here that they felt this way due to the game's design and complexity and not due to lack of knowledge.

A 30.8% agreed that they wanted to play for longer than it was meant to (C.12), although this percentage is not enough to conclude that this is the case, as a 23.1% disagreed (Table 12). This question implies that the game is challenging enough to engage users and to make them want more of it (either because playing was pleasant/fulfilling or because they didn't achieve the goals within the specific timeframe-or both).

Table 12. GEQ C.12 I wanted to play for longer than I was meant to

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Total
Frequency	2	3	2	4	2	13
Percent	15.4	23.1	15.4	30.8	15.4	100.0

Overall, combining the GEQ and our observation's results, the users' reactions were rather indifferent towards the game. All of them were concentrated while playing and were eagerly trying to reach the scenarios' objectives. Even when they failed, they would go back and retry, each time attempting different actions and procedures (which was one of our main goals to start with). However, their main milestone was the last scenario (Patches), and especially its last phase, as it was the most complex of the three and required the most trial-and-error actions by the students, going back and forth to ensure application patching is performed correctly. We strongly believe, however, that if the scenarios employed in this intervention had been tailor-made (thus created and customized) by the instructors to ensure the most possible correlation with the course's concepts and learning outcomes (as set in the courses curriculum), student engagement could have been increased, as the game would have been more adequately embedded in the learning process.

In order to better understand the criteria (factors) we set to measure any alterations pre-survey and post survey, and to be able to identify user engagement towards the serious game CyberCIEGE, we set a number of indicators, each of them corresponding to game actions and user reactions, respectively. A table containing those data as well as the pre and post survey values of each indicator can be found below (Table 13). Each criterion has a certain weight assigned to it, and so does each sub-criterion, as shown in the table:

Table 13. Qualitative analysis: Criteria and indicators of user behavior, technical knowledge and user engagement

	Criteria	Indicators	Pre-survey value	Post-survey value	Weight (100%)	Game actions
1.	**User behavior**				**30**	
1.1	Understanding of basic cybersecurity concepts	UCS1 (Logging out when leaving the room)	High	Low	7.5	Establishing the initial network
		UCS2 (Performing ofter anti-virus updates)	Neutral	Neutral	7.5	Ensure user procedural security via procedural settings
		UCS3 (Not opening attachments from unknown senders)	High	High	7.5	
		UCS4 (Understanding what a strong password consists of)	High	High	7.5	Establishing Physical Security and Individual Accountability
2.	**Technical knowledge & skills**				**30**	
2.1	Understanding physical security	UPS1 (Understanding what physical security practically is by providing examples)	High	High	7	Establishing Procedural Security and User Training
		UPS2 (Understanding the importance of physical security)	High	High	5	Establishing Physical Security to protect SECRET and TOP SECRET assets
2.2	Understanding application patches	UAP1 (Understanding the term "patches")	High	High	7	Patch web application server via configural settings
		UAP2 (Understanding the importance of patching)	Neutral	Neutral	5	Test the effectiveness of patches of applications before they are

		UAP3 (Understanding the importance of training employees for application patching)	High	High	6	applied

	Criteria	Indicators	Pre-survey value	Post-survey value	Weight (100%)	User reactions
3.	**User engagement**				**40**	
3.1	Sensory and Imaginative Immersion	SII1 (I lost track of where I was)	N/A	Neutral	2.8	Losing sense of space
		SII 2 (Time seemed to stand still and stop)		Neutral	2.8	Losing sense of time
		SII 3 (I lost track of time)		High	2.8	
		SII 4 (I didn't answer when someone talked)		Low	2.8	Losing contact with the environment
3.2	Flow	F1 (Playing seemed automatic)	N/A	Low	2.8	Playing is automatic
		F2 (I played without thinking how to play)		Low	2.8	Playing without thinking
		F3 (My thoughts went fast)		High	2.8	Thoughts go fast
3.3	Negative Effect	NE1 (I felt scared)	N/A	Low	2.8	Fear
3.4	Positive Effect	PE1 (I couldn't tell I was getting tired)	N/A	Low	2.8	No sense of tireness
		PE2 (I felt like I couldn't stop playing)		Low	2.8	Desire to not stop playing
		PE3 (The game felt real)		High	2.8	The game feels real
		PE4 (Playing made me feel calm)		Low	2.8	Playing makes users feel calm
		PE5 (I wanted to play for longer than I was meant to)		Neutral	2.8	Desire to play for longer than meant to
		PE6 (I really got into the game)		High	2.8	Interest and positive attitude towards the game

3) RQ3: Can the SBL theory components be implemented in a pedagogical instructional design's phases by the SBL theory, utilizing the serious game CyberCIEGE in a workshop?

Regarding the following:

- **RQ3a: activation of prior knowledge/experience (Introduction)**

The simulation-based learning theory consists of 4 phases: Introduction, Briefing, Scenarios and Debriefing. Each of these phases contains components (goals), the compliance to which is of high

importance in order to serve the theory's application. Below, we will examine if and how these components were served in our intervention.

During the introduction phase, the objective is to activate the learners' prior knowledge and remind them of past experiences, in order for them to find connections with the new knowledge which they have not acquired yet. They are briefly introduced to the intervention's subject and structure. In our specific case, we introduced the students to the CyberCIEGE game (as this would be their hands-on experience), describing them how it works and what were the basic concepts they would interact with. Our intervention took place during the start of the spring semester, in the context of the module *Information Systems Security,* which is an introductory cybersecurity semester-long course. The course's description follows, as copied from the university's website:

Learning Outcomes:
The purpose of the course is to acquaint students with the techniques and methods used to ensure the confidentiality, integrity and availability of the data managed by information systems and of the information systems themselves.

In this context, the learning outcomes of the course, after its successful completion, are that the students will be able:

- to understand the basic concepts of identification and authentication, access control and malware.
- to know the modern authentication techniques, access control, operating system security, database system security, malware protection, and IT systems.
- to analyze, evaluate and justify alternative authentication, identity management, and malware protection systems.
- to design authentication, identity management and access control systems.

Course Contents

- Identification and Authentication: Authentication Categories, Authentication Data, Authentication Systems, Biometric Systems.
- Identity management: examples, technologies, data protection.
- Access control: Access operations, access matrix, access control mechanisms.
- Security of Operating Systems: Operating System Security Parameters, Operating Systems Security Mechanisms, development of secure OS, case studies (Unix, Windows NT).
- Database Systems Security: Security requirements, data integrity and system availability, security for sensitive data, multi-level databases, Oracle security.
- Malware: Classification, types, methods, case studies.

- System and product security and assurance: Purpose, issues and methods of assurance, assurance criteria, evaluation systems.

Considering that the students interacted with the following scenarios: 1) Introduction, 2) Physical security and 3) Patches, -all three of which introduce the player to basic cybersecurity concepts-, and also completed pre-survey questionnaires containing relevant questions, they were asked to activate and apply prior knowledge and experience into the learning process.

- **RQ3b-i: familiarization with the environment, the case, and their roles (Briefing)**

During the Briefing part of the SBL theory, students had the first in-depth contact with the game and the whole structure of the intervention to follow: they were first introduced to the game briefly via an oral presentation by the researcher, explaining the basic concepts of the scenarios, the objectives and the game design. All of them were already familiar with *The Sims* game, so they quickly realized the concept of a simulation game set in a company's premises, where they would have to take the role of cybersecurity network specialists (practically employees of the company).

- **RQ3b-ii: setting individual roles (Briefing)**

During this phase, it is essential to provide detailed information to the students regarding their roles in the learning procedure. What matters is communicating to them the importance of setting defined responsibilities in order to achieve defined goals. In our case, each of the students had the game installed in their own computer, and it was made clear to them beforehand that they would play individually. The game is designed to assimilate to the structure of a corporation: users are the company's employees (IT specialists). They are in charge of protecting important assets and at the same time not exceeding the company's budget. This was made clear to the students before starting the game, and visual aid was used for this purpose (a presentation containing screenshots from the gameplay).

- **RQ3c-i: participation in the simulation (Scenarios)**

Students actively participate in the simulation scenarios under the instructor's supervision and guidance. However, considering that the end users are undergraduate IT students and that the game is very explanatory, as it provides steps, guidance and feedback, supervision is not mandatory, if not unnecessary. If sufficient information has been provided during the previous phase, an instructor simply makes sure that the whole procedure will be carried out without implications, and of course helps and advises if it's deemed necessary for the learners' progress and smooth learning experience. During our intervention, while the students were playing the game CyberCIEGE, (thus were participating in the simulation scenarios), the instructor was

monitoring and observing their actions, providing assistance when needed, mostly during the 3rd scenario (Patches) where students seemed to have the most difficulty (due to the scenario's complexity and duration).

- **RQ3c-ii: practice of knowledge and skills (Scenarios)**

This is the phase during which the hands-on experience is predominant. The students interact with the simulation's activities and activate knowledge they already have, to acquire new knowledge, new concepts and notions which they can contextualize and thus, use in real-life situations (this is the purpose of simulations in any case). Our sample completed three already existing scenarios of the CyberCIEGE game: Introduction, Physical Security and Patches. Due to the fact that they were IT students, most of them were familiar with most concepts present in the scenarios, which, on the one hand, served the purpose of a brief revision, but on the other hand, did not provide them with brand new information that they had never encountered before. However, even being involved in a simulative situation can enhance skills that are otherwise non present (such as problem-solving, proactive and critical thinking etc.).

- **RQ3d-i: comprehensive evaluation (Debriefing)**

Debriefing is the last phase of the SBL theory, but not less important than the previous ones, as it determines the progress of the students and measures results to reach conclusions regarding the goals set during the design of the simulation intervention. The first component in the debriefing phase is related with the students' evaluation; there are numerous means of measuring if and how the intervention affected the students' knowledge, and if it was indeed successful in helping them achieve the learning process's goals. Tests, questionnaires, interviews, etc. can be used for this purpose. In our case, post-survey questionnaires were employed to evaluate students' knowledge in relation with the following metrics: user behavior, technical knowledge and skills, and engagement. The same metrics were examined using the pre-survey questionnaire, therefore the post-survey one serves to compare the students' answers and reach conclusions. Certainly, there are other ways to achieve this, as mentioned previously (for example, tests and/or interviews). It is preferable having pre-intervention data to compare the results with, for efficiency purposes. What is of most importance here, is to reach measurable conclusions, which can then help improve the design for future use, to make it more competent and robust to achieve its purpose.

- **RQ3d-ii: reflection and critical analysis of the learning process (Debriefing)**

This, along with the next two components of the debriefing phase, can be revised by the instructor alone. The whole learning process in its entirety is analyzed to determine its efficiency and impact in the students' knowledge acquisition. Through this process, possible

mistakes/oversights in the design can be tracked and thus, avoided in the future. In our case, this step was critical to be able to define our limitations and future work possibilities, which will be thoroughly discussed in Chapter 5.

- **RQ3d-iii: the knowledge and the learning environment (Debriefing)**

It is important in this stage to determine the exact knowledge that students acquired, compare it with the goals set in the beginning, and define the learning environment(s) in which this particular intervention can take place. For example, in our case, it is possible to set it in a live computer lab, or remotely, so that each player can access the game and play using their own PC. As mentioned previously in the same chapter, it is possible to integrate this particular intervention into an e-learning program, of a short or longer duration, depending on the learning goals the instructor would want to achieve and on other factors such as time, budget, resources etc.

- **RQ3d-iv: setting new learning goals (Debriefing)**

After having examined the impact of the simulation intervention in the learning process and determined if the learning goals were achieved, it is time to consider setting new learning goals for the future. These can be goals set to be achieved through the intervention only, or through the overall learning process, if the intervention is a part of it. In our case, new goals related with the game's next scenarios could be set (also in relation with the context in which the simulation will take place). For example, the game's scenarios could be integrated into the course *Information Systems Security*, throughout the whole semester. Due to the game's flexibility, new scenarios could be created, fully adapted to the course's concepts and learning goals.

Previously, we introduced this thesis's research questions and described the research design and methodology exploited for the purposes of our intervention. In the current chapter, we will examine if our objective was met, by answering the aforementioned research questions using data gathered throughout the overall procedure.

In order to analyze pre and post questionnaire data, IBM's software (SPSS) was used to find and compare means, in order to determine if the post-questionnaire results had any positive/negative difference from the pre-questionnaire ones, and to examine the game engagement levels from the GEQ.

4.3. Results

The analysis of this experiment's qualitative results, although preliminary, due to the lack of long-term implementation of the intervention, small sample size and other limitations described in

Chapter 5, provided us with a generic understanding of the levels of Greek IT students' security awareness, and their attitude towards an intervention simulating a cyber-security critical infrastructure environment involving risk assessment, requiring critical thinking and decision-making on their end. Overall, our sample was knowledgeable as far as cyber-security concepts are concerned, and their online user behavior seems to comply with basic cyber-security logic (i.e. they all use long and complex passwords). Regarding engagement towards the game, their reaction was generally neutral to positive. The amount of time spent playing the game was insufficient for them to be able to fully engage and immerse themselves in it, thus in a more long-term and commitment-requiring intervention, engagement levels could have been analyzed further and could have potentially provided results of added value.

Moreover, the serious game we used for this intervention, CyberCIEGE, offers pedagogical affordances with regard to its pedagogical uses and to its educational quality, as we have mentioned in previous chapters, which can be seen in previous studies conducted already, employing CyberCIEGE for educational and research purposes and also in our own experiment. Among other advantages, it is a tool which is by default competitive, given that simulation can undoubtedly be used efficiently in the cyber-security field for training and learning purposes, but it is also user-friendly, it has a clear scenario structure/flow where the distribution of roles, objectives, assets is distinct, and provides constant feedback and assessment to learners.

Our third and last research question was the following: Can the SBL theory components be implemented in a pedagogical instructional design's phases by the SBL theory, utilizing the serious game CyberCIEGE in a workshop? As we described previously in detail, in the current Chapter's analysis, the simulation-based learning theory consists of certain components which are required for the theory's implementation in practice. In order for this research question to be answered, we needed to conduct the experiment and use the live observation method throughout the whole procedure, as we would have to match our notes with each component of the SBL theory to determine if the latter was indeed employed/implemented in the learning intervention and to deem if it was indeed carried out as supposed to, and if it had the expected results. Our findings showed that, indeed, the SBL components can be effectively implemented in a planned, live workshop which utilizes a simulation serious game as an intervention to the learning process.

Chapter 5 – Conclusions

5.1 Limitations

The findings of this study need to be seen in light of some limitations.
Our results are preliminary, due to several limitations which will be further discussed below.
First of all, our sample was limited to 13 students, which is a very small number to be used for reaching accurate conclusions and results. On this basis, we were only able to experimentally infer, from the data we gathered throughout the intervention, how the latter affected the learning process for the students.

Another limitation was the time constraint to meet the deadline of the thesis's submission, which prevented the study from being longitudinal. The duration of our intervention was 3 hours. A longer research (of e.g. a semester) would most probably provide concrete results and a more circumstantial data report, as our conclusions remain mere assumptions. If the duration had been longer, we would have collected data also from log files, to track the users' actions during gameplay.

Our study would have potentially been able to provide comparable data, had we had in our disposal another sample group from a different educational field. For example, it would be interesting to compare the effects of the simulation to IT students compared to students who have no information security background and experience, as the first scenarios of CyberCIEGE can be easily played even by users who are not familiar with cybersecurity concepts.

After having acknowledged our limitations, we will next present some suggestions for future work and sustainable approaches towards this thesis's goals.

5.2 Future work

CyberCIEGE can be further customized and designed to be used for larger sample sizes of students in a related context. The game is designed for training purposes, but it can also be adequately used to raise cybersecurity awareness and affect user behavior and knowledge successfully, if integrated in an educational program which will allow this kind of learning experience. Its main perk is that it is customizable; instructors can create their own scenarios according to their students' needs and not necessarily use the already existing ones. Due to lack of time and expertise in the cybersecurity field, we did not proceed with creating new scenarios for the purposes of this thesis.

What would possibly be of interest as well could be measuring game engagement levels in correlation to the users' gaming experience and their feelings towards gaming. Users who tend to play games and are familiar with game components and scenarios may develop different engagement levels than those who do not play games and do not enjoy doing so. This is of course a speculation, but it would be interesting nonetheless examining engagement from this perspective.

Even though the study we conducted provided preliminary results which, due to limitations described previously, cannot be considered representative of a large population, it can prepare the ground for a longer, tailor-made, structured and well-designed intervention to take place in a larger scale, with more learners participating, more resources and data collection tools and with no time restrictions. The methodology and design employed for the thesis' purposes can be adapted and used in a larger scale study; given that the intervention was designed to be able to be re-used (be as sustainable as possible for further use), researchers and instructors can implement it to a program to explore the field of cybersecurity education which is currently advancing, and is in need of new challenges and systematic analysis.

Appendix

1. Pre-survey questionnaire

Simulation-based learning in critical infrastructure security awareness

Pre-survey questionnaire

A. DEMOGRAPHICS

A.1 Age:

A.2 Sex:

A.3 Work experience in the IT field:

I have no experience at all I have some experience I have a lot of experience

B. ASSESSMENT

Please choose the answer which best describes each statement according to you:

1. How do you assess your knowledge on information security risk management?

   Minimal Insufficient Sufficient Good Excellent

2. Using long and complex passwords which are changed regularly is sufficient for protecting important assets.

   Minimal Insufficient Sufficient Good Excellent

3. How often do you log out of your computer when you leave the room?

   Never Rarely Sometimes Very often Always

4. How often do you check the anti-virus software or set it for automatic updates?

   Never Rarely Sometimes Very often Always

5. How often do you open attachments from incoming emails, from unknown senders?

Never Rarely Sometimes Very often Always

6. Write below an example of a strong password:

_____

7. Write two examples of physical security in a workstation.

_____

8. How important is it for a company to provide enough physical security to protect its assets?

Not important Slightly important Moderately important Important Very important

9. Are you familiar with the term "patches"?

No A little Yes

10. If you chose "Yes" in question 9, write a short definition and explain why patch management is important in your opinion.

_____

11. If you chose "Yes" in question 6, select how important it is for a company to train employees for application patching in your opinion.

Not important Slightly important Moderately important Important Very important

2. Post-survey questionnaire

Simulation-based learning in critical infrastructure security awareness

Post-survey questionnaire

A. DEMOGRAPHICS

A.1 Age:

A.2 Sex:

A.3 Work experience in the IT field:

I have no experience at all I have some experience I have a lot of experience

B. ASSESSMENT

Please choose the answer which best describes each statement according to you:

1. How do you assess your knowledge on information security risk management?

Minimal Insufficient Sufficient Good Excellent

2. Using long and complex passwords which are changed regularly is sufficient for protecting important assets.

Minimal Insufficient Sufficient Good Excellent

3. How often do you log out of your computer when you leave the room?

Never Rarely Sometimes Very often Always

4. How often do you check the anti-virus software or set it for automatic updates?

Never Rarely Sometimes Very often Always

5. How often do you open attachments from incoming emails, from unknown senders?

Never Rarely Sometimes Very often Always

6. Write below an example of a strong password:

_____

7. Write two examples of physical security in a workstation.

_____

8. How important is it for a company to provide enough physical security to protect its assets?

Not important Slightly important Moderately important Important Very important

9. Are you familiar with the term "patches"?

No A little Yes

10. If you chose "Yes" in question 9, write a short definition and explain why patch management is important in your opinion.

_____

11. If you chose "Yes" in question 6, select how important it is for a company to train employees for application patching in your opinion.

Not important Slightly important Moderately important Important Very important

C. ENGAGEMENT

Please choose the answer which best describes each statement according to you:

1. I felt scared

Strongly disagree Disagree Neutral Agree Strongly agree

2. I lost track of where I was

Strongly disagree Disagree Neutral Agree Strongly agree

3. Time seemed to stand still and stop

Strongly disagree Disagree Neutral Agree Strongly agree

4. I didn't answer when someone talked

Strongly disagree Disagree Neutral Agree Strongly agree

5. I couldn't tell I was getting tired

Strongly disagree Disagree Neutral Agree Strongly agree

6. I felt like I couldn't stop playing

Strongly disagree Disagree Neutral Agree Strongly agree

7. The game felt real

Strongly disagree Disagree Neutral Agree Strongly agree

8. Playing seemed automatic

Strongly disagree Disagree Neutral Agree Strongly agree

9. I played without thinking how to play

Strongly disagree Disagree Neutral Agree Strongly agree

10. Playing made me feel calm

Strongly disagree Disagree Neutral Agree Strongly agree

11. My thoughts went fast

Strongly disagree Disagree Neutral Agree Strongly agree

12. I wanted to play for longer than I was meant to

Strongly disagree Disagree Neutral Agree Strongly agree

13. I lost track of time

Strongly disagree Disagree Neutral Agree Strongly agree

14. I really got into the game

Strongly disagree Disagree Neutral Agree Strongly agree

3.Observation checklist and notes

Pedagogical uses	CyberCIEGE compliance	Notes
Recording	✔	Possible via log files.
First-person view	✔	Allows access to difficult to reach locations (company's premises).
Live guidance	✔	Instructions during gameplay, helpful database with articles.
Feedback	✔	Positive or negative-depending on the user's actions.
Customization and flexibility	✔	Possible to customize and create scenarios.
e-Learning potential	✔	Possible to use remotely/virtual environment.

Educational quality	CyberCIEGE compliance	Notes
Engagement	N/A	Overall reaction to the game: positive, but some found it difficult and long
Efficiency: -Active learning -Collaboration	✔	-Active learning: users use critical thinking, make a decision and take action. -Possible to collaborate with classmates to reach a game objective.

Logistical & other	CyberCIEGE compliance	Notes
No cost	✔	The game is free for educational purposes.
Support	✔	Database with articles available. Support page for instructors.
Time efficiency	✔	Virtual experience: less time-consuming than real-time experiment.

4.Consent form

Informed Consent Form

Simulation based learning in critical infrastructure security awareness: An empirical study

Elisavet Maria Katsika MSC e-Learning Postgraduate Student

1. I confirm that I have read and I understand the information sheet for the above study and have had the opportunity to ask questions.

2. I understand that my participation is voluntary and that I am free to withdraw at any time, without giving reason.

3. I agree to take part in the above study.

4. I agree to the use of anonymized quotations in publications

Signed and dated by participant and researcher

X

References

(n.d.). Retrieved from Naval Postgraduate School: https://my.nps.edu/web/c3o/cyberciege

(n.d.). Retrieved from EA : https://www.ea.com/games/simcity

Aloul, F. (2012). The need for Effective Information Security Awareness. *International Journal of Intelligent Computing Research*, 116-123.

Anderson, J. &. (1996). Situated learning and education. *Educational Researcher*, 5-11.

Arnett, A. (2017, 06 05). *Adding simulations to science lessons increases student engagement, understanding.* Retrieved from Education Dive: https://www.educationdive.com/news/adding-simulations-to-science-lessons-increases-student-engagement-underst/444219/

Auman, C. (2011). Using simulation games to increase student and instructor engagement. *College Teaching* , 154-161.

Benzel, T. (2011). The science of cyber security experimentation: the DETER project. *Proceedings of the 27th Annual Computer Security Applications Conference* (pp. 137-148). Orlando, FL, USA: ACM.

Bliss, J. &. (1989). Tools for exploratory learning. *Journal of Computer Assisted Learning*, 37-50.

Bredo, E. (1997). The social construction of learning. In G. Phye, *Handbook of academiclearning: The construction of knowledge* (pp. 3-45). New York: Academic Press.

Brown, J. &. (1989). Situated Cognition and the Culture of Learning. *Educational Researcher*, 32-42.

Chen, Y. &. (2011). Efficacy of Simulation-Based Learning of Electronics Using Visualization and Manipulation. *Educational Technology & Society, 14*(2), 269-277.

Csikszentmihalyi, M. (1990). *Flow: The psychology of optimal experience.* New York: Harper & Row.

Davies, C. (2002). Student engagement with simulations: a case study. *Computers & Education , 39*, 271–282.

Dickey, M. (2005). Engaging By Design: How Engagement Strategies in Popular Computer and Video Games Can Inform Instructional Design. *Educational Technology Research and Development*, 67-83.

Dorner, R. &. (2015). *Entertainment computing and Serious Games.* Arequipa: Springer.

Fung, C. &. (2008). Raising information security awareness in digital ecosystem with games - a pilot study in Thailand. *2nd IEEE International Conference on Digital Ecosystems and Technologies* (pp. 375 - 380). Phitsanulok: IEEE Xplore.

Gagliardi, C. &. (2016). *Advancing cybersecurity Research and Education in Europe.* ACM.

Gkioulos, V. &. (2017). Security Awareness of the Digital Natives. *Information (Switzerland)*, 13.

Gredler, M. (1996). *Educational games and simulations.* New York: MacMillan Library Reference.

Gredler, M. E. (n.d.).

Gredler, M. E. (1996). *Educational games and simulations.* New York: MacMillan Library Reference.

Grevelink, J. (2015, January). *Serious games for cybersecurity.* Tilburg: Tilburg University.

Harper, S. M. (2000). Constructivist Simulations: A New Design Paradigm. *Jl. of Educational Multimedia and Hypermedia*, 115-130.

Hendrix, M. &. (2016). Game Based Cyber Security Training: are Serious Games suitable for cybersecurity training? *International Journal of Serious Games*, 53-61.

Henry, J. &. (2017). A Measure of Student Engagement for Serious Games and IoT. *11th International Conference, Edutainment 2017* (pp. 262-270). Bournemouth, UK: Springer.

Hughes, A. (2019, November 19). *eLearning industry*. Retrieved from eLearning industry: https://elearningindustry.com/serious-games-elements-increase-engagement-knowledge-retention

Husebø, S. &. (2018). Status of Nordic research on simulationbased learning in healthcare: an integrative review. *Advances in Simulation*, 3, 12.

IBM. (2014). *IBM Security Services 2014: Cyber Security Intelligence Index.* IBM Corporation.

Jones, J. &. (2010). A comparative study of CyberCIEGE game and Department of Defense Information Assurance Awareness video. *IEEE SoutheastCon 2010 (SoutheastCon)* (pp. 176-180). Concord, NC, USA: IEEE.

Kafai, Y. B. (2006). Playing and making games for learning:. *Games and culture*, 36-40.

Kavak, H. &. (2016). A characterization of cybersecurity simulation scenarios. *Proceedings of the 19th Communications & Networking Symposium* (pp. 1-8). Pasadena, California: Society for Computer Simulation International.

Kurt, S. (2017). ADDIE Model: Instructional Design . *Educational Technology*.

Langer, E. (1997). *The Power of Mindful Learning.* Da Capo Lifelong Books.

Lave, J. &. (1991). *Situated Learning: Legitimate Peripheral Participation.* Cambridge: Cambridge University Press.

Leng, T. (2003). *Scenario Selection and Student Assessment Modules for CyberCIEGE.* Storming Media.

Li, C. &. (2016). Survey of Cybersecurity Education through Gamification. *ASEE's 123rd Annual Conference and Exposition.* New Orleans: ASEE Annual Conference & Exposition.

Magennis, S. &. (2005). Teaching and learning activities: Expanding the repertoire to support student learning. In G. &. O'Neill, *Emerging Issues in the Practice of University learning and teaching* (pp. 45-54). Dublin: AISHE.

Maheu, C. &. (2018). Effectiveness of serious games and impact of design elements on engagement and educational outcomes in healthcare professionals and students: a systematic review and metaanalysis protocol. *BMJ Open*.

Marone, V. (2016). Playful Constructivism: Making sense of digital games for learning and creativity through play, design and participation. *Journal of Virtual Worlds Research Vol. 9*, 1-18.

Michalas, A. (2017, 05 18). *Three Things We Have Learnt From The WannaCry Cyber Attack.* Retrieved from The Huffington Post: https://www.huffingtonpost.co.uk/dr-antonis-michalas/post_14993_b_16670042.html?guccounter=1.

Norman, D. (1988). *The design of everyday things.* New York: Basic Books.

NPS. (n.d.). Retrieved from CyberCIEGE: http://www.cyberciege.com/

NPS. (2006, 04 04). *Introduction Scenario.* Retrieved from Naval Postgraduate School: https://my.nps.edu/documents/107523844/108901322/IntroductionScenario.pdf/1c660719-d705-430c-88a8-0621e7b31b8c

NPS. (2006, 03 14). *Physical Security.* Retrieved from Naval Postgraduate School: https://my.nps.edu/documents/107523844/108901322/PhysicalSecurity.pdf/8ab3b0e0-159d-475e-8788-001f97bb30cc

NPS. (2011, 02 14). *Patches.* Retrieved from Naval Postgraduate School: https://my.nps.edu/documents/107523844/108901322/patches.pdf/ebf85c40-c8fe-4c4f-a6bb-84aac7cdbc1d

NPS. (2014, February 11). *Naval Postgraduate School.* Retrieved September 11, 2019, from https://my.nps.edu/documents/107523844/108901322/patches.pdf/ebf85c40-c8fe-4c4f-a6bb-84aac7cdbc1d

Papert, H. (1991). *Constructionism.* New Jersey: Ablex Publishing.

Pastor, P. &. (2010). State-of-the-art simulation systems for information security education, training and awareness. *2010 IEEE Education Engineering Conference, EDUCON* (pp. 1907 - 1916). IEEE.

Perski, O. &. (2017). Conceptualising engagement with digital behaviour change interventions: a systematic review using principles from critical interpretive synthesis. *Transl Behav Med, 7*, 254-67.

Pourabdollahiana, B. &. (2012). Serious games in manufacturing education: Evaluation of learners' engagement. *Procedia Computer Science*, 256-65.

Raman, L. A. (2014). Serious Games based approach to cyber security concept learning: Indian context. *2014 International Conference on Green Computing Communication and Electrical Engineering (ICGCCEE)* (pp. 1-5). Coimbatore: 2014 International Conference on Green Computing Communication and Electrical Engineering (ICGCCEE).

Reeve, J. &. (2004). Enhancing students' engagement by increasing teachers' autonomy support. *Motivation & Emotion, 28*, 147-69.

Ribeiro, C. &. (2014). Identifying Engagement with Learning in Serious Games. *1st Workshop on Learning Analytics for and in serious games (LASG 2014) in conjunction with the 9th European Conference on Technology Enhanced Learning (EC-TEL 2014)* (pp. 26-28). Graz, Austria: Springer.

Ross, G. &. (2003). Experimental Research Methods. In D. Jonassen, *Handbook of Research for Educational Communications and Technology* (pp. 1148-1170). Routledge.

Salazar, M. &. (2013). Enhancing Cybersecurity Learning through an augmented reality-based serious game. *IEEE Global Engineering Education Conference (EDUCON)* (pp. 602-607). Berlin: IEEE.

Sanchez Casado, L. &. (2013). NETA: Evaluating the effects of NETwork Attacks. MANETs as a case study. *Communications in Computer and Information Science*, 1-10.

Schuurink, H. &. (2008). Engagement and EMG in Serious Gaming: Experimenting with Sound and Dynamics in the Levee Patroller game. *Fun and games: International conference on fun and games* (pp. 139-149). Berlin: Springer.

Strickland, J. &. (2012). Online Course Development Using the ADDIE Instruction Design Model: The Need to Establish Validity. *SITE*, (pp. 2046-2054). New Orleans.

Švábenský, J. V. (2018). *Enhancing Cybersecurity Skills by Creating Serious Games.* Larnaca: ITiCSE.

Taher, M. &. (2014). Impact of Simulation-based and Hands-on Teaching Methodologies on Students'. *121st ASEE Annual Conference & Exposition.* Indianapolis: American Society for Engineering Education.

Takatalo, J. &. (2011). User experience in digital games differences between laboratory and home. *Simulation & Gaming, 42*, 656-73.

Thompson, M. &. (2011). Active Learning with the CyberCIEGE Video Game. *4th conference on Cyber security experimentation and test*, (pp. 1-10). San Fransisco.

Timur, K. &. (2015). The Effect of Simulation-based Learning on Prospective Teachers' Inference Skills in Teaching Probability. *Universal Journal of Educational Research, 3*(11), 775-786.

Veksler, V. &. (2018). Simulations in Cyber-Security: A Review of Cognitive Modeling of Network Attackers, Defenders, and Users. *Frontiers in Psychology*, 691.

Wach-Kakolewicz, A. &. (2016). *Perspectives on Computer Gaming in Higher Education.* Poznan.

Woolfolk, A. (1980). *Educational Psychology.* Toronto: Allyn & Bacon.

Wright, S. (2015, 12 22). *Security Awareness Training: What's The Problem?* Retrieved from Nettitude: https://blog.nettitude.com/uk/security-awareness-training-whats-the-problem