Review of Serious Games Applied to Information Systems Security Audit

Carlos Cunha[1] and Hugo Barbosa [2] [0000-0003-1205-8990]

1 Lusofona University, Porto - Portugal, carloseduardopinhodacostacunha@gmail.com
2 Lusofona University, Porto - Portugal | SIIS - Social innovation and Interactive Systems, School of Engineering of the Polytechnic of Porto, Porto, Portugal, hugo.barbosa@ulp.pt

Abstract. With the permanent evolution of the world, one thing that seems to resist the sign of the times is the classic education system. Many scholars refute this system saying that it is outdated and non-efficient, providing different solutions to remodel the current method. Among the vast options to provide a better learning experience, serious games stand out due to their benefits, such as immediate feedback, multitasking, and promoting collaborative work. This paper seeks to analyze the effectiveness of serious games when applied to a work-related situation, namely a hypothetical scenario connected with cybersecurity. To support this, there is the simple fact of an increasing number of cyberattacks, and their sophistication and effectiveness are ever-growing. A wide variety of cyberattacks and social engineering make so no company is safe. That's one of the main reasons why cybersecurity must never be overlooked in any company, since an attack can cause losses and, sometimes, may even render the company workless for hours. The course of developing a serious game is fundamentally the same as developing a normal game. But, when designing and developing the game mechanics, it's essential to never overlook the pedagogic component of it. Furthermore, after the moment of the announcement, release, and distribution, evaluation studies must be made, not only to analyze the satisfaction but also for the sharpening set of skills developed throughout the game. The game-based learning applied to cybersecurity has already hit the market, having a wide number of serious games solutions made available by companies.

Keywords: Serious Game · cybersecurity · Education · Training · Security Audit, Game-Based Learning, Simulation.

1 Introduction

Having fun and relaxing has always been the way of life of many people. Since the most remote times, human beings have developed unique ways to enjoy quality time, especially when trying to release stress. Ultimately, someone found out that competing towards an objective was a great way to entertain while sometimes developing soft and hard skills. With this, the concept of a game was born, and consequently, the idea of developing skills through games began to take place. The definition of games designed for a purpose beyond entertainment gave birth to what we know today as serious games.

Analyzing the serious games market, researchers point out a record maximum of 5.51 billion Euros in 2020, with studies expecting its value to reach 22.37 billion Euros by 2026. All this presents a new tendency of entities worldwide to invest in serious games due to their efficiency.

2 Serious Games

Throughout this section, it will be presented a small introduction to the concept of serious games, their historical moment in time of creation, their most notorious advantages, and a small guide of a framework for development.

2.1 Concept

Serious games are a branch of gaming industry, in which their primary goal is to promote learning and behavior change instead of entertainment. Meanwhile, this last point can mislead since serious games can be educational and exciting. Serious gaming has been developing itself in many areas such as military, education, marketing, healthcare, politics, and even city planning. The main point of serious games is the combination of learning strategies, knowledge, and game elements to teach specific skills, knowledge, and attitudes. Using the entertainment and engagement provided by the games, the players solve problems that simulate real-world situations. Serious games can be seen in every way as common games can, such as board games, electronic games, or card games.[1].

2.2 Origins

In 1970, Clark C. Abt publishes "Serious Game", a book where for the first time, the use of "serious games" as an oxymoron comes up. Abt is a researcher who worked for the U.S during the Cold War. One of his objectives was to train and educate using several computer games such as T.E.M.P.E.R. This game was used by military officers to study the Cold War conflict on a worldwide scale.

In this book, Abt sets the definition for a serious game: "*Games may be played seriously or casually. We are concerned with serious games in the sense that these games have an explicit and carefully thought-out educational purpose and are not intended to be played primarily for amusement. This does not mean that serious games are not, or should not be, entertaining*" [2].

Proceedings of the Digital Privacy and Security Conference 2022 | 10.11228/dpsc.04.01

2.3 Advantages

Among the vast benefits of game-based learning the following stand out:

- **Stimulates the mind** - Simple activities as playing any type of game can bring cognitive and psychological benefits, this way delaying natural aging. In some cases, game-based learning drives decision-making, which improves cognitive function and helps people learn valuable skills and lessons applicable to real life [3].
- **Improves self-esteem** - While playing, it is easier to interact with others, establish dialogue and overcome any kind of social and generational barriers. Therefore, the use of serious games for training improves the self-esteem of the student, who tries to explore and find alternative approaches to solve different situations in the process of learning [3].
- **Applicable to the real world** - Serious games applied for training enable students to understand new concepts and develop their skills throughout the game. Simulating real-life experiences creates a powerful interactive environment that makes it possible to practice, compete or cooperate, making students eager to learn and retain new information, leading to complete success when it is applied [3].
  Permanent personal development - Students are encouraged to develop their skills continuously and steadily over time, thanks to the gaming environment. Serious games for training favor skills as important as observation, motivation, overcoming criticism, strategic thinking, and, of course, soft skills. Meanwhile, games allow people just to simply be bad at them, making them realize that poor decisions or choices bring punishment to them. This way, they understand that rules are difficult to bypass and that these new concepts are meant to help them overcome themselves [3].
- **Instant feedback** - One of the benefits of game-based learning platforms is undoubtedly the possibility of obtaining immediate feedback from student performance. Serious games for training incorporate systems that permit constant monitoring. Thus, those responsible for the implementation of training can study the learning process in-depth, as well as its effect on the achievement of objectives [3].
- **Interactive nature** - Multimedia devices are very present in nowadays society and that makes people familiar with gaming elements - such as achievements, rankings, rewards, competition, levels, among others. The interactive nature of serious games enables students' engagement since all these playful elements contribute towards learning in a fun way, appropriate to the lifestyle of new generations, and favoring communication and coordination for problem-solving purposes [3].
  Collaborative Learning - Among the most important benefits of serious games for training is collaborative learning. People who learn through playing, usually do so in a collaborative environment, in which they work together to achieve a goal. By encouraging cooperation through the game, students increase their task satisfaction, feeling part of the team and are involved in achieving common goals [3].

2.4 Framework for development

With the already huge market of games, the market of serious games followed not only in market but in design methodologies. Through existing frameworks and methodologies there is a set of default steps that can be applied to most serious games.[4]

1º - Preliminary analysis Having a good project management from beginning may prevent catastrophic damage later on in the project, and game development is no exception. This step consists in setting the pedagogic goals for the game, study the target audience an technical constrains from the development.

1. Evaluating technical resources such as time,equipment, budget and technical skills. All these aspects have a serious impact in the game and should be analyzed to maximize success rate.
2. Defining all the pedagogic objectives. All soft and hard skills required and gained through the game should be identified. These skills will be tested through game mechanics.
3. Identifying target audience and context of play. Understanding target player base and the context where the game will be played can have play a major role in the success of the game.
4. Defining the pedagogic and game mechanics. Choosing appropriate mechanics is crucial when it comes to choose what genre the game will be. [4]

2º - Design The design component of the framework is all about building conceptual models, creating a balance between entertainment and the pedagogic component. Providing consistency between pedagogic mechanics and game mechanics will provide a engaging gameplay for the players. Also, progressive level difficulty is essential within the game, this provides that players develop new techniques and skills by themselves since the skills they had where not sufficient. This helps to build a more engaging gameplay but also stimulates player's creativity. A direct consequence of this is that the learning will be more effective.[4]

3º - Development This stage should provide technical guidance to develop the game while respecting the constrains discovered in the first step. The aim with the development of the game is to provide the best balance between time,skills and budget:

1. Support from a third party. Some companies who have more experience can provide either a full game or a vital support in the development of custom games. Though being a pricey solution, it will save a lot of time.
2. Off-the-shelf Game. A game that already exists can be used with a serious purpose, but the players will not be able to play the game without any type of guidance and instructions to complete the pedagogic objectives. Meaning the players will not be able to play the game by themselves.

Proceedings of the Digital Privacy and Security Conference 2022 | 10.11228/dpsc.04.01

3. Off-the-shelf Game with modifications. Some games let developers and players customize the game the way they want. If this happens a modification for the game can be implemented, letting the pedagogic part of the game be experienced alone. Implementing this solution may not consume much time or budget but it can be a challenge for the development team.
4. Assisted development. To relieve some pressure of video game development and improve the production, assisted methodologies may be implemented. This may be in form of tool kits that simplify the development process, requiring minimum amount of programming. The downside is that the options for customization are limited and complex scenarios may be very difficult to implement.
5. Full Development. This happens when the team has appropriate knowledge, time and resources and builds the game from scratch. In this methodology, the development team is fully responsible for all stages of game development.[4]

4º - Game assessment A crucial part of the development and could be compared to a user acceptance in general software development. This ensures that the game meets expectations regarding technical and pedagogic aspects. Developers can undercover bugs, improve gameplay and even modify game mechanics if really needed.[4]

5º - Deployment In this stage, there are rules that apply for the deployment of a serious game. Players are supervised and play sessions have limited time and are framed within the pedagogic plan. This stage is crucial for the game as a commercial product, the use of marketing campaigns, demonstrations and dedicated websites are among the techniques used by other companies.[4]

6º - Player assessment Finally, to determine the success of the game teaching new skills, its necessary to evaluate players. Some game mechanics can be implemented in order to track and evaluate players directly while playing. If pedagogic mechanics are perfectly implemented, players should acquire expert skills upon completion of the game.
Test surveys and questionnaires could be used in a way that does not require external intervention.[4]

3 Cybersecurity

According to [5], cybersecurity defines the practice of protecting systems, networks, and programs from digital attacks. These attacks are usually aimed at accessing, changing, or destroying sensitive information, extorting money from users, or interrupting normal business processes. Besides this, [5] also claims that implementing effective cybersecurity measures is proving more challenging due to the rise in the number of devices and attackers being innovative. An

effective cybersecurity approach has multiple layers of protection spread across computers, networks, programs, or data that one intends to keep safe. In an organization, the people, processes, and technology must complement one another to create an effective defense from cybercrime. Organizations are responsible for structuring an effective framework capable of dealing with attempted and successful cyberattacks. Technology is also essential for giving organizations and individuals the computer security tools needed to protect themselves from cyberattacks. Five main entities must be protected: end-point devices (computers, for example), smart devices, router devices, networks, and cloud servers.

In today's connected world, everyone benefits from advanced cyber-secure programs. At an individual level, a cyberattack can result in losing everything, from identity theft, extortion attempts, to loss of crucial data. On the other hand, critical services, and infrastructures, as power plants or hospitals need reassurance when fighting cyberattacks. That's the main reason why securing these, and other organizations are essential to keep our society normal functioning [6].

3.1 Types of Cyberattacks

Cybercrime is an ever-changing practice, but almost every type of attack can fall in-to these main categories:

- **Phishing** - Phishing is the practice of sending fraudulent emails that resemble reputable sources, like an online bank access point. The aim is to steal sensitive data like credit card numbers and login information. It's the most common type of cyberattack [7].
- **Ransomware** - Ransomware is a type of malicious software designed to extort money by blocking access to files or even the whole system through advanced encryption, paying the ransom won't guarantee the release of the files [8].
- **Malware** - Malware is intrusive software designed to gain unauthorized access, steal, or erase data, or cause significant damage to a computer system.
- **Social Engineering** - Social Engineering is a strategy used to trick someone to reveal sensitive information. Soliciting a monetary payment or gaining access to a computer, and therefore its data, are among the vast type of socially engineered attacks. The combination of social engineering and any of the attacks listed above can make people more likely to trust an external link, download malware, or even trust a malicious source of information [9].

3.2 COVID-19 and Cybersecurity

In consequence of the rise in cyberattacks and the fear of their information be leaked, some patients may not be as talkative about certain aspects of their medical history and/or condition, this can impact the quality of care [10].

Proceedings of the Digital Privacy and Security Conference 2022 | 10.11228/dpsc.04.01

4 Applying Serious Games to CyberSecurity

When it comes to cybercrime prevention, every measure that a person or a company takes is vital. Cyber attacks get even more sophisticated and different every hour, so there is no true way to be completely safe from them. Although regular back-ups, updated software, proper insurance that protects against cybercrime, and a well-designed data breach emergency plan can protect against a good range of cybercrimes, there is always a human element. Restrict administrative policy (the fewer people have access to sensitive data, the better) and a background check on every employee (identify criminal pasts) will always be vital to train staff.

All employees should have continuous training about cybercrime and how dangerous it can be at personal and business levels. Staff should have good knowledge about strong authentication, always making sure passwords agree to these traits:

- **It's long enough**, making it harder on brute-force attacks
- **Uses special characters** (lowercase, uppercase, numerals, and symbols)
- **Avoid complete words**, to avoid a dictionary-based attack.
- **Change regularly the password**, using the same pass for a long period can make the password vulnerable.
- **It's not shared across devices.**

Beyond a good password policy, staff should also be able to identify and know how to act upon being the target of a phishing or social engineering attack. Employees should: always check the reliability of email senders and their format; always suspect when the email sender makes an unusual or unexpected request; hover links to make sure they lead to where they say they do; and scan every attachment sent before opening it.

Social engineering falls beyond just checking sources since attackers seek to exploit the employee's will to be at service and help people. An attacker will pose as a vendor or someone in need of help to trigger certain feelings in the employee making it easier to get information from them [11].

4.1 Cyber Security Skills Represented with a LM-GM model

The LM-GM (Learn Mechanics - Game Mechanics) model can be interpreted as of having two axes. The horizontal axis lie the learning and game mechanics analogous to a breath-first search. Side or leaf nodes represent functional mechanics supporting the core. The following table represents a LG-MG model applied to cybersecurity [12]

Adapting the model presented in "Learning Mechanics - Game Mechanics" to the cyber-security theme. To use the resulting customized Learning Mechanics-Game Mechanics (LM-GM) map, the first grid should be used as a transitional layer between cyber-security skills and game mechanics [4][12].

Fig. 1: LM-GM map changed to match Cyber Security Skills [4]

Proceedings of the Digital Privacy and Security Conference 2022 | 10.11228/dpsc.04.01

4.2 Applications

Applying serious games to the cybersecurity environment is nothing new. Since the games provide a safe environment for testing and learning it is easy to get creative and explore the world of cybercrime within the games. This subsection presents some innovative ideas for implemented commercial applications.

Escape Room An example of an application of a serious game to train employees is the escape room provided by the company InfoSequre. An escape room is a set of challenges (theme-based) that a group of players must complete escaping the room, normally in less than an hour. The security awareness escape room aims to introduce the topic of cybersecurity and engage some curiosity into the players, so it is more brought up in the office. One particularity of this project is the fact that the escape room is built on a trucks' trailer, so it is easier to get access [13].

Virtual Reality Experience Virtual Reality (VR) is a computer technology developed to bring the user into a virtual-simulated environment. Stimulating multiple censorial systems, VR experiences demonstrate to be very immersive and educational. InfoSequre, the same company that provides the escape room experience, made a virtual reality game, which sets 2 teams against each other competing for which one detects the greatest number of phishing emails and consequently prevents cyber accidents. The fastest team wins the game, and the results are then announced by a security awareness professional who will discuss with the players, so no doubt remains after the game [14].

Interactive Game This online interactive game, created by The Fugle Company, lets you play as the Chief information officer (CIO) of Fugle that is getting ready to launch a bio metrically authenticated mobile payment application when suddenly, his company is targeted by a cyberattack. The game lets you choose which measures to take preventive and proactively, unfolding the story as the player makes different decisions that can lead to a bad ending or a good one. Some choices also require you to spend virtual currency reflecting on the budget before making any decision [15].

In the end, every choice made is revisited by a security specialist explaining each option and why it would succeed or fail [15].

5 Board Game Riskio as an example of a serious game applied to cybersecurity

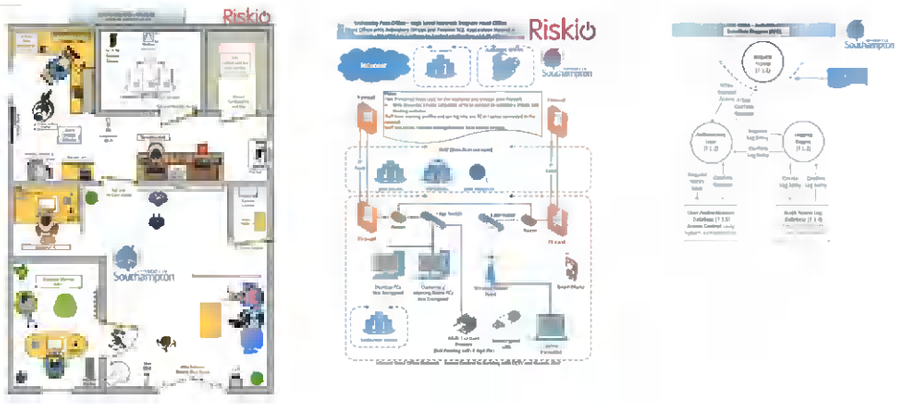
The game is designed to educate players to better manage risk situations and know what decisions to make when faced by certain types of attacks. The objective of Riskio is to give players a safe playground where they can identify threats to the organization data, learn what could be done and reflect if that's the best

Proceedings of the Digital Privacy and Security Conference 2022 | 10.11228/dpsc.04.01

decision to make. This game does not require players to have any previous experience in software development, making it easier to play with a wide variety of people with different tech related skill [16].

5.1 Game Setup

Riskio can be played in up to three boards (see Figure 2), each representing a different case scenario to protect – Office Diagram (illustrated on Figure 2a), Network Diagram (transposed on Figure 2b), and Data Flow Diagram (visualized in Figure 2c) [16].



(a) Office Diagram (b) Network Diagram (c) Flow Diagram

Fig. 2: Riskio Game Boards

The game is composed of a Game Master (GM), who's someone that has a piece of a vast knowledge of cybersecurity and is responsible for setting up the game, shuffling the three decks (see Figure 3) - attack (illustrated on Figure 3a), defense (transposed on Figure 3b), and information (visualized in Figure 3c) -, and explaining the game to new players. This game is played by rounds and has a recommended number of players varying between 3 to 5 individuals. From this group, the player on the left of the GM will be chosen to be the first attacker and at the end of each round, it will go clockwise. At the start of the game, every player is given a hand of defense cards, a personal deck from which they will choose to strengthen their defenses for the upcoming attacks. The players will take turns trying to set up an attack while the other players present valid defenses [16].

5.2 Attack phase

The attacker draws from one of the 6 small decks on the board. Each of these decks represents different kinds of cyberattacks. It is given a moment to the

(a) Attack Deck (b) Defense Deck (c) Information Deck

Fig. 3: Riskio Decks

player to think, build up a strategy and describe to the GM how that attack would occur. After judgment, the GM is going to evaluate the attacker's performance and either valid or not his attack. He will be awarded up to 3 points if it is successful [16].

5.3 Defense Phase

After the attacker declares his attack, it is time for every defender to defend. Each defender must choose a defense card from their deck at hand and place the card facing down until every defender is ready. When that occurs, the GM will ask each defender to describe how they would defend against the attack. If the validation of the defense card presents to be successful, then the defender wins up to 3 points. When every defense is evaluated, the round ends [16].

5.4 Optional Bonus Round

At the end of each round, the GM can be innovative and start a different round, in which he will be the attacker, and every player will be the defender. The attack card is drawn from the informative deck at his disposal. After hearing every defender's security scenario, he will appreciate and reward up to 3 points, similar to the defense phase [16].

6 Conclusions and Research Perspectives

Throughout this paper is revealed some advantages of adopting serious games to make people more aware of cybersecurity-related problems. Studies were presented to demonstrate that workers learned new technical terms and developed new skills, improving their perception when engaging in cybersecurity situations.

It is fair to affirm that the market of serious games is going to continue growing and, therefore, in the following decades to enhance even more. New applications, new games are going to be developed, and their applicability is going to increase, due to the need to improve the workforce's cybersecurity skills.

References

1. T. Susi, M. Johannesson, and P. Backlund, "Serious games - an overview," 11 2015. [p. 2]
2. C. Abt, *Serious Games*. University Press of America, 1987. [p. 2]
3. "Serious games for training: 8 benefits that will surprise you : Gamelearn: Game-based learning courses for soft skills training." `https://www.game-learn.com/en/resources/blog/serious-games-for-training-benefits/`. (Accessed on 12/12/2021). [p. 3]
4. A. Le Compte, D. Elizondo, and T. Watson, "A renewed approach to serious games for cyber security," in *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, pp. 203–216, 2015. [p. 4, 5, 7, 8]
5. "What is cybersecurity? - cisco." `https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html`. (Accessed on 01/14/2022). [p. 5]
6. "What is a cyberattack? - most common types - cisco." `https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html`. (Accessed on 12/13/2021). [p. 6]
7. "What is phishing? examples and phishing quiz - cisco." `https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html`. (Accessed on 12/13/2021). [p. 6]
8. "What is ransomware? - definition and protection tips - cisco." `https://www.cisco.com/c/en/us/solutions/security/ransomware-defense/what-is-ransomware.html`. (Accessed on 12/13/2021). [p. 6]
9. "What is a social engineering attack & how to stop it - avg." `https://www.avg.com/en/signal/what-is-social-engineering`. (Accessed on 12/13/2021). [p. 6]
10. C. M. Williams, R. Chaturvedi, and K. Chakravarthy, "Cybersecurity risks in a pandemic," *J Med Internet Res*, vol. 22, p. e23692, Sep 2020. [p. 6]
11. "Best practices for how to train employees for cyber security." `https://www.coxblue.com/8-tips-and-best-practices-on-how-to-train-employees-for-cyber-security/`. (Accessed on 12/16/2021). [p. 7]
12. "sv-lncs." `https://arxiv.org/ftp/arxiv/papers/1805/1805.08053.pdf`. (Accessed on 12/17/2021). [p. 7]
13. "Security awareness escape room — infosequre." `https://www.infosequre.com/security-awareness-escape-room`. (Accessed on 12/14/2021). [p. 9]
14. "Security awareness vr experience truck - infosequre." `https://www.infosequre.com/security-awareness-virtual-reality-experience-truck`. (Accessed on 12/14/2021). [p. 9]
15. "About targeted attack: The game defend your data. choose wisely. succeed or fail.." `http://targetedattacks.trendmicro.com/about-the-game.html`. (Accessed on 12/14/2021). [p. 9]
16. S. Hart, A. Margheri, F. Paci, and V. Sassone, "Riskio: A serious game for cyber security awareness and education," *Computers and Security*, vol. 95, p. 101827, 2020. [p. 10, 11]