Review of Serious Games for Cybersecurity and Privacy Skills Training

Wendel da Silva Guimarães

Lusófona University, Porto – Portugal
weguimaraess@gmail.com

Abstract. Cybersecurity is nowadays required by any company or service, anywhere in the world. Every day this sector has a high investment in order to improve its technology and the techniques applied to it, in that same context several companies pay services and professionals that offer guarantees to maintain the security of your business and thus avoid any breach for an attack, besides to offer training to various professionals in all areas in order to avoid possible threats or vulnerabilities in the daily use of computer equipment, from simple e-mails to access to confidential information.

Similar to the growth of this area, there is a growth in the sector of serious games, these with varied purposes, in the case of this paper, we will deal here with serious games aimed at developing skills related to cyber security and privacy, where they will have a fundamental role in the professional development of the user. Currently, serious games are seen and used as tools for the development and correction of behaviors that can compromise the security of a system and help to correct them.

This paper aims to investigate how effective the use of serious games can be for training from ordinary users as well as even cyber security professionals, thus being able to portray the positive points and analyze the changes generated after their use.

Keywords: Games, Serious Games, Training, Security, Privacy

1 Introduction

As soon as we talk about cybersecurity the first thing that crosses our minds are the different types of viruses, types of attacks, information leaks and other aspects related to this, most of them linked to more serious matters. When we talk about games, we have a contrast, we associate the term with aspects related to leisure, fun, entertainment, all in a more pleasant and fun tone. However, unlike the tone addressed for games in general, we also adopt a more serious tone when we talk about the serious games theme, a theme that will be addressed in this article. Serious games are games that focus on a specific goal and not only on entertainment, these games seek to pass a different experience to the user and are mostly intended for purposes such as training, education, developing a skill, etc. At the moment there are already several sectors that make use of serious games for the purpose of learning, thus, games are used as tools for

10.11228/dpsc.03.01.010

assimilation of concepts and developments in general. It is common to see some of these sectors use serious games as a fundamental part of training, examples of which are training of students in the field of medicine that use simulation as a way to apply the concepts studied, develop decision skills among other factors. One of the areas that also make use of serious games is Cybersecurity, mostly applied with the purpose of training professionals, workers, students or even ordinary users. According to [1] "20% of the organizations who took part in the survey are using games or simulations as part of their learning solutions".

Next in the paper we will see the following topics:

- Serious games and their importance
- A brief review about cybersecurity
- The context of serious games within the cybersecurity environment
- The development of privacy skills through serious games
- Conclusion

2 Serious games and their importance

We already know that serious games are used as tools to give your player a "serious" content, which can aim at a form of training or development, however, this does not remove the fact that it is still a game, even with "serious" content being played, the game itself can be fun. They are formatted with game elements, there may be scenarios, characters and other aspects commonly seen in entertainment games, the difference here is the fact that the whole game is developed with a learning purpose, the whole focus of what is developed and presented within that game it was done with the same purpose towards the player and he must be able to convey his message. According to [2] "Playing can be part of the learning process because the subject to be learned is, at least in some respects, essentially playful. The use of serious games in the learning process therefore illuminates the fundamental nature of the subject being taught ".

Games have been used for educational purposes at least since the 20th century, they became popular in classrooms in the 60s and 70s, however, the term "serious games" only came to be used decades ahead, where the term was applied to electronic games that passed some form of learning. These games became subjects of study for some years and when they realized the advantages they brought, they started to use games with learning purposes in different sectors.

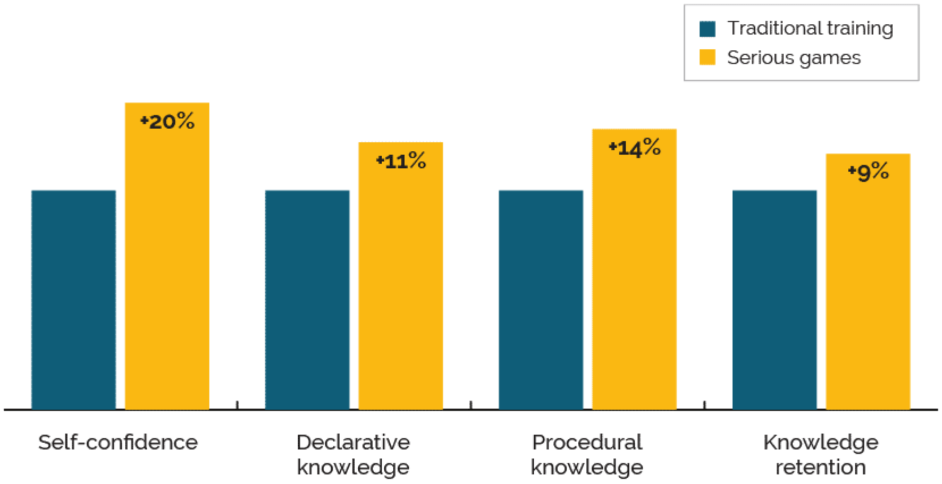

Fig. 1. Statistics about serious games (SymVision Education)

3 A brief review about cybersecurity

Given the current scenario where cybercrime is becoming more and more “common” and the forms of attack are developed in order to be more effective, the tendency is that these attacks do not stop, and with all companies and organizations being their potential targets it is necessary there are methods and policies to be adopted that can prevent these attacks from existing.

As a way of responding to these cyberattacks cybersecurity arose, acting as an active defense practice that works to avoid possible risks existing in the system and network environments, there are several ways to adopt cybersecurity, be it via antivirus software, and other tools or via hardware with firewall protections and equipment. Cybersecurity practices aim to protect against malicious attacks, avoid possible vulnerabilities and so on. It is important to note that, over the years, new forms of attacks emerge, so cybersecurity cannot be left behind and must always have its defense practices, software and hardware updated in order to try to prevent and prevent these attacks.

With all this, the cybersecurity sector is a “new” sector in the market, however there is already a large investment on the part of companies, considering that it is something essential today. According to [3] “the industry's overall growth is expected to be 12% a year through 2024, going from $ 120 billion a year in 2017 to more than $ 300 billion.”

And not only software and hardware make up the cybersecurity sector, this is also an “educational” sector, to consider what as [4] said “The biggest threat is within organizations", referring that the company's users can adopt practices that leave the system vulnerable.

In research released by [5] "Investing in employee security training and awareness can significantly reduce security-related risks from anywhere between 45 and 70 percent" and "there is an 80 percent chance that organizations with $ 200 million in annual revenue will have to pay up to $ 2.5 million a year due to insecure employee behavior. There is a 20 percent likelihood the costs from inappropriate employee behavior surpass $ 8 million ".

3.1 Internet use around the world and cybercrimes

Everywhere in the world you can see the growing trend of using the internet as an essential part of everyday life, in addition to computers, today we have Smartphones, SmartTVs, tablets, among other devices that make constant use of the internet.

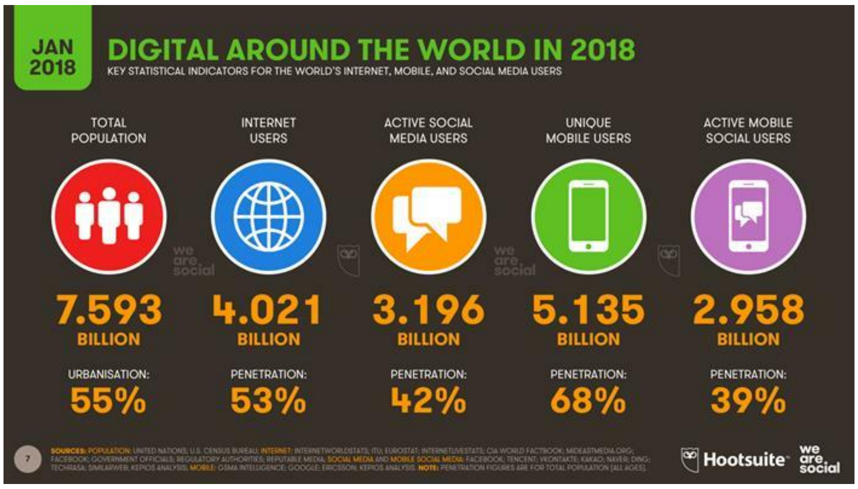

Fig. 2 Statistics about internet [6]

Together with ordinary users, companies and professionals from all over the globe use the internet in the most diverse ways for the purpose of work.

Going hand in hand with the increasing use of the internet we have cybercrime, where as the internet and its technologies advance, cybercrime develops more effective and less detectable techniques of invasion, data theft and confidential information, among other types of attacks.

The practice of cybercrime has become so common that according to [7] "about 65% of internet users have already been victims of some form of cybercrime.", When talking about cybercrime [8] said "We believe that data is the phenomenon of our time. It is the world’s new natural resource. It is the new basis of competitive advantage, and it is transforming every profession and industry. If all of this is true - even inevitable - then cybercrime, by definition, is the greatest threat to every profession, every industry, every company in the world.”

With the rise of cybercrime and the growing number of attacks, according to [9] “Global Analysis organizations that suffered at least one breach in 2016 lost an average of $ 4 million.”

As an example of consequences generated, we can see a famous case of a cybercrime that was reported by [10] “For a period of two years, ending in early 2015, a group of Russian-based hackers managed to gain access to secure information from more than 100 institutions around the world. The cyber criminals used malware to infiltrate banks' computer systems and gather personal data. They were then able to impersonate online bank staff to authorize fraudulent transfers, and even order ATM machines to dispense cash without a bank card. It was estimated that around £ 650 million was stolen from the financial institutions in total.

4 The context of serious games within the cybersecurity environment

Given the cybersecurity contexts, we know that this is also a training sector, with the aim of passing user policies on use, avoiding vulnerabilities, forms of defense, all to minimize the chances of a possible attack and to know how to protect themselves, and it is the from that we make use of the Serious Games.

Serious games when applied in the context of cybersecurity are used as training tools, thus having a more interactive form of learning than other more “conventional” training, these games aim to transmit a message of awareness about cybersecurity and thus pass on knowledge about the subject for these people, one of the examples of games that make use of this training mechanics involving cybersecurity is the “CyberCIEGE” of [11].

According to [12] “Development of CyberCIEGE was sponsored by the US Navy, the Naval Education and Training Command, the Office of Naval Research, the Biometrics Task Force, the Office of the Secretary of Defense, and the National Science Foundation.” And about the game “CyberCIEGE enhances information assurance and cyber security 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.”

At the moment there are games that cover different groups of users, as both professionals and home users need to have knowledge about cybersecurity, an example of a game that can be given to both groups is the "Anti-Phishing Phil" developed by [13] and that according to [14] "Anti-Phishing Phil is an engaging online game that teaches you how to identify phishing URLs, where to look for cues in web browsers, and how to use search engines to find legitimate sites. Play for 10 minutes and learn the basics of how to spot phishing attacks. Anti-Phishing Phil is hosted by Wombat Security, and requires you to login with your CMU credentials."

There are currently several studies that portray how efficient it is to use game elements in the learning context, regardless of the age group in which the user is found, the benefits are clearly seen, thus providing positive effects and results mostly, both for the user, whether a home user or a professional, both for the company that will have an environment with safer use of its employees. You can see in the *Table 1* some examples of case studies of some games and the results they generate.

Table 1 – Papers about CyberSecurity Training Games [15]

Paper	***Game Name***	***Game Type***	***Methodology***	***Results***
[16-20]	Anti Phishing Phil	Mobile application training safety of link URLs	Think aloud, pre-test & post-test experimental vs. control, SUS usability questionnaire	Positive impact on learning, awareness and phishing susceptibility

[21-27]	CyberCIEGE	3D virtual world (sims style)	Unclear ([22]) Experiment & selfassessment ([23]) Theoretical review of cognitive principles ([24])	Sufficiently flexible to illustrate a wide range of topics and positive early indication ([23]) Positive ([24]) Unclear, but there is a need to create a science of games ([25])
[28]	"The Internet"	Unclear	Literature review	A review of elements a security network game should have
[29]	Internet Hero	Puzzle mini-games	Experiment with children	The children liked the games
[30]	PicoCTF	Web-based	Survey	Positive educational experience according to students & instructors

5 The development of privacy skills through serious games

It is commonly seen nowadays that the use of information obtained through users improves and helps to personalize their services, based on their personal tastes and in addition to making some actions more practical and simple, at first this may seem attractive to the point from the point of view of the common user, since he will mostly prefer the convenience adopted through the use of his information. On the other hand, we have a threat to the privacy of the user, where he often has no control over his own personal data or where they are used, it is possible that the user has personal data being used by third parties that not even the user had realized that he had given consent to do so.

This type of "theft" of information is based on the user's naivety and lack of knowledge about privacy, where he provides his data by himself, and these can be used in an improper way.

The term adopted for this type of action is “misuse” where it refers to the misuse of data, as defined when the data was initially collected. Often linked to the fact of inducing the user to error.

An example of misuse reported in [31] refers to “Employees at AT&T call centers in Mexico, Colombia and the Philippines were found to have stolen the names and full or partial Social Security numbers of about 280,000 of the wireless carrier's customers in the United States. The workers sold that information to third parties.”

In the same way that there are serious games to conduct cybersecurity training, there are also serious games that are used as a form of training in order to develop the user's privacy skills, they try through an interactive way to show the user the best decisions to be taken when they involve personal data or information and in addition to establish forms of safe navigation that do not compromise that same data and information.

“Some research studies show that video games encourage the acquisition of certain skills and improve student comprehension of learning materials presented through a video game”. [32]

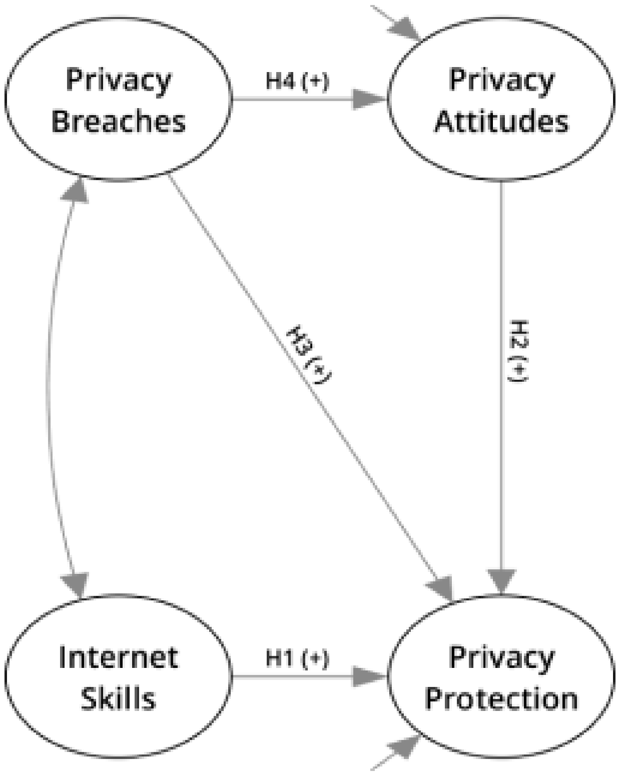

Fig. 3 Overview of the structural online privacy model [33]

The *figure 3* aims to illustrate the concept of Privacy Protection and thus demonstrate the existing structure of online privacy.

6 Conclusion

In this article we saw about serious games and their uses in the cybersecurity sectors and in the development of skills related to user privacy. Based on the research carried out, we saw that serious games can be used as interactive forms of learning and skill development, these are used as different ways of transmitting knowledge than more conventional methods. It is noteworthy that this form of learning tends to be most effective in its majority, since it is a much more active and rewarding way for those who are learning, there is satisfaction on the part of them and a desire to continue with the game, differently from watching classes, documentaries and other conventional means that are not so stimulating for those who are learning. Another advantage of serious games is that they are able to transmit diverse experiences to their "player", something that is not very possible when in training environments or classes, examples of this are seen in simulations, mainly in the area of health in which these simulations are used to develop decision-making skills, which in real life may be able to save lives.

In the cybersecurity scenario, serious games can be used as excellent training tools, considering that most users today do not have as much knowledge about cybersecurity and no sense of the consequences and risks that this can bring, serious games are great ways to engage these same users both in the corporate and home environment, where in addition to passing on the necessary knowledge on the subject, it tries to show safe ways and security policies that can be adopted by them.

This article made me understand a little more about the cybersecurity sector and how important it is to have knowledge in order to have a safe environment. Together with that, I was also able to realize the importance of the serious gaming sector today and its effectiveness, bringing with it ways of learning and raising awareness, a form that should be more applied and distributed in different sectors, being able to transmit the knowledge of a pleasant and attractive way for more people around the globe and thus minimize the threats that reside in cyberspace.

References

1. The Towards Maturity 2012 Benchmark Report: Bridging the Gap (2012).
2. Huizinga, J.: Homo Ludens: A Study of the Play Element in Culture. Beacon Press, Boston. (1955, originally published in 1938).
3. Research Firm Global Market Insights, https://www.gminsights.com/, last accessed 2020/12/01.
4. Eben Louw, EY Senior Manager of Forensic & Integrity Services Department: Conference "Cyber Crime: from prevention to forensic response - EY" (2019).
5. Wombat Security Technologies and Aberdeen Group.: New Research From Aberdeen Group and Wombat Security Confirms Security Awareness and Training Measurably Reduces Cyber Security Risk (2015).
6. Hootsuite, used by https://www.app-scoop.com/blog/digital-transformation-why-its-important-to-your-organization, last accessed 2020/12/11 (2018).
7. NortonLifeLock Inc, https://www.nortonlifelock.com/us/en, last accessed 2020/12/01.
8. Ginni Rometty, IBM Corp.'s Chairman, President and CEO (2015).
9. Ponemon Institute's 2016 Cost of Data Breach Study (2016).
10. The New York Times: Bank Hackers Steal Millions via Malware (2015).
11. The Center for Information Systems Security Studies and Research (2014).
12. Naval Postgraduate School – US Navy, https://nps.edu/, last accessed 2020/11/15.
13. CMU Usable Privacy and Security Laboratory (CUPS), https://www.cmu.edu/iso/aware/phil/index.html, last accessed 2020/11/17.
14. Carnegie Mellon University, https://www.cmu.edu/, last accessed 2020/11/17.
15. Maurice Hendrix , Ali Al-Sherbaz and Victoria Bloom, "Game Based Cyber Security Training: are Serious Games suitable for cyber security training?", Department of Computing, School of Computing, Electronics and Maths, Coventry

University, UK and Department of Computing, School of Science and Technology, The University of Northampton, UK (2016).

16. Arachchilage G. and Asanka N., "Security awareness of computer users: A game based learning approach," Brunel University, School of Information Systems, Computing and Mathematics (2012).
17. Arachchilage N. A. G. and Love S., "A game design framework for avoiding phishing attacks," Comput. Hum. Behav., vol. 29, no. 3, pp. 706–714 (2013).
18. Arachchilage N. A. G. and Love S., "Security awareness of computer users: A phishing threat avoidance perspective," Comput. Hum. Behav., vol. 38, pp. 304–312 (2014).
19. Nyeste P. G. and Mayhorn C. B., "Training Users to Counteract Phishing," in Proceedings of the Human Factors and Ergonomics Society Annual Meeting, vol. 54, pp. 1956–1960 (2010).
20. Sheng S., Magnien B., Kumaraguru P., Acquisti A., Cranor L. F., Hong J., and Nunge E., "Antiphishing phil: the design and evaluation of a game that teaches people not to fall for phish," in Proceedings of the 3rd symposium on Usable privacy and security, pp. 88–99 (2007).
21. Cone B. D., Irvine C. E.,. Thompson M. F, and Nguyen T. D., "A video game for cyber security training and awareness," Comput. Secur., vol. 26, no. 1, pp. 63–72 (2007).
22. Cone B. D., Thompson M. F., C. E. Irvine, and T. D. Nguyen, Cyber Security Training and Awareness Through Game Play. Springer (2006).
23. Fung C. C., Khera V., Depickere A., Tantatsanawong P., and Boonbrahm P., "Raising information security awareness in digital ecosystem with games-a pilot study in Thailand," in Digital Ecosystems and Technologies (2008).
24. Greitze F. L., Kuchar O. A., and Huston K., "Cognitive science implications for enhancing training effectiveness in a serious gaming context," J. Educ. Resour. Comput. JERIC, vol. 7, no. 3, p. 2 (2007).
25. Irvine C. E., Thompson M. F., and Allen K., "CyberCIEGE: an information assurance teaching tool for training and awareness," DTIC Document (2005).
26. Irvine C. E. and Thompson M. F.,, "Simulation of PKI-enabled communication for identity management using CyberCIEGE," in MILITARY COMMUNICATIONS CONFERENCE, 2010-MILCOM 2010, pp. 906–911 (2010).
27. Thompson M. F and Irvine C. E., "Active Learning with the CyberCIEGE Video Game.," in CSET (2011).
28. Irvine C. E. and Thompson M., "Teaching objectives of a simulation game for computer security," DTIC Document (2003).
29. Kayali F., Wallner G., Kriglstein S., Bauer G., Martinek D., Hlavacs H., Purgathofer P., and Wölfle R., "A Case Study of a Learning Game about the Internet," in Games for Training, Education, Health and Sports, Springer, pp. 47–58 (2014).
30. Chapman P., Burket J., and Brumley D., "PicoCTF: A Game-Based Computer Security Competition for High School Students," 2014 USENIX Summit Gaming Games Gamification Secur. Educ. 3GSE 14 (2014).
31. The New York Times: F.C.C. Fines ATT $25 Million for Privacy Breach (2015).
32. Conolly, T., Stansfield, M., Boyle, L..: Games-Based Learning Advancements for Multy-Sensory Human Computer Interfaces: Techniques and Effective Practices. IGI GlobalPublishing, (2009).
33. Büchi, M., Just, N., & Latzer, M. - Caring is not enough: The importance of Internet skills for online privacy protection. Information, Communication & Society (2016).