Abstract

Now that topics like cyber security appear on the public agenda, there is a need to up-scale skills quicker and quicker by enhancing training, including by gamification solutions. The purpose of this research is to analyse the status of cyber security gamification solutions and identify best practices for their potential re-use. This qualitative case study explores gamification solutions and their uses in Europe. The data gathering phase revealed from practitioners what the last years' literature is pointing to: great potential, but not yet a high adoption rate. Also, it was interesting to see the links of this topic and the Digital Agenda in terms of Technology Enhanced Learning (TEL) in cyber security, but it proved not to be so much developed in the end. Also, for myself as a practitioner and doctoral candidate, the implications of this research can help better understand where we head on from here.

In conclusion, my research on cyber security education in line with other scholars (Hassan, 2016; Asquer, 2014; Bista et al., 2014; Coronado Escobar & Vasquez Urriago, 2014; Gordon et al., 2014; Nelson, 2012; Raphael et al., 2010) shows that learning in public administration should employ better, innovative open gamified solutions.

There is a need for more research data to advance this work. Through this investigation I join the call for further analysis and search for practical implementation. The implications of this research can help better understand the status quo with qualitative data and advance new indicators currently missing in terms of public policy making.

Keywords: TEL-technology enhanced learning, cyber security, public administration, eSkills, LLL-lifelong learning, EU Digital Agenda, Gamification.

1 INTRODUCTION

Nowadays, administrations both at central and regional level are under pressure to deliver 'more with less' as referred often by governments. Training as part of lifelong learning is under scrutiny too, to deliver the best methods in terms of costs and efficiency, take for example ERASMUS+ programme. Technology Enhanced Learning (TEL) was adopted unevenly across countries and regions and did not follow a certain strategy, with the hope that it would bring great results as reported in the Digital Agenda dashboard at European level or in national cyber security strategies. The overall aim of the Digital Agenda is to deliver sustainable economic and social benefits from a digital single market perspective. The objective of this Agenda is to chart a course to maximise the social and economic potential of ICT, most notably the internet, a vital medium of economic and societal activity: for doing business, working, playing, communicating and expressing ourselves freely. Successful delivery of this Agenda will spur innovation, economic growth and improvements in daily life for both citizens and businesses. The Digital Agenda for Europe is one of the seven flagship initiatives of the Europe 2020 Strategy, set out to define the key enabling role that the use of Information and Communication Technologies -ICT will have to play if Europe wants to succeed in its ambitions for 2020. Now that topics like cyber security appear on policy makers agenda there is a need to up-scale skills quicker and quicker by enhancing training, including by gamification solutions. The purpose of this research is to analyse the status of cyber security gamification solutions and identify best practices for their potential re-use. The qualitative case study explores gamification solutions and their uses in Europe. Moreover, this is also a personal story. I am interested in this topic since my professional background includes working with European Union countries in advancing many types of eLearning solutions for better understanding of cyber security at all levels of populations. Genuinely concerned in this, I do hope that narrowing down the research will help to explore some success cases as of 2017.

A detailed literature review conducted by two Massachusetts Institute of Technology (MIT) scholars (Ramirez et al., 2016) describe cyber security as a new field springing out of many old ones where to date little attention has been given to standardising terminology, let alone the development of standards of research. The systematic review of inter-organisational information security (Karlsson et
al., 2015) found that most published research and studies are either descriptive, philosophical or theoretical, with most only using subjective and argumentative methods, with relatively very few studies that combine theoretical work and empirical data. Overall their investigation confirmed the commonly-held view by the academics that the field would benefit from a more systemic and more rigorous evidence-based approach. Furthermore, as reported (Meyer, 2015) cyber games may be the bet to take for such high stakes policies like cyber and one statement of a 'high flyer', John. N. Stewart, Chief Security and Trust Officer for Cisco, while speaking about workforce and training, described the key to cyber security awareness training is to 'make it personal, make it interesting, and make it relevant. Personal can be either as simple as having actors in videos speak in native languages for multiple cultures, or as complicated as creating and using real-life events and getting a full interactive game for employees.' And here we start with a first advocate for games in cyber security education. Within a cyber-ecosystem human vulnerabilities account for a high percentage of vulnerabilities exploited by attackers according to vendors’ annual reports but yet the focus of cyber security in information technology has been on systems, tools and technology. The human actor is generally considered 'the weakest link'. At the same time it is common knowledge that better training is the way forward for mitigation of attacks and preparation of users. But a new report (SAM HLG, 2016) articulates that calling for knowledgeable and responsible users should not be used as a step towards imparting blame to users for issues beyond their awareness, control or power, this SAM HLG study calls on several footsteps to be considered both at EU and national level:

- Education and building a culture among professionals that focuses on resilience of systems
- Fit-for-purpose curricula should take into account the multidisciplinary nature of cyber security challenges and involve a balance between technical aspects, competences from social sciences and legal matters
- Support the deployment of the means - including technologies and processes - for user choice and control over their digital identities, footprints and personal data
- Support the development of an EU cybersecurity industry, 'made in Europe'
- Promote cybersecurity education curricula and lifelong cybersecurity training to build talent and sustain the skills of professionals. Make cyber security education more attractive to students
- Support the development of evidence collection methods, including sharing of evidence and best practices
- Improve the mutual trust between national players
- Develop and monitor cybersecurity standards and practices

For all the reasons mentioned above, I consider the topic of cyber security education to be of high-importance and I would like to contribute to it.

2 METHODOLOGY

For this particular identified topic there is the gap of what happens in practice, in public versus private sectors and new solutions being undocumented since cyber security is considered as a new interest. My research is drawing from policy requirements (Digital Agenda, 2010) with a follow-up on what governments of EU countries do in practice to implement policy. With this I hope to contribute to documenting the changes and drawing conclusions on best practices and solutions to share.

For the purpose of the study the following questions will be explored: RQ1. How have different gamification methods been used in cyber security online education for administrations in Europe?

RQ1.1 What are the common gamification strategies used?; RQ1.2 Why is gamification used and which technologies enable it?; RQ1.3 What technical features are most useful in terms of gamification? I will try to answer them by both desktop research and gathering of data from survey and interview.

This small-scale research will be based on constructivist grounded theory as a way to analyse data. Considered as a best fit, I am going to use Charmaz's approach (Charmaz, 2008), namely I am going to combine analysis of context, action and interpretation in order to start the sense-making process then to end up with a conceptual understanding. In order to research on this topic I planned and organised the work as follows: reading phase, data collection phase and analysis phase. I built an online survey and send it to 15 professionals in cyber security and also requested 2 structured

4995
interviews with professionals working in cyber security in Belgium where I reside. All data were gathered in the English language, the survey used a public tool hosted by the European Commission and the results will be made available to the participants. The research design follows a mixed approach with quantitative data and qualitative data to be gathered and used. A manual, non-automated analysis was applied. The strategy for the validity of results is based on the trustworthiness of professionals and their declared experience [question nr 1. survey] in the field interviewed/surveyed and the governmental data reported. The literature was selected, having in mind the wish to reference recent material together with already established research. The search was performed within the publications offered online by Lancaster University but also by using public search engines. The structure of the literature review was organised around the concepts of gamification linked to cyber security. In this research, I make use of central concepts like gamification, TEL, cyber security, and the EU Digital Agenda, defined for the purpose of this research as below.

Gamification is a practice of enhancing a specific service by implementing game design elements in a non-game context to enhance the user’s general value creation and knowledge (Huotari & Hamari, 2011; Deterding et al., 2011). Deterding et al. (2011) explain gamification as ’the use of design elements characteristic for games in non-game contexts’. Accordingly, gamification reflects the use of game thinking including progress mechanics (such as points systems), player control (such as avatar use), rewards, collaborative problem solving, stories and quizzes, and competition in non-game situations (Deterding et al., 2011; Kapp, 2012). Underlying gamification is an understanding of motivation as significantly correlated with and predictive of desirable human outcomes such as achievement, success, and the attainment of distinction and rewards (Kapp, 2012).

The gamification of learning is an educational approach to motivate students to learn by using video game design and game elements in learning environments.

Technology enhanced learning (TEL) is the use of technology as part of a learning process.

By using cyber security we refer to the international standard (International Telecommunications Union ITU recommendation -T X.1205, approved in 2008). Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment of an organisation and user’s assets. Those assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cyber security strives to ensure the attainment and maintenance of the security properties of the assets against relevant security risks in the cyber environment. The general security objectives comprise the following: availability, integrity (which may include authenticity and non-repudiation) and confidentiality.

The Digital Agenda identifies where Europe needs to focus its efforts to put this virtuous cycle in motion. It comprises policy priorities for the bloc of EU28 countries and the development of cyber security strategies including pillars like cyber security education through gamification. The dashboard is updated annually with accurate data from national governments.

Further on, the phase of literature review gave interesting results. Titles abound when we search for gamification literature but at the same time the topics vary on a large scale from using gamification in mobilising students in school, then workforce, development of processes and design for games, utilising games to generate awareness. The same idea of abundance of sources is shared in a 2015 research study (Markopoulos et al, 2015) mentioning that the research published in different magazines or books is mainly theoretical and there was a need already at that time of more experimental data and insights into the behaviour of participants. The authors called for further studies mentioning however that there is more and more interest. Furthermore, an exhaustive literature review was conducted by Caponetto (Caponetto et al. 2014) between 2012 and 2014 and the results emerging were very much indicating the increase of popularity of gamification techniques applied in a variety of educational settings. Additionally the concept of gamification has benefited by this popularity by gaining clarity in use and an established definition among both researchers and practitioners.

However the literature becomes scarce when getting closer to the relevance to my field of research, namely searching by the key words gamification together with cyber security. I found particularly interesting an article talking about innovative practices in teaching information security and technology related subjects (Carol, 2014) since the co-authors focus on interactive learning and innovation and how different gamified solutions can improve learning of students and answer in a modern way to the learning needs of each one involved.
However these essays do not give specific information on the questions of my specific project. It sets a good basis of understanding that gamification in learning has several facets and numerous people are interested to use gamified solution in their field of practice.

Furthermore, in a piece of work (Mackenzie et al., 2015) focusing on cyber security skills, I found an interesting idea that combined gamification and entrepreneurial perspectives with the objective in mind to understand how to best build cyber security skills in a cost-effective manner. For the purpose of building cybersecurity skills while emphasising a third stream, attacker types, to create training scenarios for lifelong learning. According to the authors, the use of such methods would enable employees and leaders to use role-play scenarios in an effort to build skills and awareness.

Moreover, we are encouraged to think like a hacker in a business school article (Esteves et al., 2017) that advocates for gamification in cyber security education. The authors summarise in keywords the complexity of the problem and usefulness of cyber security education and introduce a gamified approach following the same process for the information flow, 'How hackers approach an attack'.

3 RESULTS

A survey was sent to professionals in cyber security in order to map any kind of information relevant to the research questions. To run a good survey there is no trivial task trying to achieve good clarity and structure. I tested it before with a peer and received comments and feedback. Once the ‘crush test’ was done, the next step was to send in due time the link to the selected participants from a personal network of contacts. The timing was quite short and just during the Easter holiday. The selection of participants from personal contacts took into account the field of practice, geographical reach and availability via online channels. At the start I intended to send the survey to 15 persons and conduct 2 interviews; however, the timing and availability meant that I received back the results from 11 persons and 1 interview. The data collected shows a spread of knowledge and experience. In the cover letter of the survey, I deliberately chose to add a definition used in the literature by theoreticians when talking about gamification, with the idea in mind that this piece of information would set the context straight for answering the next questions from the same understanding: Gamification is the use of game elements and game-design techniques in non-game contexts to engage people and solve problems (Deterding et al., 2011; Werbach and Hunter, 2012; Zichermann and Cunningham, 2011).

Then another check for validity of the survey was the first question on experience in order to validate know-how. How long have you been involved in cyber security? All 11 participants in the survey declared more than 3 years of experience setting them a seniority level.

The countries in Europe known best in terms of cyber security practice; For the second question where I tried to map the geographical coverage for the expertise there was a very wide reach of declared knowledge encompassing 12 countries, as follows: Belgium, Bulgaria, Estonia, France, Germany, Hungary, the Netherlands, Poland, Romania, Spain, Switzerland and the United Kingdom. Separate from that, one respondent identified with an international organisation like the European Commission.

The research questions were then mapped to different set of questions: RQ1. How different gamification methods have been used in cyber security online education for administrations in Europe?; RQ1.1 What are the common gamification strategies used?; RQ1.2 Why is gamification used and which technology enables it?; RQ1.3 What technical features are most useful in terms of gamification? I will next map the answers to the questions.

- How would you qualify the importance of cyber security online education: 1-5(highest)
  - 5 participants scored with 4
  - 5 participants scored with 5
  - 1 participant scored with 1
- How would you describe cyber security online education in general?
  - Poor in resources considered by 4 respondents
  - Work in progress considered by 7 respondents
  - Rich in resources, no respondent considered it
• What about the use of gamification in cyber security online education:
  o Poor in resources considered by 5 respondents
  o Work in progress considered by 5 respondents
  o Rich in resources considered by 1 respondent

• In terms of cyber security education, how do you consider the use of gamification in private organisations’ environments:
  o Poor in resources considered by 6 respondents
  o Work in progress considered by 5 respondents
  o Rich in resources, no respondent considered it

• The use of gamification in public administration environments:
  o Poor in resources considered by 9 respondents
  o Work in progress considered by 2 respondents
  o Rich in resources, no respondent considered it

• What are the common gamification strategies used by public administrations in Europe?
  Answering this question, respondents mentioned the following: awards, quizzes, bug bounty, crisis management, incident management, cyber exercises (coordination between participants) mentioned once only while Capture the Flag exercises (on individual basis) was mentioned by 2 respondents.
  We also registered 3 respondents with 'none used', 3 respondents with 'do not know', also 1 respondent mentioned 'Not sure. But it seems relatively underdeveloped.'

• Why is gamification used and which technology enables it?
  While tackling this important question of why, several mentions were registered and I should mention several highlights: Gamification enables an easier digestion of IT security information; gamification allows participants to try new approaches in an environment where the impact of failure is minimum. According to a respondent this enhances the learning-by-failure approach. Also respondents mention that cyber exercises role and capture the flag competitions-CTF are to use a lot of technologies and rely on Open Source Intelligence (OSINT), custom development and real-time communication-technologies (voice, chat) to coordinate between the participants. Furthermore one respondent writes that gamification is good for nurturing commitment. Also that scoreboards and leader boards are good means to implement gamified environments, to catch the attention of users, mainly. One main idea present in replies is that gamification helps to improve awareness and consolidate learning, and the fact that it is organized as a game/challenge makes it more attractive.
  Technology-wise the respondents mentioned: web technology; mainly web-based, to ensure scalability and contain cost; web enables gamification and makes cyber security knowledge easily accessible to average users; CTF puts together many technologies or can focus on specific ones. We should mention that capture the flag (CTFs) competitions are games organized with a training purpose in online environments with the objective to capture a flag after some tasks were solved.

• What technical features are most useful in terms of gamification?
  In terms of features the respondents mentioned: Public Acknowledgment of the best (Hall of Fame/Rewards/Diploma); Possibility to replay and see what would have changed; Statistics on the progress, comparison with other people (ranking?); Visuals; Physical security, encryption; Ease of use; Broad compatibility with existing and reasonably recent browsers; Fluency and performance; Potentially integration in the work environment is a plus; but also an interesting answer more on 'think like attacker type': identifying vulnerabilities and exploiting them. We should also mention that 'Hall of Fame' usually refers to a list of individuals or organisations that achieved particular tasks to the benefit of a larger community e.g. discovered a vulnerability in a software and made a responsible disclosure to the third party concerned participating this way to a software improvement.

• Do you know about a best practice story in gamification on cyber security? Please name it or add the link to it.
In terms of best practice the respondents mentioned: Bug Bounty programs; EU cyber security agency (ENISA) flagship project Cyber Europe by 2 respondents but also Cyber Crisis Cooperation Technical Playground; Use strong passwords; secure code warrior, www.securecodewarrior.com ; Root Me https://www.root-me.org/. We should mention that ‘Bug Bounty’ usually refers to a specific programme where individuals can receive recognition and compensation for reporting bugs, especially those pertaining to exploits and vulnerabilities. Also 'Cyber Europe' is an exercise played by public and private organisation in the EU. According to the managing agency (ENISA) this is a series of EU-level cyber incident and crisis management exercises, simulations of large-scale cyber security incidents that escalate to become cyber crises. The exercises offer opportunities to analyse advanced technical cyber security incidents but also to deal with complex business continuity and crisis management situations. Cyber Europe exercises feature exciting scenarios, inspired by real-life events, developed by European cyber security experts. Thus each of the exercises is effectively a flexible learning experience for the participants.

- Regarding the interview conducted, there were 5 summary points to be added here:

  The board usually decide on which solution to use for training on a cost-benefit type of approach; there is a big interest in gamification but the adoption rate is not high; usually the gamification solutions for training are part of a package with incident response and triage; the solutions used are developed in house and can be used only by the specific organisation that developed it since the IT security rules are organisation based, that is why there are some best practices but used by limited amount of people in the private sector while the public sector has even a lower adoption rate because of costs. The data gathering phase I believe revealed from practitioners what the last years’ literature is pointing to: great potential, but not yet high adoption rate. Furthermore, these findings can be summarised according to the research questions, as below:

**Figure 1 Findings.**

What can be done further is to develop non-proprietary gamification solutions, also serious games, both web-based but also in cardboard format that can be shared by public administrations and used for their workforce training and consolidate learning. This is a supplementary line of work that can follow this small-scale project. In the same line there is recent work (Eizondo et al., 2016) that
reviewed existing serious games for cyber security awareness, teaching and training, showing that these games have a great pedagogical potential. The authors concluded that their use is most often limited to formal contexts and ideally these limitations could be overcome if serious games were released in informal contexts, without degrading their pedagogical advantages. They also tackle gamification by developing on the serious games concept (Abt, 1970; Zyda, 2005; Sawyer, 2002) as a human-computer rule based contest using entertainment to communicate and pass learning objectives. From their review of commercial products and literature, it appears that besides serious games great pedagogic potential for cyber security learning, also the large number of industry awards received by some of these games shows that businesses approve their usefulness and effectiveness. Furthermore, speaking about design and efficiency, Kapp (2012) identified that effective game design involves four elements like progress mechanics, player control, problem solving, story or scenario. They went on developing an innovative approach and avatars for further use. They acknowledge though the limited practice and testing. The findings may well be not revealing the entire picture of the topic since it is small scale, however it is a decent overview backed by both literature and practitioners’ knowledge. Additionally, since the development of gamified solutions for public administration is still in its inception, the Digital Agenda dashboard may point in the future also to examples in this sense in order to promote them and scale-up small projects that can work for all of Europe. To my knowledge, the Cyber Europe exercise is one example that is well known in the technical communities, but for general awareness more can be done.

3.1 Implications of findings

The data presented may develop on further implications that I did not see before. For example, as I was saying in the introduction, I work in the field and I had the impression that the cooperation on gamification was better with more resources available; however, both literature and practitioners point to another reality. Probably a larger mapping is needed to identify gamified solution that exist but are un-known'. An opportunity would be to identify those solutions and support their scale-up in Europe. Another question that arises is why companies do not share more their innovative ideas in learning, making them better known and used. Probably there is a need of sharing communities' development in this sense.

4 CONCLUSIONS

By conducting this small case study research I wanted to contribute to documenting the status quo with qualitative data and advance new indicators currently missing in terms of public administrations’ use of gamification for cyber security education. Also it was interesting to see the links of this topic and the Digital Agenda in terms of TEL in cyber security, which proved to be not so much developed in the end. Also, for myself as a practitioner and doctoral candidate, the implications of this research can help better understand where we head on from here. In conclusion, my research on cyber security education, in line with other scholars (Hassan, 2016; Asquer, 2014; Bista et al., 2014; Coronado Escobar and Vasquez Urriago, 2014; Gordon et al., 2014; Nelson, 2012; Raphael et al., 2010) shows that learning in public administration should employ better, innovative open gamified solutions. In accordance with the research presented with the title, governments should play games (Hassan, 2016). There is a need for more research data to advance this work. Through this investigation I join the call for further analysis and search for practical implementation, myself included, being committed to it both from professional and academic perspectives

ACKNOWLEDGEMENTS

Thank you: professor Don Passey and Dr. Kyungmee Lee, University of Lancaster; all respondents to the survey and interview; peer reviewers.

REFERENCES


