Systematically Applying Gamification to Cyber Security Awareness Trainings

A framework and case study approach

Iris Rieff [1517503]

Faculty of TPM, Delft University of Technology

March 2018

***Abstract*— Internet-enabled interconnectivity of ICT assets is increasingly adopted in organizations worldwide. Despite the benefits, threats to organizational assets are just around the corner. An organization's vulnerability to such threats is increased when employees working with ICT systems are unaware of cyber security. There are several ways to raise cyber security awareness, but the increasing number of cyber security incidents suggests that these methods lack effectiveness. Gamification offers promising results due to its ability to counter several weaknesses of existing trainings, for example related to motivation and engagement. It is presumed that incorporating gamification in cyber security awareness trainings could increase their effectiveness. A framework is designed to guide developers in gamifying cyber security awareness trainings. An empirical case study proved the usability of the framework through gamifying an existing cyber security awareness training and comparing participant experiences of the existing training and the gamified training. In sum, the cyber security awareness training was successfully gamified and its perceived effectiveness was proven.**

Keywords **gamification, cyber security awareness, training context, framework design, case study**

I. INTRODUCTION

Information, communication, and technology (ICT) is one of the most fast-paced fields in current societies all over the world. Organizations are increasingly connecting their key ICT assets to the internet, which has several benefits. Business processes can be automated, communication is quicker, and information can be stored more effectively (Sheahan, 2017). However, the interconnectivity poses increased or new risks, for example due to the introduced remote access. These risks is increased when employees who work with the ICT systems are unaware of proper behavior or lack the required knowledge and skills in order to do this. Raising cyber security awareness seems easier said than done considering the vast amount of cyber related incidents, for example severe data leaks of privacy sensitive information, ransomware that interrupts entire business processes, and successful hacks targeting various corporations or critical infrastructures (McGrath, 2016; NOS, 2018).All these incidents contained a human error that could have been prevented by sufficient cyber security awareness.

Following Lohrmann, there are several ways to raise cyber security awareness, for example by implementing cyber security awareness programs or trainings. However, cyber security awareness is still an issue in many organizations and society as a whole (Franke & Brynielsson, 2014; Joshi et al., 2012). This suggests that current programs that focus on raising cyber security awareness are lacking effectiveness.

Many commonly applied cyber security awareness training techniques, like online trainings or e-learnings, face issues inter alia due to participant perceptions. For example, such trainings are often perceived as time-consuming, non-inviting, or intimidating (Patten, 2015). Gamification is proposed as a promising and emergent technique that can be incorporated in cyber security awareness trainings to tackle such issues. Gamification can be defined as *the application of game design principles in non-gaming contexts* (Robson, Plangger, Kietzmann, McCarthy, & Pitt, 2015).

A particular benefit of applying gamification in training or education contexts is that it stimulates the motivation and engagement of participants. It is presumed that this increases the chances of a successful program. For example, information might be conveyed

more easily or the retention of information might be improved due to the application of gamification. However, research regarding a systemic application of gamification in existing cyber security awareness training contexts is missing. Therefore, this research project aims to answer the following main research question.

Research question *How can gamification be applied to a training context that aims to affect cyber security awareness?*

Answering this research question involves formulating answers to the following sub-questions.

1) *What constitutes and influences cyber security awareness?*
2) *What gamification concepts are applicable to cyber security awareness trainings?*
3) *What framework can be designed to gamify existing cyber security awareness trainings?*
4) *What is the perceived effectiveness of an application of the designed framework?*

For this purpose, section II addresses the background and related work regarding gamification and cyber security awareness. Next, section III elaborates on the methodologies that are applied to answer the research questions. Afterwards, section IV contains the execution of the research project. Section V discusses the results of this research. Conclusions are drawn in section VI. Next, limitations of this research are addressed in section VII. Finally, section VIII regards directions for future research based on this research project.

II. BACKGROUND AND RELATED WORK

One of the key reasons behind lacking cyber security awareness in many organizations is the severe shortage of specialists regarding cyber security (Assante & Tobey, 2011). Next, it is often difficult for organizations to distinguish what knowledge and skills are relevant to raise cyber security awareness of its employees and how to do this effectively by training (Caldwell, 2013). This section addresses the fields of cyber security awareness and gamification as a promising technique to raise cyber security awareness.

A. Cyber Security Awareness

Cyber security can be described as *the harmonization of capabilities in people, processes, and technologies; to secure and control both authorized and/or unlawful access, disruption, or destruction of electronic computing systems (hardware, software, and networks), the data and information they hold* (Ani, He, & Tiwari, 2016). Thus, the triad of cyber security consists of people, processes and technologies. Properly aligning and strengthening the three underlying parts of this triad contributes to the cyber security of organizations.

Another definition of cyber security is *all the approaches taken to protect data, systems, and networks from deliberate attack as well as accidental compromise, ranging from preparedness to recovery* (Kassicieh, Lipinski, & Seazzu, 2015). This definition complements previous definition by illustrating that there are several approaches that an organization can adopt to increase its cyber security. For example, different approaches might affect different parts of the cyber security triad of people, processes and technologies. Many of the approaches that are currently adopted focus primarily on the technologies side of cyber security (Howarth, 2014). By neglecting the people and processes aspects of cyber security awareness, these approaches might not be adequate for tackling the problem of lacking cyber security. Some authors state that cyber security awareness is the most important factor considering cyber security of organizations (Jiemei, Xuewei, Dongxia, & Lan, 2014). In other words, addressing cyber security awareness through approaches focusing on the people aspect might effectively improve the cyber security of organizations.

Cyber security awareness can be defined as *thoughtfulness on security, enabling individuals (workforce employees and managers) to recognize security concerns and respond accordingly* (Ani et al., 2016). As such, cyber security awareness is a subset of situational awareness that is regarding a cyber context (Franke & Brynielsson, 2014). An additional definition of cyber security awareness is *assessing the level of vulnerabilities in an entity, while providing participants with general knowledge in detecting and avoiding successful penetration attempts* (Adams & Makramalla, 2015). This definition differs from previous definition due to its adversarial perspective. A definition of cyber security awareness that widens this perspective is *the ability of the user to recognize or avoid behaviors that would compromise cyber security; practice of good behaviors that will increase cyber security; and act wisely and cautiously, where judgment is needed, to increase cyber security* (Toth & Klein, 2013). Through previous definitions it can be presumed that recognition regarding cyber security awareness can only be

fostered if participants of a cyber context are provided with sufficient knowledge regarding cyber security. Additionally, next to understanding the importance and possible implications of cyber security awareness, the extent to which people behave in accordance with this understanding might be equally important (Parsons et al., 2017).

There are several training techniques that are adopted by organizations to influence the cyber security awareness of their employees, for example annual presentations or e-learnings. An upcoming and promising technique that can be incorporated in a cyber security awareness training context to potentially increase their effectiveness is gamification.

B. Gamification

Gamification is a concept that started peaking interest around 2010 (Zichermann & Cunningham, 2011). The phenomenon is often described as *the application of game design principles in non-gaming contexts* (Robson et al., 2015; Werbach & Hunter, 2012). Elaborating on these design principles leads to another definition of gamification as *the use of game thinking including progress mechanics (such as points systems), player control (such as avatar use), rewards, collaborative problem solving, stories, and competition in non-game situations* (Deterding, Dixon, Khaled, & Nacke, 2011; Kapp, 2012). This definition complements previous definition through providing concrete examples of design elements, but lacks an explanation of the purpose behind the application of gamification. There are literary sources that address this aspect of gamification, for example by describing gamification as *a transformative socio-technical systems design practice for motivational affordances in the service of human flourishing* (Deterding, 2014). By combining insights and previous definitions, it can be derived that gamification is often applied to stimulate behavior changes through increased engagement and motivation of participants.

Reviewing literature and recent studies provides numerous examples where contexts that included competitive elements successfully encouraged and stimulated participants to change their behavior (Gavas, Memon, & Britton, 2012). Including competitive and/or cooperative elements in a non-game context is an example of incorporating gamification. Gamified contexts provide a safe environment for participants to practice their behavior or skills under pressure. Despite the numerous examples of digital or online gamified environments, gamification can also be incorporated in a tabletop context as well, for example by including elements from a card game or a board game (Gondree, Peterson, & Denning, 2013). In the end, several studies concluded that gamified environments are often preferred over non-gamified environments by participants (Baxter, Holderness Jr, & Wood, 2015). However, research that concerns how to properly apply gamification in existing cyber security awareness contexts to benefit from such advantages is lacking.

III. METHODOLOGY

First, literature studies are performed regarding cyber security awareness, gamification concepts, and the process of applying gamification. These literature studies consist of journal papers, as well as conference papers and dissertations due to the preliminary research. Based on the insights of these literature studies, a framework is designed that provides a systematic approach to gamify cyber security awareness trainings. This framework is evaluated based on expert interviews. Next, an existing cyber security awareness training is selected and gamified using this framework, illustrating the usability of the framework. Finally, an empirical case study is performed in which the gamified training is executed by participants and compared to the existing training as executed by other participants. Based on the results of pre-training and post-training questionnaires, the perceived effectiveness of the trainings can be (statistically) evaluated.

IV. LITERATURE AND CASE STUDIES

This section addresses the knowledge gap regarding the systematic application of gamification in cyber security awareness contexts.

A. Constructs of Cyber Security Awareness

Research that considers what actually constitutes and influences cyber security awareness is lacking (Alotaibi, Furnell, Stengel, & Papadaki, 2016). Awareness is often point of discussion, opinions are not really converging, and it seems hard to characterize(Dodge Jr, Carver, & Ferguson, 2007).

An initial foundation for the constructs of cyber security awareness is statements regarding ‘skills’ and ‘capabilities’ regarding cyber security. Here, the relation between ‘skills’ and ‘capability’ can be elaborated; some authors describe capability as the *product of knowledge, skills, and tools* (Johnson, 2015). There are additional authors that regard knowledge and skills, but

they consider tools only to *describe capability on a generic context* (Ani et al., 2016).

Next to capability, knowledge and skills, many authors address behavior as a construct of cyber security awareness. For example, while employees might possess adequate capabilities, knowledge and skills, it is not guaranteed that they act accordingly (Alotaibi et al., 2016). An underlying reason might be that there is often a trade-off between convenience and behaving in a cyber security aware manner (Calic, Pattinson, Parsons, Butavicius, & McCormac, 2016; Manke & Winkler, 2012). Some authors state that it is more likely to affect behavior through attitude changes (Thomson & von Solms, 1998).

In addition to the discussed constructs, there appears to be additional factors that constitute and influence cyber security awareness or the individual constructs itself. Cyber security awareness can be regarded internally and externally. For example, there can be several individual, organizational, or intervention factors that affect the (constructs of) cyber security awareness of employees (Parsons et al., 2017).

B. Gamification Concepts for Cyber Security Awareness

Common cyber security awareness training techniques such as e-learnings or regular presentations are often considered intimidating, time-consuming, and non-inviting (Patten, 2015). A training technique that can be incorporated in cyber security training contexts to challenge these negative perceptions is called gamification. Gamification is often related to promising results regarding attention, feedback, and motivation (Kassicieh et al., 2015). Literature shows that the majority of gameful cyber security awareness trainings are actual games instead of applications of gamification. Since the body of knowledge that addresses gamification in cyber security awareness trainings is scarce, gamification in educational contexts is also regarded.

Following some authors it is of utter importance for the success of a gamified environment to select the appropriate gamification concepts (Kapp, 2012). However, research that adequately addresses such concepts is scarce (Hamari, Koivisto, & Sarsa, 2014). An exemplar framework is the Octalysis framework. This framework illustrates eight motivational drives that can be invoked in order to motivate people to perform activities; meaning, empowerment, social influence, unpredictability, avoidance, scarcity, ownership, and accomplishment (Chou, 2015). Chou states that there should be a balance of these drives in order to accomplish a successful gamification. Next, gamification mechanics should be balanced with the objectives of the training and they should fit with the sense or purpose of participants (Tinati, Luczak-Roesch, Simperl, & Hall, 2017).

A framework that concretely addresses specific gamification elements is the MDA framework (da Rocha Seixas, Gomes, & de Melo Filho, 2016; Zichermann & Cunningham, 2011). This framework includes mechanics, dynamics, and aesthetics as concepts of gamification. These concepts can be further elaborated into specific components like points, levels, and rewards. A variant of the MDA framework is the MDE framework, which includes multi-directional relationships between the different gamification components (Robson et al., 2015). Next, the aesthetics concept is replaced with an emotions concepts. This is in line with various authors who state that aesthetics are more applicable in a full-blown game context, whereas emotions are more applicable in a gamification context (Landsell & Hägglund, 2016).

Another framework that is valuable when studying gamification concepts is the framework from Marczewski. This framework complements previous frameworks and models by incorporating both motivations and gamification components and relating these to six different player types; socializers, philanthropists, disruptors, free spirits, players, and achievers (Marczewski, 2015). Next, some authors state that the implementation of gamification concepts that are beneficial for a specific target might have an opposite effect on other individuals (Mohamad, Salam, & Bakar, 2017; Thiel & Lehner, 2015). As such, incorporating a balance of gamification elements in gamified cyber security awareness trainings might avoid or limit such unanticipated effects.

C. Designing and Evaluating a Framework

An often cited source that addresses the process of applying gamification is the 6D framework (Werbach & Hunter, 2015). Following these authors, there are six steps to follow when applying gamification as illustrated below.

1) Define business objectives.
2) Delineate target behaviors.
3) Describe your players.
4) Devise activity loops.
5) Don't forget the fun.
6) Deploy the appropriate tools.

Executing step one to five ensures a fit between the selected methods, the envisioned environment, and its purpose. Next, step six regards actual gamification elements as addressed previously.

Other research that regards the process of applying gamification is the study from Huang and Soman. These authors established five steps when regarding the application of gamification in the field of education.

1) Understanding the target audience and the context.
2) Defining learning objectives.
3) Structuring the experience.
4) Identifying resources.
5) Applying gamification elements.

Interestingly, both the steps from Huang and Soman and the 6D framework from Werbach and Hunter regard gamification elements last.

An additional model that describes the process of gamification is the Sustainable Gamification Design (SGD) model (Raftopoulos, 2014). The seven steps as derived from this model are displayed below.

1) Establish project needs and objectives, and ethical foundations.
2) Map project motivations, methods and outcomes.
3) Stakeholder mapping and user or player personas.
4) Creative problem-solving and ideation through participatory/co-design.
5) Exploring suitable gamification technology options.
6) Selecting appropriate gameplay and game mechanics.
7) Prototype, pilot, test, iterate and launch the gamified application.

In order to construct a framework design, the seven guidelines from Hevner concerning design science are regarded (Hevner, March, Park, & Ram, 2004). These guidelines, as illustrated below, aid developers of an artifact to acquire an understanding of the specific design problem and its solution (Hevner et al., 2004).

1) *Design as an Artifact:* Design-science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation.
2) *Problem Relevance:* The objective of design-science research is to develop technology-based solutions to important and relevant business problems.
3) *Design Evaluation:* The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods.
4) *Research Contributions:* Effective design-science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies.
5) *Research Rigor:* Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact.
6) *Design as a Search Process:* The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment.
7) *Communication of Research:* Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences.

Since all these frameworks, models and guidelines are not tailored to a cyber security awareness context, the results of the previous literature studies will be used towards designing a framework for guiding developers of a gamified cyber security awareness training.

Since the initial framework design is primarily based on theoretical knowledge, the framework is evaluated by consulting cyber security awareness and gamification experts. Comments and feedback are collected regarding their expertise and practical experience and the initial framework design is adjusted accordingly. The results section of this article illustrates and discusses the resulting framework.

D. Illustrating the Usability of the Framework

After evaluating and adjusting the framework, its usability is illustrated. For this purpose, an online Deloitte cyber security awareness training is gamified. The existing training is selected based on duration, expected prior knowledge, addressed cyber security awareness topics, target participants, and the generalizable applicability of the training. The cyber security awareness related content was extracted along with the objectives of the training.

E. Perceived Effectiveness of Cyber Security Awareness Trainings

The existing cyber security awareness training and the gamified training are compared in order to evaluate their perceived effectiveness. A comparative study is performed that involves eight participants which execute the non-gamified cyber security awareness training and eight participants which execute the gamified training. Each participant fills in a pre-training questionnaire and a post-training questionnaire with questions

regarding (perceived effects on) their level of cyber security awareness. The results are used to discuss the perceived effectiveness of raising cyber security awareness through this particular gamified training that resulted from applying the framework.

V. RESULTS

This section discusses the results from the performed literature studies and the executed case study.

A. Cyber Security Awareness Constructs

The literature study towards constructs of cyber security awareness led to the newly developed model as visualized in 1 regarding what constitutes and influences cyber security awareness. As such, cyber security awareness is affected by capability and behavior. In turn, capability consists of two constructs; knowledge and skills. Besides, the behavior construct encompasses actions and attitude. Capability and behavior do not directly influence each other. However, there might be indirect influences at play. Finally, the yellow hexagon illustrates contextual factors that might affect cyber security awareness in general or its constructs. These factors might be individual, organizational or related to intervention (Parsons et al., 2017). Note, there might be other factors and these might differ per situation, organization or employee.

B. Gamification Mechanics for Cyber Security Awareness Trainings

Table I provides a newly categorized overview of gamification mechanics as applicable for cyber security awareness trainings that resulted from the performed literature study.

Following this literature study, mechanics are the more practical and design oriented gamification concepts. In other words, these are the primary elements that a developer can incorporate in a gamified cyber security awareness training. Note that some gamification mechanics can fit several categories.

C. Design and Evaluation of a Framework

From literature it became apparent that a framework for gamifying cyber security awareness trainings should incorporate the fact that relevant content for every participant should be provided by the training. Next, the framework should reflect the fact that cyber security awareness trainings must include up to date content, for example regarding current and future trends. Such trends can either be internal, e.g. demands or policies of organizations, or external, e.g. potential cyber threats.

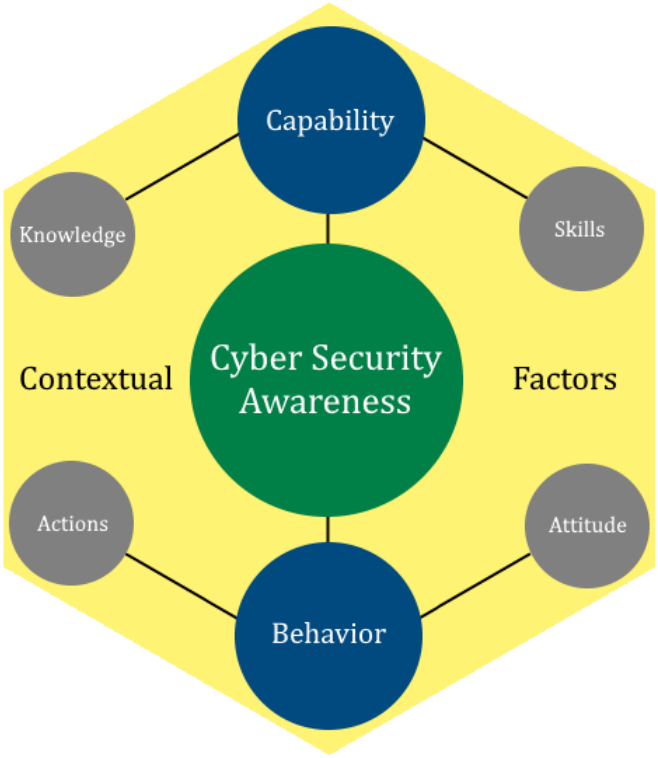

Fig. 1. Constructs of Cyber Security Awareness

TABLE I
OVERVIEW OF GAMIFICATION MECHANICS

Categories	Gamification Mechanics
Cooperation / Competition	Leaderboards Social Guilds Roles Avatars Virtual Goods
Prices	Badges / Medals Trophies Achievements Awards, Trading & Gifting / Rewards
Adventures	Challenges Actions Quest / Goal / Mission Boss Battles
Progression	Progress Bar / Status Points / XP Levels Feedback / Reports
Surprises	Unlockable Content Easter Eggs Lottery / Game of Chance Notifications

Additional insight comprises the impression that the framework should consider multiple forms of communication. For one, different types of cyber security awareness content might call for different types of communication. For example, as discussed earlier, complex content might better be provided in print, while less complex content can be transferred verbally. Next, the framework for gamifying cyber security awareness trainings should reflect the derived insight regarding the length of such trainings. As mentioned, it can be assumed that shorter, repeated trainings provide more advantages than long, singular trainings. For one, these short and repeated sessions promise improved retention and lower the barrier for employees to participate in such trainings. Finally, a gamified cyber security awareness training should be gamified via the framework in such a way that there are game elements in place that can appeal to every participant. In other words, each participant should be able to feel positively affected through at least one game element as implemented in the gamified cyber security training. The resulting framework requirements can be seen in Table II.

Three frameworks and models regarding the process of applying gamification are analyzed and the resulting steps as derived from analyzing previous research from Huang and Soman (2013), Raftopoulos (2014), and Werbach and Hunter (2015) are displayed below.

1) Objectives
2) Context
3) Structure
4) Resources
5) Diverge
6) Converge
7) Build
8) Evaluate

These steps form the initial structure of the framework for guiding developers of a gamified cyber security awareness training. In order to develop the framework design, the seven design-science research guidelines from Hevnes, as addressed in Section IV, are also regarded and applied to the context of gamification and cyber security awareness trainings.

1) *Design as an Artifact:* Visual representation of process of gamifying existing cyber security awareness trainings. A framework is designed, visualizing the different steps of this process.
2) *Problem Relevance:* The underlying organizational problem is a lack of cyber security awareness and how to raise this effectively through the use of gamification in training contexts.

TABLE II
DISTILLED REQUIREMENTS TOWARDS A FRAMEWORK FOR GAMIFYING CYBER SECURITY AWARENESS TRAININGS

Categories	Requirements
CSA	- Establish business targets and learning objectives - Distinguish relevant topics and content regarding learning objectives - Make sure the content is recognizable and relevant for participants - Perform continuous monitoring; check content's relevance and up to date
Gamification	-Identify motivations of participants and align gamification tactics (ARCS+G) - Apply different gamification concepts to appeal to different participants - Make sure the gamification concepts align with the objectives
Additional	- Perform an analysis of cultural and lifestyle differences that might affect training experiences and results - Adopt a flexible approach; possibilities to change or adjust particular modules -Enable customization, e.g. to different users, message to be delivered, or content - Offer different delivery methods, e.g. print for complex information Provide short sessions on regular basis to improve retention

3) *Design Evaluation:* The artifact is evaluated by performing observed expert interviews. The use of the artifact is demonstrated through its application to an existing cyber security awareness training.
4) *Research Contributions:* A key research contributions is the design artifact itself as a possible solution to the identified organizational problem. Next, the cyber security awareness constructs model contributes metrics to be used in cyber security awareness research and practice.
5) *Research Rigor:* Literature studies concerning cyber security awareness and gamification are performed to construct the framework. The framework is evaluated through expert interviews and its usability is illustrated through a case study.
6) *Design as a Search Process:* The research is conducted in an iterative way regarding both theory and practice. Literature studies towards an initial framework design is followed by expert interviews and a case study. These means result in an adjusted framework and a gamified training.

Fig. 2. Framework

7) *Communication of Research:* The research is communicated and presented through a framework with two layers of abstraction. One layer for a quick overview, one layer with in-depth information regarding the underlying processes.

The designed framework is evaluated through expert interviews and adjusted accordingly. The resulting framework is displayed in figure 2. As indicated by the different colors, the framework consists of three phases: fundamentals, blueprint, and design. The steps of these phases correspond to the steps for gamifying trainings as discussed previously.

The fundamentals phase comprises two steps; objectives and context. These steps consider an analysis of the objectives of the training and its context. The blueprint phase consists of the resources and structure steps. These steps guide developers of gamified cyber security awareness trainings to a training structure while taking into consideration the available resources. The design phase encompasses the diverge, converge, and build steps. The diverge step includes the generation of ideas. In the converge step, these ideas are evaluated and selected based on criteria like KPIs related to the objectives of the training. These can also be based on the constructs of the cyber security awareness model as established earlier. During the final step, build, prototypes are built in order to test the developed cyber security awareness training.

The yellow circles in the framework illustrate (interim) results; these illustrate the aim of each phase. Here, training scope addresses an analysis of existing cyber security awareness training and the objectives of the current training. Next, blueprint & toolbox encompasses an overview of content from the analyzed trainings and possible options and the initial structure of the current training. Finally, training roll-out is the final deliverable; a training that is ready to be rolled-out. Next to these (interim) results, feedback loops are present. The improve feedback loop is activated when test runs with the prototype illustrate room for improvement. As such, iterations within the design, converge, or build step can result. The other feedback loop, re-evaluate, is activated when the training is rolled-out. This feedback loop includes regular checks, for example whether the training still aligns with the context or objectives of the training and whether the contents of the training are still up-to-date and relevant.

D. Evaluated Application of the Framework

The usability of the framework is illustrated through gamifying an existing cyber security awareness training by using the designed framework. Next, pre-training and post-training questionnaires are performed with eight participants for the existing digital training and eight participants for the gamified table-top training. Cyber security awareness and its four constructs, participation, and interaction are key questioned aspects. The averaged quantitative results of the four different questionnaires of the non-gamed, existing training and gamified training are presented in tables III and IV. Here, CSA means cyber security awareness.

TABLE III
AVERAGED RESULTS (NON-GAMIFIED TRAINING)

	Pre-Training	**Post-Training (Effect)**
CSA	4.06	2.50
Attitude	4.13	2.25
Knowledge	3.38	2.50
Skills	3.63	2.25
Actions	4.00	2.00
Participation	N/A	2.88
Interaction	N/A	2.38

TABLE IV
AVERAGED RESULTS (GAMIFIED TRAINING)

	Pre-Training	**Post-Training (Effect)**
CSA	3.88	2.81
Attitude	4.00	2.75
Knowledge	3.56	2.63
Skills	3.69	2.25
Actions	4.06	2.63
Participation	N/A	3.88
Interaction	N/A	4.13

The results suggest that on average the participants perceived their level of cyber security already quite high prior to the training. This might affect the score of 'affected cyber security awareness' of the post-training questionnaires. Next, every aspect (besides skills) received a higher averaged score in the gamified cyber security awareness training, when comparing the results of both post-training questionnaires. Additionally, both participation and interaction aspects scored higher on average in the gamified training when compared to the post-training results of the existing training. Finally, 75% of the participants would recommend the gamified cyber security awareness training, whereas 50% would recommend the existing,

non-gamified training.

The results of Tables III and IV suggest that the participants of the gamified training perceived a greater effectiveness of the training than the participants of the existing training. In order to assess the significance of these results, a one-tailed t-test is applied with the null hypothesis H_0 that the scores of the gamified training are samples from the score distribution of the non-gamified training. The chosen level of significance is 0.05.

One participant in the gamified training stood out in scoring (very low) perceived effectiveness in all aspects of the training. This participant noted that he/she expected a full-blown game and more fun. As such, the gamified training did not meet his/her expectations. Therefore, the same null hypothesis is assessed twice; once using all results of the questionnaires and once while excluding the results of this particular participant of the gamified training.

TABLE V
THE p-VALUE OF THE NULL HYPOTHESIS H_0 ON PERCEIVED INCREASED ASPECTS.

	p-value using all results	**p-value excluding one set of results**
CSA	0.304	0.170
Attitude	0.203	0.171
Knowledge	0.422	0.288
Skills	0.500	0.369
Actions	0.098	0.033
Participation	0.096	0.024
Interaction	0.006	0.000

The results of the null hypothesis can be seen in Table V. In case of regarding all results of the questionnaires, it can be concluded that the null hypothesis can be rejected only for the interaction aspect (< 0.05) and thus that only the perceived increase in the interaction aspect is significant. The perceived effect on cyber security awareness or on any of the constructs attitude, knowledge, skills and actions is not significantly increased by the gamification. In case of excluding the results of a notable low-scoring participant, it can be concluded that the null hypothesis for the actions, participation and interaction aspects can be rejected (< 0.05) and thus that only the perceived increase in the actions, participation and interaction aspects is significant.

In the end, when comparing the results of the questionnaires, it should be noted that the expectations of the participants should be aligned with the goal of the (gamified) training. Furthermore, it can be presumed that this particular application of the framework results in a successful gamification of the existing cyber security awareness training.

VI. CONCLUSIONS

Few literature exists on the application of gamification on cyber security awareness trainings. Here, capability, behavior and contextual factors are described as key parts of cyber security awareness. In this sense, capability consists of the constructs knowledge and skills. Next, behavior encompasses the constructs knowledge and skills. Here, a construct is described as a characteristic that constitutes and influences specific aspects of cyber security awareness. Finally, next to these constructs, contextual factors play a role in cyber security awareness contexts. These factors could be explained through individual, organizational or intervention factors. A model is developed which displays these factors along with the constructs of cyber security awareness and visualizes the relations. As such, the model can be used towards identifying or prioritizing specific aspects of cyber security awareness that can be improved through training. In this way, cyber security awareness might be raised more effectively.

Secondly, gamification concepts for the purpose of raising cyber security awareness through training are established. Several frameworks address characteristics like motivational drives, mechanics, and player types. Regarding the applicability of the identified gamification concepts to cyber security awareness, research shows that there is little information regarding applied gamification concepts in specific cyber security awareness contexts. Studies regarding different applications of gamification concepts suggest that leaderboards, badges/medals, points, quest/goal/mission and feedback are key gamification mechanisms. In the end, there are no reasons to assume that such gamification concepts are not applicable to cyber security awareness contexts.

Thirdly, a framework for gamifying cyber security awareness trainings is established. The described steps for this structure are: objectives, context, structure, resources, diverge, converge, build, and evaluate. Next, previous insights regarding cyber security awareness and its constructs are integrated with these steps to provide a framework design for gamifying cyber security awareness trainings. The usability of this frame-

work is evaluated by performing several interviews with experts in the field of cyber security awareness and gamification. Next, the framework was adjusted according to their comments and feedback. The resulting framework consists of the following phases: fundamentals, blueprint, and design. The fundamentals phase encompasses the steps objectives and context, as derived from the frameworks and models analyses. Next, the blueprint phase consists of the structure and resources steps. Finally, design includes the diverge, converge, and build steps. Next to the phases and the associated steps; (interim) results, feedback loops, and coherence between cyber security awareness aspects are visualized. This framework guides developers towards successfully gamifying cyber security awareness trainings.

Fourthly, the usability of the framework and the perceived effectiveness of a resulting training is assessed by following a two-step approach. First, gamifying an existing cyber security awareness training by using the designed framework. Secondly, a comparative study regarding the results of pre-training and post-training questionnaires of eight participants of the existing training and eight participants of the gamified training. The training selected for gamification was executed and analyzed in order to derive cyber security awareness content and to identify the key objectives of the training. The resulting gamified table-top training uses the cyber security awareness constructs model as KPIs. Gamifying this specific training by using the designed framework illustrates its usability. Next, the questionnaires aim to show to what extent the gamification has been successful and include questions regarding cyber security awareness (change), the four KPIs; knowledge, skills, actions, and attitude, and aspects like participation and interaction. The results of the questionnaires show that each KPI scores higher in the gamified training, with skills receiving an equal score. Also participation and interaction receive a higher average score in the gamified training when compared to the existing training. Additionally, 75% of the participants of the gamified training would recommend the training, compared to 50% of the participants of the existing training who would recommend the training. However, the scores are not significantly higher for the gamified training except for the interaction aspect. If one notable low-scoring participant is excluded, the aspects actions, participation and interaction are significantly higher for the gamified training. The low scores of this particular participant can (partially) be explained by his/her expectation that the gamified training would be a full-blown game. In sum, this particular application of the framework resulted in a successful gamification of an existing cyber security awareness training.

Finally, combining previous insights provides an answer to the presented research question.

Research question *How can gamification be applied to a training context that aims to affect cyber security awareness?*

Firstly, cyber security awareness is constituted and influenced by the four constructs knowledge, skills, action and attitude and contextual factors. Secondly, five categories of gamification concepts (cooperative/competitive, prices, adventures, progression, and surprises) are established that are applicable to cyber security awareness contexts. This led to a framework, evaluated by expert interviews, for gamifying cyber security awareness trainings. The usability of the framework is illustrated through applying the framework, i.e. developing a gamified cyber security awareness training. This study also included an empirical case study with pre-training and post-training questionnaires. Results show a higher perceived increase in cyber security awareness in the gamified training when compared to the existing training, although not significantly higher. In the end, the evaluated framework provides a successful tool for gamifying cyber security awareness trainings.

VII. LIMITATIONS

There are several limitations that can be identified from performing this research. First, since research in the field of gamification and cyber security awareness is quite preliminary, additional sources were consulted, e.g. conference papers, white papers, and dissertations. Using these sources as references might have affected the results or conclusions of this research.

Next, since the dynamic field of gamification and cyber security awareness, the theories as derived from literature studies might not always reflect current practices or recent trends. In turn, this might affect the practical appropriateness of the designed framework.

Additionally, there are assumptions underlying the identified gamification concepts as applicable to cyber security awareness. However, these assumptions might need to be researched and validated, i.e. to what extent is each gamification concept applicable to specific cyber security awareness topics or trainings? For example, some concepts might be more appropriate in an ‘offline’

setting whereas other gamification concepts are more appropriate in e-learning contexts.

For the purpose of providing a clear overview, the designed framework is a simplification of the gamification process of cyber security awareness trainings. For example, some phases or steps might be executed concurrent instead of purely sequential. Besides, some steps or phases might be iteratively executed.

The performed empirical case study might suffers from limitations. For example, by providing the experts the initial design of the framework might have affected their creativity or perspective on gamification as a process regarding cyber security awareness. In other words, the framework might have turned out very differently if it was co-designed from scratch with these experts. Next, the framework as adjusted according to expert consultation was not evaluated. This might affect (the results of) developed gamified cyber security awareness trainings.

Next, since the case study is based on a single case, this might affect the drawn conclusions regarding the usability of the framework. For example, selecting multiple existing trainings or developing multiple gamified trainings might lead to different results and conclusions. In this case, the framework has not been evaluated for online or digital gamified cyber security awareness trainings, since the current gamified training was developed as a table-top training.

Finally, there are limitations regarding the comparative study of the existing and the gamified cyber security awareness training. For one, next to the parameters under investigation, additional aspects differed between these trainings. For example, the existing training is provided in a digital, online format whereas the gamified training is provided in a paper-based, tabletop format. Next, the existing training is executed by individuals, whereas the gamified training is executed in duos. This could have affected the results from the questionnaires since participants might have influenced each other. Besides the differences, the content of the trainings is as equal as possible, since this was not up to investigation. A possible limitation here is that the content might not be adequate, up to date, or suit for the type of gamification. Taking the content as a starting point, the resulting gamified cyber security awareness training might be unsatisfactory. This limitation exist due to the methodology of using a comparative study for measuring the perceived effectiveness of an application of the designed framework. In practice, there is more freedom in the framework to add, remove, or adjust content when developing a gamified cyber security awareness training. Moreover, the limited number of participants of the existing and the gamified training is a limitation of this research. With an increased number of participants, the null hypothesis would more likely be rejected and an extrapolation or generalization of the results is more reliable. Finally, the case study only regarded the perceived effectiveness of the trainings and this might differ from the actual effectiveness.

VIII. FUTURE RESEARCH

An initial recommendation for future research regards quantifying the influence of the different constructs (knowledge, skills, attitude and actions) on cyber security awareness. Next, the contextual factors can be elaborated or researched on their influence on specific constructs of cyber security awareness.

Future research could also encompass the applicability of the identified gamification concepts in specific training settings. For example, some concepts might be more applicable in competitive cyber security awareness environments, whereas other are more applicable in cooperative environments. Also the impact of particular gamification elements on raising cyber security awareness or its constructs can be studied.

Next, future research could focus on tailoring the framework to specific topics of cyber security awareness. Furthermore, a new or existing framework that regards gamification can be (quantitatively) compared to the current framework.

Future research could also extend this research by applying the framework in different settings, with different player types, with more participants, or in a longer time frame. For example, developing different gamified cyber security awareness trainings and comparing them in their effectiveness of raising (constructs of) cyber security awareness.

Finally, since organizations can differ greatly in their focus and priorities regarding important cyber security awareness themes and topics, this might affect the designed framework or the resulting gamified trainings. Future research could study the effects of (organizational) cultures on gamified cyber security awareness trainings or how to incorporate such aspects in the designed framework.

REFERENCES

Adams, M., & Makramalla, M. (2015). Cybersecurity skills training: an attacker-centric gamified approach. *Technology Innovation Management Review*, *5*(1).

Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2016). A review of using gaming technology for cyber-security awareness.

Ani, U. P. D., He, H. M., & Tiwari, A. (2016). Human capability evaluation approach for cyber security in critical industrial infrastructure. In *Advances in human factors in cybersecurity* (pp. 169–182). Springer.

Assante, M. J., & Tobey, D. H. (2011). Enhancing the cybersecurity workforce. *IT professional*, *13*(1), 12–15.

Baxter, R. J., Holderness Jr, D. K., & Wood, D. A. (2015). Applying basic gamification techniques to it compliance training: Evidence from the lab and field. *Journal of Information Systems*, *30*(3), 119–133.

Caldwell, T. (2013). Plugging the cyber-security skills gap. *Computer Fraud & Security*, *2013*(7), 5–10.

Calic, D., Pattinson, M. R., Parsons, K., Butavicius, M. A., & McCormac, A. (2016). Naïve and accidental behaviours that compromise information security: What the experts think. In *Haisa* (pp. 12–21).

Chou, Y.-K. (2015). Actionable gamification: Beyond points. *Badges, and Leaderboards, Kindle Edition, Octalysis Media (Eds.)*.

da Rocha Seixas, L., Gomes, A. S., & de Melo Filho, I. J. (2016). Effectiveness of gamification in the engagement of students. *Computers in Human Behavior*, *58*, 48–63.

Deterding, S. (2014). Eudaimonic design, or: Six invitations to rethink gamification.

Deterding, S., Dixon, D., Khaled, R., & Nacke, L. (2011). From game design elements to gamefulness: defining gamification. In *Proceedings of the 15th international academic mindtrek conference: Envisioning future media environments* (pp. 9–15).

Dodge Jr, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. *computers & security*, *26*(1), 73–80.

Franke, U., & Brynielsson, J. (2014). Cyber situational awareness–a systematic review of the literature. *Computers & Security*, *46*, 18–31.

Gavas, E., Memon, N., & Britton, D. (2012). Winning cybersecurity one challenge at a time. *IEEE Security & Privacy*, *10*(4), 75–79.

Gondree, M., Peterson, Z. N., & Denning, T. (2013). Security through play. *IEEE Security & Privacy*, *11*(3), 64–67.

Hamari, J., Koivisto, J., & Sarsa, H. (2014). Does gamification work?–a literature review of empirical studies on gamification. In *System sciences (hicss), 2014 47th hawaii international conference on* (pp. 3025–3034).

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS quarterly*, *28*(1), 75–105.

Howarth, F. (2014). The role of human error in successful security attacks. *Security Intelligence Website. IBM Security Intelligence*.

Huang, W. H.-Y., & Soman, D. (2013). Gamification of education.

Jiemei, Z., Xuewei, F., Dongxia, W., & Lan, F. (2014). Implemention of cyber security situation awareness based on knowledge discovery with trusted computer. In *Asia-pacific web conference* (pp. 225–234).

Johnson, T. A. (2015). *Cybersecurity: Protecting critical infrastructures from cyber attack and cyber warfare*. CRC Press.

Joshi, A., Ramani, V., Murali, H., Krishnan, R., Mithra, Z., & Pavithran, V. (2012). Student centric design for cyber security knowledge empowerment. In *Technology enhanced education (ictee), 2012 ieee international conference on* (pp. 1–4).

Kapp, K. M. (2012). *The gamification of learning and instruction: game-based methods and strategies for training and education*. John Wiley & Sons.

Kassicieh, S., Lipinski, V., & Seazzu, A. F. (2015). Human centric cyber security: What are the new trends in data protection? In *Management of engineering and technology (picmet), 2015 portland international conference on* (pp. 1321–1338).

Landsell, J., & Hägglund, E. (2016). *Towards a gamification framework: Limitations and opportunities when gamifying business processes.*

Lohrmann, D. (2014). *Ten recommendations for security awareness programs.* Retrieved January 2018, from https://www.govtech .com/blogs/lohrmann-on-cybersecurity/ Ten-Recommendations-for-Security-Awareness -Programs.html

Manke, S., & Winkler, I. (2012). *The habits of highly successful security awareness programs: A cross-company comparison* (Tech. Rep.). Technical report, Secure Mentem, 2012. http://www. securementem. com/wp-content/uploads/2013/07/Habits_white_paper.

pdf.

Marczewski, A. C. (2015). *Even ninja monkeys like to play: Gamification, game thinking and motivational design*. CreateSpace Independent Publishing Platform.

McGrath, S. (2016). *Lack of security awareness poses a major threat to businesses.* Retrieved January 2018, from http://www.computerweekly.com/microscope/news/4500278103/Lack-of-security-awareness-poses-a-major-threat-to-businesses

Mohamad, S. N. M., Salam, S., & Bakar, N. (2017). An analysis of gamification elements in online learning to enhance learning engagement. *Proceedings of the 6th International Conference on Computing & Informatics*.

NOS. (2018). *Ook belastingdienst getroffen door ddos-aanval.* Retrieved January 2018, from https://nos.nl/artikel/2214339-ook-belastingdienst-getroffen-door-ddos-aanval.html

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (hais-q): two further validation studies. *Computers & Security*, *66*, 40–51.

Patten, B. (2015). *How gamification is changing employee training.* Retrieved January 2018, from https://www.trainingindustry.com/content-development/articles/how-gamification-is-changing-employee-training.aspx

Raftopoulos, M. (2014). Towards gamification transparency: A conceptual framework for the development of responsible gamified enterprise systems. *Journal of Gaming & Virtual Worlds*, *6*(2), 159–178.

Robson, K., Plangger, K., Kietzmann, J. H., McCarthy, I., & Pitt, L. (2015). Is it all a game? understanding the principles of gamification. *Business Horizons*, *58*(4), 411–420.

Sheahan, K. (2017). *What are the advantages of information technology in business?* Retrieved January 2018, from https://www.smallbusiness.chron.com/advantages-information-technology-business-774.html

Thiel, S.-K., & Lehner, U. (2015). Exploring the effects of game elements in m-participation. In *Proceedings of the 2015 british hci conference* (pp. 65–73).

Thomson, M. E., & von Solms, R. (1998). Information security awareness: educating your users effectively. *Information management & computer security*, *6*(4), 167–173.

Tinati, R., Luczak-Roesch, M., Simperl, E., & Hall, W. (2017). An investigation of player motivations in eyewire, a gamified citizen science project. *Computers in Human Behavior*, *73*, 527–540.

Toth, P., & Klein, P. (2013). A role-based model for federal information technology/cyber security training. *NIST special publication*, *800*(16), 1–152.

Werbach, K., & Hunter, D. (2012). *For the win: How game thinking can revolutionize your business*. Wharton Digital Press.

Werbach, K., & Hunter, D. (2015). *The gamification toolkit: Dynamics, mechanics, and components for the win*. Wharton Digital Press.

Zichermann, G., & Cunningham, C. (2011). *Gamification by design: Implementing game mechanics in web and mobile apps*. " O'Reilly Media, Inc.".