# Systematically Applying Gamification to Cyber Security Awareness Trainings

*A framework and case study approach*

Master thesis submitted to Delft University of Technology

in partial fulfilment of the requirements for the degree of

**MASTER OF SCIENCE**

in **Complex Systems Engineering and Management**

Faculty of Technology, Policy and Management

by

Iris Rieff

Student number: 1517503

To be defended in public on March 27th 2018

## Graduation committee

| | |
|---|---|
| Chairperson | : Prof.dr. M.J.G. van Eeten, Section POLG |
| First Supervisor | : Dr.rer.soc. H.K. Lukosch, Section Policy Analysis |
| Second Supervisor | : Dr.ir. W. Pieters, Section Safety and Security Science |
| External Supervisor | : R. Osseyran MSc, Deloitte (Cyber Risk Advisory) |

# Preface

Since I was little I have always been interested in pretty much everything computer related. I remember when I was asked as a little girl what I wanted to become when I grow up and I answered an inventor or technician. This answer always made people raise their eyebrows for not being a popular answer, e.g. veterinarian. Nowadays, I continue to like technology and coming up with innovative solutions to existing challenges or problems.

My computer related passion revolves around both hardware and software. During my bachelor and master studies I enjoyed several 'hello world' courses along with a course in which I had to build and program a Segway related robot. During such courses, questions were often raised regarding privacy and security, especially when working with personal data, using open source software or when connecting things to the internet. This is when the field of cyber security and cyber security awareness peaked my interest. For this reason, my choice for a master specialization was fairly easy due to the existence of the 4TU cyber security specialization. After this specialization, I had the opportunity to join the NCS3 (National Cyber Security Summer School) past summer. I really enjoyed all cyber security related courses during my specialization and the NCS3 and therefore decided to continue on this topic by incorporating it in my thesis.

Another recurring topic in this thesis is gamification. I have always been fond of games and intrigued by the logic and strategies behind them. For example, I am very interested in how game developers can come up with something so dynamic, engaging and unceasing entertaining. After organizing several (board) game nights I am surprised by the enthusiasm, motivation and changes in behavior these games can trigger. This is one of the reasons why I started to look into the topic of gamification during my master program. In this graduation project I wanted to regard both of these fields that appeal to me – cyber security and gamification – and try to identify where they overlap and where they can add value to one another towards a synergetic relation.

I decided to do my graduation project externally to create an opportunity to put my knowledge and theoretical background into practice. I was glad that Deloitte liked my thesis proposal and decided to hire me as a graduate student for the duration of my graduation project. In the past few months I met many great people and experienced cyber security awareness and gamification in practice. I would really like to thank my first supervisor Heide Lukosch for her extensive feedback on my writings, the time she freed to have face to face meetings, and her moral support. Next, I like to thank my second supervisor Wolter Pieters for his sharp questions and shared insight due to his incredible knowledge and expertise regarding cyber security and cyber security awareness. Thirdly, I am thankful for my external supervisor Raoel Osseyran who facilitated several introductions with great people and our coffee breaks in which we thoroughly discussed my progress regarding my thesis and my learning objectives. Next, I am extremely grateful for the various experts, especially Carl Mattern and Robbin van den Dobbelsteen, who took the time to discuss my thesis and the valuable feedback they provided on my framework which took my graduation project to a next level. Last but not least I like to thank my (new) friends and family and my boyfriend Alex in particular for being so supportive and patient with me in good and lesser times. In the end I am very pleased with these past few months in which I experienced being a graduate student at Deloitte Cyber Risk Advisory and I look forward to the well-deserved offsite event this March!

Iris Rieff

Delft, March 2018

# Summary

One of the most fast-paced fields of current industries is Information and Communication Technology. ICT offers organizations many benefits, like automation of processes, quick and effective communication, and storage and protection of information (Sheahan, 2017). Nowadays, most of an organization's ICT-related assets are connected to the internet. Unfortunately, due to these internet connections, ICT assets become more vulnerable to cyber related incidents. Examples of such incidents are the order of the day, take for example news regarding data leaks that expose privacy sensitive data of organization's customers (NOS, 2017a, 2017b). The risks of exposed vulnerabilities are even greater when employees working with the ICT systems are unaware of these vulnerabilities and are unaware of the need for cyber security. Inappropriate behavior can result in severe cyber security incidents. In sum, cyber security awareness lays the foundation of an organization's ability to achieve and maintain adequate cyber security to prevent incidents.

Several ways exist to increase cyber security awareness (Lohrmann, 2014). A particular method that shows promising results in fields related to cyber security awareness is gamification. In order to familiarize oneself with this phenomenon, gamification can be defined as: '*The application of game design principles in non-gaming contexts.*' (Robson, Plangger, Kietzmann, McCarthy, & Pitt, 2015, p. 1). Previous research into this topic, including a literature review, showed several benefits of the application of gamification in cyber security contexts (Adams & Makramalla, 2015; Boopathi, Sreejith, & Bithin, 2015; Fouché & Mangle, 2015; Margalit, 2016). One of the envisioned benefits of gamification as applied to cyber security awareness is increased engagement.

Currently, limited scientific sources address applying gamification to cyber security awareness training. Next, no structured approach exists that could aid training developers in gamifying programs that aim to raise cyber security awareness. Such an approach should be based on the constituents and influences of cyber security awareness and gamification concepts that are applicable to this field. However, this proves to be a knowledge gap in current research. In this thesis, this gap is addressed by performing literature studies regarding cyber security awareness and gamification concepts. This resulted in a cyber security awareness constructs model and a categorized overview of gamification mechanics as applicable to cyber security awareness.

The derived insights of the literature studies were used to design a framework for applying gamification to cyber security awareness trainings. This framework aims to aid developers in properly gamifying the specific environment. The framework was evaluated by performing interviews with cyber security awareness and gamification experts. This resulted in an adjusted framework for applying gamification to cyber security awareness trainings. Next, in order to illustrate its usability, the framework was used to gamify an existing cyber security awareness training. This resulted in a gamified cyber security awareness training offered in a table-top format. An empirical case study in which the gamified training was compared to the existing training illustrated a successful application of gamification.

This graduation project took place at Deloitte; a company that is a frontrunner in the field of cyber security and related awareness and is open to innovative approaches, such as gamification, to address these fields.

# Table of Contents

# List of Figures

# List of Tables

# 1. Introduction

In this section, an introduction of the research project is provided. First, the research problem is addressed along with the research approach of this research. Subsection 1.3 elaborates on its scientific and societal relevance. Finally, the structure of the remainder of this thesis is provided.

## 1.1 Research Problem

This subsection addresses the research problem, the problem statement, the scope and the research questions of this thesis.

### 1.1.1 Problem Exploration

When reviewing recent literature on the topic of cyber security, many challenges for this field surfaced. Firstly, there is a severe lack of security awareness in society and organizations (Franke & Brynielsson, 2014; Joshi et al., 2012). This contributes to an increase in the number of incidents from phishing, data leaks, security breaches and cyber-attacks every year (McGrath, 2016). From these incidents, 93% involves phishing (Verizon, 2017). Several studies state that the human factor is the underlying reason for the significant increase in cyber incidents (Noell, 2017).

Addressing awareness of cyber security remains difficult for there is a severe shortage of cyber security specialists (Assante & Tobey, 2011). A reason for this shortage might be the little emphasis on cyber security education (Joshi et al., 2012). This shortage of cyber security knowledge and skills is one of the most notable reasons why organizations struggle to acquire and maintain adequate security of their cyber domains. Unfortunately, following some authors, properly meeting this shortage can take up to 20 years when adopting current methods (Caldwell, 2013).

The cyber security field possesses extra characteristics that challenge organizations worldwide. A challenge is the fact that this field is extremely fast-paced and dynamic (Caldwell, 2013). This increases the need for proper education since both new and existing professionals need to be updated regularly on cyber security developments for organizations to maintain an adequate level of cyber security and related awareness. A final challenge is that the organizations often lack a definition of an employee´s required cyber security awareness (A. Wilson & Ali, 2011). In other words, it is hard for organizations to establish what knowledge and skills are 'effective' for which employees and how to properly address these in their training (Caldwell, 2013).

There exist several training methods that organizations can apply to educate their employees regarding cyber security awareness, for example online training via ISACA (Meadows, 2016). However, one size does not fit all and there is a need for the ability to make changes without damaging the integrity of the training (McCoy & Fowler, 2004). Additionally, many trainings are perceived as intimidating, non-inviting, or time-consuming (Patten, 2015). These perceptions might affect the employees' motivation, the retention of the offered knowledge or skills, and thus the overall effectiveness of the cyber security awareness training.

One training technique that promises the desired flexibility and encouragement is the application of gamification. There are several examples in recent literature where competitive environments successfully stimulated and encouraged participants to improve their cyber security awareness (Gavas, Memon, & Britton, 2012). Such environments are a safe way to offer participants a chance to practice under pressure. These gamified environments can include digital elements, but they can also be developed as a tabletop game e.g. a card or a board game (Gondree, Peterson, & Denning, 2013).

### 1.1.2 Knowledge Gap

First, cyber security awareness is an emerging topic and recently, it has received an increased amount of attention from media and research. A fundamental question that arises is what contributes to cyber security awareness. Whereas studies exist that provide a definition of cyber security awareness, a clear overview of the constituents or influences of cyber security awareness on a deeper level is lacking.

Secondly, gamification is a promising technique to increase the motivation and engagement of a training's participants. Moreover, some research concluded that participants preferred gamification over other cyber security awareness training methods (Baxter, Holderness Jr, & Wood, 2015). However, no research has been conducted on the combinatory field of applying gamification to cyber security awareness training contexts. Many gamification elements can be applied to trainings, but it is not clear from literature which elements may be useful in cyber security awareness trainings.

Thirdly, there are few guidelines that developers can adopt when aiming to incorporate gamification in existing trainings. There are a handful of models and frameworks that address gamification as a process, but none of them target cyber security awareness. Therefore, one might be left to wonder how to tackle the challenges of applying gamification in cyber security awareness trainings. One of the underlying knowledge gaps is how gamification can be systematically applied to cyber security awareness trainings.

### 1.1.3 Problem Statement

The identified knowledge gap that will be bridged in this research regards what constitutes and influences cyber security awareness and how one can apply gamification in cyber security awareness trainings. Bridging this knowledge gap aims to address the lack of effective and systematical approaches for gamifying cyber security awareness trainings. The problem statement is: *there is no systematic approach for effectively applying gamification to cyber security awareness trainings.*

### 1.1.4 Scope

Cyber security awareness trainings can be found in education and in organizational contexts. This thesis will focus on cyber security awareness trainings in the context of organizations. Every employee faces cyber security threats, e.g. via email, but employees who are adequately educated on these risks might be more aware. It might be presumed that technical employees are better informed on risks regarding cyber security. Therefore, this project will focus on cyber security awareness programs that require no prior knowledge and are targeted to non-technical employees. Regarding the leading design paradigm gamification, it will be regarded in a wide sense due to the preliminary research in the field of cyber security awareness and gamification. In other words, anything on the spectrum from adding game elements to serious games will be regarded. The discussed systematic approach for applying gamification to cyber security awareness trainings is aimed to guide training developers who possess basic knowledge or experience with cyber security and gamification.

### 1.1.5 Research Questions

This subsection introduces the main research question of this project. Next, sub-questions are posed. These sub-questions relate to the main research question, the knowledge gap, and the problem statement as identified previously.

The main research question of this research project is:

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

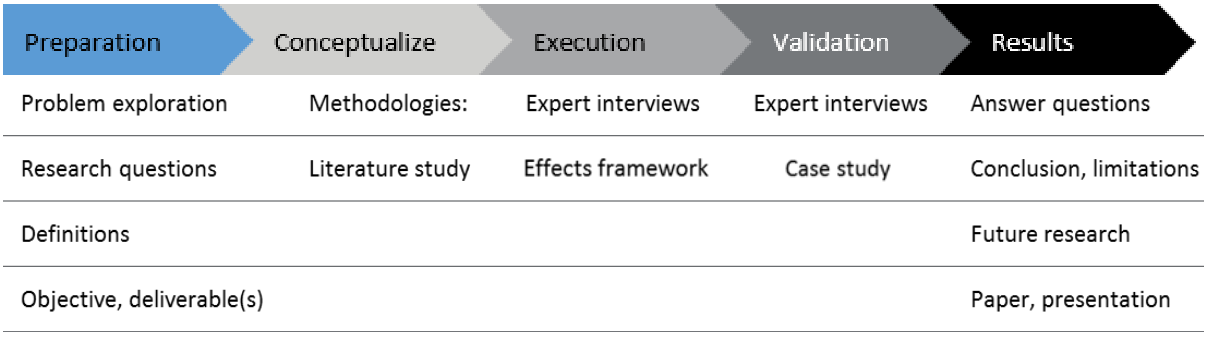
After formulating this question, several sub questions were formulated. These questions are related and relevant for solving the underlying research problem:

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 cyber security awareness trainings?
4. What is the perceived effectiveness of an application of the designed framework?

## 1.2 Research Approach

First, the concepts of cyber security awareness and gamification will be elaborated. Secondly, a systemic approach will be developed to gamify cyber security awareness trainings. The deliverables are: a model that illustrates what constitutes and influences cyber security awareness, an overview of gamification elements applicable to cyber security awareness, a framework for gamifying cyber security awareness programs, and an illustration of the theoretical framework in a practical setting. The last deliverable illustrates the usability of the framework.

For this purpose, the research activities per phase are as follows:



| Preparation | Conceptualize | Execution | Validation | Results |
|---|---|---|---|---|
| Problem exploration | Methodologies: | Expert interviews | Expert interviews | Answer questions |
| Research questions | Literature study | Effects framework | Case study | Conclusion, limitations |
| Definitions | | | | Future research |
| Objective, deliverable(s) | | | | Paper, presentation |

*Figure 1 Visualization of research activities*

### 1.2.1 Research Methods

In this section, the research methods are discussed. These methods are specified per sub-question of this project.

*What constitutes and influences cyber security awareness?*

Answering this theory-oriented sub-question will involve addressing the definition of cyber security awareness that will be used in the remainder of the research project. This delineation will be based on a literature survey into existing definitions of cyber security awareness. Additionally, current practices in cyber security awareness training and education will be identified. The derived insights will be used for designing a framework for gamifying cyber security awareness trainings.

*What gamification concepts are applicable to cyber security awareness trainings?*

This question will be answered by first providing the definition of gamification (elements) that will be used in the remainder of the project. Next, which of these different elements can be applied to cyber security awareness will be analyzed. For this purpose, state-of-the-art literature need to be reviewed by performing desk research.

*What framework can be designed to gamify cyber security awareness trainings?*
Answering this sub-question will be three-fold. First, theory will be regarded that consists of frameworks and models that discuss the process of applying gamification. Secondly, combining the results with previous insights from literature on cyber security awareness and gamification will result in the framework design. Thirdly, insights into the usability of the designed theoretical framework will be derived. This will be done by consulting experts in the field of gamification and cyber security awareness (trainings). After evaluating the framework with these experts, the framework will be adjusted according to their comments and suggestions.

*What is the perceived effectiveness of an application of the designed framework?*
First, an existing cyber security awareness training will be selected in order to develop a gamified training following the adjusted designed framework. This gamified training illustrates the usability of the designed framework. Next, an empirical case study will be performed in which both the existing training and the gamified training will be executed by participants who will be questioned before and after the training. In this way, the perceived effectiveness of the gamified training will be evaluated. In the end, it can be demonstrated to what extent the framework worked in this particular case.

## 1.3 Relevance

In this section, the scientific and societal relevance of this research project are explained. Finally, the last subsection addresses how this research project fits the CoSEM curriculum and the chosen track and specialization.

### 1.3.1 Scientific Relevance

By applying knowledge derived from gamification literature to the context of cyber security awareness, this research project improves and extends current understanding of the process of gamifying cyber security awareness trainings. Next, since many theories regarding gamification in the context of cyber security awareness have not been researched empirically, this research is scientifically relevant due to the illustration of a proposed combinatory approach.

### 1.3.2 Societal Relevance

Researching the application of gamification to cyber security awareness is societally relevant since the resulting deliverables of this research can aid organizations in effectively improving and maintaining an adequate level of cyber security awareness. In other words, this project emphasizes the importance of preventive cyber security measures like building awareness in order to minimize the organization’s vulnerability to attacks or other incidents. This implicit business need is also derived from talks with several experts from Deloitte. As a result, the added value of this research is to provide insight regarding the application of gamification to increase cyber security awareness. Ideally, this should lead to less successful attacks and incidents and therefore minimize the impact on organizations. Note that the results of this research might also be valuable to the public sector, for example regarding cyber security awareness programs of municipalities.

### 1.3.3 Fit with CoSEM Curriculum, Track and Specialization

The Complex Systems Engineering and Management master of the faculty of Technology, Policy and Management focusses on socio-technical systems. In the context of this project, both aspects, social and technical, are represented by employee awareness and cyber security respectively.

These aspects are intertwined and cannot be adequately addressed separately, thus increasing the complexity of this project. Additionally, the curriculum of CoSEM focusses on designing in such socio-technical contexts. Also in this project, a design is constructed: a framework for gamifying an existing cyber security awareness training environment.

During this master, the Information and Communication track was followed. This track is well represented during this project due to the focus on ICT and the human aspects that are related to it. For example, ICT aspects of cyber security should be regarded through analyzing behavior aspects in order to be well implemented. Lastly, also the Cyber Security specialization is well represented during this thesis. This specialization provided the necessary perspectives regarding both technical and social aspects of cyber security. For one, in order to keep up with technological innovations in the domain of cyber security, human behavior and mindset have to adapt regularly.

## 1.4 Structure

The remainder of this thesis is structured as follows: Section 2 addresses key concepts of this thesis in order to grasp the remainder of this project. In Section 3, the research methodology will be addressed. Section 4 until section 7 elaborate on the sub-questions of this research. Next, Section 8 will provide conclusions of this project, followed by a discussion of the implications, limitations and future research in Section 9. Finally, Section 10 will provide a reflection on this thesis project.

# 2. Key Concepts

This section regards the results of a literature study of sources that address key terminology to be used in the remainder of this project.

## 2.1 Cyber Security and Awareness

In this section the terms cyber security and related cyber security awareness are discussed.

### 2.1.1 Cyber Security

In order to grasp the concept of cyber security awareness, first the concept of cyber security needs to be clarified. Existing literature embraces various definitions of cyber security. Some authors describe it 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). This underlying triad of people, processes and technologies is also addressed by other authors as 'prime to success' of any system that aims to add value (Ramakrishnan & Testani, 2011). In the context of cyber security, 'success implies effective cyber-secure operations that guarantee pre-set system objectives' (Ani et al., 2016). The next subsection continues on discussing this triad in the context of cyber security awareness.

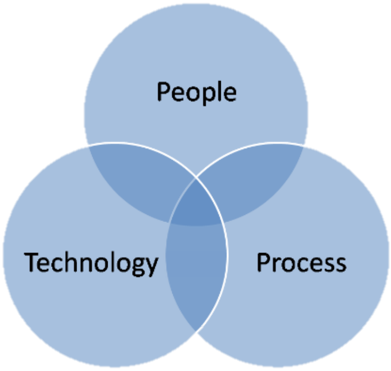


*Figure 2 People, process, technology triad*

In addition to the definition of cyber security as illustrated previously, other authors define cyber security as '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 highlights the fact that a compromise might be accidental, for example due to a lack of cyber security awareness of users of such systems. This emphasis is important to keep in mind for the remainder of this thesis.

Clarifying the term cyber security, a previous literature review showed that many literary sources use 'information security' analogous to 'cyber security' or vice versa (Rieff, 2017). However, these terms do not quite represent the same phenomenon (Safa, Von Solms, & Furnell, 2016). For one, cyber security also regards ethical considerations related to human victims or attackers and the protection of other assets besides information resources (Von Solms & Van Niekerk, 2013). On the other hand, information security also includes non-ICT related aspects of security next to availability, integrity, and confidentiality. In other words, the concepts of information security and cyber security do overlap, so called ICT Security (Von Solms & Van Niekerk, 2013), but also regard additional matters. The relation between the discussed security concepts is visualized in Figure 3.

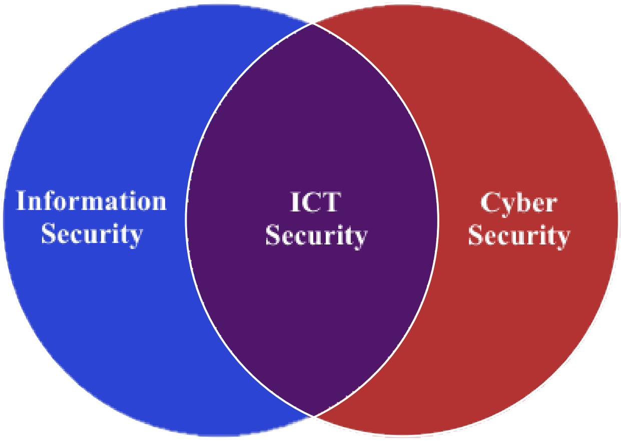


*Figure 3 Illustrating security concepts*

In the remainder of this project, the terminology of cyber security will be used. This means that, as illustrated in the previous figure, sources that regard the concept of information security while addressing ICT-related aspects of security will also be used for this research. This terminology, the ICT side of information security together with cyber security, forms the best match with this research project due to the expressed focus on awareness whilst regarding ICT threats like phishing. The next subsection will continue on the concept of awareness.

### 2.1.2 Cyber Security Awareness

As illustrated in Figure 2 of the people, process, and technology triad; cyber security issues are often technology enabled issues instead of purely technical. However, most of existing solutions regarding cyber security focus primarily on technology strategies without regarding the people and process aspects (Howarth, 2014). However, users typically interact with technologies to manage processes (Ani et al., 2016). This thesis will focus on the people aspect of the triad in order to address the topic of cyber security awareness. This people aspect typically involves 'characterizing issues of communications, knowledge, skillsets, behavior, and relationships that define the human elements of an industrial critical infrastructure' (Ani et al., 2016). In this perspective, cyber security awareness regards 'thoughtfulness on security, enabling individuals (workforce – employees and managers) to recognize security concerns and respond accordingly' (Ani et al., 2016).

There exist several other explanations of the phenomenon currently addressed as cyber security awareness. For example, Jiemei et al. mention that cyber security (situation) awareness 'aims to provide the cyberspace's global security views and states for administrators' (Jiemei et al., 2014). While this definition regards the people aspect by mentioning administrators, its scope might be too narrow. Also Franke & Brynielsson explain cyber security awareness from a situational awareness perspective by stating that cyber security awareness is a subset of situational awareness that concerns a cyber context (Franke & Brynielsson, 2014). Even though there is little consensus on the meaning of situational awareness, it can be defined as 'all knowledge that is accessible and can be integrated into a coherent picture, when required, to assess and cope with a situation' (Sarter & Woods, 2009). Kokkonen adds to this situational awareness perspective by regarding it as 'the volume of time and space gathering information and elaborating understanding of what is happening and prediction of what will happen in the near future' (Kokkonen, 2016). This definition emphasizes both the view on the current situation and what might be ahead. In comparison with this definition, other authors include actual cyber security aspects in their definition of cyber security awareness. An example is when defining cyber security awareness as 'assessing the level of vulnerabilities in an entity, while providing participants with general knowledge in detecting and avoiding successful penetration attempts' (Adams & Makramalla, 2015).. Other definitions of awareness often do incorporate the behavioral aspects related to cyber security. An examples of such a definition of awareness 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). Franke & Brynielsson also regard these behavior aspects, but mention them more as a result of cyber security awareness by stating that awareness is primarily 'a mental state that can be reached to a varying degree' (Franke & Brynielsson, 2014).

In a way, Parsons et al. combine previous definitions that regard the knowledge or mental state of users and their resulting behavior by stating that information security awareness 'should consider both the extent to which an organization's employees understand the importance and implications of information security, and the extent to which they behave in accordance with the organization's information security policies and procedures' (Parsons et al., 2017). The next subsection continues on the need and importance of cyber security awareness.

### 2.1.3 Why Cyber Security Awareness?

One of the objectives of increasing cyber security awareness is minimizing cyber risk. In this sense, cyber risk can be understood as 'an adversary who tries to abuse one or more corporate information assets which will have direct or indirect consequences for the organization' (Buith, 2016). Many organizations try to reduce this risk by investing heavily in technological developments for their cyber security. However, some authors believe that 'there is no static technical defensive measure that can mitigate the threat introduced by user behavior' (Dodge, Carver, & Ferguson, 2007). Also Kassicieh et al. state that while an organization might have the best automated controls in place, there will always be flaws and, in the end, it depends on an employee to spot these flaws and to act accordingly' (Kassicieh et al., 2015). In other words, despite the fact that many organizations continue to invest remarkable amounts of money in technological developments for their cyber security, they should also recognize that the technical outcomes 'need the endorsement of the workforce' (Ani et al., 2016).

Besides the technological innovations that can aid the cyber security of organizations, the human aspect of cyber security, awareness and the related behavior, should not be overlooked (Safa et al., 2016). For example, as early as 1993, Wood and Banks stated that companies should better prioritize human error as a major threat to information security. They mentioned that companies should pay sufficient and continuous attention to this aspect in order to mitigate and prevent problems to their security (Wood & Banks, 1993). Some authors add to this by stating that without improving or even regarding the cyber security awareness of their employees, organizations might be unable to acquire adequate cyber security (Ani et al., 2016). Also Navarro illustrates this need for cyber security awareness and the misconception of many organizations by stating that the workforce is an organization's key cyber security asset; not their security technologies, laws or regulations (Navarro, 2007). More specifically, Anderson states that 'the flexibility of the human mind and its ability to spot oddities' is an invaluable asset' (Anderson, 2013).

Other authors emphasize the importance of awareness by stating that it might help employees in avoiding 'avoid situations that may be harmful' (Underhay, Pretorius, & Ojo, 2016). Some authors even believe that building awareness and making sure that people adopt adequate practices regarding cyber security  is 'one of the best ways of combating cybercrime' (Alotaibi, Furnell, Stengel, & Papadaki, 2016). Also Evangelopoulou & Johnson state that inadequate awareness is a significant factor of failing cyber security performance (Evangelopoulou & Johnson, 2015).

*Figure 4 The weakest link (adopted from https://infotrust.com.au)*

Up until today, computer or security related mistakes of employees are still considered 'one of the top threats to IT security in organizations' (Whitman & Mattord, 2011). More specifically, it is the 'naïve and accidental' behavior of employees that is the key cause of an organization's cyber security issues (Schultz, 2005). In other words, the human factor might be the weakest link of an organization's cyber security (Aloul, 2012; Ani et al., 2016; Arachchilage & Love, 2014; Khidzir et al., 2016; Schneier, 2015). Adversaries know this and by targeting this vulnerability they hope to break into the organization via unaware or uneducated employees (Khattak, Manan, & Sulaiman, 2011). Ani et al. also endorse the importance of addressing this people aspect by stating that employees are the 'most targeted vectors for malicious cyber actors' (Ani et al., 2016). As a result, most of information security breaches can be traced back to the human error (Parsons et al., 2017; Wheeler, 2017).

Paradoxically, cyber security awareness is often still an overlooked aspect of security programs and little is done to build awareness in organizations (Aloul, 2012). In the remainder of this thesis, a promising technique called gamification will be addressed that could aid this process of building cyber security awareness among employees.

## 2.2 Gamification

In this subsection, the concept of gamification is elaborated. First, key definitions are introduced. Next, the reason behind addressing gamification during this thesis is discussed. Finally, how gamification is related to the previously addressed topic of cyber security awareness is addressed.

### 2.2.1 Definition

Gamification is a phenomenon that started growing interest since around 2010 (Zichermann & Cunningham, 2011). Due to this relative infancy, research regarding this concept is still quite preliminary. Additionally, several definitions exist regarding gamification.

An often cited definition of gamification is: 'the application of game design principles in non-gaming contexts.' (Robson et al., 2015, p. 1; Werbach & Hunter, 2012). This definition can be concretized when elaborating on these design principles. For example some authors explain gamification comprises '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). An example of gamification is Ribbon Hero, in which users of Microsoft Office learn how to use the ribbon interface in a gameful way (Marczewski, 2013).

The concept of gamification can be clarified when extending previous definitions by incorporating the purpose of the intervention. An example of such a definition is provided by Alberts and Findlay, who state that gamification is 'the integration of the mechanics that make games fun and absorbing into non-game platforms and experiences in order to improve engagement and participation' (Alberts & Findlay, 2011). Also Robson, Plangger, Kietzmann, McCarthy and Pitt include a purpose of using gamification in their definition of gamification by adding 'in order to change behaviors' (Robson, Plangger, Kietzmann, McCarthy, & Pitt, 2016).

Some authors describe gamification more as an intentional process whilst describing the purpose of the intervention. For example, Huotari and Hamari define gamification as: 'a process of enhancing a service with (motivational) affordance in order to invoke gameful experiences and further behavioral outcomes'. (Huotari & Hamari, 2012, p. 19). Also Ruboczki describes gamification as a process, but this author involves the human mind in his definition by stating that 'gamification is a psychological process, utilizing public recognition and online competition to generate interest' (Ruboczki, 2015).

Finally, there are authors that highlight the social-technical context of gamification whilst describing its purpose. For example, Deterding describes gamification as: 'a transformative socio-technical systems design practice for motivational affordances in the service of human flourishing' (Deterding, 2014). This emphasis on the social-technical nature of the intervention and the focus on designing fits perfectly with a thesis project for the Complex Systems Engineering and Management master. The next subsection illustrates what makes gamification a promising subject for this thesis.

### 2.2.2 Why Gamification?

As McGonigal stated 'games have the potential to impact in our daily lives if they are used to tackle real world problems' (McGonigal, 2011). For example, in the medical field gamification contributed to sustainable engagement, improved motivation and improved knowledge acquisition of participants (Pesare, Roselli, Corriero, & Rossano, 2016). Fu adds to this by stating that both recruiting and retaining participants can be improved due to the effects of gamification (Fu, 2011). Other authors, for example Ruboczki, agree on the statements that gamification could aid in keeping participants focused and motivated, but adds that it is most successful if the gamified environment appeals to the social- or game passions of participants (Ruboczki, 2015). Finally, some authors illustrate the benefits of gamification by explaining its added value for teams, for example by stating that gamification can 'improve teamwork and transform routine tasks by motivating employees through "play" and competition within the same team and across teams (Korolov, 2012; Zichermann & Cunningham, 2011).

Due to the perceived benefits of gamification as introduced previously, gamification is often applied in a context of learning or education. In this context, gamification can also be deployed in order to affect behavior (Underhay et al., 2016). Of course, there are several training or education methods that aim to achieve similar purposes, but some authors state that in order to influence behavior, ongoing engagement is important and gamification is its vital enabler (Iacovides, Jennett, Cornish-Trestrail, & Cox, 2013; Szantner, 2015). Next to sustainable engagement, some authors state that when comparing gamification to other training methods, gamification is best in actively involving participants (Ruboczki, 2015; Zichermann & Linder, 2013). Finally, gamification is promised to greatly improve the motivation of participants to aim higher and to achieve better results when compared to other methods, especially when established in a collaborative environment (Burke, 2016).

Note that it might be naïve to think about the application of gamification as a silver bullet solution. In other words: 'just because gamification is trendy does not mean that it always works or is the best strategy' (Robson et al., 2016). For example, Alberts and Findlay believe that gamification is only a viable option to influence behavior if there are motivation issues (Alberts & Findlay, 2011). Also De-Marcos, Garcia-Cabot, and Garcia-Lopez state the potential of gamification when a lack of motivation is a recurrent issue (De-Marcos, Garcia-Cabot, & Garcia-Lopez, 2017). On the other hand, other authors state that gamification in general could be 'harmful towards the general objective of the project' (Thiel, 2016a) and that participants might perhaps 'question the seriousness or importance of the project (Thiel, 2016b). As a result, one might presume that gamification is no one-size-fits-all approach and that there are several challenges to its application. Examples of potential hurdles are when achievements and rewards are not perceived as equivalent, when there are unintended consequences, when intrinsic values are getting undermined or when the gamified environment interferes with (social) norms (Alberts & Findlay, 2011). In the next subsection, the previously discussed concepts of gamification and cyber security awareness will be related.

### 2.2.3 Relating Gamification to Cyber Security Awareness

Research into the combinatory field of gamification and cyber security awareness is both preliminary and developing (Alotaibi et al., 2016). However, many of the addressed promises of gamification as a training method can be translated to the field of cyber security awareness. For one, research shows several games regarding cyber security awareness that were successful in motivating, engaging and assessing and acquiring knowledge (Amorim, Hendrix, Andler, & Gustavsson, 2013; Fouché & Mangle, 2015). More specifically, some authors show that gamification proves to be a successful method in reducing the overall number of successful attacks that aim to exploit human vulnerabilities (Adams & Makramalla, 2015). As a matter of fact, until now, even the 'majority of the studies proved to be effective in creating awareness among the users' (Alotaibi et al., 2016). Some practical examples of the application of gamification in an cyber security awareness context are CyberCIEGE, CyberProtect, and CyberSense (Raman, Lal, & Achuthan, 2014).

On the other hand, some authors mention specific challenges that arise for the application of gamification to the field of cyber security awareness. For example, Margalit states that applying gamification to cyber security awareness calls for a clear understanding of what specific cyber security related knowledge is required (Margalit, 2016). Next, it is often unclear how this knowledge should be conveyed with the gamified environment (Margalit, 2016) or how to actually implement gamification in cyber security awareness trainings (Robson et al., 2015). Nevertheless, Alotaibi et al. state that using gamification for building cyber security awareness is positively received (Alotaibi et al., 2016). However, when regarding literature, it seems difficult to assess the effectiveness of gamification as applied to cyber security awareness even though it is assumed to be positive (Margalit, 2016). A starting point could be to perform comparative studies to address the effects of non-gamified and gamified environments on cyber security awareness. The next section addresses the research methodologies as applied in this thesis.

# 3. Research Methodology

In this section, the research methodologies that will be applied in this thesis are elaborated. The following subsections address literature study, design-science, interviews, and case study as applied methodologies.

## 3.1 Literature Study

Section 2 addressed the concepts of cyber security awareness and gamification and was written after performing a literature study into scientific literature that regarded either gamification or cyber security awareness or both. First, the topics cyber security and cyber security awareness were analyzed in order to identify previous key research in these fields and to compare and contrast the corresponding findings. Next, the topic of gamification and the combination of cyber security awareness and gamification were studied by performing a literature study. This combinatory field forms the perspective for the remainder of this thesis.

During the extensive literature studies, several literary sources are accessed; IEEE Digital Library, ACM Digital Library, Emerald, Scopus, ScienceDirect, Springer, Google Scholar, and Research Gate. Researching these sources for academic literature that addresses gamification and cyber security awareness leads to the following literary types: books, conference papers, white papers, articles, theses, reports, journals, working papers, and dissertations. Despite the variety in types of information, the academic body of knowledge that adequately regards both gamification and cyber security awareness appears to be rather small. For this reason, no types of literature are prematurely excluded, for example conference papers and theses are initially taken into consideration regarding the several literature studies of this thesis. The same holds for the year of publication, which is often perceived as a measure for excluding literature from literature studies. However, since the scientific body of information regarding gamification and cyber security awareness is quite small, the year of publication is not a reason for exclusion per se. In this sense, the more recent publications are preferred over older ones, but older publications are not necessarily disregarded. For example, when older publications address a particular phenomenon regarding gamification or cyber security awareness and more recent publications that adequately address this phenomenon are missing, the older publications are still taken into consideration regarding the literature studies. Note that while both gamification and cyber security awareness are rather new topics of research, the vast majority of the consulted literature is still under ten years old and all of the referred literature stems from the period 1979-2017.

Literature study is an important methodology of this thesis. Several searches are performed in the literary sources as addressed in previous paragraph. The first searches are performed to establish the sections that regard the key concepts of gamification and cyber security awareness. Key words like gamification and cyber security awareness are obvious search terms that are used. Next to these, also key words like games (with a purpose), (situational) awareness, and information security (awareness) are used. Several combinations with these key words are attempted to acquire the necessary and appropriate literature for performing the literature studies towards answering the research questions.

When regarding the first two research questions, additional and more specific literature studies are performed. For example, the first question regards cyber security awareness and trainings that address this concept. As a result the searches also include terms like learning, teaching, education, and training next to the keywords as addressed in the previous paragraph. During these searches with several combinations of the illustrated key words, the same rules apply regarding year of publication and information type. The reason for this is when the scope of the research question is decreased, the fewer literary sources are available towards answering this question.

The second question regards gamification and cyber security awareness trainings. In this sense, this question builds upon the knowledge and insight gained from answering the first research question. However, this question shifts the focus towards gamification. Hence, it is necessary to consult additional literature that addresses gamification in the context of cyber security awareness towards answering this question. The process and exclusion rules as addressed earlier is also applied during the literature study for the second research question. To extend the amount of relevant literature which could contribute towards answering this and future research questions, references from previously addressed works are also consulted. For example, answering the third and fourth research question might also require additional theoretical foundation regarding the framework and its usability.

In the end, the literature studies provide the necessary information regarding gamification and cyber security awareness for designing a framework for gamifying cyber security awareness trainings. As such, literature study is regarded as an appropriate methodology in order to provide the theoretical backbone for this framework.

## 3.2 Design-science

This methodology is regarded when designing the framework for applying gamification to existing cyber security awareness trainings. In this sense, by applying this methodology, an answer to the latter part of the third research question concerning a framework can be formulated based on the insights and answers to the previous research questions. Information systems research is useful to regard for answering this question due to its focus on both technology and behavior. One part of this methodology regards behavioral science, which focusses on the 'development and justification of theories that explain or predict phenomena related to the identified business need' (Hevner, March, Park, & Ram, 2004). In this case, this relates to cyber security awareness and gamification and the associated behavioral aspects. The other part of this methodology consists of design-science, which is described as 'the building and evaluation of artifacts designed to meet the identified business need' (Hevner et al., 2004). In particular, the framework design from research question three aligns with the building aspect of design-science. As such, design-science will be applied in order to develop a framework for gamifying cyber security awareness trainings. Finally, especially the evaluation aspect of the design-science methodology is used to provide an answer to the question concerning the usability of the designed framework. In sum, combining behavior science with design-science provides a suitable methodology to create and evaluate the framework for gamifying cyber security awareness trainings.

## 3.3 Expert Interviews

This methodology is applied in a semi-structured fashion for answering parts of the third research question of this thesis, i.e. regarding the design and the evaluation of the framework. For this purpose, several gamification and cyber security awareness experts of Deloitte are consulted. With the derived insights from these interviews, the preliminary framework from research question three is improved. These interviews limit the potential risks from designing a framework that is primarily based on theoretical knowledge. For example, a risk is that this framework might not actually resemble current trends and practices. Therefore, after the interviews with experts from the field, the framework will be adjusted based on their comments in order to be usable in practice.

## 3.4 Experimental Case Study

During the experimental case study, the cyber security awareness training is gamified by following the adjusted framework. First, an existing cyber security awareness training is selected. Both the objectives of the training and the actual content are regarded. Next, these characteristics of the training provide a foundation towards a gamified version of this training. This gamified version of the cyber security awareness training is constructed following the designed framework. In this sense, first-hand experiences from using the designed framework towards applying gamification are derived. Next, by applying the framework to a cyber security awareness training, an empirical foundation is provided regarding the usability of the framework. This application results in a gamified cyber security awareness training.

## 3.5 Questionnaire

Using questionnaires in this research facilitates a combinatory study; a group of people participates in the existing cyber security awareness training, and a group of people participates in the gamified training. The homogeneity of both of these groups is carefully considered. For example demographics like age and gender, but also role within the organization are regarded. Before and after executing the trainings a round of questions is asked. As such, two questionnaires are filled in by the participants of the gamified and the non-gamified (existing) cyber security awareness trainings. The questions consider several user experience aspects and constructs of cyber security awareness as derived from answering the first research question. Participants are asked to estimate the effects of the training on their personal environment and their individual awareness. The perceived effects of the training are scored and the results of the non-gamified training are compared to the results of the gamified training. A null hypothesis is used for each metric in order to quantitatively evaluate whether the gamification produces significantly higher results in terms of the predefined metrics. Additionally, the comments of the participants of the non-gamified training are compared with the comments of the participants of the gamified training. In this sense, the questionnaires prove the perceived effectiveness of the gamified cyber security awareness training which stems from the application of the framework.

# 4. Cyber Security Awareness Constituents and Influences

Following the key concepts section, literature addresses a triad consisting of people, process, and technology when regarding cyber security. This triad illustrates that issues regarding cyber security can often be traced back to several aspects, instead of just technical aspects. Next, the literature study shows that many cyber security issues are the result of accidental behavior, instead of intentional behavior. More specifically, most issues regarding cyber security can be traced back to the human error. As such, literature often addresses the human factor as the weakest link of an organization's cyber security. This illustrates the importance of cyber security awareness of users of IT systems. In other words, regarding the triad, if the awareness of users and their resulting behavior is inadequate, technologies and processes might be harmed as a result. This is in line with the literature study that illustrated several authors who believe that cyber security awareness is one of the greatest contributors to cyber security. In turn, it is vital for organizations that concern cyber security risks mitigation strategies to focus on cyber security awareness of their employees (Safa et al., 2016). However, when regarding literature, one quickly finds out that the scientific body that considers what actually constitutes and influences cyber security awareness is quite small (Alotaibi et al., 2016). Besides, the discussed definitions of cyber security awareness provide little guidance regarding fostering desired behavior from a cyber security perspective. Therefore, in the remainder of this thesis, cyber security awareness will be regarded as a combination of previous definitions. For one, awareness will be addressed as a state-of-mind of an employee; a characteristic that can be present in various degrees. Next, awareness will be addressed as something dynamic; something that can be influenced by providing knowledge, guidelines or otherwise. In other words, awareness is regarded both internally as externally; an ability that can be influenced and which can affect the environment of its 'owner' due to his or her practices and behavior. This section continues on characteristics of cyber security awareness by answering the following sub-question: what constitutes and influences cyber security awareness? First, characteristics that describe cyber security awareness are addressed. Additionally, there are several methods that organization can apply to constitute and influence cyber security awareness. These are addressed in the second subsection.

## 4.1 Constructs of Cyber Security Awareness

There are several examples in literature and sources like news that illustrate when the level of cyber security awareness of employees was inadequate; take the numerous reports of data leaks or organizations that got hacked due to some kind of human error (Oever, 2015; Voorst, 2016). Authors believe that such incidents happen because the tremendous growth in developments regarding cyber security while awareness 'has not kept pace' (Alotaibi et al., 2016). In order to assess the level of cyber security awareness, specific characteristics are needed to describe what constitutes cyber security awareness. Besides, such characteristics can be used to compare cyber security awareness in different contexts, for example after an intervention has taken place. Such characteristics that constitute and influence cyber security awareness will be described as constructs for the remainder of this thesis.

Several authors started the discussion regarding what constitutes or influences cyber security awareness by noting that 'awareness is a random variable that is very difficult to characterize due to user's individual nature' (Dodge et al., 2007). Unfortunately, research often stops at this point or describes the process of influencing awareness, e.g. via certain training methods. However, some statements from literature can still be used to distill what constitutes cyber security awareness. For example, some authors write about the demand for 'a more effective and skilled cyber workforce' (Ani et al., 2016). One can presume that in order for employees to be described as effective and skilled in the field of cyber security, they should possess some level of cyber security awareness. In other words, skills are a construct that could be used to describe cyber security awareness. Next to skills, capabilities are also mentioned in literature as a construct of cyber security awareness (Ani et al., 2016; Navarro, 2007). Johnson describes capability as the 'product of knowledge, skills, and tools' (Johnson, 2015). Despite the fact that it remains rather vague what is meant with tools, this definition of capability does provide further direction towards the constructs of cyber security awareness. Also Ani et al. focus on knowledge and skills rather than tools since tools 'describe capability on a generic context' (Ani et al., 2016).

Next to cyber security skills and capabilities, some statements from literature can be turned around to illustrate additional cyber security awareness constructs. For example, when inadequate cyber security awareness is explained by employees who do not sign off when leaving their office, one can presume that signing off when leaving the office is illustrating some level of cyber security awareness. Other inverted examples are when passwords are inaccessible to others, when on-screen information is not visible to those who should not see it, or when someone backs up their data regularly (Thomson & von Solms, 1998). Next, refraining from 'browsing unsafe websites, downloading suspicious software, sharing passwords among peers and using unprotected wireless networks' illustrates when someone possesses a certain level of cyber security awareness (Liang & Xue, 2010). Finally, some authors describe 'reading security concerns, verifying content, practicing safe shopping, using common sense, using email filters, updating software, logging off, and taking caution when using Bluetooth and Wi-Fi networks' as facets of cyber security awareness (Underhay et al., 2016). When analyzing the examples from this paragraph on a higher level, the common denominator seems to be behavior. This construct is important since inadequate behavior could result in cascading effects; unauthorized access could lead to stolen confidential information which in turn could lead to more cyber security incidents or cybercrime (Khidzir et al., 2016).

Next to cyber security awareness constructs that can be associated with behavior, skills or capabilities, some authors also mention relations between knowledge and cyber security awareness (Galba, Solic, & Lukic, 2015). Note that previous characteristics regarding behavior, knowledge, skills or capabilities are related, but they are not analogous. For example, while an employee possess certain knowledge or skills, this does not imply that he or she behaves accordingly. Some authors state that the awareness of employees who possess good knowledge regarding cyber security is often very limited (Alotaibi et al., 2016). Additional authors recognize this and aim to address how to influence the behavior construct. For example, Thomson & Von Solms state that large inducements could result in behavior changes, but believe that these changes might not be permanent (Thomson & von Solms, 1998). They state that changes in behavior due to attitude changes are more likely to be lasting behavior changes (Thomson & von Solms, 1998). Establishing long-lasting cyber security awareness and associated behavior remains complicated. Some authors address this by emphasizing the trade-off between security and getting-the-job-done (Calic, Pattinson, Parsons, Butavicius, & McCormac, 2016). For example, employees could value convenience over cyber security when downloading emailed files that could potentially make their daily tasks easier (Parsons et al., 2017). In other words, in order to establish lasting cyber security aware behavior, it is important for employees to be able to carry out their daily tasks in a secure way. Some authors emphasize that in order for this cyber security aware behavior to become permanent, the behavior should have the potential to evolve to subconscious behavior (Thomson & von Solms, 1998). That is to say, employees should behave adequately without having to remember or to think about how they should behave cyber security aware. In other words, attitude is an important construct regarding cyber security awareness in order to affect cyber security aware behavior. Attitude can in general be described as a feeling or opinion about something (Cambridge_Dictionary, 2018). It is 'a state of readiness that will impact an individual's response to any situation' (Moore & Asay, 2017). As such, someone's attitude can have a significant impact on how someone judges the world around him or her. For example, how someone judges the importance of cyber security awareness or to what extent someone feels affiliated with the concept.

Cyber security awareness is regarded in this thesis as both internally and externally; something an employee can possess in various degrees, which can be influenced, and something that can have an effect on (the context of) the employee. The previously distilled constructs of cyber security awareness; knowledge, skills, capabilities, attitude and behavior, are in line with this perspective. These constructs can be complemented and related when regarding the information security awareness model of Parsons et al. as displayed on the right side (Parsons et al., 2017). This model illustrates that individual, intervention, and organizational factors can affect the information security awareness of employees. In this model, information security awareness consists of knowledge, attitude and behavior (Parsons et al., 2017).

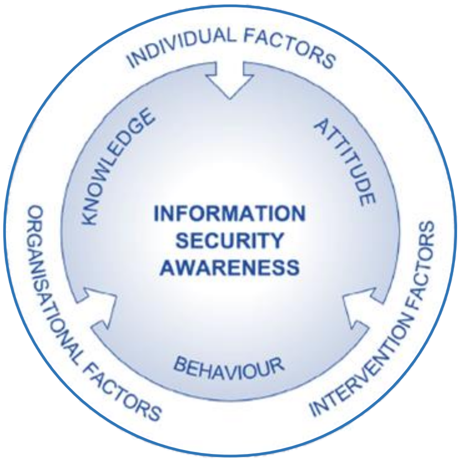


*Figure 5 Information Security Awareness Model (Parsons et al., 2017)*

Another model is regarded that also incorporates several of previously distilled constructs. This model can be seen in Figure 6. Despite the fact that this model is focused on performance criteria in general, thus not being tailored to the context of cyber security awareness, it might provide an interesting basis when combining it with previous insights.

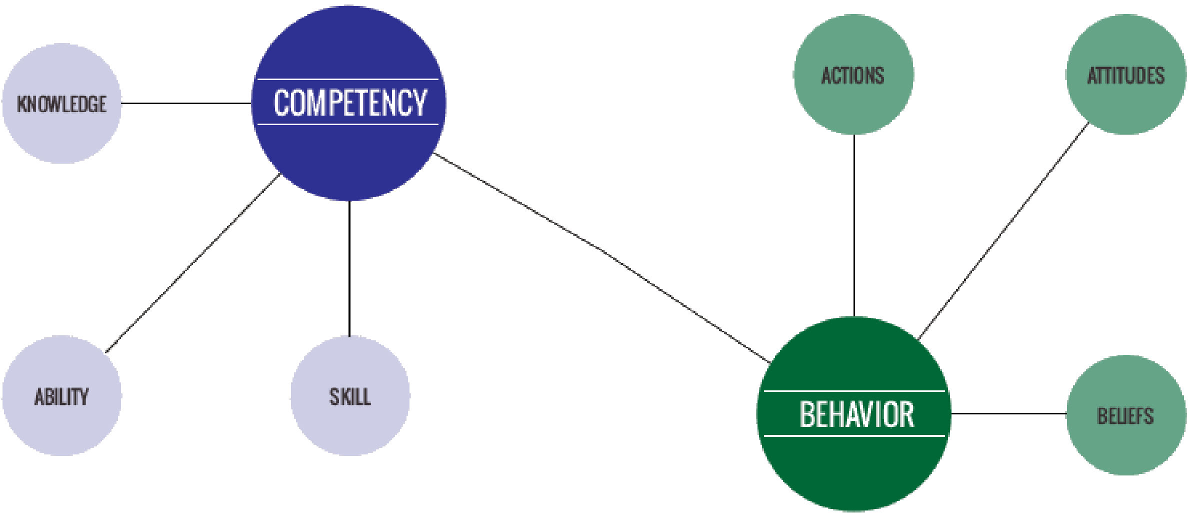


*Figure 6 Performance Model (Blaga, 2014)*

The constructs as distilled from literature; knowledge, skills, capabilities, attitude and behavior, will be combined with the two models as displayed previously to provide a visual illustration of how this thesis addresses the constructs of cyber security awareness and how these constitute and influence cyber security awareness. In the model in Figure 8, it can be seen that capability, as described in cyber security awareness literature, replaces the competency aspect from the model in Figure 6. In the created model in Figure 8, capability encompasses the previously discussed constructs knowledge and skills. The ability aspect from the model in Figure 6, is implicitly present in the capability construct in Figure 8.

The construct behavior is influenced by attitude, as discussed earlier. One may presume that actions, as illustrated in the model in Figure 6, are also applicable to cyber security awareness. Therefore, this construct is also included in the cyber security awareness constructs model. Note that capability and behavior both influence cyber security awareness, but not each other in this model. Also the beliefs element of the model in Figure 6 was not included in this model. The reason for previous design choices is the fact that there was no literature that stated that capability and behavior affect one other in a cyber security awareness context, nor that beliefs play a role in this context. Finally, the yellow hexagon illustrates the contextual factors that are at play in different situations and that could affect various constructs of cyber security awareness. Following Parsons et al., these factors come in the categories individual, organizational and intervention (Parsons et al., 2017). Since further research might provide insight into additional factors, the umbrella term 'contextual factors' is used in this model. For the remainder of this thesis, the focus will be primarily on intervention factors, since training methods to impact cyber security awareness will be regarded.

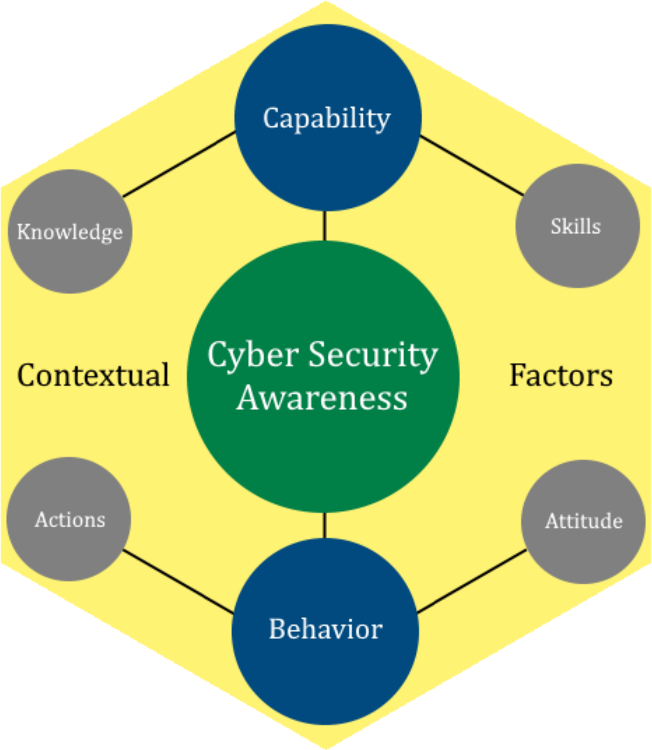


*Figure 7 Cyber Security Awareness Constructs Model*

In the designed model, it can be seen that there are two constructs that influence capability, and two constructs that influence behavior. The capability and behavior construct then influence cyber security awareness. In other words, in order to affect cyber security awareness, the four primary constructs – knowledge, skills, actions, and attitude – can be addressed. Within these constructs, one might presume that a variety of aspects can contribute to each specific construct. For example, each employee might possess different levels of knowledge regarding different topics that relate to cyber security awareness. Regarding cyber security awareness topics, following the National Institute of Standards and Technology (NIST) there are several topics that can be addressed in any cyber security awareness context in order to raise awareness. These topics are illustrated in Table 1 (M. Wilson & Hash, 2003).

*Table 1 Cyber Security Awareness Topics (M. Wilson & Hash, 2003)*

| Cyber Security Awareness Topics |
|---|
| Password usage and management – including creation, frequency of changes, and protection |
| Protection from viruses, worms, Trojan horses, and other malicious code – scanning, updating definitions |
| Policy – implications of noncompliance |
| Unknown e-mail/attachments |
| Web usage – allowed versus prohibited; monitoring of user activity |
| Spam |
| Data backup and storage – centralized or decentralized approach |
| Social engineering |
| Incident response – contact whom? "What do I do?" |
| Shoulder surfing |
| Changes in system environment – increases in risks to systems and data (e.g., water, fire, dust or dirt, physical access) |
| Inventory and property transfer – identify responsible organization and user responsibilities (e.g., media sanitization) |
| Personal use and gain issues – systems at work and home |
| Handheld device security issues – address both physical and wireless security issues |
| Use of encryption and the transmission of sensitive/confidential information over the Internet – address agency policy, procedures, and technical contact for assistance |
| Laptop security while on travel – address both physical and information security issues |
| Personally owned systems and software at work – state whether allowed or not (e.g., copyrights) |
| Timely application of system patches – part of configuration management |
| Software license restriction issues – address when copies are allowed and not allowed |
| Supported/allowed software on organization systems – part of configuration management |
| Access control issues – address least privilege and separation of duties |
| Individual accountability – explain what this means in the organization |
| Use of acknowledgement statements – passwords, access to systems and data, personal use and gain |
| Visitor control and physical access to spaces – discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity |
| Desktop security – discuss use of screensavers, restricting visitors' view of information on screen (preventing/limiting "shoulder surfing"), battery backup devices, allowed access to systems |
| Protect information subject to confidentiality concerns – in systems, archived, on backup media, in hardcopy form, and until destroyed |
| E-mail list etiquette – attached files and other rules. |

In the reviewed literature regarding cyber security awareness, themes like confidentiality, information security, and privacy are addressed most often. This is also reflected in the list of cyber security awareness topics as addressed in Table 1. Therefore, these themes and topics will be the primary focus of the remainder of this thesis. Note that different organizations might have a different focus and different priorities regarding what themes and topics are most important for their cyber security posture and their cyber security awareness program. Therefore, existing trainings for Deloitte employees regarding cyber security awareness will be analyzed later in this thesis and based on these trainings, a selection on these topics is made for the gamified training.

## 4.2 Methods to Raise Cyber Security Awareness

After discussing the constructs of cyber security awareness, it is interesting to analyze what methods can be adopted to influence these constructs and raise awareness of employees. For the remainder of this thesis, methods that aim to constitute or raise awareness among employees will be described as cyber security awareness training (methods). This is in line with the definition of Kassicieh et al. who describe such training as 'the use of dedicated sessions to increase knowledge of and compliance with cyber security policies' (Kassicieh et al., 2015). In such sessions, employees study principles and practices related to cyber security (awareness) (Kassicieh et al., 2015). Next to this definition that regards cyber security awareness policies, principles and practices, additional definitions exist. For example, Toth and Klein describe cyber security awareness training as a method to inform employees of 'acceptable use of and risk to the organization's organizations systems' (Toth & Klein, 2013). These authors address training as a way for employees to acquire knowledge, skills, and competencies regarding cyber security awareness (Toth & Klein, 2013). This aligns with the constructs of cyber security awareness as addressed previously.

It is important for organizations to provide cyber security awareness training to their employees in order to effectively deal with cyber security threats (Alotaibi et al., 2016; Anderson, 2013; Cone, Irvine, Thompson, & Nguyen, 2007; Drevin, Kruger, & Steyn, 2007). Such trainings are believed to be a 'crucial response to a growing number of intrusions and attacks' (Nagarajan, Allbeck, Sood, & Janssen, 2012). In fact, some authors state that such trainings are 'one of the most important aspects of an organization's security posture' (Dodge et al., 2007). Next to this increase in the number of attacks, new cyber threats arise constantly. For this reason, some authors believe that 'training should be done regularly, e.g. twice a year' (Aloul, 2012). Due to the nature of current trainings, employees often consider them as boring (Kassicieh et al., 2015). Next, trainings are often (perceived as) 'compliance for compliance's sake' which contributes to the resentment of employees who feel that cyber security is undervalued by the organization (Kassicieh et al., 2015). In other words, instead of providing training for compliance's sake, it is important to provide training from a holistic perspective (Anderson, 2013).

Raising awareness among employees proves easier said than done. A reason might be that raising awareness in fact faces two challenges: making employees notice and identify their level of knowledge, skills and behavior, and secondly encouraging them to improve these levels (Kassicieh et al., 2015). However, it remains hard to keep employees aware and it seems even more difficult to change the attitude of employees towards implementing best practices (Kassicieh et al., 2015). In other words, it is hard to keep up adequate cyber security awareness and related behavior among employees. A reason for this is that adequate cyber security awareness practices and behavior are often perceived by employees as less convenient than continue to behave in their usual less secure way (Manke & Winkler, 2012). Next, training cyber security awareness takes time, which could also be used for other projects. As a result, employees may perceive training negatively (Manke & Winkler, 2012). To counter this, cyber security awareness trainings should be 'tailored to be as specific as possible to the social group to which an individual employee belongs'(Kassicieh et al., 2015). Paradoxically, these trainings should also account for various backgrounds and experiences regarding cyber security awareness (Kassicieh et al., 2015). In other words, it is important to customize the cyber security awareness trainings (Underhay et al., 2016; Yap, 2011). Next to specifying the trainings, it is vital that employees get actively engaged in order for the trainings to be effective (Alotaibi et al., 2016; Anderson, 2013; Manke & Winkler, 2012). A promising way to achieve this is to consider various learning styles that participants might have and incorporate them into the training (Näckros, 2002; Underhay et al., 2016). Next, concrete examples of risks and experiences from the real world should be provided during these cyber security awareness trainings in order to achieve a more hands-on-experience (Kassicieh et al., 2015).

Keeping previous challenges and recommendations in mind, there are several ways to execute cyber security awareness trainings. However, next to regulations like CERT and disseminating information, specific approaches to raise security awareness are often missing (Alotaibi et al., 2016). Next, when cyber security awareness approaches are reserved to annual presentations, it limits the efficacy of the program (Kassicieh et al., 2015). Thus, without specific approaches, it is unlikely that employees apply the taught material to their daily tasks (Aloul, 2012). Deloitte offers tailored (online) training courses, learnings, webinars, videos and simulations to improve the cyber security awareness of employees and clients  (Deloitte, 2018b). These and other training methods each have their advantages and drawbacks. Personal training, for example, is the oldest most common way of training. Despite its familiarity, its effectiveness 'depends on the size of participants, the mood, and authentic of the tutor, the relationship between the presenter and listener' (Ruboczki, 2015). Next, this classroom style training method is often criticized due to unachieved learning objectives or lack in focus on problem solving skills (Raman et al., 2014). Finally, it is a costly way to train cyber security awareness for example due to travel and location costs. Another training method often applied to cyber security awareness is e-learning. Advantages of this method are that it is more cost effective than personal training and it is easier to organize; employees do not have to be at the same place at the same time. However, adequate feedback is often missing and tutors have fewer tools to motivate participants (Ruboczki, 2015). Online trainings are another method in which cyber security awareness can be trained. The advantage of such trainings is that it can facilitate huge amounts of participants and it can be made openly accessible. However, online cyber security awareness trainings can call for stable internet connections and specific hard- and software. Next, interactions between tutor and participants (or between participants) is often limited (Ruboczki, 2015). Finally, such passive computer- or web-based trainings often fail to challenge and engage participants and provide little dialogue for elaboration (Cone et al., 2007).

The technique that can be adopted in various of the discussed training methods to counter several of the addressed drawbacks these methods, for example when regarding attention, motivation, feedback and time investment is gamification (Kassicieh et al., 2015). Some general reasons for using gamification were introduced in section 2. This paragraph compares previous traditional methods to training methods that incorporate gamification. In this regard, some authors describe gamification as 'enjoyable, long-term, impulsive and motivating' (Ruboczki, 2015). Next, gamification shows to improve participants' performance in practical assignments and to encourage social interactions (De-Marcos et al., 2017). Such interactions are beneficial, for employees are more likely to comply with adequate cyber security aware behavior if they know that others are doing it (Kassicieh et al., 2015). Besides, it proves that  'peer pressure is more effective than financial incentives or increased information' (Kassicieh et al., 2015). In other words, the strategy of many organizations to increasing the amount of cyber security awareness information that employees are exposed to, will not be effective in raising their cyber security awareness. Next, when comparing gamified trainings to traditional trainings, the environment of gamification allows participants to practice their knowledge, skills, and behavior in a 'more realistic, stressful environment, which is key in being able to apply the theoretical knowledge' (Underhay et al., 2016). Next, with gamification applied to a training method, participants can also educate themselves in cyber security awareness 'in private at their own pace, without fear of the stigma, judgement, or ridicule that classroom settings can engender' (Fouché & Mangle, 2015). In the end, several authors seem to believe that integrating traditional training methods with game methods can be equally or even more effective than traditional training methods alone (Cone et al., 2007; Kassicieh et al., 2015).

In addition to the promising advantages, gamification can incorporate various aspects that are regarded effective for learning. For example, storytelling, in which a narrative spikes interest and makes learning material more memorable due to its appeal to imagination (Kassicieh et al., 2015). Next, flipped learning can be incorporate in a gamified cyber security awareness training in which 'homework' is performed with the tutor while participants go through the cyber security awareness learning material in their own time (Kassicieh et al., 2015). Finally, there are social psychology techniques that can be applied to trainings to improve their effectiveness in changing behavior (Thomson & von Solms, 1998). These techniques are: directly changing behavior, changing behavior to influence attitude, changing attitude through persuasion (Thomson & von Solms, 1998). Directly changing behavior can be done for example through awarding small tokens to employees who behave cyber security aware. When other employees notice this behavior or the small rewards it could act as a motivation (Thomson & von Solms, 1998). Changing behavior to influence employees' attitude could be done through self-persuasion, for example when participants themselves provide reasons for changing their behavior towards cyber security aware behavior. Finally, changing attitude through persuasion is for example when employees are subject to forced exposure of necessary cyber security awareness information. Following Thomson & von Solms, this is the preferred technique (Thomson & von Solms, 1998). However, comprehension, acceptance and retention are necessary in order for this technique to be effective in changing behavior (Thomson & von Solms, 1998). Comprehension considers the medium to transmit cyber security awareness information. The rule here is: complex information should be provided in print, while less complex information can be provided verbally (Thomson & von Solms, 1998). Acceptance regards i.a. the expertise of the tutor (Thomson & von Solms, 1998). In other words, when the tutor is an expert in the field of cyber security awareness, chances of acceptance of the employees regarding the provide information are highest. Finally, retention regards repetition in order to increase the chances of memorability (Thomson & von Solms, 1998). This illustrates again that raising cyber security awareness requires more than a one-shot approach.

Some authors provided further recommendations for tackling cyber security awareness, or the human element of cyber security. For example, Kassicieh et al. recommend a two-pronged approach consisting of trainings and messages. This can be seen in the orange rimmed parts of Figure 9. In other words, providing awareness messages next to training would have a greater impact on raising cyber security awareness among employees than providing training alone (Kassicieh et al., 2015). For this effect, it is necessary that the messages are concise, up-to-date and relevant, for example regarding recent trends (Kassicieh et al., 2015). Another benefit of incorporating such varying awareness messages is the fact that employees can acquire more knowledge than in infrequent short trainings alone (Kassicieh et al., 2015). Next, these messages need little time investment from employees when compared to cyber security awareness trainings. This is beneficial, since 'too much information at one time can prevent people from processing or using that information' (Kassicieh et al., 2015).

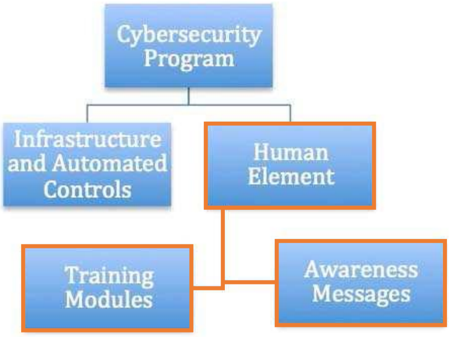


*Figure 9 Improving the Human Element of Cyber Security (Kassicieh et al., 2015)*

For the remainder of this thesis, previous insight will be combined. In other words, aspects from gamification, training, and messages will be used in conjunction.

This section provides insight in the constituents and influences of cyber security awareness. The analyzed literature and models show a few shortcomings for the purpose of answering the research question; what constitutes and influences cyber security awareness. For example the models have a generic focus i.e. they are not specified to cyber security awareness. Next, clear relationships or causality between the different aspects are lacking. The developed model derived insights from these existing models in order to illustrate the constructs of cyber security awareness and their interrelations. This model consists inter alia of the key distinguished constructs capability and behavior. Behavior and capability regarding cyber security awareness is influenced by actions, attitude, knowledge, and skills. Besides the model, an overview is provided regarding cyber security awareness topics in order to raise cyber security awareness via training. Finally, advantages and drawbacks of training types are addressed. This illustrates that gamification is a promising technique to incorporate in trainings in order to counter some of the drawbacks and to be more effective in raising cyber security awareness. The next section will address several gamification concepts that can be used for the purpose of raising cyber security awareness among employees.

# 5. Gamification Concepts for Cyber Security Awareness

During the key concepts section, literature proved that research regarding gamification is still in its infancy. Multiple definitions of the phenomenon were addressed in this previous section. Analyzing these different gamification definitions provides an initial impression regarding the process, design principles, purposes of an intervention, and the human mind. Next, the definitions also highlight gamification and its social-technical context, which fits the Complex Systems Engineering and Management master program. In this thesis, gamification will be addressed as a collection of a variety of components as addressed by definitions provided in literature. As such, using game techniques is regarded in a wide perspective. This means that not only contexts in which an entirely new experience is created will be regarded, also called serious games, but also contexts in which game elements are added to existing contexts (Deterding et al., 2011). In Table 2 the components as derived from the studied literature are visualized in the newly created categories attribute, action, and purpose. Attribute describes the more static properties of gamification. Next, action describes the more dynamic characteristics of gamification; gamification as a verb. Finally, purpose illustrates the potential intentions underlying the gamification intervention.

*Table 2 Components of gamification*

| Attribute | Action | Purpose |
|---|---|---|
| Game design principles | Integration of game mechanics | Improve engagement |
| Non-game context | Process of enhancing | Change behavior |
| Social-technical | Psychological process | Generate interest |
| Mechanics, rewards | Design practice | Improve participation |

Due to the promising benefits of gamification as discussed in the key concepts section, many training or education methods are replaced by gamification or turned into a hybrid form that incorporates elements from both gamification and traditional training methods. Regarding this thesis, one might presume that tackling cyber security issues that can be traced back to human awareness and related behavior might also benefit from gamification. The fact that there is a variety of benefits regarding the application of gamification highlights exactly why there is a need for more research in gamification, its integration in existing training methods and the resulting effects of this application. Regarding this thesis, research in the combined field of gamification and cyber security awareness should be continued in order to provide further guidelines and to extend and strengthen the scientific body regarding the topic.

This section continues on addressing the sub-question: what gamification concepts are applicable to cyber security awareness trainings? As such, various gamification concepts are analyzed and addressed whether they might be applicable to cyber security awareness and cyber security awareness training. First, the focus is on gamification and its applications for the purpose of training. Next, the applicability of gamification on cyber security awareness and related trainings is addressed.

## 5.1 Common Gamification Concepts for Training Purposes

In section 2, gamification was inter alia described as 'a transformative socio-technical systems design practice for motivational affordances in the service of human flourishing' (Deterding, 2014). The most common application of gamification is training (De-Marcos et al., 2017). Within the field of training, one of the most gamified learning environments regards topics associated with computer science (Mohamad, Salam, & Bakar, 2017). Despite the popularity of gamification for educational purposes, there is little evidence yet about its effectiveness (Raman et al., 2014). Yet, it is believed that gamification can improve performance, productivity, and user engagement (Mohamad et al., 2017). What is paramount for the design of effective gamified trainings is that the appropriate gamification concepts should be selected (Kapp, 2012). However, well-established frameworks regarding gamification are scarce (Hamari, Koivisto, & Sarsa, 2014). One of these frameworks is the Octalysis framework from Chou, as can be seen in Figure 10 (Chou, 2015). This framework regards eight types of motivational drives that drive people to perform activities. It should be noted that different drives might drive different people in different ways. The bottom drives of the Octalysis are related to black hat gamification, whereas the top drives are related to white hat gamification (Chou, 2015). These gamification types relate to negative and positive motivations respectively. Next, drives on the left are referred to as left brain, and drives on the right are referred to as right brain (Chou, 2015). This means that the left side represents intellectual and logical drives, whereas the right side represents creative and social drives. In the end, in order for gamification to be successful, it is important that there is a balance between the drives from both types of gamification and between the drives from either side of the brain (Chou, 2015). Whereas this framework provides a properly structured overview of the different motivations that might drive employees during training, it is rather abstract which makes it difficult to distill actual gamification concepts to apply to trainings.

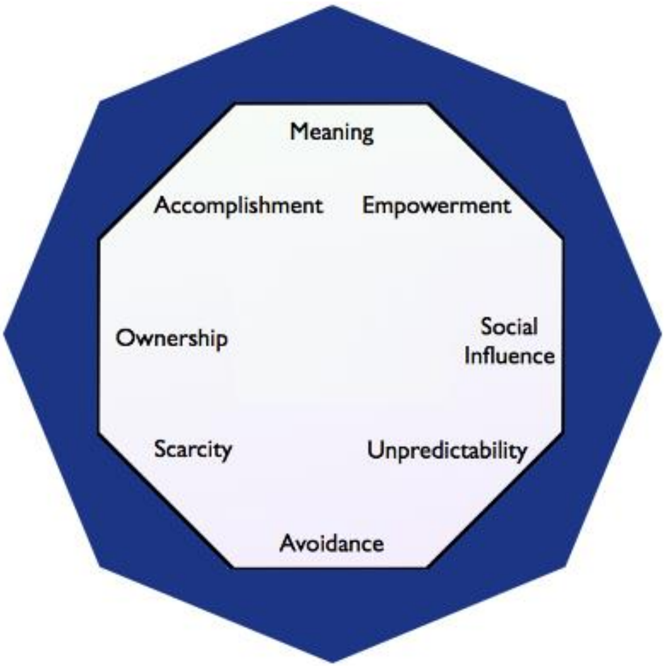


*Figure 10 Octalysis Framework (Chou, 2015)*

An additional framework that is one of the most prevalent frameworks of designing gamification is the MDA (mechanics, dynamics, aesthetics) framework (da Rocha Seixas, Gomes, & de Melo Filho, 2016; Zichermann & Cunningham, 2011). Here, mechanics are the functional components – the rules and levers – of the gamified environment. These represent the processes that stimulate the engagement of participants (Werbach & Hunter, 2015). Next, dynamics are the interactions that participants have with these game mechanics (da Rocha Seixas et al., 2016). These aspects require important considerations although they cannot be implemented directly into the gamified environment (Werbach & Hunter, 2015). Finally, aesthetics represent the experiences and how the participants feel during these interactions (Zichermann & Cunningham, 2011). Each of these three aspects of the MDA framework can be expanded into specific components (Werbach & Hunter, 2015); this is visualized in Table 3. Other authors supplemented these components after performing a study into applied game elements. For example, Mohamad et al. found additional applied components including; reports, progress, notifications, roles/character, quest/goal/mission, and avatars (Mohamad et al., 2017). These authors also addressed collaboration, which can supplement the competition component as addressed in Table 3. The components from Table 3 and the ones mentioned previously are more specific, design-wise, than aspects like narrative and feedback as introduced in previous subsection or aspects like accomplishment and unpredictability as illustrated in the Octalysis from Chou. However, such abstract aspects might be equally important for the effectiveness of the gamified training since these aspects can appeal to the motivation of participants (Ruboczki, 2015). Additional examples of such aspects are opportunities for collaborative problem solving and social elements like forum or chat (Ruboczki, 2015). Here, it should also be noted that gamification concepts could have different effects for different types of participants; some concepts might even discourage participants while being beneficial for others (Bowser et al., 2014; Mohamad et al., 2017; Prestopnik, Crowston, & Wang, 2017; Thiel & Lehner, 2015).

*Table 3 MDA Framework Components (Hamzah et al., 2015)*

| Mechanics | Dynamics | Aesthetics |
|---|---|---|
| Points | Rewards | Satisfaction |
| Levels | Status | Pleasure |
| Challenges | Achievement | Envy |
| Virtual Goods | Self-Expression | Respect |
| Leaderboards | Competition | Connection |
| Badges | Altruism | |
| Gifts and Charity | | |

Some aspects of the MDA framework receive criticism from researches in the field of gamification. One of these aspects is the one-directional relationship of the MDA framework between the designer of the gamified environment and the participant. Some authors like Robson et al. have adjusted the framework to fit their criticism. The framework of Robson et al. incorporates emotions instead of aesthetics to illustrate the user experience (Robson et al., 2015). These authors state that emotions are more appropriate when regarding gamification and that aesthetics are more relevant in an actual game context (Landsell & Hägglund, 2016). Next, Robson et al. emphasize that the relations between mechanics, dynamic and emotions are key towards successful gamification (Landsell & Hägglund, 2016). As can be seen in Figure 11, these relations that were missing in the MDA framework are actually incorporated in the MDE framework. Whereas this framework extends the MDA framework regarding the complexity of relations between various gamification concepts, it lacks guidelines regarding the actual design of a gamified environment such as those associated with the MDA framework. However, one might be able to rephrase the components from the aesthetics category of the MDA framework to fit the emotions category of the MDE framework.

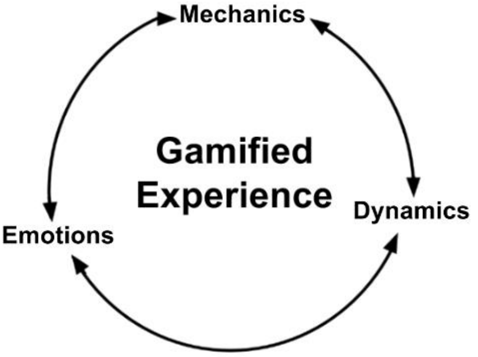


*Figure 11 MDE Framework (Robson et al., 2015).*

An additional framework that illustrates several gamification concepts is shown in Figure 12. This framework relates specific gamification concepts, including several concepts from previous frameworks, to specific player types. Here, six player types are addressed; free spirits, achievers, players, socializers, philanthropists, and disruptors. These player types are visualized in the bigger hexagon. In the smaller hexagon, the key motivation of each player type is shown; autonomy and self-expression, mastery, rewards, relatedness, purpose and meaning, and change

(Marczewski, 2015). Next, it is interesting to see that the squares at the edges of the hexagon resemble several of the game mechanics as illustrated in Table 3. Of course, deviations might exist, for example, employees might not perfectly fit a certain player type, but this framework provides a proper systematic overview towards designing a gamified training and what concepts to consider regarding player types. When designing a gamified training for employees, it is important not to restrict to a singular concept, like points, for using additional concepts can 'awaken creativity, leave room for errors, promote the exchange of experiences collaboratively and build learning situations in which they are free to make choices' (da Rocha Seixas et al., 2016). This is in line with previous notions of tailoring gamified environments to different player types and purposes of the environment while being aware of the fact that not all concepts might work for every participant.

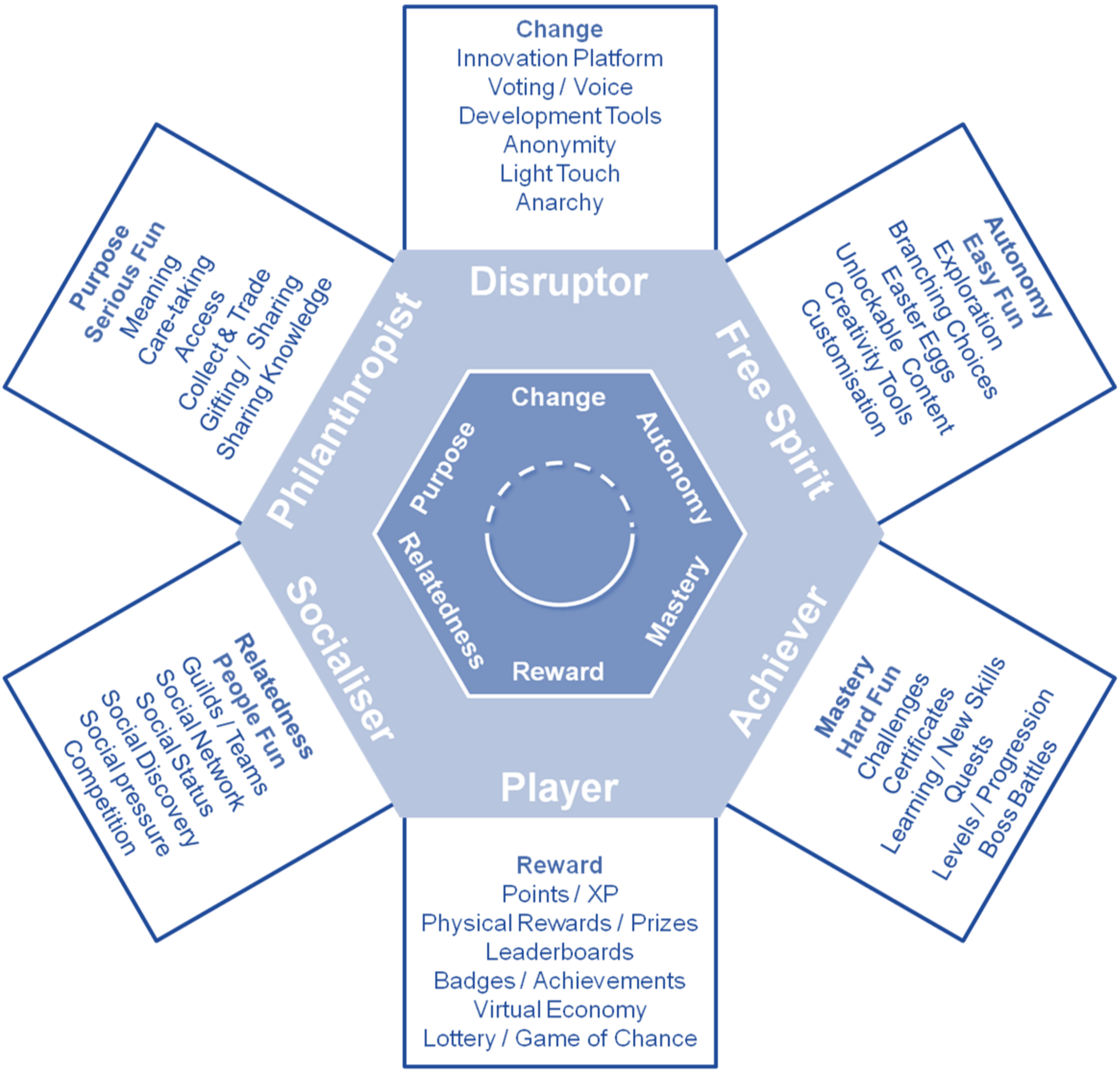


*Figure 12 Player Types and Gamification Framework (Marczewski, 2015)*

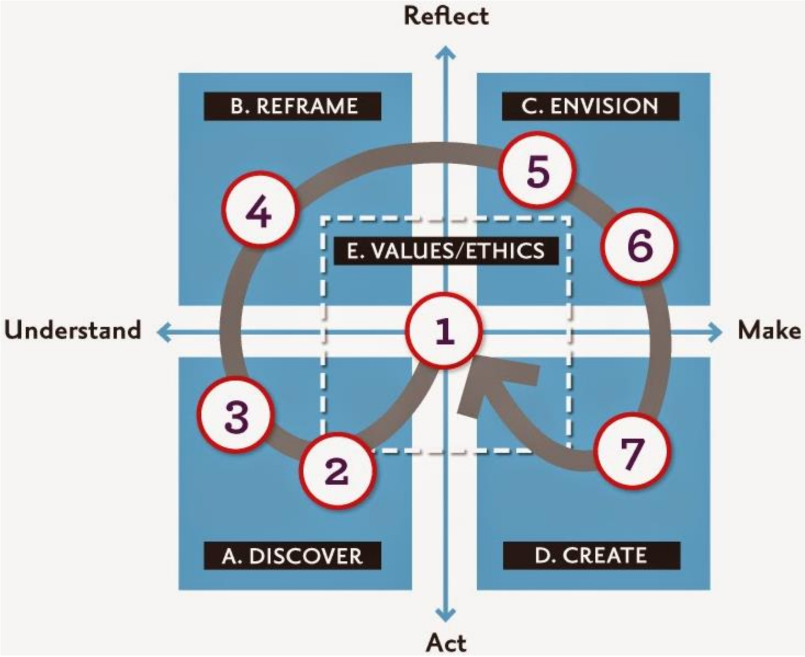


*Figure 13 Sustainable Gamification Design Model (Raftopoulos, 2014)*

When applying gamification concepts to training contexts, ethical questions might surface. For example, how ethically correct are the instruments that are in place to motivate employees? The following model is one of the few models that reflects such ethical aspects. The Sustainable Gamification Design (SGD) model is a human-centered model that takes into account value creation benefits and value destruction risks towards sustainable and responsible results (Landsell & Hägglund, 2016). The SGD model is shown in Figure 13. The model includes two axes – understand-make and act-reflect – and four quadrants – discover, reframe, envision, and create. These elements are based on research into widely applied and tested taxonomies and models (Raftopoulos, 2014). What stands out from the SGD model is the center part; values/ethics, which are often implied or neglected in other gamification frameworks (Landsell & Hägglund, 2016). Following Raftopoulos, values and ethics should be regarded in every phase of the development in order to achieve value creation benefits (Raftopoulos, 2014). The displayed model also visualizes this process towards sustainable gamification as suggested by Raftopoulos.

When analyzing previous frameworks, it is apparent that motivation is a dominant element of gamification, since it is present in every framework or model as addressed previously. Next to this dominant aspect, player types, values and ethics, and value creation are considered by various authors as key aspects of gamification. In the end, the discussed frameworks seem to overlap at some points and are complementary to each other at other points. One might suggest that in order for gamification to be properly applied in training environments, a combinatory framework should be designed that considers multiple of these gamification concepts as discussed previously. This overarching framework would fit the fact that there seems to be no one-size-fits-all approach towards gamifying training environments (Schöbel, Söllner, & Mishra, 2017). For example, the framework could incorporate the theory regarding player types by enabling tailoring the gamification of trainings to different player types. While doing this, it is important to acquire an adequate balance of story, play and aesthetics (Prestopnik et al., 2017). Next to tailoring gamified environments to different participant types, it might be needed to apply different approaches or strategies for different gamified trainings in order to be effective (Mohamad et al., 2017). For example, different game mechanics, dynamics or aesthetics can have a different impact on employees depending on the purpose of the gamified environment (da Rocha Seixas et al., 2016; Mohamad et al., 2017). The next subsection continues on gamification concepts and focusses on their applicability to environments regarding cyber security awareness.

## 5.2 Applicability to Cyber Security Awareness Contexts and Trainings

Cyber security awareness trainings are a specific field of trainings that could benefit from the application of gamification (Kassicieh et al., 2015). Today, more and more academic institutions and organizations are incorporating elements from game theory and behavioral theories towards raising cyber security awareness (Raman et al., 2014). Whereas traditional training methods are perceived negatively when participants are feeling challenged, games are often perceived positively when being challenging (Kassicieh et al., 2015). This illustrates a training potential of applying gamification to existing cyber security awareness trainings. As a result, the gamified environment could properly prepare employees towards actively noticing cyber security vulnerabilities and risks (Kassicieh et al., 2015).

For many trainings, and perhaps especially for cyber security awareness trainings, it is important that the gamified environment resembles a real life situation in order to 'provide a tangible connection between the training material and the real office environment' (Kassicieh et al., 2015). For this reason, one might presume that not every gamification concept as discussed previously is equally appropriate to apply to cyber security awareness trainings. Next to applying the right gamification concept it might be equally important to apply the right amount of gamification e.g. different mechanics. For example, too many (different) gamification mechanics might affect the transparency of the objectives of the cyber security awareness training and the participants their sense of purpose (Tinati, Luczak-Roesch, Simperl, & Hall, 2017).

Cyber security trainings, and in particular gamified ones, that adequately reflect real world situations are rare and underexplored (Kassicieh et al., 2015). Several authors researched the current situation regarding applications of gamification to cyber security awareness. A recent example is Alotaibi et al. who reviewed several major studies that regarded the incorporation of gamification in cyber security awareness contexts (Alotaibi et al., 2016). An overview of these studies is visualized in Table 4.

*Table 4 Overview of Studies into Gamification for Cyber Security Awareness (Alotaibi et al., 2016)*

| Authors | Gamification | Type | Methods | Results |
|---|---|---|---|---|
| Arachchilage N. A. G. and Love S., 2013 | Anti-Phishing Phil | Mobile gaming application: Training for links (URL) safety | Usability questionnaire | Improved learning and susceptibility of phishing |
| Arachchilage N. A. G. and Love S. 2014 | Anti-Phishing | Mobile gaming application: Training for links (URL) safety | Review | Improved learning |
| Ariyapperuma S. and Minhas A., 2005 | Next generation security - NGSEC | Web based gaming application | Review of tasks and performance | Significant improvements identified among users in performing security tasks |
| Dasgupta et al., 2013 | Control Alt Hack | Mobile Puzzle game | Assessment based on Puzzles | Effective in creating awareness |
| Denning et al, 2013 | - | Review | Survey of teachers | Effective game for model dissemination |

| | | | | |
|---|---|---|---|---|
| Geers K., 2010 | Baltic Cyber Shield - BCS | Training exercise with virtual attackers and defenders | Review | Recommendations for improving IT infrastructure |
| Gondree et al., 2013 | - | Mobile Board game | Multi-player assessment (group study) | Positive feedback, need for more evaluation |
| Irvine C. E. and Thompson M, 2003 | The Internet | - | Review | Positive impacts of games with recommendations |
| Kayali et al., 2014 | Internet Hero | Puzzle game | Experiment study | Improved awareness |
| Nyeste P. G. and Mayhorn C. B., 2010 | Anti-Phishing | Mobile gaming application: Training for links (URL) safety | RCT, pre & post experimental study | Improved learning and susceptibility of phishing |
| Pastor et al., 2010 | - | Multiple games | Review | Recommended developing and using more tools in games |
| Schweitzer D. and Brown W., 2009 | - | Visual presentation | Presentation (Education) case study | Positive experience of users in using interactive visualization |

When regarding Table 4, the recurrent theme of games that consider cyber security awareness is anti-phishing. This is in line with the fact that phishing is one of the most used target vectors and its possible devastating impact on organizations. It is interesting that several of the cyber security topics as illustrated in Table 1 can also be related to this anti-phishing theme, for example unknown e-mail/attachments, social engineering, and protect information subject to confidentiality concerns. It is apparent from Table 4 that most gamified cyber security awareness environments are provided digitally or include digital elements. This reflects the benefits of computer- and web-based training methods as discussed in subsection 4.2. Finally, when regarding the results as presented in Table 4 it can be presumed that applying gamification to cyber security awareness overall had a positive impact. Nevertheless, it remains unclear which specific gamification concepts were applied and how these relate to the discussed benefits or positive impacts. Next, when analyzing the studied examples it proves that most of the examples are actual games instead of applications of gamification to cyber security awareness. This distinction might affect the conclusions that can be drawn from analyzing this table. For example, the application of gamification to cyber security awareness trainings might have different results than games that concern cyber security awareness.

Whereas Table 4 provides a suitable overview for analyzing the current situation regarding games as applied to cyber security awareness, it could be supplemented by research that focuses on actual gamification concepts and which has an extended focus on training purposes. This was found in studies performed by Mohamad et al., as illustrated in Table 5. Analyzing this table, several of gamification concepts as addressed in section 5.1 can be seen. For example, the items from ‘gamification’ as presented in Table 5 relate closely to the game mechanics as addressed in section 5.1. It is interesting to note that some of these gamification mechanics are used way more frequently than others in a training context. For example, leaderboards, badges/medals, points, levels, and quest/goal/mission are used in (over) 50% of the analyzed studies. On the other hand, actions, roles, avatars, and awards, trading & gifting/rewards are only used once. The gamification mechanic called challenges is not present in any of the studies. Whereas this table provides suitable guidelines for applying gamification concepts like game mechanics to training purposes, it should be noted that not every study considered a cyber security awareness training context. This might affect assumptions regarding the applicability of the addressed gamification mechanics to this specific type of trainings.

*Table 5 Gamification Applied to Training (Mohamad et al., 2017)*

| Gamification | Bianchini et al., 2016 | Khaleel et al., 2016 | Measles & Abu-Dawood, 2015 | Morrison et al., 2014 | Stanculescu et al., 2016 | Werbach & Hunter, 2015 |
|---|---|---|---|---|---|---|
| Leaderboards | ✓ | ✓ | | | ✓ | |
| Badges/Medals | ✓ | ✓ | | ✓ | ✓ | ✓ |
| Points | ✓ | | | | ✓ | ✓ |
| Levels | ✓ | ✓ | | | ✓ | ✓ |
| Awards, Trading & Gifting/Rewards | | | ✓ | | | |
| Progress Bar/Status | | ✓ | | ✓ | | |
| Challenges | | | | | | |
| Actions | | | | | ✓ | |
| Roles | | | | | ✓ | |
| Feedback/Reports | | ✓ | | | ✓ | |
| Quest/Goal/Mission | ✓ | ✓ | ✓ | ✓ | | ✓ |
| Avatars | | | | | | ✓ |

There are additional authors that discuss benefits of applying specific gamification concepts to training contexts. For example, Daud, Sazilah, Siti, & Azizul stated six gamification concepts that 'can ensure learning engagement': redeemable points, check points, rewards, trophies/badges and memory games (Daud, Sazilah, Siti, & Azizul, 2016). These align with the most commonly applied gamification mechanics for training purposes as distilled from Table 5. Next, Yussoff discussed education and training and stated that the best gamification concepts for these purposes are peer grading, skills points, wally games, virtual goods, rewards, trophies and badges (Yusoff, 2016). Interesting elements are peer grading, wally games, and virtual goods for they are not mentioned earlier. However, virtual goods are present in Table 3 and peer grading might be a specific example of feedback; which is a gamification mechanic that is discussed previously. There are additional authors that mention virtual goods when regarding commonly applied gamification concepts, for example da Rocha Seixas et al. mention these together with points, levels, challenges, trophies, badges/medals, and ranking or score table (da Rocha Seixas et al., 2016). Interestingly, these authors state that challenges are commonly applied, but this gamification mechanic was not present in any of the studied cases by Mohamad et al. Next, besides the ranking or score table, all these gamification concepts were discussed previously. However, this ranking or score table might be related to leaderboards, which is a gamification mechanic that was addressed earlier. Finally, De-Marcos et al. discuss challenges, rewards and social game's mechanics as tools towards the engagement of participants and means to 'foster collaborative knowledge production' (De-Marcos et al., 2017). These mechanics were mentioned before, except the social mechanics. The lack of mentions of these social mechanics is interesting since, as illustrated in previous subsection, social game mechanics play an important role for several player types.

Several authors discuss the applicability of gamification to the context of cyber security awareness. However, research that addresses the applicability of specific gamification concepts to the context of cyber security awareness training is lacking. For example, research regarding gamification concepts like dynamics and aesthetics or emotions as applied to cyber security awareness training. Therefore, it is proposed to combine the discussed insights to provide reasonable assumptions for the applicability of gamification elements as applied to cyber security awareness trainings. As such, aspects of mechanics, dynamics, and aesthetics from the MDA framework overlap and can be complemented with aspects related to player types from the Player Types and Gamification Framework as discussed in section 5.1. Next, the gamification mechanics can be compared with Table 5 on gamification and training contexts. This illustrates that there are many more gamification mechanics that might be promising in training contexts, but these are currently unaddressed in research on gamification and training. Finally, despite the fact that Table 4 does not provide specific gamification mechanics regarding cyber security awareness, some examples can still be decomposed in such mechanics. For example, 'virtual attackers and defenders' might comprise different competitive gamification mechanics like roles. As such, the process regarding distilling gamification mechanics from the analyzed theory results in the items displayed in the second column of Table 6.

*Table 6 Categorized overview of Gamification Mechanics applicable to cyber security awareness trainings*

| Categories | Gamification Mechanics |
|---|---|
| **Cooperation/Competition** | Leaderboards |
| | Social |
| | Guilds |
| | Roles |
| | Avatars |
| | Virtual Goods |
| **Prizes** | 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 |

Previous research addresses various gamification mechanics, but it is refrains from addressing the suitability of these mechanics to cyber security awareness trainings. However, the analyzed theory illustrates that different types of gamification mechanics satisfy different needs for motivation. Next, different learning objectives might benefit from different types of gamification mechanics. It is presumed that such characteristics are no different for trainings tailored to the topic of cyber security awareness. As such, a categorized overview of gamification mechanics can be useful in order to establish and align the purpose of the cyber security awareness training, possible motivations to be stimulated, and the role of gamification in this regard. In turn, such categories can aid developers in the process of generating and selecting ideas for the cyber security awareness training. For these purposes, the synthesized gamification mechanics were categorized into: cooperation/competition, prizes, adventures, progression, and surprises. The category cooperation/competition is constructed based on the presence of gamification mechanics that trigger a form of rivalry or collaboration among participants. Prizes is a constructed as a separate category that contains gamification mechanics with winning or awarding characteristics. The category adventures is a category of gamification mechanics that possess characteristics of a journey or a (long-term) purpose that participants might live up to. Next, the progression category contains mechanics that can be used to illustrate change, increase, or improvement. Finally, the surprises category was constructed with gamification mechanics that possess characteristics related to uncertainty or chance. As such, Table 6 provides a clearer overview and a more practical tool for developers of gamified cyber security awareness trainings while aligning the attribute and purpose components of gamification from Table 2. Note that some gamification mechanics might belong to multiple categories; the table is a simplified visualization. For example, the gamification mechanic virtual goods can also fit the prizes category. Due to the emphasis on gamification mechanics, Table 6 regards the more practical or design oriented concepts of gamification; mechanics are the primary elements a designer can directly incorporate in a gamified environment. However, the more abstract concepts of gamification as addressed in the previous section, for example aesthetics and emotions, might be equally important. Therefore such concepts will also be considered next to the previously selected mechanics towards designing a framework for gamifying existing cyber security awareness trainings.

In the end, Table 6 illustrates newly categorized gamification mechanics that are applicable to cyber security awareness. Note that in the context of cyber security awareness trainings, restricting to one type of gamification mechanics is discouraged. This is in line with the fact that there might be several types of participants which could experience particular gamification mechanics differently. Finally, every cyber security awareness training context could benefit from a tailored approach regarding gamification mechanics. However, previous research illustrates that elements like leaderboards, badges/medals, points, levels, and quest/goal/mission are used most often. Therefore, it is proposed that careful incorporation of these mechanics in a cyber security awareness training could always yield promising results.

# 6. Gamifying Cyber Security Awareness Trainings

In this section, the following sub-question is answered: what framework can be designed to gamify cyber security awareness trainings? In order to answer this research question, the gamification concepts as addressed in section 5 are aligned with the derived insights regarding cyber security awareness and related training contexts from section 4. In the following subsection, important requirements to be kept in mind before and during the design of the framework are highlighted. Next, existing guidelines regarding the process of applying gamification are addressed. The combination of information is incorporated into a framework design in subsection 6.3. Finally, subsection 6.4 addresses the evaluation of the designed framework based on expert interviews.

## 6.1 Important Requirements; Extending Gamification and Cyber Security Awareness

Before gamifying cyber security awareness trainings, it is important to consider the dynamic needs of employees and the differences in lifestyle and cultural practices that might reside in the organization (Alotaibi et al., 2016). As a result, developing a framework towards gamifying cyber security awareness trainings might require a flexible approach for there might not be a silver bullet approach of gamification concepts that appeal to each employee type. Next, not every cyber security awareness topic might resonate well with every gamification concept. In other words, different gamification concepts might be more appropriate or effective in conveying particular cyber security awareness knowledge or behavior through trainings. For this reason, some authors mention building different gamified modules per cyber security awareness topics (Breuer & Bente, 2010). A framework that incorporates the option of developing such modules fits with flexibility requirements as addressed previously and requirements imposed by the cyber security awareness field. For example, it is necessary to provide continuous monitoring and updating of these modules in order for the gamified cyber security awareness training to reflect new and emerging threats. As a result, it might be easier to adapt a specific module of a cyber security awareness training than to adapt an entire training that is developed as one entity. Note that it is important to make sure that changes to specific modules will not compromise the integrity of the cyber security awareness training as a whole (McCoy & Fowler, 2004).

As discussed previously, it can be assumed that there are several important requirements regarding the flexibility of context and content of a cyber security awareness training. For example, some authors suggest that such content 'needs to be customized for different users' (Aloul, 2012). Also Thomson & von Solms stated that tailoring the content of trainings 'to address specific groupings of employees within the organization' will make them more effective (Thomson & von Solms, 1998). Regarding the grouping process of employees, it is important to carefully consider which employees belong to which group in order to make sure the training is relevant for them and that the provided examples or exercises resemble their personal working environment as closely as possible (Thomson & von Solms, 1998). In other words, a framework that could guide developers of a gamified cyber security awareness training into this grouping and tailoring process could be very helpful. Besides the actual content of a cyber security awareness training, it can be presumed from subsection 4.2 that the method of delivering this content needs to be carefully considered as well. For example, some authors state that this way of communicating needs to be tailored to the different types of participants (Aloul, 2012). An additional benefit of integrating flexibility in delivery methods is that more people might be reached by the provided cyber security awareness training (McCoy & Fowler, 2004). Finally, the gamified cyber security awareness training needs flexibility in order to reflect current or future security policies and demands that an organization selected to be satisfied (McCoy & Fowler, 2004; Underhay et al., 2016). In sum, a framework for gamifying cyber security awareness trainings might needs to incorporate various options for different content and different ways of transferring this content.

As mentioned in subsection 4.2, repetition plays a significant role in the memorability of knowledge and behavior. This means that, in order to affect cyber security awareness among employees, the retention of the provided cyber security awareness content can be improved by exposing employees to this content on a more regular basis. As a result, gamified cyber security trainings might be developed in such a way that each training takes fewer time than traditional trainings. This is in line with the fact that 'people tend to "tune out" if something does not grab their attention or if it is too long' (Thomson & von Solms, 1998). One way of accomplishing retention by repetition is thus to provide the gamified cyber security awareness trainings in a number of short sessions. This reduces the required consecutive time for employees, which makes taking part in such trainings more feasible and attractive for them. For one, employees will not be removed from other tasks for long periods of time and will not get truly behind with their workload (Thomson & von Solms, 1998). Next, shorter training sessions 'help to ensure the employee's full participation and attention' (Thomson & von Solms, 1998). It should be noted, however, that developing such a gamified cyber security awareness training which has a sufficient scope and depth in its contents on the one hand and which can be completed in under half an hour might be challenging (Kassicieh et al., 2015).

Next to requirements regarding the cyber security awareness content and the training context itself, gamifying existing cyber security awareness trainings calls for adequate 'instructional design learning objectives and engaging game design to encourage learners to practice and develop their skills' (Buchanan, Wolanczyk, & Zinghini, 2011). This engagement and encouragement are the 'primary mechanisms that enable motivational processes' to contribute to training (Hamzah, Ali, Saman, Yusoff, & Yacob, 2015). In the end, the motivation of participants of a cyber security awareness training is a vital factor towards the success of the training (Hamzah et al., 2015). In other words, while developing a framework for gamifying existing cyber security trainings, this motivation aspect needs to be carefully considered. This might be a challenging task, since different participants might be motivated by different needs or different kinds of game elements (De-Marcos et al., 2017). Fortunately, the MDA/MDE framework, Octalysis model, and the model of Marczewski from subsection 5 provided some insight into such motivations and how they relate to gamification and different player types. For the purpose of developing a framework for gamifying existing cyber security awareness trainings, extended insight into specific game elements and how these relate to particular motivations of participants could be useful. This insight could be derived from analyzing research from Hamzah et al. who studied an extension of the ARCS (attention, relevance, confidence, satisfaction) model of motivational design and its relation to gamification; the ARCS+G model. Additionally, the authors addressed the applicability of gamification and its relations with specific motivations to learning. A combinatory overview of their findings is presented in Table 7.

*Table 7 ARCS+G Model and Motivational Design (Hamzah et al., 2015)*

| Categories | Sub-categories | Strategies/tactics |
|---|---|---|
| **Attention** | Perceptual Arousal | - Use interesting image<br>- Use animation<br>- Maximize visibility |
| | Inquiry Arousal | - Create interactive e-learning applications<br>- The interface should be easy to navigate<br>- Balance aesthetics, usability and visibility |
| | Variability | - Put information first<br>- Use attractive interface<br>- Use up-to-date content |
| **Relevance** | Goal Orientation | - Conduct need assessment<br>- Determine the goal |
| | Motive Matching | - Look at the learners' point of view<br>- Make learners as a partner in the development process |
| | Familiarity | - Use subject matter experts<br>- Modify existing e-learning applications |
| **Confidence** | Learning Requirements | - Train learners to use e-learning applications<br>- Let learners know what is expected of them |
| | Success Opportunities | - Provide situations for learners to experience success with e-learning applications |
| | Personal Responsibility | - Create e-learning applications that enable learners to self-monitor |
| | Reward | - Learners can claim rewards by using the point |
| | Status | - Using levels to signify completion of intermediate goals in the e-learning |
| | Competition | - Using leaderboard to show the leading scorers of e-learning applications. |
| **Satisfaction** | Intrinsic reinforcement | - Provide feedback to show benefits of using e-learning applications |
| | Extrinsic Rewards | - Give incentives to improve performance |
| | Equity | - Standardize scoring measurements for learner tasks and accomplishments |
| | Achievement | - Using badges to reward learners as well as recognize their achievement and accomplishment |
| | Self-expression | - Using virtual goods such as clothing, weapons or jewelry |
| | Altruism | - Giving a gift to other learners will pull the learner into the e-learning, and then learners are motivated to send gifts to all learners |

Table 7 illustrates several gamification elements from several of the gamification concepts from subsection 5. Next, several of the sub-categories of the ARCS+G model resemble some of the dynamics from the MDA/MDE framework as illustrated in subsection 5. This model gives some additional insight regarding how to attract or engage participants for trainings in general, but the model is not targeted for cyber security awareness specifically. This might affect the conclusions that can be drawn from Table 7 towards developing a framework for gamifying cyber security awareness trainings. However, it might still be assumed that attention, relevance, confidence, and satisfaction are also important towards effective gamified cyber security awareness trainings. Thus, keeping these categories in mind whilst developing a framework for such trainings is well advised. Next, incorporating the proposed strategies/tactics in a cyber security awareness context might have different effects on particular motivations of participants or their engagement in general. Additionally, the research of Hamzah et al. focused particularly on e-learning contexts. This might also affect the conclusions that can be drawn from Table 7 or the effects of incorporating the mentioned strategies/tactics. However, regarding these uncertainties, Hamzah et al. emphasized that the model 'has a design that can be customized with a variety of learning conditions, and can be expanded according to the desired requirements' (Hamzah et al., 2015). In other words, it might still be assumed that applying the strategies/tactics from Table 7 in a cyber security awareness training context has positive effects on (the motivations of) participants. Therefore, these strategies/tactics will be taken into consideration for the development of a framework for gamifying cyber security awareness trainings. Finally, while Table 7 presents some game mechanics like badges and virtual goods, not all strategies/tactics can be directly translated into tangible guidelines to be used in a framework for gamifying cyber security awareness trainings. Note that such strategies/tactics might be equally important, therefore careful consideration of such elements is warranted.

*Table 8 Distilled requirements towards a framework for gamifying cyber security awareness trainings*

| Categories | Requirements |
|---|---|
| **Cyber security awareness** | 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 whether content is relevant 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 |

In conclusion, this subsection shed light on important requirements towards designing a framework for gamifying existing cyber security awareness trainings. These requirements regarded gamification, cyber security awareness and additional fields that deemed relevant towards this framework. The categories and associated requirements are visually illustrated in Table 8. 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. 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. In the next subsection, guidelines regarding the process of gamification will be addressed.

## 6.2 Existing Guidelines Regarding the Process of Applying Gamification

This subsection will extend the acquired knowledge and derived insights regarding gamification, inter alia from Table 8, by closer examining the act of applying gamification itself. This aligns with the action component of gamification, as illustrated earlier in Table 2. Key authors who studied this act of 'gamifying' are Werbach and Hunter. According to these authors, gamification is best designed following six steps (Werbach & Hunter, 2015). The six steps are illustrated below. The six steps are often referred to as the 6D framework, a mnemonic since each of the steps starts with a D.

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.

An interesting thing to note regarding this framework is the fact that game elements as addressed earlier will be regarded in the last step. Following Werbach and Hunter, the first five steps are required in order for the gamification to be effective in achieving what is intended with the gamified environment (Werbach & Hunter, 2015). The first five steps are the proposed way in order to derive which techniques would fit the particular environment and its purpose. Regarding the context of cyber security awareness trainings, the 6D model is presumed to be very useful. For example, for the effectiveness of such trainings – gamified or not – properly identified business objectives and target behaviors might be key indicators. Therefore, insights and models from subsection 4 regarding cyber security awareness and cyber security awareness trainings can be used during the first two steps of the 6D framework.

The third step from Werbach and Hunter regards players. This is in line with requirements as addressed earlier and the player type model from subsection 5. For example, tailoring gamified cyber security awareness trainings can be done by making different building blocks. In this way, different modules might be assembled for participants who belong to a particular player type. Participants might know their own player type, but there are also (online) tests available in order to distill what player type one belongs to.

The fourth step regards activity loops. Here, Werbach and Hunter address engagement and progression loops. These activity loops structure the core gameplay elements of a system. The engagement loop regards motivation, action, and feedback. An example is where a participant of a cyber security awareness training wants to achieve a particular objective. Next, this participant will act in a certain way to aim to achieve this objective. Finally, feedback should be provided to the participant in order to trigger engagement and to renew motivation. The progression loop can take various forms, an example is when a cyber security training is provided in a series of smaller modules that each contribute to the overall objectives (as defined in step 1). In this way, it can become clearer what the progression of participants is in relation to defined (business) objectives and target behaviors.

Step five is to remind the designer of the gamified environment of the participants to ensure that they have a positive experience. Finally, as mentioned, step 6 regards the game elements and to assess which align best with the previous five steps. For this step, the models and frameworks as discussed in subsection 5 will be useful. In the end, the 6D framework illustrates that gamifying is no easy task and that careless applications of game elements will unlikely provide sufficient results (Huang & Soman, 2013; Kapp, 2012).

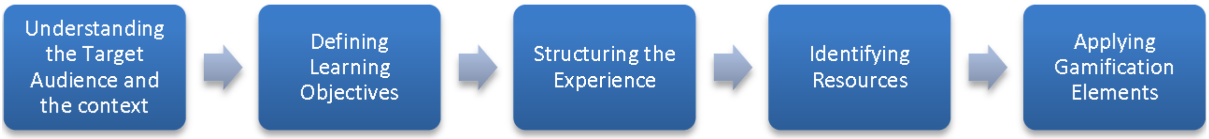

Understanding the Target Audience and the context
Defining Learning Objectives
Structuring the Experience
Identifying Resources
Applying Gamification Elements

*Figure 14 Process to Apply Gamification in Education (Huang & Soman, 2013)*

Additional authors address the process of applying gamification. For example, Huang & Soman studied the application of gamification in education (Huang & Soman, 2013). Following these authors, this process involves five steps, as visualized in Figure 14. These five steps align quite well with the 6D framework from Werbach and Hunter, e.g. understanding the target audience and the context can be related to step three of the 6D framework which considers the players of the gamified environment. The first step as described by Huang & Soman also emphasizes the context of the program. For example, a proper understanding of the context can improve the results of a cyber security awareness training, e.g. achieving predetermined objectives or demands. In the end, both frameworks regard game elements at the last steps. In the next subsection, both models towards applying gamification will be further compared towards constructing a framework for applying gamification in the context of existing cyber security awareness trainings.

## 6.3 Towards a Framework for Applying Gamification to Cyber Security Awareness Trainings

Previous subsection illustrated several bodies of knowledge regarding the process of applying gamification. However, these do not specifically regard cyber security awareness or cyber security awareness trainings. It is presumed that the 6D framework and the five steps from Huang & Soman can still provide valuable insight for the purpose of constructing a framework for gamifying existing cyber security awareness trainings, but it is important to regard the requirements as addressed earlier in this section due to this specific context. In other words, the process of gamifying a cyber security awareness training might follow similar steps as applying gamification in general, but the framework needs to be carefully tailored to the specific context of cyber security awareness trainings. The first step towards this framework involves an analysis of previous models regarding the process of applying gamification in order to develop new insight for a framework for gamifying cyber security awareness trainings. For this purpose, the SGD model from Raftopoulos, the 6D framework Werbach & Hunter, and the five steps from Huang &

Soman as discussed previously will be regarded. The following three tables (Table 9, 10, and 11) recapitulate the steps as discussed by these authors.

*Table 9 Steps in SGD model (Raftopoulos, 2014)*

| Raftopoulos |
|---|
| 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 |

*Table 10 Steps in 6D model (Werbach & Hunter, 2015)*

| Werbach & Hunter |
|---|
| 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 |

*Table 11 Steps from Huang & Soman (Huang & Soman, 2013)*

| Huang & Soman |
|---|
| 1. Understanding the target audience and the context |
| 2. Defining learning objectives |
| 3. Structuring the experience |
| 4. Identifying resources |
| 5. Applying gamification elements |

The analysis regarded which steps of these three models align, which contrast and which steps could complement each other towards an umbrella overview of the process of applying gamification. Hence, this analysis extends the insights derived from previous subsection regarding the 6D framework from Werbach & Hunter and the five steps from Huang & Soman. The results of the analysis of the three models are illustrated in Table 12 below. For example, as can be seen in the third row of Table 12, the third step from Huang & Soman, structuring the experience, relates to devise activity loops, as described in the fourth step of the 6D framework. Both of these steps focus on milestones or stages that contribute to overall objectives of the gamified environment and therefore provide the structure of the gamified environment. Following the first row of Table 12, defining learning objectives, step two from Huang & Soman, relates to define business objectives; step one of the 6D framework. Also step two of the 6D framework, delineate target behaviors, could be related to the learning objectives step of the process as described by Huang & Soman. Next, these steps from both Werbach & Hunter and Huang & Soman align with the first two steps from Raftopoulos. In sum, several steps from previous research can be integrated and complemented into the proposed combinatory steps.

*Table 12 Combinatory steps in the process of applying gamification*

| | Steps from previous research | | |
|---|---|---|---|
| Combinatory steps | Raftopoulos | Werbach & Hunter | Huang & Soman |
| 1. Objectives | 1, 2 | 1, 2 | 2 |
| 2. Context | 3 | 3 | 1 |
| 3. Structure | - | 4 | 3 |
| 4. Resources | 5 | - | 4 |
| 5. Diverge | 4 | - | - |
| 6. Converge | 6 | 6 | 5 |
| 7. Build | 7 | - | - |
| 8. Evaluate | - | - | - |

As can be seen in Table 12, step five from the 6D framework of Werbach and Hunter is missing in the proposed combinatory steps. It is proposed that this step, don't forget the fun, should be regarded at any phase of gamifying a cyber security awareness training. In this sense, the framework could add value by guiding developers of a gamified environment to analyze several types of fun and how to translate these into the gamified cyber security awareness training. Next, it is envisioned that the framework for gamifying cyber security awareness trainings would have a separate step called evaluate. This step was not explicit in any of the previous models or frameworks. However, it is presumed to be an important step towards assessing the gamification process and the gamified cyber security awareness training itself.

In order to construct a framework design based on the established combinatory steps, the seven guidelines from Hevner concerning design science are regarded (Hevner et al., 2004). These guidelines aid developers of an artifact to acquire an understanding of the specific design problem and its solution (Hevner et al., 2004). The designed artifact aims to solve an unsolved problem or solve a known problem in a more effective or efficient way (Hevner et al., 2004). In this graduation project, the artifact is designed to understand and solve the problem of applying gamification in cyber security awareness trainings in order to raise awareness. The framework shall guide developers through this process of gamification in a systematical way. As such, the framework aims to solve a known problem in a more efficient and effective way. Table 13 illustrates the seven guidelines from Hevner as applied to the context of this research; designing a framework towards applying gamification to cyber security awareness trainings.

*Table 13 Applied Design-Science Research Guidelines (Hevner et al., 2004)*

| Guideline and description | Towards a CSA + gamification framework |
|---|---|
| *Guideline 1: Design as an Artifact*<br>Design-science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation. | Visual representation of process of gamifying existing cyber security awareness trainings. A framework is designed, visualizing the different steps of this process. |
| *Guideline 2: Problem Relevance*<br>The objective of design-science research is to develop technology-based solutions to important and relevant business problems. | 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. |
| *Guideline 3: Design Evaluation*<br>The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods. | 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. |
| *Guideline 4: Research Contributions*<br>Effective design-science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies. | 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. |
| *Guideline 5: Research Rigor*<br>Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact. | 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. |
| *Guideline 6: Design as a Search Process* | The research is conducted in an iterative way regarding both theory and practice. Literature |

| | |
|---|---|
| The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment. | 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. |
| *Guideline 7: Communication of Research* Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences. | 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. |

As illustrated in Table 13, the first guideline considers the design artifact. In the case of applying gamification in cyber security awareness training contexts, a model seems appropriate in order to visualize the distinct steps of this process. The second guideline addresses the problem relevance. In this case, the framework addresses a business need regarding raising cyber security awareness. This need is addressed by providing a solution, a framework, to systematically apply gamification to cyber security awareness trainings in order to raise cyber security awareness more effectively. The third guideline regards the evaluation of the design. In this graduation project, both the designed framework and its usability regarding the process of gamifying are evaluated. The fourth guideline concerns research contributions. In this case, the framework itself is considered a key contribution next to the cyber security awareness constructs model from 4.1. Next, guideline five regards the research rigor. In this project, methodologies like literature studies, expert interviews, and case studies are performed in order to construct and evaluate the framework and its usability. The sixth guideline addresses design as a search process. In this case, the process towards a framework follows an iterative approach whilst analyzing both theory and practice regarding gamification and cyber security awareness. Finally, following the seventh guideline, the research is communicated in a visual framework design. The framework consists of two layers; a layer which provides a general overview, and a layer with details and in-depth information regarding the gamification process. Following the applied guidelines, the design process towards the framework is continued from the steps as derived from Table 12. These steps form the preliminary structure of the framework; objectives, context, structure, resources, diverge, converge, build, and evaluate. Several of these steps can be regarded to comprise a particular phase of the process of applying gamification. The identified phases are called: fundamentals phase, blueprint phase, design phase, and evaluation phase, as illustrated in the legend of Figure 15. Figure 15 presents the envisioned framework towards gamifying cyber security awareness trainings and uses colored arrows to represent these phases. The next paragraphs elaborate on the identified phases and the associated steps.

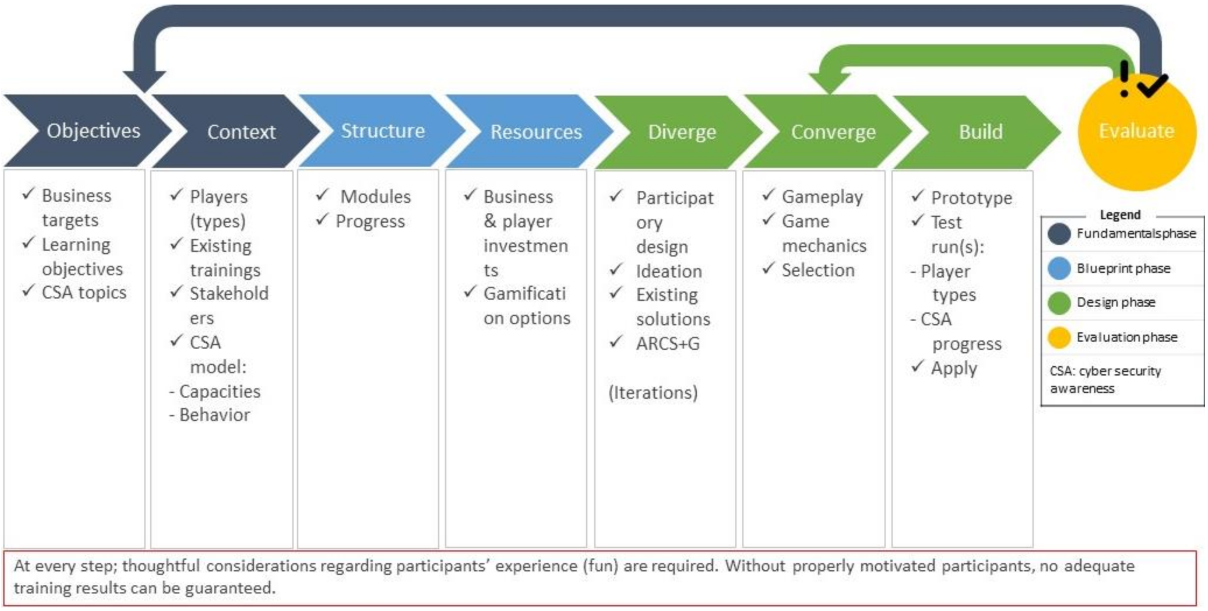


*Figure 15 Framework guiding the process of applying gamification to cyber security awareness trainings*

The first phase, fundamentals, comprises the objectives and context steps. In this phase, the emphasis is on the underlying motivations and the envisioned purposes of the gamified cyber security awareness training as discussed in sections 4.2 and 5. The importance of establishing objectives stems from previous insights regarding applying gamification and insights regarding effectively raising cyber security awareness from section 4. For example, the success of a gamified cyber security awareness training depends inter alia on a careful alignment of objectives and game mechanics. This relates to the requirements regarding gamification and cyber security awareness as illustrated in Table 8. Also the context of the training is considered in the fundamentals phase, for example the participants of the gamified cyber security awareness training. This relates to player types as discussed in section 5. Additionally, the context step considers the cyber security awareness constructs model as developed in section 4. This model is useful for establishing the current state or baseline regarding (different constructs of) cyber security awareness of participants. With this information the effectiveness of the training can be assessed afterwards. Finally, it is suggested to analyze existing trainings that aim to address similar objectives as addressed in the objectives step.

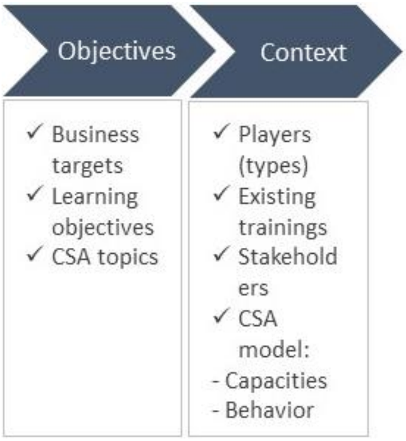


*Figure 16 Fundamentals phase*

The next phase, blueprint, consists of the structure and resources steps. These steps aim to provide the developer of the gamified cyber security awareness training guidance towards structuring the training whilst considering the available resources. The structure step regards modules and progress. These aspects can be linked to cyber security awareness concepts and player types as identified earlier this section. Next, the modules aspect relates to the additional requirements as established in Table 8. The resources step considers an analysis of investment, for example regarding the time that employees can spend on cyber security awareness trainings. This relates to the repetition and retention requirements from Table 8. Next, an initial analysis of gamification options is suggested. As discussed previously, gamification should be aligned with the objectives of the training and the sense of purpose of participants. The initial analysis provides the scope for further analyses during the next phase, for example regarding possible gamification mechanics that fit cyber security awareness topics and objectives.

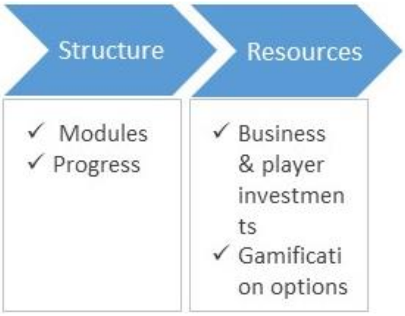


*Figure 17 Blueprint phase*

The third phase, design, comprises the diverge, converge, and build steps. The first two steps, diverge and converge, are related to the ‘wybertjesmodel’ of creative problem solving (Bakker & Buijs, 1979). In this regard, the first step, diverge, includes idea generation regarding potential or partial solutions for the gamified cyber security awareness training. Previous research indicated that similar gamification concepts might work beneficial for some participants while being counterproductive for others. Therefore, participatory design is suggested in the diverge step in order to distinguish promising gamification concepts, for example per cyber security awareness topic or learning objective. Previous analyses regarding existing cyber security awareness trainings or promising gamification solutions for a cyber security awareness training can be expanded in another level of abstractness in this step. Next, the ARCS+G model as addressed in section 6.1 can be regarded in this step to distinguish strategies or tactics to fit different modules, objectives or topics of the cyber security awareness training. This step might benefit from several iterations before continuing to the converge step. For example, ideas might lead to different ideas or might be combined into new ideas. The next step, converge, includes an evaluation and selection of these ideas. Both the diverge and converge step can benefit from the developed Table 6. The categorized overview of gamification mechanics can be used to generate or select ideas for the cyber security awareness training, as illustrated in Table 14. For example, the categories and game mechanics can be compared to the learning objectives of the training in order to assess the suitability of the ideas. This also relates to the requirements from Table 8, for example regarding the alignment of motivation, gamification and objectives. Iterations of the diverge and converge step are also possible, for example when the converge step brought up new potential solutions for the gamified cyber security awareness training or when solutions turn out to be infeasible. The third step of the design phase, build, considers building a prototype based on the selected ideas regarding gameplay and game mechanics and testing the prototype. An example of such tests could involve a reflection on the progress of participants regarding cyber security awareness. As such, the CSA model can be used to distinguish the effect of the training on different constructs of cyber security awareness when compared to the baseline results.

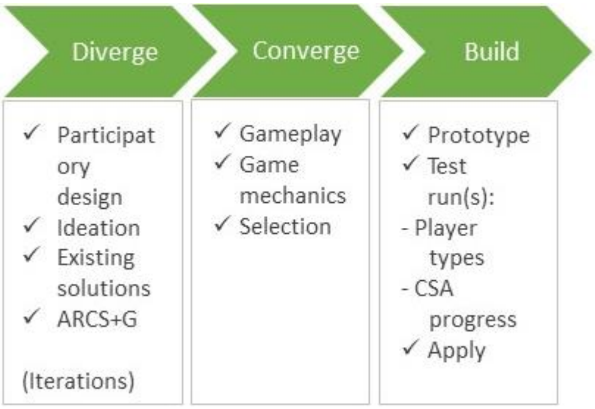


*Figure 18 Design phase*

*Table 14 Example of using the overview of gamification mechanics in cyber security awareness trainings development*

| Categories | Gamification Mechanics | Ideation |
|---|---|---|
| Cooperation/Competition | Leaderboards | |
| | Social | |
| | Guilds | |
| | Roles | |
| | Avatars | |
| | Virtual Goods | |
| Prizes | 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 | |

After the build phase, the gamified cyber security awareness training is evaluated in the evaluation phase. As can be seen in Figure 15, this step is visualized in a different way due to the different characteristics of this phase. In this phase, the results of the evaluation of the gamified cyber security awareness training determine how to proceed with the training. For example, when test runs turn out positive and the gamified training seems ready to roll out, it can be implemented (on a greater scale). Note that after implementation of the gamified cyber security awareness training, regular checks are recommended, inter alia whether the training is still properly aligned with the defined objectives and context. In the context of cyber security awareness this is especially important, since trends, for example in the threat landscape, are fast-paced and needs to be accounted for in the training. This relates to requirements regarding relevant and up to date content as illustrated in Table 8. On the other hand, objectives might change, for example with regards to cyber security awareness, and the training needs to be aligned with such changes. In sum, such checks are illustrated in the framework by the feedback loop from the evaluation phase to the fundamentals phase; the blue arrow. These feedback loops align with requirements regarding continuous monitoring and flexibility as illustrated in Table 8.

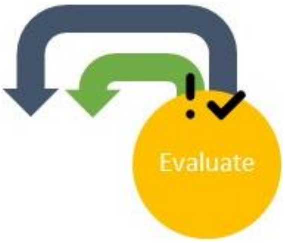


*Figure 19 Evaluation phase*

In the framework, an additional feedback loop is presented in green. This loop from evaluate to the design phase illustrates when the results of the evaluation of the gamified cyber security awareness training pose some questions or considerations that need to be regarded before implementing the gamified cyber security awareness training. In this case, it is recommended to return to the drawing table and enlarge the solution space at the diverge step or to select from the previously identified solutions at the converge step. In the end, a new or adjusted prototype can be developed in the build step of the design phase in order to address the questions or considerations from the previous iteration.

In the end, this section provided a framework to guide developers through the process of gamification as applied to the context of cyber security awareness trainings. In order to assess the designed framework, the next subsection aims to answer the question regarding how the framework can be evaluated.

## 6.4 Expert Interviews to Evaluate the Designed Framework

After developing an artifact, it should be thoroughly evaluated, formally represented, and communicated effectively (Hevner et al., 2004). In this case, the designed framework from Figure 15 that is primarily based on theoretical knowledge will be evaluated with experts in the field of cyber security awareness and gamification. Experts are selected for these interviews based on their expertise in these fields e.g. applied gamification to raise cyber security awareness or contributed to projects regarding cyber security and gamification. As such, expert interviews with three employees from Deloitte are set up to discuss the use and applicability of the framework in real-life scenarios. These employees are selected based on a background or expertise in cyber security awareness and gamification. Next, experience of working at Deloitte Cyber is regarded in order to derive information concerning the perceived practices of projects about cyber security awareness. Following these criteria, one junior manager from Cyber Strategy, one junior manager from the Secure team, and one director from the Cyber Strategy team are contacted. Additional information and characteristics regarding the selected experts is not provided in order guarantee a level of anonymity of the experts. The interviews involve questions regarding prior experiences, recommendations regarding gamification, first impressions of the framework, and actually discussing different steps and aspects of the designed framework. The face-to-face interviews took between 30 minutes and one hour and were audio-taped and transcribed. The raw results from interviews can be regarded in Appendix B Expert Interviews. The results of the interviews are incorporated into the previously designed framework, which results in the framework as visualized in Figure 20. Next paragraphs will elaborate on the framework adjustments.

Based on comments from the experts, the steps 'structure' and 'resources' are switched. In this way, the available resources provide the bandwidths for structuring the training. Next, several interim results are explicitly added to the framework to aid developers of gamified cyber security awareness trainings. Following expert opinion, these adjustments make it more clear what the aim is of each phase. Furthermore, it helps to interpret the level of abstractness in each of the phases. As can be seen in Figure 20, yellow circles now clarify the deliverables at the end of each phase. For one, 'training scope' provides an overview of key objectives of the cyber security awareness training and an analysis of existing cyber security awareness trainings. Next, the 'blueprint and toolbox' deliverable provides an overview of cyber security awareness content from the analyzed trainings and an analysis of options for the cyber security awareness training and its overall structure. Finally, 'training roll-out' means that the gamified training is ready to roll-out.  Table 15 visualizes the interim results and the aspects addressed in the interim results.

*Table 15 Interim results and aspects*

| | Aspects |
|---|---|
| Training scope | *Business targets* |
| | *Learning objectives* |
| | *Topics* |
| | *Stakeholders & players* |
| | *Existing trainings* |
| | *KPIs* |

| | Aspects |
|---|---|
| Blue-print & toolbox | *Investment* |
| | *Existing solutions* |
| | *Platform* |
| | *Modules* |
| | *Progress* |

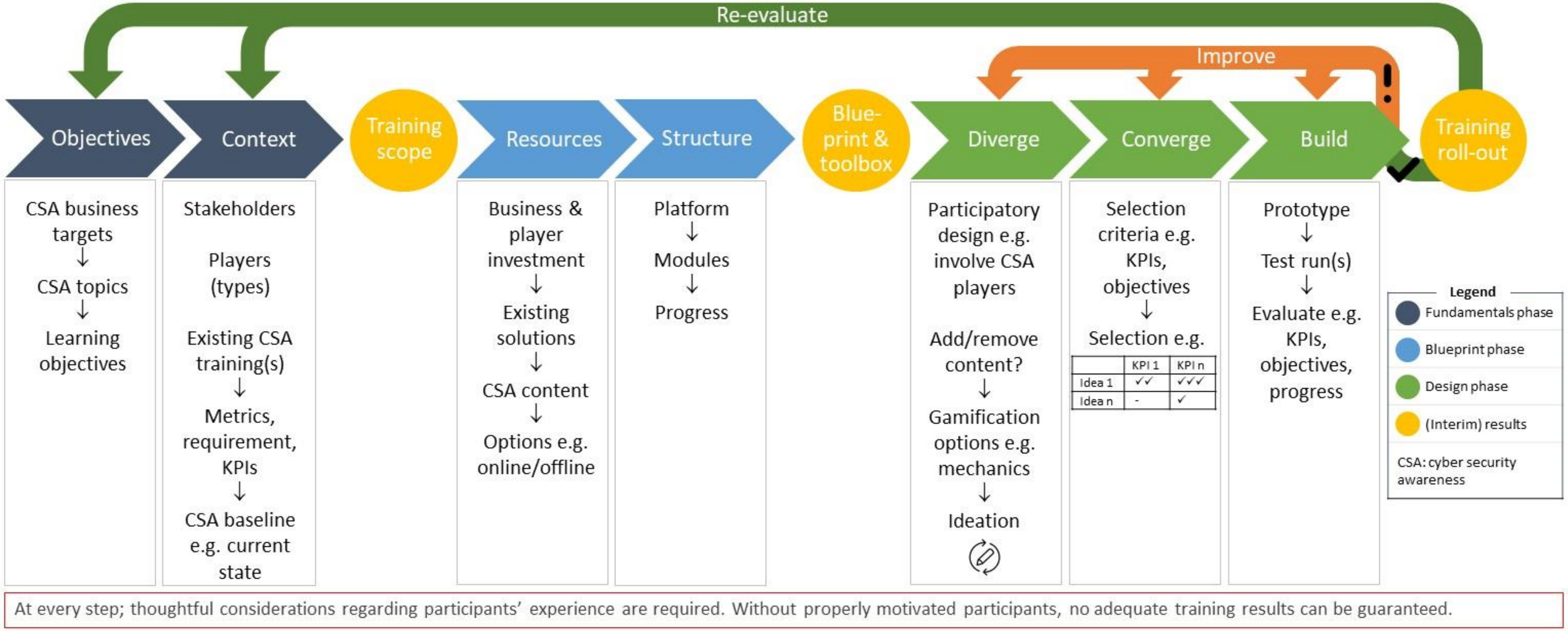
| | Aspects |
|---|---|
| Training roll-out | *Add/remove CSA content* |
| | *Selection criteria* |
| | *Prototype* |

The feedback loops are also adjusted based on the expert interviews. The arrows are now displayed in green and orange which correspond better with their notion of 'ok' and 'warning'. For additional clarification, the arrows are accompanied by 're-evaluate' and 'improve' as suggested by the experts. Finally, the arrows now visualize better that re-evaluation can involve either 'objectives', or 'context' or both. The improve feedback loop can also involve an iteration through the entire design phase or regard specific steps from this phase. Based on expert comments, this was not clear in the initial framework. An additional adjustment regards the roll-out of the training. This was mentioned by the experts as rather unclear in the visualization of previous framework. Now, only when the results of the gamification process regarding the cyber security awareness training are satisfactory, the training should be rolled-out. Otherwise, as visualized by the orange arrow before 'training roll-out', the 'improve' feedback loop will activate.

The design phase also faced some notable changes based on the expert interviews. For example, although the blueprint phase explicitly regarded cyber security awareness content in the 'resources' step, the 'diverge step' of the design phase now reviews this content. For example, is there sufficient or is there too much content? Does the content align with the envisioned gamification or the envisioned training and its purposes? These questions surfaced during the interviews. For one, the amount or format of the contents of an existing cyber security awareness training might require adjustments in order to fit a gamified cyber security awareness training. Next to this, a visualization is added in the 'diverge' step of the design phase to illustrate that this step might benefit from multiple iterations. Next, the 'converge' step is clarified by explaining the selection process, which uses the selection criteria as derived from the 'objectives' step. Next, there are several ways to make a selection of the ideas from the 'diverge' step. A possible approach of making a selection of ideas, as suggested by the experts, is visualized in the table at the bottom of the 'converge' step. Note that using checkmarks in this table is just one of the possible ways of doing this. Following the comments of the experts, euros or low/medium/high or otherwise might also work. Finally, in the 'build' step of the design phase, the prototype is evaluated based on the defined KPIs and objectives from previous phases. Based on expert comments, next to these KPIs and objectives, aspects like feasibility, scalability and costs could also play a role in the evaluation. After the evaluation, it is decided whether to make adjustments or to roll-out the training, as can be seen in the feedback loops.

Regarding the contents of each step, hierarchy and coherence are now displayed by adopting black downward arrows. Based on expert comments, this was missing in the visualization of the initial framework. Next, some terms are shifted to other steps or phases of the gamification process for they deemed more appropriate there. For example, following expert opinion, analyzing existing solutions will be regarded in the resources step of the blueprint phase. Next to shifting terms, some terms are adjusted or made more explicit based on the results of the expert interviews. For example, 'metrics, requirements, KPIs' are considered clearer terms than 'CSA model', which was proposed as an exemplar tool. Using these new terms also provide more room to maneuver and more room for creativity; there might be other relevant models to consider. Finally, some terms are added to the content of the framework based on the expert interviews. For example, explicitly assessing the current state regarding cyber security awareness in the context step.

In conclusion, this section addressed several categorized requirements towards designing a framework for gamifying cyber security awareness trainings. Next, the process of gamification was analyzed which resulted in a combinatory model regarding the steps of applying gamification. Consecutively, design-science research was applied to this case based on the guidelines from Hevner (2004). Integrating these previous insights with newly developed models, e.g. the cyber security awareness constructs model and the categorized gamification mechanics for cyber security awareness trainings, resulted in a framework for gamifying cyber security awareness trainings. This framework was evaluated using expert interviews and adjusted accordingly. The next section regards the usability and perceived effectiveness of the framework and a resulting gamified cyber security awareness training.


Re-evaluate
Improve
Objectives
Context
Training scope
Resources
Structure
Blue-print & toolbox
Diverge
Converge
Build
Training roll-out
CSA business targets ↓ CSA topics ↓ Learning objectives
Stakeholders
Players (types)
Existing CSA training(s) ↓ Metrics, requirement, KPIs ↓ CSA baseline e.g. current state
Business & player investment ↓ Existing solutions ↓ CSA content ↓ Options e.g. online/offline
Platform ↓ Modules ↓ Progress
Participatory design e.g. involve CSA players
Add/remove content? ↓ Gamification options e.g. mechanics ↓ Ideation
Selection criteria e.g. KPIs, objectives ↓ Selection e.g.
KPI 1
KPI n
Idea 1
✓✓
✓✓✓
Idea n
-
✓
Prototype ↓ Test run(s) ↓ Evaluate e.g. KPIs, objectives, progress
Legend
Fundamentals phase
Blueprint phase
Design phase
(Interim) results
CSA: cyber security awareness

At every step; thoughtful considerations regarding participants' experience are required. Without properly motivated participants, no adequate training results can be guaranteed.

*Figure 20 Framework for gamifying cyber security awareness trainings*

# 7. Perceived Effectiveness of a Framework Application

This section builds upon the designed framework. An answer is formulated to the following research question: what is the perceived effectiveness of an application of the designed framework? In this case, effectiveness regards the degree to which the gamified cyber security awareness training is successful in contributing to the cyber security awareness of participants. This section addresses applying the framework to an existing cyber security awareness training in order to establish that the framework accurately represents a gamification process. First, an existing cyber security awareness training is selected in subsection 7.1. Next, this existing training is gamified in section 7.2 by using the adjusted framework from subsection 6.4. Finally, there is a case study where both participants of the existing training and participants of the gamified training will be analyzed and questioned. Comparing the responses to parameters under investigation finalizes the evaluation of the designed framework and the developed gamified training.

## 7.1 Selection of a Non-gamified Cyber Security Awareness Training

In this subsection, first, several non-gamified cyber security awareness trainings are regarded. Next, a description is provided of the selected training for the application of the designed framework.

### 7.1.1 Cyber Security Awareness Trainings Offered by Deloitte

Deloitte has established a security awareness learning academy where several aspects of cyber security awareness are addressed. Raising cyber security awareness among employees via the learning academy is an important tool for the company in order to be vigilant and resilient regarding cyber related incidents. Separate faculties of the learning academy are: anti-corruption, confidentiality, ethics, information security, and privacy (Noell, 2017). These themes are aspects that could be addressed in the different constructs from Figure 8 to establish cyber security awareness. For example, knowledge regarding privacy or attitude regarding confidentiality. As derived from analyzing the learning academy platform, anti-corruption encompasses i.a. policies and risks regarding corruption (Noell, 2017). Confidentiality regards safeguarding confidential information and client trust (Noell, 2017). Next, ethics concern principles, values, integrity and quality (Noell, 2017). Information security focusses on unauthorized access or use of information (Noell, 2017). Finally, privacy entails policies, procedures, standards and guidelines regarding data protection and handling personal information (Noell, 2017).

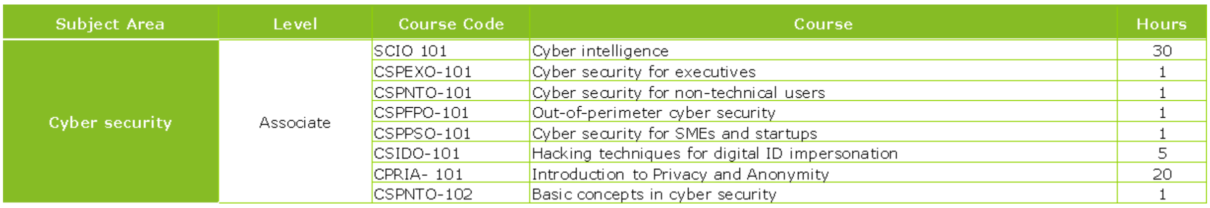
Next to the Deloitte security awareness learning academy, additional cyber security awareness trainings were acquired via an employee of Deloitte Madrid with expertise in training, education and awareness. As such, information regarding the Deloitte Cyber Academy was retrieved. On this online platform, cyber security trainings are offered to external and internal practitioners. Different levels of knowledge and expertise are addressed in the online courses and diplomas and certificates can be achieved by successfully completing the courses. There are two catalogues behind the Cyber Academy that illustrate the areas of expertise; there is one technical catalogue and one awareness catalogue. After closer examination of these catalogues, primarily the awareness catalogue seems to address the topic of cyber security and cyber security awareness.

In order to pick an existing training that is suitable for the application of the framework, for the scope and duration of this thesis project, it should be evaluated based on the aim of the research question. In this case, to demonstrate how the framework can be applied and how effective the gamified training is perceived. There are several considerations and requirements for the training to pick for the case study and the remainder of this research. First of all, it is not feasible to pick a training of over 30 hours. This would make it unreasonably complex to gamify the training and would create a significant barrier towards getting participants for both the existing and the gamified training. As a result, a training of one hour seems more appropriate for the purpose and duration of this thesis project. Next, getting a fair number of appropriate participants for the case study on the existing and the gamified training requires a training that is targeted to a relatively wide audience. For example, trainings that target SMEs, startups or executives will decrease the number of potential participants for this case study. Hence, such trainings are also excluded for the purpose of applying the designed framework and performing a case study. Finally, trainings that do not require prior knowledge, experience or completed trainings are ideal for the purpose of answering this research question. This aligns with the considerations of acquiring participants for this training and the gamified training.

After closer examination of the trainings, the security awareness learning academy are very specific regarding the company Deloitte, the functions of its employees, its clients, or its client projects. Next, recalling the cyber security awareness topics from Table 1, each of the learning academy trainings only addresses a very specific part of these topics. In the end, using one of these trainings for the case study might not lead to proper generalizable results. Next, it would only shed light on a tip of the iceberg regarding cyber security awareness. However, these themes do illustrate the priorities of the organization regarding cyber security awareness. Therefore, using a training with an 'umbrella' focus would be more appropriate for the purpose of applying the framework. In other words, a training that addresses several of the prioritized concepts related to the themes from the learning academy and the topics from Table 1. The analysis of the existing training results in the following selection criteria for the existing training to be gamified:

1. The training should be aimed to increase cyber security awareness.
2. The training should executable within one hour.
3. The training should be applicable to a wide audience.
4. The training should not require any prior knowledge, experience or other completed trainings.
5. The training should address a broad scope of cyber security topics.

Each training from the security awareness learning academy is targeting a specific cyber security topic, which makes these trainings unsuitable for the purpose of this research. The cyber academy trainings as visualized in Figure 21 include a broader scope of cyber security topics.



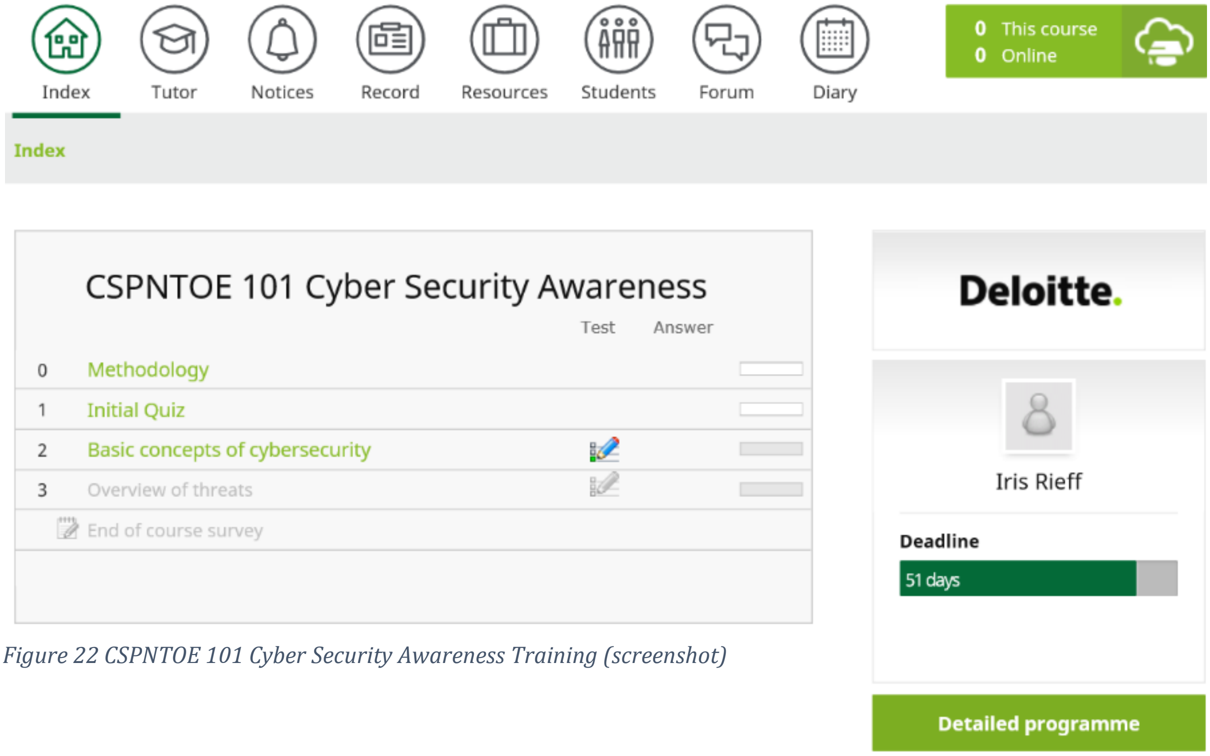
| Subject Area | Level | Course Code | Course | Hours |
|---|---|---|---|---|
| Cyber security | Associate | SCIO 101 | Cyber intelligence | 30 |
| | | CSPEXO-101 | Cyber security for executives | 1 |
| | | CSPNTO-101 | Cyber security for non-technical users | 1 |
| | | CSPFPO-101 | Out-of-perimeter cyber security | 1 |
| | | CSPPSO-101 | Cyber security for SMEs and startups | 1 |
| | | CSIDO-101 | Hacking techniques for digital ID impersonation | 5 |
| | | CPRIA- 101 | Introduction to Privacy and Anonymity | 20 |
| | | CSPNTO-102 | Basic concepts in cyber security | 1 |

*Figure 21 Cyber Academy trainings regarding cyber security*

Within the subject area of cyber security, at the associate level, eight trainings are offered as visualized in Figure 21. Two of these trainings are unsuitable for the case study based on their duration. Next, two of the trainings are unsuitable due to their target group, e.g. executives and SMEs. Finally, one training is unsuitable due to the tight spectrum of topics addressed in the trainings; out-of-perimeter cyber security. In other words, after applying the same selection process as addressed previously, two trainings resulted as suitable for the case study. However, it seems that these trainings should ideally be completed consecutively. As a result, the first of these trainings is picked for the purpose of this phase of the thesis project.

### 7.1.2 Description of Selected Non-gamified Cyber Security Awareness Training

The selected training is an online training called CSPNTOE 101 Cyber Security Awareness. Figure 22 provides a screenshot of an initial screen of this non-gamified training.



CSPNTOE 101 Cyber Security Awareness

| | | Test | Answer |
|---|---|---|---|
| 0 | Methodology | | |
| 1 | Initial Quiz | | |
| 2 | Basic concepts of cybersecurity | | |
| 3 | Overview of threats | | |
| | End of course survey | | |

Iris Rieff

Deadline

51 days

*Figure 22 CSPNTOE 101 Cyber Security Awareness Training (screenshot)*

First, in the section of this training called methodology, the workings of the platform are explained. Next, there is an initial round of five questions which participants have to complete by scoring 100% in order to proceed with the training. If participants score less than 100%, they can return and adjust their answers according to the right answers. After finishing the questions, there is a section which addresses basic concepts of cyber security and which ends with a short test consisting of three questions. The section addresses in particular the term cyber security, corporate assets susceptible to cyber-attacks, objectives of protection, and defying cyber-attacks. After this second section and the associated questions, there is a section called overview of threats which ends with test consisting of five questions. The section starts with a video that illustrates a real life scenario of a company facing a cyber-attack. This video is the only example of other media that was used in this training besides written text. After the video, malware and fraud schemes, social engineering, spam, phishing, APTs, passwords and credentials e.g. authentication factors, credential theft, black markets, trends and best practices are addressed in the section. Note that all tests of the three sections consist of multiple-choice questions.

When regarding the addressed cyber security awareness topics, the training provides a combination of topics that can be related to the themes from the security awareness learning academy. For example, confidentiality can be related to susceptible corporate assets, ethics can be related to best practices, and privacy can be related to objectives of protection and privacy. Especially information security can be related to several of the topics as addressed in the training, e.g. social engineering, malware, and cyber-attacks. The overall objective of the CSPNTOE 101 training is to 'train non-technical people on the basis of cyber security and describe the basis guidelines to security awareness at the work place' (Deloitte, 2018a). The training focusses on protecting the key assets of an organization and providing 'a first line of defense against cyber-attacks' (Deloitte, 2018a). These aspects can be associated with the contents of the objectives and contexts steps of the fundamentals phase as visualized in the designed framework from Figure 20. The associated learning objectives from the selected training are: recognizing and detecting cyber fraud, knowing common cyberattacks and entry vectors, representing a barrier for cybercriminals, protecting digital assets and detecting and alerting about possible intrusions (Deloitte, 2018a). One of the challenges to the effectiveness of this training is the fact that it is offered as an e-learning, a platform that often fails to engage employees and thus fails to achieve long-term success. However, the learning objectives and content of this training can be useful in order to provide a training that might counter some of the challenges due to gamification. Therefore, the next subsection uses these aspects towards the development of a gamified training.

## 7.2 Developing a Gamified Cyber Security Awareness Training

This subsection focusses on putting the designed framework to practice. Each of the phases will be addressed, along with the interim results.

### 7.2.1 Fundamentals phase

The steps and interim results of the first phase of the adjusted framework is visualized in Figure 23. This phase is largely addressed in previous subsection. The analysis of the cyber security awareness training derived the business targets, topics, learning objectives, players, and current state of cyber security. Metrics, requirements or KPIs were not addressed in the analyzed training. Therefore, the metrics from the CSA model as developed in section 4.1 are used. Recalling this model, knowledge and skills form an aspect of cyber security called capability. Next, actions and attitude form the other aspect of cyber security called behavior. The four constructs, knowledge, skills, actions, and attitude, will be regarded as metrics or KPIs for the 'context' step of the fundamentals phase. This concludes the two steps from the fundamentals phase, which results in the deliverable 'training scope' as illustrated in Table 16.

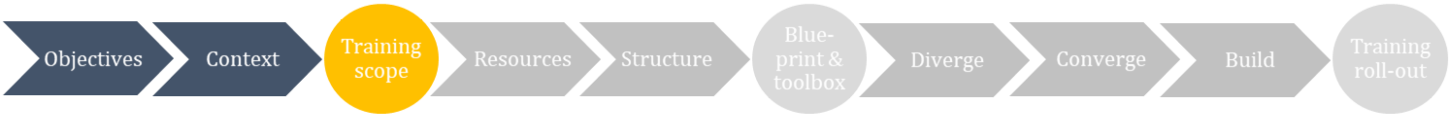


*Figure 23 Fundamentals phase*

*Table 16 Training Scope: aspects and implementation for the gamified training*

| Interim Result | Aspects | Implementation |
|---|---|---|
| Training scope | *Business targets* | Protecting the organization's key assets against cyber-attacks by increasing general cyber security awareness of non-technical employees |
| | *Learning objectives* | Recognizing and detecting cyber fraud, knowing common cyberattacks and entry vectors, representing a barrier for cybercriminals, protecting digital assets and detecting and alerting about possible intrusions |
| | *Topics* | Cyber security and objectives, cyberattacks and trends, security versus privacy, assets |

| | | |
|---|---|---|
| | | susceptible to attacks, defense mechanisms, malware, passwords and credentials, data leakage and prevention, social engineering, phishing, and best practices |
| | *Stakeholders & players* | Employees of the organization |
| | *Existing training(s)* | CSPNTOE 101 Cyber Security Awareness |
| | *KPIs* | Knowledge, skills, actions, attitude |

### 7.2.2 Blueprint phase

The blueprint phase consists of the 'resources' and 'structure' steps and the blueprint & toolbox deliverable as illustrated in Figure 24. The business and player investment resources imposed that the training should ideally take approximately one hour. The CSPNTOE 101 online training was executed in order to derive the cyber security awareness related content. A final element of the 'resources' step is to assess options for gamifying this training while taking into consideration the objectives, context, and resources. As such, several online options were regarded to build and distribute the gamified training, for example the digital platform of the current training, as well as the Deloitte learning academy. It turned out to be difficult to get access to these platforms and to get the rights to adjust content or to provide a new training. A third regarded initiative is Mindgame.eu, a website that addresses activating people by using game mechanics in order to realize behavior changes (Mindgame, 2018). The website displays their projects in several categories. Interestingly, some of them correspond with some constructs of cyber security awareness, e.g. attitude, knowledge, and skills. For the duration of this thesis, it was not feasible to use this platform to develop and provide a gamified training. Another option is the website of Cybersave Yourself (CSY), which provides a game that is part of a campaign for education and research regarding the field of cyber (CSY, 2018). The website also provides a toolkit via SURF.nl for several institutions, including the Delft University of Technology, in order to develop their own campaign (SURFnet, 2018). Unfortunately, the toolkit does not provide tools to develop and distribute a gamified training.

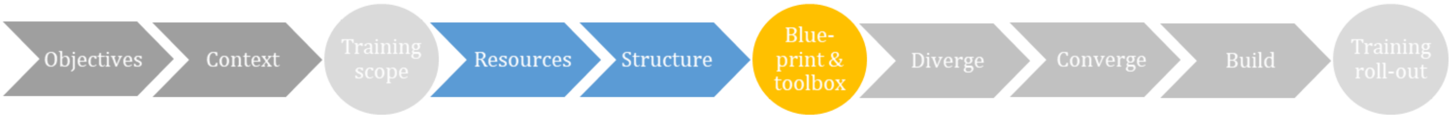


*Figure 24 Blueprint phase*

Next to online options to develop and distribute a gamified cyber security awareness training, 'offline' options were explored. Based on projects at Deloitte, like a 'portable' escape room regarding cyber security that was discussed during the expert interviews, the idea of a cyber security awareness escape room surfaced. However, the business investment regarded earlier in the resources step of the framework excludes this option considering the time needed for developing such a gamified training. Another project at Deloitte regards a board game on malware based on the game Monopoly. This game, Malwopoly, was also discussed during the expert interviews. This seems a good option regarding the business investment earlier in the resources step for gamifying an existing training. However, such a game would easily take over one hour to complete. Interviews proved that a more 'eventlike' gamification rather than to match existing games sounds more promising for participation. As a result, the aim was to incorporate the 'event' aspect of an escape room with the less complex development characteristics of a tabletop game. This resulted in an analysis of Escape Room The Game from Identity Games (Identity_Games, 2018). Escape Room The Game is a tabletop game platform that combines escape room event characteristics. It is a cooperative game for around three to five players. There are multiple one-hour scenarios that can be played with this platform, each consisting of three parts. Each part of a scenario is finished by providing a code consisting of four keys. If the code is correct, participants can advance to the next part of the scenario. A scenario is successfully completed when participants provide three correct codes within an hour. In sum, Escape Room The Game possesses various characteristics towards a viable platform to use for the development and the delivery of a gamified cyber security awareness training. Note that since Escape Room The Game is a commercially offered game, agreements need to be established between organizations and Identity Games in order to use this property for developing gamified trainings.

The remainder of the 'structure step' from the blueprint phase considers the modules and progress of the training. The existing cyber security awareness training consists of three parts. In the gamified training by using the Chrono Decoder from Escape Room The Game, this could still be developed in such a way. Next, the existing training had a duration of approximately one hour. This also aligns with a gamified cyber security awareness training based on Escape Room The Game. Finally, progress was not very clear in the existing training. However, by using the Chrono Decoder in the gamified training, this could be developed in a much more explicit way. Table 17 provides an overview of the blueprint & toolbox deliverable with the related aspects and the implementation of these in the gamified cyber security awareness training.

*Table 17 Blueprint & Toolbox: aspects and implementation for the gamified training*

| Interim Result | Aspects | Implementation |
|---|---|---|
| Blueprint & toolbox | *Investment* | The training should last for approximately one hour |
| | *Existing solutions* | Different existing online and offline solutions were analyzed e.g. CSY and escape rooms |
| | *Platform* | The platform from Escape Room The Game will be used for the gamified training |
| | *Modules* | The gamified training will consist of three modules |
| | *Progress* | Progress of the three modules of the training can be tracked via the Chrono Decoder |

### 7.2.3 Design phase

The design phase consists of three steps, as visualized in Figure 25. The phase starts with the 'diverge' step. In this step, potential participants were involved to discuss their opinions and ideas regarding a gamified cyber security awareness training. These persons will not function as participants in the case study for their inside information regarding the trainings might skew the results. It became clear that the amount of content as provided in the existing training is overwhelming. As a result, it seems that the more content is provided the less information will stick. Therefore, content was removed based on a focus on the topics that aligned most with the training scope. As such, resulting topics are: cyber security e.g. trends and objectives, attack vectors, malware, social engineering, phishing, deep web, black markets, passwords and credentials, credential theft, defense measures, and best practices e.g. reporting incidents.

Next, several categories of gamification options were explored, for example several cooperative options and different kinds of puzzles. Ideas can also be inspired by previous interim results, for example possibilities offered through the use of the Chrono Decoder. Also, previously distilled cyber security awareness topics were associated with gamification options. Based on these associations, additional iterations followed in order to derive more ideas for the gamified cyber security awareness training. The results of this process are visualized in Table 18.

*Table 18 Gamification categories and ideation for the gamified training*

| Gamification categories | Ideation |
|---|---|
| **Cooperation** | Malware; examples and objectives |
| | Passwords and credentials |
| | Decrypting password; roles |
| | Quiz regarding provided content |
| | Cyber security trends and objectives |
| **Prizes** | Award with name of the team; achievement |
| | Poster with best practices; trophy |
| **Adventures** | Working towards impersonation; goal |
| | Identifying social engineering target; mission |
| | Identify malware of the adversary; quest |
| **Progression** | Use of the Chrono Decoder; status |
| | Key per solved puzzle towards code |
| | Chrono Decoder for incorrect code; feedback |
| | Stages towards story completion; levels |
| | Requesting hints; feedback/report |
| **Surprises** | Providing incoming emails; unlockables |
| | Input via new messages or notes; notifications |

In the 'converge' step the selection criteria for the gamified cyber security awareness training were analyzed. Given the results of previous steps, additional selection criteria besides the four KPIs from the 'context' step surfaced. For example, storyline and gameplay, as discussed in sections 4.2 and 5.1, can severely benefit the experience of participants. Next, gamification options should be linked to the cyber security awareness content in order to justify the design of the gamified training. In the end, several of the concepts that scored best on such aspects were combined. For example, a clear storyline regarding the process of social engineering was developed in order to contribute to participant experience and to improve the perception of a real-life scenario. Also, clear and logical transitions between the 3 phases of the gamified training should align with the storyline.

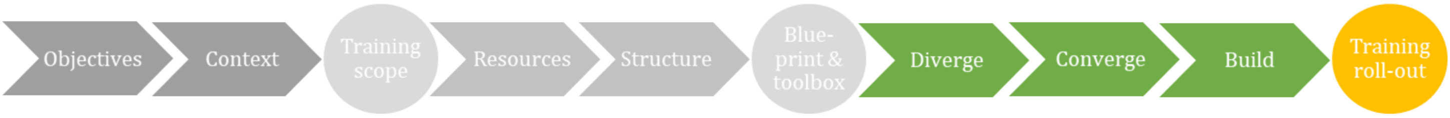


*Figure 25 Design phase*

The 'build' step of the design phase involves building a prototype. This was an extensive process of (re)thinking, (re)designing and (re)printing. First, paper-based sketches were developed and adjusted before making more sophisticated, digital versions. For example, social media profiles and the associations between these profiles were figured out before actually building digital designs. The finished prototype was walked through in order to distinguish any flaws before testing it with two participants under observation (first pilot study). The participants both have a background and experience with ICT. After the evaluation based on observation and discussion with the participants, the prototype faced some major adjustments. For one, all three phases of the training were simplified. For example, some social media accounts were adjusted or removed, the password retrieval was simplified, and the way to get to the final code was clarified. A second pilot study with three other participants was performed. Two of the participants followed the ICT track of the SEPAM bachelor. The participants of both pilot studies will not be part of the case study for this might affect the results. After evaluating the second pilot study, additional adjustments were made. For example, the texts for the introduction and the three different parts was shortened and social media accounts were adjusted to avoid confusion. Finally, the gamified cyber security awareness training was ready for the case study. Table 19 illustrates the discussed training roll-out and the implementation of the associated aspects. The next subsection briefly describes the resulting gamified training.

*Table 19 Training Roll-out: aspects and implementation for the gamified training*

| (Interim) Result | Aspects | Implementation |
|---|---|---|
| Training roll-out | *Add/remove CSA content* | Content was selected based on i.a. learning objectives, i.a. attack vectors, defense measures, and best practices |
| | *Selection criteria* | Next to the discussed KPIs, gamification selection criteria were regarded, i.a. storyline |
| | *Prototype* | The prototype was adjusted based on the evaluations of two pilot studies |

### 7.2.4 Short Description of Developed Gamified Training

The challenge consists of three parts and is ideally played with two to three participants. First, the participants are provided an introduction of Cyber: A War Next. The story regards a fictional telecom company called MCLT that has recently developed a promising innovation. Eve is interested in retrieving the secret corporate information regarding this innovation. In the remainder of the challenge, participants help Eve to access this information via credential theft, sending malware, and impersonating an employee of MCLT. In the final part, the participants are asked for advice how to raise cyber security awareness of the employees of MCLT in order to prevent future cyber incidents.

In each part of Cyber: A War Next, a code consisting of four keys must be found that can be entered into the Chrono Decoder. The game includes six different key types, each stating different information corresponding with the codes that can be found during the game. Once a code has been found, the four keys should be put from left to right into the Chrono Decoder. If the code entered is incorrect, an 'error' sound is played and one minute will be deducted from the remaining time. If the code is correct, a 'confirmation' sound is played. Once the correct code is found, the next part of the challenge may be started and after finding three correct codes within 60 minutes, the game is finished. Participants will hear a 'victory' sound and will receive a certificate of completion with their time, team name, and 10 best practices.

*Table 20 Training content and material provided in each of the three parts of the gamified training*

| Parts | Provided reading material | Addressed content |
|---|---|---|
| 1 | Hacker Handbook | Social engineering |
| | Social media profiles (Facebook, Twitter, and Linked-In) | Identity theft, impersonation |
| | MOOC notes | Phishing, malware |
| 2 | Terms and Conditions of Black Market Exchange | Passwords and credentials (theft) |
| | Inbox | Impersonation |
| | Received email | Malware |
| | Tablet with website | DeepWeb, black markets |

| | | |
|---|---|---|
| | Password retrieval post-it | Authentication factors |
| | Post-it on credential theft | Five steps of credential theft |
| 3 | Cyber Memo | Cyber-attacks, trends |
| | Protector Publications | Cyber security concepts and objectives |
| | Quiz | Reflection on previous topics |

In each part, the players retrieve new information in the form of (physical) handbooks, social media accounts, notes, etc. The information consists of (gamified) training material and contains hints, puzzles and information to find the correct code. When the Chrono Decoder makes a 'beep-beep' sound, participants can opt to ask for a hint.  Table 20 shows the content and reading material that is provided in each of the three parts. The remainder of the developed gamified training can be found in Appendix D Gamified Training. In the end, the gamified cyber security awareness training addresses primarily the internal angle of cyber security as described in section 4.1. In other words, primarily the angle of cyber security awareness that can be influenced and which an employee possesses in a certain degree is targeted with this training, not so much the effect that cyber security awareness can have on (the context of) an employee.

## 7.3 Case Study Regarding Cyber Security Awareness Trainings

This subsection addresses a case study regarding the developed gamified cyber security awareness training. As such, participants of the training are questioned regarding the perceived effectiveness of the gamified training. In other words, to what extent the training successfully contributes to their cyber security awareness.  Since the results of the questionnaires will be used in an anonymized way, the actual filled-in questionnaires will not be provided in this thesis. Appendix E Questionnaires provides the blank pre-training and blank post-training questionnaires. The pre-training questionnaire is useful to make participants aware of their cyber security awareness and the results of the pre-training questionnaires can be used to establish a current state or baseline regarding the level of cyber security awareness among participants. Both the pre-training and post-training questionnaires comprise a series of open and five-point interval questions.

Several employees of Cyber Risk Services from Deloitte are contacted in-person or via email for this case study. This includes people from the three underlying departments Strategy, Secure, and Vigilant & Resilient, from all job grades. As such, both new hires and experienced non-technical employees are contacted as possible participants for this case study. In the end, 16 employees are available for the case study. The participants are divided in two groups, each consisting of eight participants.  The division is based on creating two groups that are as similar as possible; a mixture of gender, age, experience, and function. While under observation, each participant will fill in a pre-training questionnaire, participate in a cyber security awareness training, and fill in a post-training questionnaire. One group participates in the non-gamified, existing training and one in the training that is gamified following the designed framework. The application of the designed framework was initially illustrated by developing a gamified cyber security awareness training following this framework. A lot of useful information could be retrieved by getting participants to participate in this training and the existing training and to ask questions beforehand and afterwards. The averaged results of the five-point interval questions of the four different questionnaires can be regarded in Table 21. The 'pre' columns represent the participants their perceived current state of the KPIs. Next, the 'post' columns represent the participants' perception of how much the KPIs were affected by the training. The KPIs cyber security awareness and its constructs are explained to the participants when providing the questionnaires. The results regarding the existing training are discussed first, followed by the results regarding the gamified training.

The results of the pre-training questionnaire of the existing, non-gamified cyber security awareness training revealed that the level of cyber security awareness is scored fairly high on the five-point scale, namely 4.06 as presented in Table 21.

The results of the post-training questionnaire of the existing training showed that participants felt that the training did not severely affect their cyber security awareness level, i.e. 2.5 on a 5 point scale. This might be because this level already scored quite high on the pre-training questionnaire. It is interesting to note that the construct of cyber security awareness that received the lowest score on average, knowledge, is affected the most through the existing cyber security awareness training. Next, participation and interaction were scored below average (2.88 and 2.38 respectively) by the participants of the existing cyber security awareness training. Finally, only half of the participants would recommend the existing cyber security awareness training. Note that the participants that would not recommend the training also gave the lowest average scores in general.

*Table 21 Averaged results of the four different questionnaires*

| | Existing training | | Gamified training | |
|---|---|---|---|---|
| | Pre | Post (effect) | Pre | Post (effect) |
| Cyber security awareness | 4.06 | 2.50 | 3.88 | 2.81 |
| Attitude | 4.13 | 2.25 | 4.00 | 2.75 |
| Knowledge | 3.38 | 2.50 | 3.56 | 2.63 |
| Skills | 3.63 | 2.25 | 3.69 | 2.25 |
| Actions | 4.00 | 2.00 | 4.06 | 2.63 |
| Participation | - | 2.88 | - | 3.88 |
| Interaction | - | 2.38 | - | 4.13 |

The results of the pre-training questionnaire of the gamified cyber security awareness training illustrate that participants ranked the actions and attitude constructs the highest of the four constructs, 4.06 and 4.00 respectively. Again, as was the case with the results of the pre-training questionnaire of the existing cyber security awareness training, knowledge is the construct that received the lowest score on average, followed by skills. The results of the pre-training questionnaires of the existing and the gamified training revealed that the key topics expected to be touched upon were malware and phishing. Interestingly, this aligns with the content of both trainings as discussed in sections 7.1 and 7.2.

The results of the post-training questionnaire of the gamified training show that, similar as the results of the post-training questionnaire of the existing training, affecting the cyber security awareness level of participants received the highest score. When comparing the rest of the results with the results of the post-training questionnaire of the existing training, it shows that every aspect received a higher score in the gamified training, with skills receiving an equal score. However, the order of cyber security awareness and its constructs differ when comparing the results of the after-training questionnaires of both the existing and gamified training. It is interesting to see that the construct with the second highest score of the pre-training questionnaire of the gamified training, attitude, is also the construct that is perceived to be the most affected by the gamified training. The scores of both participation and interaction also scored well above average, 3.8 and 4.1 respectively, which is higher than the average scores of these aspects from the existing training.

The average scores per aspect suggest that the gamified training outperforms the existing non-gamified training. The question is whether the scores of the gamified training are significantly higher than the scores of the existing training. A t-test can be applied to evaluate the significance of the higher scores. The null hypothesis $H_0$ is that the scores of the gamified training are samples from the score distribution of the existing training and that the gamified training results are not significantly higher than the non-gamified training results. The variance of the different aspects in existing and gamified training are comparable, so the t-test is applied assuming equal variances in the scoring results of the existing and gamified training. Since the t-test aims to test whether the gamified training outperforms the existing training, the t-test will be one-tailed. The chosen level of significance is 0.05. The t-test results are visualized in Table 22.

*Table 22 The p-values of the null hypothesis that the scores of the gamified training are samples from the score distribution of the non-gamified training*

| Perceived increased aspects | P-value |
|---|---|
| Cyber security awareness | 0.304 |
| Attitude | 0.203 |
| Knowledge | 0.422 |
| Skills | 0.500 |
| Actions | 0.098 |
| Participation | 0.096 |
| Interaction | *0.006* |

As can be seen from Table 22 the p-values of all aspects except for interaction are greater than the level of significance of 0.05. Thus, the $H_0$ hypothesis can only be rejected for the interaction aspect. This means that the results of the gamified training are not significantly increased with respect to the results of the existing training, except for interaction. The interaction of the gamified training is significantly increased compared to the interaction in the existing training. It should be noted that the lack of significance for the other categories may be partially explained by the small sample size (eight for both the gamified training and the non-gamified training). With a small sample size, differences in scores should be quite large in order to find a significant increase.

When analyzing the results of the questionnaires, the scores provided by one participant stood out. Also during the observations during gamified training, it seemed that this participant perceived the training differently when compared to other participants. For example, the participant commented in the post-questionnaire that (s)he 'expected a game and more fun'. It is presumed that the gamification elements from the training did not match the player type of this participant and hence that this participant was not motivated or engaged through the use of these elements. For example, there were no signs that the participant felt part of the storyline or understood the (logic behind) different puzzles or riddles of the training. This aligns with previous insights regarding the importance of aligning gamification elements with participant types. Due to the sample size of the groups, one set of strikingly low scores can have a tremendous effect on the conclusions that can be drawn from the case study. For this reason, the effect of excluding these differing results from this particular participant on the significance is regarded. Similar to previous analysis, a one-tailed t-test is performed to evaluate the significance. The null hypothesis $H_0$ is again that the scores of the gamified training are samples from the score distribution of the existing training and that the gamified training results are not significantly higher than the non-gamified training results. The chosen level of significance is again 0.05. The results of this t-test are visualized in Table 23. As can be seen in this table, the p-values of every aspect except for actions, participation, and interaction are greater than the significance level of 0.05. In other words, the $H_0$ hypotheses can be rejected for the actions, participation, and interaction aspects. This means that in this case the results of these aspects of the gamified training are significantly increased with respect to the results of the existing training. When comparing these results with the results from Table 22, there are three aspects (actions, participation, and interaction) that received significant increased results instead of one (interaction). In other words, both aspects that are closely related to promising benefits of gamification, participation and interaction, received significantly increased results. Next, one aspect of cyber security awareness, the actions construct, received significantly increased results. In the end, excluding the results of the differing questionnaire produced more significantly increased results, among which an aspect directly related to cyber security awareness.

*Table 23 P-value of the null hypothesis with exclusion of the results of one selected participant*

| **Perceived increased aspects** | **P-value** |
|---|---|
| Cyber security awareness | 0.170 |
| Attitude | 0.171 |
| Knowledge | 0.288 |
| Skills | 0.369 |
| Actions | *0.033* |
| Participation | *0.024* |
| Interaction | *0.000* |

The gamified training is perceived better at some additional aspects next to the aspects as illustrated in Table 22 and Table 23. For example, participants mentioned that the gamified training guided them effectively through the content. This contrasts with notions regarding improving the effectiveness of the existing training, e.g. statements of too much content and questions that did not reflect this (amount of) content. Next, the existing training faced some comments regarding the balance between fear and what to do as a user. Since the gamified training shed light on both the hacker side and the defender side, this balance might be improved. Finally, as was the case with the post-training questionnaire results of the existing training, the participants of the gamified training who would not recommend the training provided the lowest average scores in general. Interestingly, in case of the gamified training, 6 out of 8 participants would recommend the training, compared to 4 participants of the existing training.

This section illustrated the usability of the designed framework and the perceived effectiveness of an application of the designed framework through an empirical study. It can be presumed from analyzing the results of the questionnaires that the gamification of the existing cyber security awareness training had different effects on the participants. This can be explained by the difference in the participants' expectations of the gamified training. Overall, the gamification of the training was successful and resulted in increased perceived cyber security awareness constructs compared to the existing training, although not significant when taking all participants into account. When the remarkably low scores of a selected participant were excluded, the gamification resulted in a significant perceived increase in the actions construct of cyber security awareness when compared to the existing training.

# 8. Conclusions

In this section, conclusions will be drawn from this thesis. The conclusions will be structured per research question as stated in the title of each of the following subsections. Subsequently, an overall conclusion will be provided.

## 8.1 What constitutes and influences cyber security awareness?

Cyber security awareness is explained as constituted and influenced through capability, behavior, and contextual factors. Here, constructs are described as characteristics that constitute and influence aspects of cyber security awareness. As such, capability consists of the constructs knowledge and skills. Next, behavior consists of the constructs actions and attitude. Next to constructs, contextual factors could encompass many types of factors, for example individual, organizational or intervention factors (Parsons et al., 2017). The relations between the different constructs of cyber security awareness and the contextual factors are visualized in a newly developed cyber security awareness constructs model. The model can be used to effectively raise cyber security awareness.

Several training techniques exists that aim to raise cyber security awareness by affecting its constructs. Examples of such trainings techniques are presentations, classroom courses, webinars, and e-learnings (Deloitte, 2018b). Raising awareness is no easy task; many of the discussed training techniques fail to effectively achieve an increase in all appropriate cyber security awareness constructs. An effective way to achieve this is to tailor the training to the participants and to provide information that is relevant for the participants. Next, participants should feel engaged for the training to have an effect on the constructs of cyber security awareness. A promising technique to stimulate participation, motivate and engage participants is gamification. As such, gamification provides the direction for this research into its possibilities for raising cyber security awareness.

## 8.2 What gamification concepts are applicable to cyber security awareness trainings?

Gamification is a promising technique for education and training purposes (Burke, 2016). Several generic frameworks that regard gamification concepts for training purposes have been developed. First, the Octalysis framework addresses eight motivational drives (Chou, 2015). This framework shows the importance of possible underlying motivations of potential participants of a gamified training. The framework is rather abstract regarding concrete gamification concepts. Next, the mechanics, dynamics, aesthetics (MDA) framework and its components provides a different perspective and adds value by providing instances of specific gamification concepts (da Rocha Seixas et al., 2016; Zichermann & Cunningham, 2011). This framework received some criticism from several gamification researchers, which has been adjusted in the mechanics, dynamics, emotions (MDE) framework (Robson et al., 2015). An important difference between the MDA and MDE frameworks is that aspects from aesthetics might be more applicable to game settings, whereas emotions might be more applicable to gamified contexts. Next, emotions can also be related to motivational drives, for example as discussed in the Octalysis framework. Another framework, the player types and gamification framework, addresses several of the gamification concepts from the MDA and MDE framework and illustrates the relations to six specific player types. Also motivational factors are considered in this framework, which could be related to the Octalysis framework. Finally, the sustainable gamification design (SGD) model is one of the only models that regards ethical considerations of using gamification for education or training purposes. In the end, all discussed frameworks are compared and contrasted which resulted in an overview of 22 gamification concepts that are possibly applicable to gamified trainings. As such, this overview can be used for gamifying trainings.

When regarding the applicability of the gamification concepts to specifically cyber security awareness contexts, it became clear that many cyber security awareness trainings are serious games, which differs from gamification. There is little information regarding the applied gamification concepts in these cyber security awareness contexts. There are no reasons to assume that specific applications of gamification (other than cyber security awareness) are initially not applicable to a cyber security awareness context. Note that restricting to one type of gamification mechanics is discouraged in the context of cyber security awareness since different types of participants could experience particular gamification mechanics differently. Therefore, every cyber security awareness training requires a tailored approach regarding gamification mechanics. In conclusion, studies regarding different applications of gamification concepts suggest that leaderboards, badges/medals, points, quest/goal/mission and feedback are key gamification mechanisms.

## 8.3 What framework can be designed to gamify cyber security awareness trainings?

Answering this research question involves an analysis of important requirements extending the fields of gamification and cyber security awareness, an analysis of the process of gamification, and combining the derived insights with the results of previous research questions. Important requirements for the effectiveness of gamified trainings are time, content scope, flexibility, regular (re)evaluation, and repetition.

An example of an existing framework that describes the gamification process is the 6D framework (Werbach & Hunter, 2015). This framework consists of 6 chronological steps of applying gamification, each starting with the letter D. Interestingly, only the last step regards gamification concepts. The remainder of the steps of the 6D framework concern the intentions of the gamified environment. This aligns with previous paragraph that illustrated that there are several requirements extending the field of gamification that need to be taken into account before gamifying trainings. For example, it is important to distinguish the objectives of the gamified training in order for the gamification concepts to properly align with the purpose of the training. Such objectives can be related to constructs of cyber security awareness: knowledge, skills, attitude and actions. Another framework is the five-step approach of Huang & Soman. Insights from the previously described SGD framework (Raftopoulos, 2014), 6D framework and the five steps of Huang & Soman have been compared and combined with analyzed definitions of gamification into an initial structure of a framework for developing gamified cyber security awareness trainings.

The designed framework consists of four phases; fundamentals, blueprint, design, and evaluation. The first phase consists of the 'objectives' and 'context' steps. The blueprint phase consist of the 'structure' and 'resources' steps. Next, the design phase consists of the 'diverge', 'converge', and 'build' steps. Finally, the evaluation phase consists of an 'evaluate' step. From this phase, two feedback loops exist depending on whether the gamified training needs some adjustments or whether it is ready to roll-out. This framework is designed to guide developers of gamifying existing cyber security awareness trainings.

Since the designed framework is primarily based on theoretical insights, it was evaluated by performing expert interviews. The designed framework is adjusted based on derived insights from these interviews with Deloitte experts in the field of gamification and cyber security awareness. Key adjustments are the hierarchy of and the coherence between the different cyber security awareness aspects within each of the steps of the framework. Next, an explicit visualization of the interim results from each of the phases is provided in the adjusted framework. Also the feedback loops are visually adjusted to reflect possible points of entry. Besides, the 'improve' feedback loop is triggered after the build phase and the 're-evaluate' feedback loop is triggered after the adjusted 'training roll-out'. Finally, some cyber security awareness related content of the steps of the framework is added, shifted, adjusted or made more explicit based on expert consultation.

## 8.4 What is the perceived effectiveness of an application of the designed framework?

Answering this question consists of two parts: firstly, using the designed framework to gamify an existing cyber security awareness training and secondly, by analyzing and comparing the experienced cyber security awareness changes of the participants of the existing and the gamified training.

One of the cyber security awareness trainings from Deloitte was selected for gamification. The selection was established based on the duration of the cyber security awareness training, the scale and scope of covered cyber security awareness topics, prerequisites of the training, the target group of the training, and the generalizability of the training. The selected training is the online course CSPNTOE 101 Cyber Security Awareness. This one-hour training is targeted to relatively non-technical employees and consists of three parts. Each part ends with a short test and after successfully completing the three tests and a survey participants get a certificate. The training was executed and analyzed in order to derive cyber security awareness content for the purpose of developing a gamified cyber security awareness training with the designed framework.

Based on the analysis of the selected cyber security awareness training, a gamified cyber security awareness training is developed to assess the usability of the designed framework. The previously evaluated and adjusted framework is used for this purpose. Note that the majority of the derived content of the CSPNTOE 101 training is not modified for comparison purposes of the case study. The process of applying gamification to the CSPNTOE 101 training towards a gamified cyber security awareness training demonstrates the usability of the designed framework.

The second part of answering the question regarding the perceived effectiveness of the gamified training involved a case study regarding the gamified training and the existing CSPNTOE 101 training. Eight participants executed the CSPNTOE 101 training and eight participants executed the gamified cyber security awareness training. Each participant filled in a pre-training questionnaire and a post-training questionnaire. The questionnaires contain questions regarding perceived awareness (change) and perceived change in terms of the four KPIs: skills, knowledge, actions and attitude. The average score of each of the KPIs was higher in the gamified training, except for the skills KPI which receives an equal score. Next, both participation and interaction received a higher average score regarding the gamified training compared to the existing training. Finally, 75% of the participants of the gamified training would recommend the training, compared to 50% of the participants of the existing training.

A one-tailed t-test is applied in order to evaluate whether the scores of the gamified training are significantly higher than the scores of the existing training. The null hypothesis is that the scores of the gamified training are samples from the score distribution of the existing training and that the gamified training results are not significantly higher than the non-gamified training results. The $H_0$ hypothesis was only rejected for the interaction aspect. This means that the interaction results of the gamified training are significantly increased with respect to the results of the existing training. Since the scores provided by one of the participants differed greatly when compared to the other participants, the effect of excluding the scores of this participant on the significance of the evaluated aspects is assessed. A one-tailed t-test with the same null hypothesis as discussed previously illustrated that it was rejected for the actions, participation, and interaction aspects. In other words, excluding the differing results of one of the participants illustrated three aspects (actions, participation, and interaction) that received significant increased results instead of one (interaction) when including these results. In sum, both participation and interaction as related to gamification received significantly increased results. Next, the actions aspect of cyber security awareness received significantly increased results. The difference in perceived effectiveness for the gamified training can partially be explained by the expectations of the participant, who expected something like a serious game.

In the end, combining the conclusions provides an answer to the main research question of this thesis: *how can gamification be applied to a training context that aims to affect cyber security awareness?* Answering this question involved establishing the constructs of cyber security awareness – knowledge, skills, actions, and attitude – and contextual factors. Next, different gamification concepts and their interrelations were analyzed, e.g. player types, motivations, game mechanics, and the process of gamification. These insights were combined with the insights regarding cyber security awareness in order to design a framework for gamifying cyber security awareness trainings. An empirical study was performed by using the designed framework to develop a gamified cyber security awareness training. Next, 16 persons participated in the existing and gamified training and the results suggest that the gamified training resulted in higher experienced increase in cyber security awareness than the existing training. This implies that the application of gamification can be regarded as successful in this case. In the end, the framework was evaluated and it is a successful tool for applying gamification to a training context aimed to affect cyber security awareness.

# 9. Discussion

This section provides a discussion on the performed research and the resulting thesis. The first subsection addresses implications of this research on societal and scientific fields. Next, potential limitations of this research will be addressed. Finally, recommendations for future research will be provided in the last subsection.

## 9.1 Implications of Research

Possible implications of the performed research are addressed in this section. First, scientific implications are addressed. Next, societal implications will be discussed.

### 9.1.1 Scientific Implications

This research provides several scientific contributions. First of all, this thesis provides a new model of distinct constructs that constitute cyber security awareness. This contributes to the field of science due to new insights into the relations between the different constructs, the aspects behavior and capability, and the relation with cyber security awareness. The implication of this research result, among others, is that it provides a new starting point for empirical research. For example, what is the impact of an increase of a specific construct on the level of cyber security awareness?

This thesis also contributed an overview of gamification concepts applicable to cyber security awareness contexts. An implication that results from this contribution is that it aids future research into the field of gamification and cyber security awareness contexts. For example, research that focuses on the impact of particular gamification elements on raising cyber security awareness.

Thirdly, this research provided an evaluated framework for developing gamified cyber security awareness trainings. This framework contributes to scientific and applied research due to new insights regarding the hierarchy and coherence between several cyber security awareness aspects and different steps of the gamification process. Next, the framework can be applied to several types of trainings or be generalized to fit awareness trainings in general.

### 9.1.2 Societal Implications

The four constructs – knowledge, skills, attitude and actions – that can be affected to influence cyber security awareness as developed in this research have societal implications as well. For example, these constructs can be used as KPIs by organizations aimed to raise the cyber security awareness of their employees. Next, specific trainings or messages regarding cyber security awareness can be tailored to affect specific constructs of cyber security awareness.

The contributed overview of gamification concepts as applicable to cyber security awareness trainings also provide value to society. For example, this overview could be used by organizations to identify possible combinations for a gamified cyber security awareness context. In this sense, the overview provides valuable input for brainstorms and discussions regarding feasible options to gamify an existing cyber security awareness context.

Finally, organizations can use the framework to guide the development of their own gamified cyber security awareness trainings. Furthermore, the usability of the framework in a practical gamification of an existing training was demonstrated. Next, organizations could also develop their own, tailored version of the framework to reflect their own cyber security awareness policies, services or priorities.

## 9.2 Limitations

There are several limitations that can be distinguished from performing this research.

During the process of answering the first two research questions, various literary sources were regarded that concern cyber security awareness and gamification. However, due to the fact that research in these fields is rather preliminary, the amount of literature that is appropriate for answering the research questions is limited. This resulted in the use of few journal papers next to the use of literary sources like white papers, conference papers, and dissertations. Consulting such sources might affect the results or the drawn conclusions from this research.

Next to the inclusion of several types of literary sources, drawing conclusions that are solely based on theoretical works while working towards a practical case study of applying gamification might have unanticipated effects. For example, due to the fact that both gamification and cyber security are fast-paced fields, theory that concern these topics might not adequately reflect current trends or practices. In turn, it might affect the appropriateness of the framework or the gamified cyber security awareness trainings that result from its application.

Regarding the researched gamification concepts as applicable to cyber security awareness trainings, there are assumptions that might need to be validated. For example, to what extent is every of the identified gamification concepts equally applicable to any type of cyber security awareness training? In other words, some gamification concepts might be more appropriate for cyber security awareness e-learnings while other gamification concepts might be more appropriate in an 'offline' setting.

Regarding the designed framework, it should be noted that it is a simplified overview of the actual process of gamifying cyber security awareness trainings. For example, some of the illustrated steps might be executed in parallel instead of sequential. Next, some phases might occur more than once, for example when iterations occur in the design phase of the gamification process. Such aspects regarding the sequence of steps and possible feedback loops are simplified in the framework to provide a clear overview of the process in order to guide the developers of the gamified cyber security awareness training. However, these simplifications and assumptions as visualized in the framework could have unforeseen effects on the use of the framework. In other words, the visualization itself might (over)simplify the gamification process and therefore might pose additional limitations to this research.

The methodology of evaluating the designed framework by expert interviews contains additional limitations of this research. For one, the proposed framework design might limit the creativity or the experts' perspective on how to approach the gamification process.  For example, the framework might have turned out differently when developing the framework from scratch with these experts or their consult. Furthermore, the framework was also adjusted based on the feedback of the experts. The adjusted framework has not been extensively evaluated in its current form.

The executed application of gamification to an existing cyber security awareness training also poses some limitations. For example, due to time constraints of this thesis project, the gamification process might not be executed as extensively as possible. For example, in this research, only one of the existing trainings was gamified using the evaluated framework. The illustration of the usability of the framework is therefore only based on one gamification instance and the drawn conclusions could be different for other gamification instances or for other types of gamification. For example, the usability of the framework has not been illustrated for online gamified trainings.

For the purpose of a sharp comparison of the two groups of participants for the existing and the gamified training, both trainings should be as equal as possible. In other words, as many variables and parameter should be equal in both settings with variety in the ones under investigation. In this case, the variables for research are related to the application of gamification concepts. However, additional variables and parameters differed in the existing and gamified setting. First of all, the existing training is provided in a digital, online format. This differs from the paper-based, tabletop gamified cyber security awareness training. Next, the gamified training was executed by duos, while the existing training is targeted at individual participation. This might affect the results from the questionnaires since the participants of the gamified training might influence each other. Finally, some participants might have differed from the target group as stated in the existing training. For example due to their experience with cyber security awareness or for being more technical than 'non-technical'. Next to the possible differences, the content of the trainings was kept as equal as possible, since this was no variable up for investigation. This means that, despites selecting some topics and adding questions based on the existing content to the gamified training, no content was severely adjusted. However, a possible limitation from this is the fact that content might not be of adequate quality or might not be up to date. Using this content as a starting point for a gamified cyber security awareness training might result in an unsatisfactory training. This is a limitation of using the methodology of a comparative case study for the purpose of illustrating the usability of the framework. In practice, there would be more freedom to adjust content, for this is also regarded within several steps of the framework. Finally, the number of participants of the existing and the gamified training might be a limitation of this research. With an increased number of participants, an extrapolation or generalization of the results is more reliable. Next, with an increased number of participants, the null hypothesis would more likely be rejected. Finally, the case study only regarded the perceived effectiveness of the trainings, this might differ from the actual effectiveness of the training. In other words, not measuring the actual effectiveness of the trainings or comparing the actual effectiveness with the perceived effectiveness of the trainings might be a limitation of this research.

## 9.3 Future Research

Based on the performed research, its implications, and the addressed limitations, recommendations for future research can be formulated. First of all, research can quantify the influence of the constructs knowledge, skills, attitude and actions on cyber security awareness within the cyber security awareness model. For example, the influence of contextual factors on specific constructs can be researched through performing a case study. Next, there might be additional factors or interactions that were neglected in this research that need to be taken into account in order to provide a complete overview of cyber security awareness.

Regarding the overview of gamification concepts as applicable to cyber security awareness contexts, future research can concern the applicability of specific gamification concepts in specific training settings. For example, some gamification concepts might be more applicable to online competitive environments, whereas other concepts might be more applicable in offline cooperative environments. Next, the effects of particular gamification concepts on raising specific constructs of cyber security awareness or cyber security awareness in general can be assessed by implementing different gamification mechanics in a particular training.

Next, the evaluated designed framework provides an interesting starting point for further research. Research could focus on tailoring this framework to fit specific topics of cyber security awareness. Additionally, a new or extended version of the framework could be developed. Besides, frameworks can be (quantitatively) compared to the framework as designed in this research by means of (multiple) gamifications of the same training with the different frameworks and measuring the (perceived) effectiveness of both gamified trainings.

Future research can also extend current research by applying the framework in a longer time frame, in different settings, with different player types, larger groups of respondents. For example, comparing different applications of the framework to the same existing cyber security awareness training might led to interesting insights regarding the effectiveness of affecting knowledge, skills, attitude, and actions concerning cyber security awareness. Next, future research could also regard the actual increased effectiveness due to gamification instead of the perceived increased effectiveness due to gamification. For example by comparing the response rates of a phishing test of the two groups of participants; the group that participated in the existing training and the group that participated in the gamified training.

Finally, future research could regard the effect of different cultures or organizational cultures on the designed framework. In turn, such cultures might also affect the resulting gamified trainings as developed following the designed framework.

# 10. Reflection

This section provides a reflection on the performed research; the project, the process, and the product. Next, subsection 10.4 regards a reflection on this thesis concerning CoSEM, the I&C track and the Cyber Security specialization.

## 10.1 Project

One of the first choices regarding this thesis project is to carry it out at an external organization. I am very happy with the opportunity I got to do this project at Deloitte. This provided a nice balance between theory and practice by combining university and organization. During this thesis project I made additional choices, decisions and assumptions due to the interaction and feedback from my supervisors and Deloitte gamification and cyber security awareness experts.

By performing extensive literature studies in order to grasp the topics of gamification and cyber security awareness, little practical insights were derived during the earlier phases of this thesis project. In later phases of this project, this balance was restored by incorporating expert views and performing a case study. However, one might be left to wonder if earlier inclusion of practical insights might have resulted in a different set-up or different results, for example regarding the framework or the case study.

Many choices and decisions were made while regarding the triangle of time, cost, and scope and quality. In this sense, the time aspect was often the binding factor, due to the duration of this thesis project. However, since I was aiming for high quality, in several phases of this thesis project I made time for this project e.g. by making it a priority during evenings, weekends and holidays. Next, sometimes the scope was adjusted to provide the desired quality given the available time. In the end, I am pleased with the choice for this project regarding gamification and cyber security awareness. I am still really interested in the possibilities of combining these fields and I am looking forward to continue to do projects regarding either one of these field or a combination of these fields.

## 10.2 Process

During the entirety of writing my thesis, I was doing this project at Deloitte. This provided a unique opportunity to see the applicability of the knowledge and insights derived during the CoSEM master in practice. Next, several gamification and cyber security awareness experts were in close proximity and were very helpful to aid me in various aspects for my thesis. In general, the process of this project turned was quite good; I managed to stick to the planning without making severe adjustments to either the planning or the project.

Several of the major adjustments to the process of this thesis resulted from the mid-term meeting. At this stage I had completed roughly three out of four research questions. However, for the purpose of achieving a more comprehensive thesis, I decided to stretch the scope of my project for the few weeks to come. As a result, the planning was significantly adjusted to incorporate practical insights regarding expert interviews, a gamification design, and an empirical study to check the usability of the theoretical framework and the perceived effectiveness of the resulting gamified training. Despite the ambitious planning and the risks associated with such a planning, the process of this project continued rather smooth. I am glad that I decided for such a turnaround and stepped-up for this challenge. It was hard work to keep up the pace, but it made the thesis project more of a whole than if I decided to continue on the current direction. I am really thankful for my supervisors who thought along with me for achieving this.

## 10.3 Product

This thesis project resulted in several deliverables besides this thesis as a whole. First of all, a model of cyber security awareness was developed which includes several constructs of cyber security awareness and contextual factors. The model provides a simplified overview of key aspects of cyber security awareness and how they relate. I am glad that I managed to develop this model and curious for what future research could bring regarding this model, its relations, or quantitative conclusions.

The part of this research that concerned gamification concepts as applicable to cyber security awareness resulted in an overview that was very helpful for the remainder of this thesis. For example, during the development of a gamified cyber security awareness based on applying the theoretical framework these gamification concepts were regarded. In addition to this, the overview of gamification concepts provides various directions for future research as discussed previously, so I am glad I could make this contribution.

The evaluated framework provides an additional crucial product of this thesis project. It provides a guide for future developers of gamified cyber security awareness trainings and a starting point for future research. Incorporating practical experience and insights from Deloitte experts and combining it with the theoretical knowledge from extensive literature studies into this framework was a valuable learning project. Developing and testing an actual gamified cyber security awareness training adds to this experience. The resulting gamified cyber security awareness training is a nice additional product as well. I really enjoyed experiencing the balance between theory and practice.

## 10.4 Within Curriculum

The master of Complex Systems Engineering and Management focusses on designing solutions that address large and complex socio-technical challenges for organizations. In this way, technical, institutional, economic, and social perspectives play a role when developing such solutions. A major topic of this thesis is cyber security awareness; in general this consists of socio-technical aspects due to the human factor and its relations with technical systems and technology. Bringing gamification into the equation in order to impact the effects of trainings for raising cyber security awareness extends the complexity and illustrates the multidisciplinary character of this thesis project. Finally, the Information and Communication track and the Cyber Security specialization are well represented in this thesis due to the focus on human (inter)actions with ICT and the possible impact on cyber security as a whole. Next, the track and specialization provided a valuable foundation of knowledge, insights and skills to start analyzing the field of cyber security awareness and gamification.

During this thesis, inter alia a framework was designed for guiding developers during the process of gamifying cyber security awareness trainings. This project has several managerial consequences when the designed framework gets applied into practice, for example regarding policies and regulation of gamified cyber security awareness trainings. For the duration of this thesis project, such managerial strategies were out of scope but they illustrate the extent of possible solutions like the designed framework. Besides, applying the designed framework in practice calls for ethical considerations inter alia due to the choices of gamification techniques and their impact. In sum, cyber security awareness and gamification were intertwined topics during this thesis which increased the complexity of the project but made it extremely interesting and valuable for both science and society at the same time.

## Bibliography

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

Alberts, K., & Findlay, K. (2011). Gamification: How Effective Is It? Retrieved from http://www.slideshare.net/ervler/gamification-how-effective-is-it

Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2016). A Review of Using Gaming Technology for Cyber-Security Awareness.

Aloul, F. (2012). The need for effective information security awareness. *Journal of Advances in Information Technology, 3*(3), 176-183.

Amorim, J. A., Hendrix, M., Andler, S. F., & Gustavsson, P. M. (2013). *Gamified training for cyber defence: Methods and automated tools for situation and threat assessment.* Paper presented at the NATO Modelling and Simulation Group (MSG) Annual Conference 2013 (MSG-111), 2013.

Anderson, K. (2013). Can we make security awareness training stickier? *ISSA Journal (January 2013)*, 10-15.

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.

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior, 38*, 304-312.

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

Bakker, H., & Buijs, J. (1979). Systematisch probleem oplossen. *TU Delft.*

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.

Blaga, A. (2014). What is the difference between competencies and behaviors when establishing performance criteria? Retrieved from http://www.performancemagazine.org/what-is-the-difference-between-competencies-and-behaviors-when-establishing-performance-criteria/

Boopathi, K., Sreejith, S., & Bithin, A. (2015). Learning Cyber Security Through Gamification. *Indian Journal of Science and Technology, 8*(7), 642-649.

Bowser, A., Hansen, D., Preece, J., He, Y., Boston, C., & Hammock, J. (2014). *Gamifying citizen science: a study of two user groups.* Paper presented at the Proceedings of the companion publication of the 17th ACM conference on Computer supported cooperative work & social computing.

Breuer, J. S., & Bente, G. (2010). Why so serious? On the relation of serious games and learning. *Eludamos. Journal for computer game culture, 4*(1), 7-24.

Buchanan, L., Wolanczyk, F., & Zinghini, F. (2011). *Blending Bloom's taxonomy and serious game design.* Paper presented at the Proceedings of the 2011 International Conference on Security and Management (July 2011), SAM.

Buith, J. (2016). Cyber Value at Risk in the Netherlands. Retrieved from https://www.thehaguesecuritydelta.com/images/deloitte-nl-risk-cyber-value-at-Risk-in-the-Netherlands.pdf

Burke, B. (2016). *Gamify: How gamification motivates people to do extraordinary things*: Routledge.

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.* Paper presented at the HAISA.

Cambridge_Dictionary. (2018). Attitude. Retrieved from https://dictionary.cambridge.org/dictionary/english/attitude

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

Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A video game for cyber security training and awareness. *Computers & Security, 26*(1), 63-72.

CSY. (2018). Wat is Cybersave Yourself? Retrieved from https://www.cybersaveyourself.nl/

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.

Daud, R., Sazilah, S., Siti, N., & Azizul, M. (2016). *Modelling a Mobile Gamification Model to Increase Student Engagement: An Analysis using Analytic Hierarchy Process.* Paper presented at the Proceedings of 2nd Asia International Conference.

De-Marcos, L., Garcia-Cabot, A., & Garcia-Lopez, E. (2017). Towards the Social Gamification of e-Learning: a Practical Experiment. *INTERNATIONAL JOURNAL OF ENGINEERING EDUCATION, 33*(1), 66-73.

Deloitte. (2018a). CSPNTOE 101 Cyber Security Awareness.

Deloitte. (2018b). Cursusaanbod Deloitte Academy. Retrieved from https://www2.deloitte.com/nl/nl/pages/academy/articles/cursusaanbod-deloitte-academy.html

Deterding, S. (2014). Eudaimonic design, or: Six invitations to rethink gamification. *Rethinking Gamification*, 305–323.

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

Dodge, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. *Computers & Security, 26*(1), 73-80.

Drevin, L., Kruger, H. A., & Steyn, T. (2007). Value-focused assessment of ICT security awareness in an academic environment. *Computers & Security, 26*(1), 36-43.

Evangelopoulou, M., & Johnson, C. W. (2015). *Empirical framework for situation awareness measurement techniques in network defense.* Paper presented at the Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 2015 International Conference on.

Fouché, S., & Mangle, A. H. (2015). *Code hunt as platform for gamification of cybersecurity training.* Paper presented at the Proceedings of the 1st International Workshop on Code Hunt Workshop on Educational Software Engineering.

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

Fu, Y. C. (2011). The game of life: Designing a gamification system to increase current volunteer participation and retention in volunteer-based nonprofit organizations. *Undergraduate Student Research Awards, 2*.

Galba, T., Solic, K., & Lukic, I. (2015). An Information Security and Privacy Self-Assessment (ISPSA) Tool for Internet Users. *Acta Polytechnica Hungarica, 12*(7), 149-162.

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.* Paper presented at the System Sciences (HICSS), 2014 47th Hawaii International Conference on.

Hamzah, W., Ali, N. H., Saman, M., Yusoff, M. H., & Yacob, A. (2015). Influence of Gamification on Students' Motivation in using E-Learning Applications Based on the Motivational Design Model. *International Journal of Emerging Technologies in Learning, 10*(2).

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. *Research Report Series: Behavioural Economics in Action, Rotman School of Management, University of Toronto*, 1-29.

Huotari, K., & Hamari, J. (2012). *Defining gamification: a service marketing perspective.* Paper presented at the Proceeding of the 16th International Academic MindTrek Conference.

Iacovides, I., Jennett, C., Cornish-Trestrail, C., & Cox, A. L. (2013). *Do games attract or sustain engagement in citizen science?: a study of volunteer motivations.*

Paper presented at the CHI'13 Extended Abstracts on Human Factors in Computing Systems.

Identity_Games. (2018). Escape Room The Game. Retrieved from https://escaperoomthegame.com/nl-nl/

Jiemei, Z., Xuewei, F., Dongxia, W., & Lan, F. (2014). *Implemention of Cyber Security Situation Awareness Based on Knowledge Discovery with Trusted Computer.* Paper presented at the Asia-Pacific Web Conference.

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.* Paper presented at the 2012 IEEE International Conference on Technology Enhanced Education (ICTEE).

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?* Paper presented at the Management of Engineering and Technology (PICMET), 2015 Portland International Conference on.

Khattak, Z. A., Manan, J.-l. A., & Sulaiman, S. (2011). Analysis of open environment sign-in schemes-privacy enhanced & trustworthy approach. *Journal of Advances in Information Technology, 2*(2), 109-121.

Khidzir, N. Z., Ismail, A. R., Daud, K. A. M., Ghani, M. S. A. A., Ismail, S., & Ibrahim, A. H. (2016). Human Factor of Online Social Media Cybersecurity Risk Impact on Critical National Information Infrastructure. In *Advances in Human Factors in Cybersecurity* (pp. 195-207): Springer.

Kokkonen, T. (2016). *Architecture for the Cyber Security Situational Awareness System.* Paper presented at the International Conference on Next Generation Wired/Wireless Networking.

Korolov, M. (2012). Gamification of the Enterprise. *Network World, 9*(2012), 31-33.

Landsell, J., & Hägglund, E. (2016). *Towards a Gamification Framework: Limitations and opportunities when gamifying business processes.* (Master Thesis), Institutionen för informatik, Umeå University.

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems, 11*(7), 394.

Lohrmann, D. (2014). Ten Recommendations for Security Awareness Programs. Retrieved from Government Technology website: 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*. Retrieved from http://www.securementem.com/wp-content/uploads/2013/07/Habits_white_paper.pdf

Marczewski, A. C. (2013). *Gamification: a simple introduction*: Andrzej Marczewski.

Marczewski, A. C. (2015). *Even Ninja Monkeys Like to Play: Gamification, Game Thinking and Motivational Design*: CreateSpace Independent Publishing Platform.

Margalit, O. (2016). *Using Computer Programming Competition for Cyber Education.* Paper presented at the 2016 IEEE International Conference on Software Science, Technology and Engineering (SWSTE).

McCoy, C., & Fowler, R. T. (2004). *You are the key to security: establishing a successful security awareness program.* Paper presented at the Proceedings of the 32nd annual ACM SIGUCCS conference on User services.

McGonigal, J. (2011). *Reality is broken: Why games make us better and how they can change the world*: Penguin.

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

Meadows, R. (2016). ISACA Offers Guidance, Training Tools During Cyber Security Awareness Month. Retrieved from http://www.isaca.org/About-ISACA/Press-room/News-Releases/2016/Pages/ISACA-Offers-Guidance-Training-Tools-During-Cyber-Security-Awareness-Month.aspx

Mindgame. (2018). Activating People. Retrieved from https://mindgame.eu/

Mohamad, S. N. M., Salam, S., & Bakar, N. (2017). *An Analysis Of Gamification Elements In Online Learning To Enhance Learning Engagement.* Paper presented at the Proceedings of the 6th International Conference on Computing & Informatics (ICOCI 2017).

Moore, T. J., & Asay, S. M. (2017). *Family resource management*: Sage Publications.

Näckros, K. (2002). Empowering users to become effective information security and privacy managers in the digital world through computer games. In: Sociable Media Group (MIT).

Nagarajan, A., Allbeck, J. M., Sood, A., & Janssen, T. L. (2012). *Exploring game design for cybersecurity training.* Paper presented at the 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems.

Navarro, L. (2007). Train employees-your best defense-for security awareness. *SC Magazine Online*.

Noell, A. (2017). Security Awareness Learning Academy. Retrieved from https://wt.deloitteresources.com/gs/sa_learning_academy/Pages/Home.aspx

NOS. (2017a). Loterijen melden lek in bestand deelnemersgegevens. Retrieved from https://www.nos.nl/artikel/2166299-loterijen-melden-lek-in-bestand-deelnemersgegevens.html

NOS. (2017b). Rekenkamer Rotterdam: systeem gemeente zo lek als een mandje.

Oever, R. v. d. (2015). Zo makkelijk kan het fout gaan: 4 nieuwe voorbeelden van hacken. Retrieved from https://www.mt.nl/dossiers/zo-makkelijk-kan-het-fout-gaan-4-nieuwe-voorbeelden-van-hacken/88200

Oreskes, N., Shrader-Frechette, K., & Belitz, K. (1994). Verification, validation, and confirmation of numerical models in the earth sciences. *Science, 263*(5147), 641-646.

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 from https://www.trainingindustry.com/content-development/articles/how-gamification-is-changing-employee-training.aspx

Pesare, E., Roselli, T., Corriero, N., & Rossano, V. (2016). Game-based learning and Gamification to promote engagement and motivation in medical learning contexts. *Smart Learning Environments, 3*(1), 1-21.

Prestopnik, N., Crowston, K., & Wang, J. (2017). Gamers, citizen scientists, and data: Exploring participant contributions in two games with a purpose. *Computers in Human Behavior, 68*, 254-268.

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.

Ramakrishnan, S., & Testani, M. (2011). People, Process, Technology—The Three Elements for a Successful Organizational Transformation. *IBM Path Forward to Business Transformation. IBM Centre for Learning and Development*, 1-21.

Raman, R., Lal, A., & Achuthan, K. (2014). *Serious Games based approach to cyber security concept learning: Indian context.* Paper presented at the Green Computing Communication and Electrical Engineering (ICGCCEE), 2014 International Conference on.

Rieff, I. (2017). *Benefits and Challenges of Applying Gamification in Cyber Security*. Literature Review. Delft University of Technology.

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.

Robson, K., Plangger, K., Kietzmann, J. H., McCarthy, I., & Pitt, L. (2016). Game on: Engaging customers and employees through gamification. *Business horizons, 59*(1), 29-36.

Ruboczki, E. S. (2015). *How to develop cloud security awareness.* Paper presented at the 2015 IEEE 10th Jubilee International Symposium on Applied Computational Intelligence and Informatics (SACI).

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security, 56*, 70-82.

Sarter, N. B., & Woods, D. D. (2009). Situation awareness: A critical but ill-defined phenomenon. *The International Journal of Aviation Psychology, 1*(1), 45-57.

Schneier, B. (2015). *Secrets and lies: digital security in a networked world*: Wiley.

Schöbel, S., Söllner, M., & Mishra, A. N. (2017). Does the Winner Take it All? Towards an Understanding of why there might be no One-Size-Fits-All Gamification Design.

Schultz, E. (2005). The human factor in security. *Computers & Security, 24*(6), 425-426.

Sheahan, K. (2017). What Are the Advantages of Information Technology in Business? Retrieved from https://www.smallbusiness.chron.com/advantages-information-technology-business-774.html

SURFnet. (2018). Cybersave Yourself Toolkit. Retrieved from https://wiki.surfnet.nl/display/CSY/Cybersave+Yourself+Toolkit

Szantner, A. (2015). Massively Multiplayer Online Science. *Inter-Disciplinary.net*, pp. 1–6.

Thiel, S.-K. (2016a). *A Review of introducing Game Elements to e-Participation.* Paper presented at the Conference for E-Democracy and Open Government (CeDEM).

Thiel, S.-K. (2016b). *Reward-based vs. Social Gamification: Exploring Effectiveness of Gamefulness in Public Participation.* Paper presented at the Proceedings of the 9th Nordic Conference on Human-Computer Interaction.

Thiel, S.-K., & Lehner, U. (2015). *Exploring the effects of game elements in m-participation.* Paper presented at the Proceedings of the 2015 British HCI Conference.

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.

Underhay, L., Pretorius, A., & Ojo, S. (2016). *Game-based enabled e-learning model for e-Safety education.* Paper presented at the IST-Africa Week Conference, 2016.

Verizon. (2017). *2017 Data Breach Investigations Report (DBIR)* (10th ed.).

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97-102.

Voorst, S. v. (2016). Gestolen laptop veroorzaakt mogelijk datalek bij verschillende gemeenten. Retrieved from https://tweakers.net/nieuws/118607/gestolen-laptop-veroorzaakt-mogelijk-datalek-bij-verschillende-gemeenten.html

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.

Wheeler, P. (2017). The Human Factor Report. Retrieved from https://www.proofpoint.com/us/human-factor-2017

Whitman, M. E., & Mattord, H. J. (2011). *Principles of information security*: Cengage Learning.

Wilson, A., & Ali, A. (2011). The Biggest Threat to the US Digital Infrastructure: The Cyber Security Workforce Supply Chain. *Academy for Studies in Business, 3*(2), 15.

Wilson, M., & Hash, J. (2003). Building an information technology security awareness and training program. *NIST special publication, 800*(50), 1-39.

Wood, C. C., & Banks, W. W. (1993). Human error: an overlooked but significant information security problem. *Computers & Security, 12*(1), 51-60.

Yap, J. (2011). *Virtual fun and challenge: Case study of learning cybercrime in second life.* Paper presented at the Defense Science Research Conference and Expo (DSR), 2011.

Yusoff, A., M., Sazilah, S., Siti, N. M. M. & Daud, R. (2016). *Gamification element Through Massive Open Online Courses in TVET: An Analysis using Analytic Hierarchy Process.* Paper presented at the Proceedings of 2nd Asia International Conference.

Zichermann, G., & Cunningham, C. (2011). *Gamification by Design: Implementing Game Mechanics in Web and Mobile Apps*: O'Reilly Media, Inc.

Zichermann, G., & Linder, J. (2013). *The gamification revolution: How leaders leverage game mechanics to crush the competition*: McGraw Hill Professional.

# Appendices

This section of the thesis consists of the appendices. Appendix A provides the scientific article, as required for graduating CoSEM students. Note that this article is written using LaTeX and is also provided in a separate pdf-file. Please regard the pdf version for the proper layout of the article. Appendix B regards the expert interviews from evaluating the designed framework. Next, Appendix C addresses the basic instructions for the gamified cyber security awareness training. Appendix D considers the different parts of the gamified training. Next, Appendix E regards the blank pre-training and post-training questionnaires and their anonymized quantitative results.

## Appendix A Scientific Article

# 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 timeconsuming, 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 Aware-ness*

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 & Hagglund, 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 designscience 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 managementoriented 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 AwarenessTrainings*

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 Aware-ness 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

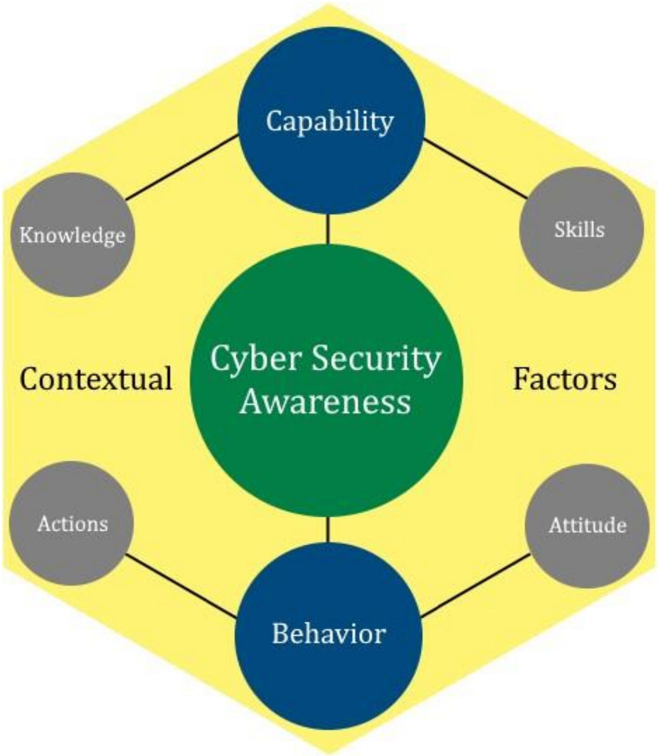


Fig. 1. Constructs of Cyber Security Awareness

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.

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.

TABLE I

OVERVIEW OF GAMIFICATION MECHANICS

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

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.

TABLE II

DISTILLED REQUIREMENTS TOWARDS A FRAMEWORK FOR GAMIFYING CYBER SECURITY AWARENESS TRAININGS

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

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.
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.
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.

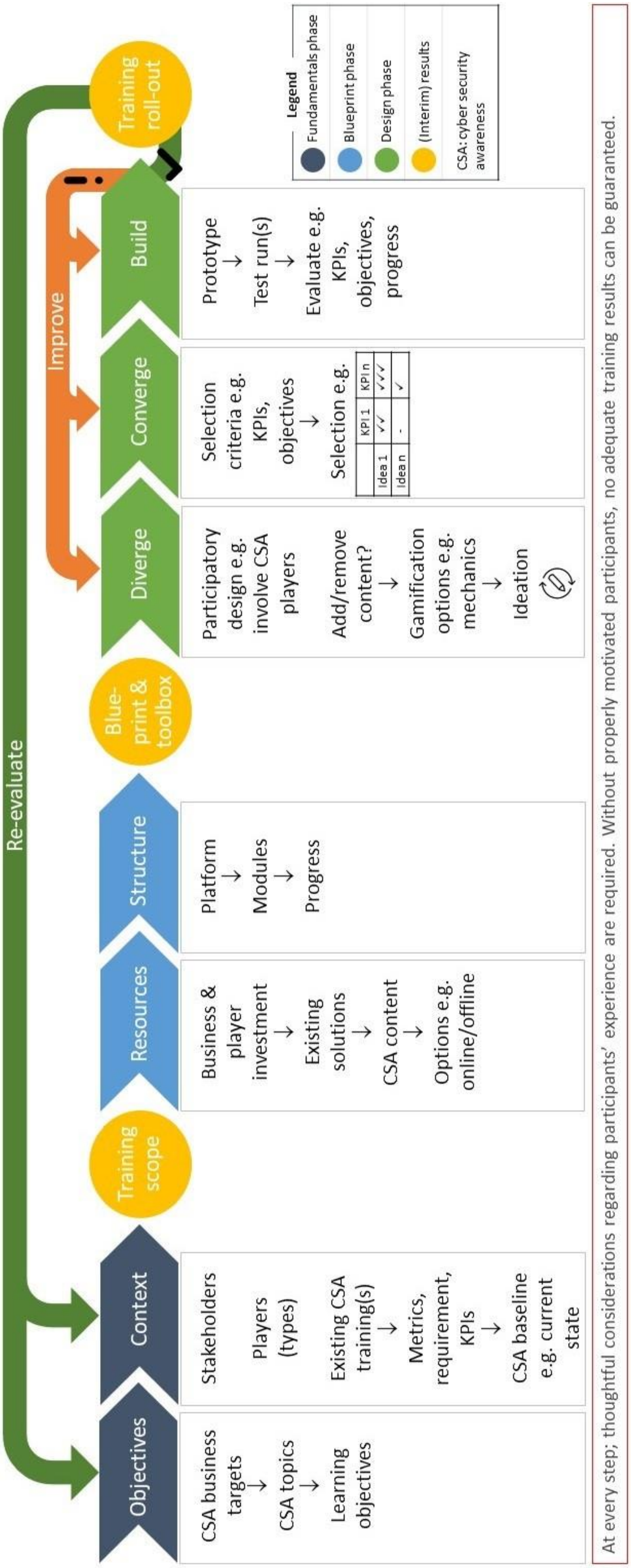

Re-evaluate
Improve
Objectives
CSA business targets → CSA topics → Learning objectives
Context
Stakeholders
Players (types)
Existing CSA training(s) → Metrics, requirement, KPIs → CSA baseline e.g. current state
Training scope
Resources
Business & player investment → Existing solutions → CSA content → Options e.g. online/offline
Structure
Platform → Modules → Progress
Blue-print & toolbox
Diverge
Participatory design e.g. involve CSA players
Add/remove content? → Gamification options e.g. mechanics → Ideation
Converge
Selection criteria e.g. KPIs, objectives → Selection e.g.
KPI 1
KPI n
Idea 1
✓✓
✓✓✓
Idea n
-
✓
Build
Prototype → Test run(s) → Evaluate e.g. KPIs, objectives, progress
Training roll-out
Legend
● Fundamentals phase
● Blueprint phase
● Design phase
● (Interim) results
CSA: cyber security awareness
At every step; thoughtful considerations regarding participants' experience are required. Without properly motivated participants, no adequate training results can be guaranteed.

Fig. 2. Framework

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 rolledout. 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 nongamified 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 framework 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 fullblown 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). Na¨ıve 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., & Hagglund, 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/wpcontent/uploads/2013/07/Ha bits 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 ddosaanval.* 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.”.

## Appendix B Expert Interviews

In this appendix, the elaboration of the expert interviews will be provided.

### Interview (1)

1. **How are you involved in the topic of cyber security awareness?**

In mijn rol als junior manager bij secure komt het onderwerp natuurlijk wel eens ter sprake. Zelf geef ik demo's en trainingen met betrekking tot dit topic, bijvoorbeeld rondom een hacker mindset.

2. **What are your experiences with gamification?**

Ik was onderdeel van het team rondom Malwopoly. Dit is een spel gebouwd om het technische concept assembly te illustreren. We zagen bij assembly gelijke kenmerken als bij het spel Monopoly. Zo zijn er bijvoorbeeld afwijkingen in de chronologie van een proces, een jump naar specifieke plekken, bijvoorbeeld onder bepaalde condities. Mede door deze gelijkenis heeft Malwopoly vorm gekregen; het simplistisch over proberen te brengen van een complexer concept.

3. **What are your experiences with the application of gamification in the context of cyber security awareness?**

Malwopoly is niet perse gebouwd rondom het thema awareness, het gaat meer in op technische concepten. Naast Malwopoly als voorbeeld van toegepaste gamification geef ik cursussen rondom malware. Vaak is zo een cursus is opgebouwd uit tracks. Iedere track sluit af met een aantal vragen. Bij de verplichte vragen is een leaderboard geïmplementeerd. Dit leaderboard is live te zien voor de deelnemers en de trainers. Aan de ene kant geeft dit de deelnemers een gevoel van competitie. Anderzijds geeft dit informatie aan de trainer bijvoorbeeld waar extra sturing nodig is. Naast dit verplichte onderdeel is er een stukje CTF (capture the flag). Dit vrijwillige onderdeel is beschikbaar zodra je klaar bent met een track. Hier kun je verdiepende vragen vinden of vragen rondom content die nog niet uitgelegd is. Dit komt vervolgens ook op het scorebord. Tijdens de cursus kijken we dus technisch gezien naar wat participanten begrijpen en kunnen, anderzijds wordt er ook gekeken naar hoe men omgaat met vragen of als er zaken niet worden begrepen. Bijvoorbeeld; stellen ze vragen aan de trainer, en hoe verloopt de samenwerking onderling.

4. **What are your recommendations towards applying gamification to cyber security awareness trainings?**

Vanuit Malwopoly vind ik dit erg lastig om te zeggen, aangezien ik niet persoonlijk dicht bij het design betrokken ben geweest. Zodoende kan ik je niet helpen aan lessons learned op dit gebied. Met betrekking tot de malware cursus, daar loop je wel eens tegen issues aan. Bijvoorbeeld, hoe ga je om als mensen niet goed presteren. Stel je voor dat iemand laag op het leaderboard staat. Dit zien trainers en die benaderen de persoon. Simpelweg; mensen die lager op het scorebord staan worden vaker benaderd door trainers. Dit kan iemand vervelend vinden en het gevaar is dat iemand daardoor gedemotiveerd kan raken. Een afweging hier zou zijn om als er met grote groepen wordt gewerkt, en er is een leaderboard geïmplementeerd, om slechts de top 5 best presterende participanten te laten zien.

**Framework introduction**

5. **What are your first impressions of the framework?**

Als ik zo de onderste zin lees, ben ik het niet zo eens met het fun aspect. Wat mij betreft hoeft fun niet perse, gamification kan ook dusdanig worden toegepast om iets simpeler te maken, niet perse leuk.

Bijvoorbeeld, Malwopoly is om op een simpelere manier iets complexers over te brengen. Desalniettemin vind ik het framework een gestructureerd uiterlijk hebben. Ik heb wel het idee dat ik eerst wat nadrukkelijker naar de stappen moet kunnen kijken voordat ik iets uitgebreid over het framework kan zeggen.

*This framework is to aid people in applying gamification to existing cyber security awareness trainings. It visualizes a four phased approach consisting of eight steps.*

**6. How does this information affect your impression of the framework?**

Wat me zou helpen bij dit framework is als je een voorbeeld van een toepassing ervan zou verstrekken. Voor de rest lijken de fases en stappen me duidelijk. Ik vraag me alleen af wat het verschil is tussen de resources stap en het design onderdeel van het framework. Wellicht is resources meer gebaseerd op het doel en design meer gericht op de oplossing. Daarnaast, ik zou zeggen dat je ook een evaluatieslag hebt voordat je naar de converge stap gaat. Ik zie het zo voor me dat je bij de diverge stap pros en cons opstelt per de (deel)oplossingen en deze bijvoorbeeld mapt naar fun, knowledge transfer of andere zaken die belangrijk blijken uit de objectives. Hier zou je nog low, medium, high of euro's aan kunnen koppelen om zo onderscheid te kunnen maken tussen de (deel)oplossingen. Op basis hiervan kun je uiteindelijk de beste of meest suitable selecteren.

**7. To what extent do you recognize these phases and steps (practical experience)?**

Ik denk dat de blueprint fase en design fase deels overlappen, of parallel aan elkaar gebeuren. Je kunt wel een blueprint maken en daarna pas gaan kijken wat er in de markt beschikbaar is, maar dan moet je wellicht weer terug naar je blueprint. Bij de resources stap zou ik suggereren dat je bandbreedtes bepaalt, zo zijn er meerdere waardes acceptabel. Deze waardes zijn uiteindelijk afhankelijk van de oplossing. Bij de diverge stap komen er verschillende oplossingen naar voren. Het zou ook kunnen dat bij de converge stap verschillende oplossingen samengevoegd worden. Hierbij is het belangrijk om in deze fase te kijken naar je objectives. Tenslotte herken ik modules, zoals beschreven in de structure stap, ook in Malwopoly waar verschillende chapters een rol spelen. Structure stel ik me dan ook zo voor dat je er achter komt dat je bepaalde zaken kunt combineren of juist opsplitsen.

**8. How can this phased approach be improved according to your expertise?**

Ik stel me zo voor dat als je een pilot hiermee draait je je framework kunt toetsen in de praktijk. Door dit te doen weet je of je framework werkt. Ten tweede heb je het voorbeeld waar ik al eerder naar refereerde; een voorbeeld van een toepassing van je framework. Daarnaast zie ik het voor me dat er nog een stap of iets anders plaatsvindt tussen diverge en converge; een trechter. Hier zou bijvoorbeeld terug gekeken kunnen worden naar investments en naar objectives en gemapt worden op deze zaken.

**9. What do you think the arrows represent?**

De pijlen zijn om te kijken of je mapt naar objectives; je evalueert als het ware aan de hand van de doelen die gesteld zijn. Je kijkt of je veroorzaakt wat je wilt veroorzaken. De groene pijl gaat hierbij over spelelementen, kijken of je wel de doelen kan behalen die gesteld zijn. Deze pijl gaat over als er iets fout is gegaan, de andere als het goed is gegaan.

*Red flag(s) feedback loop: return to design phases. Ok feedback loop: regular checkups; e.g. objectives.*

10. **Do you agree with these feedback loops? (Do you think there should be other feedback loops?)**

Ik zou de pijlen sowieso anders visualiseren als je ook naar andere stappen in de design phase kan gaan dan puur de converge stap waar de pijl nu naar wijst. Daarnaast vraag ik me af of het wel gebruikelijk is om terug te gaan naar de build fase. De enige situatie die ik me kan indenken is als je prototype niet goed is. In theorie zou je een ander prototype kunnen bouwen van een bestaand idee, maar ik denk dat je dan een stap terug zou gaan nog; dus naar de diverge stap, je ideeën stap. Kortom, misschien moet de build fase wel los gevisualiseerd worden.

11. **What do you think of the contents of the steps?**

(Het antwoord op deze vraag is tijdens het beantwoorden van eerdere vragen al naar voren gekomen)

12. **How can the contents of these steps be improved according to your expertise?**

Naast wat we al hebben besproken denk ik dat een introductie van evaluatie metrics gepast is. En een document met wat je met de verschillende termen bedoelt en hoe je deze kunt gebruiken.

13. **What two remarks or recommendations do you have regarding this framework?**

Er zit een logische structuur in het framework. Je moet wellicht nog even kijken hoe je de verschillende fases in elkaar haakt. Bijvoorbeeld; soms heb je een element uit een vorige stap nodig.

14. **Can I contact you if I have further questions?**

Natuurlijk.

## Interview (2)

1. **How are you involved in the topic of cyber security awareness?**

In short, there are two angles to this story. I am currently the Dutch capability owner of cyber and awareness. I take part in all kinds of activities concerning this topic. It is about leveraging best practices, helping clients and ensuring them that we can advise them on their awareness challenges. On the content; I was a CISO and in this role I kicked of an awareness campaign with all kinds of classical ways to raise awareness. There were also quite a few innovative ones in which we aimed to activate employees towards being a measure against potential cyber security threats. In the end it is all about behavioral change.

2. **What are your experiences with gamification?**

Both in observations and experience around it. I think if you want to establish a behavioral change, gamification, making things more fun, making complex information more accessible in a fun way, can contribute to making information stick to the target audience. Next, information will stick for a longer period of time. In this way, you can get the message across and start changing the awareness of changing behavior of employees. I think this is more than you can achieve with only sending your target group information via classical ways – updates, e-learnings, etcetera – things that are more static. I believe if participants can also see the consequences of their choices, this can lead to sense making of their decisions. This is the extra mile that you can get from gamification. I am a true believer of when you want to change behavior, the platform must relate to the context of the target. So, it should be relevant and in order to make it stick. Next, you need to make the potential impact of the choices of employees explicit and how this looks like. If you work with a statical medium, this is very difficult. I think gamification can better embed those elements.

3. **What are your experiences with the application of gamification in the context of cyber security awareness?**

I was an interim CISO for a big university in the Netherlands. Here they created a game on cyber awareness with a focus on relevant aspects, threats and risks for higher educational institutions within the Netherlands. This was made very contextual and they added the fun factor, but it was fairly limited on the impact of decisions. However, they added a competition model. I was able to contact different departments or different faculties and could engage them to take part in this awareness raising method. This is very different from pushing people to do an e-learning; I could engage them through the competition element. Through this competition, different groups could battle and could win something that was handed over by the board. Another example of my experiences is when several approaches were combined in a global and corporate situation with different cultures. Here, easy games like basic puzzles were combined with gamification of all kinds of existing campaigns and cyber security awareness activities. The puzzles had an added value for being usable over various countries, cultures and languages. The puzzles were especially useful for creating attention, not necessarily the actual impact, that was primarily established through all the gamified aspects. These gamified aspects were integrated in a platform through which you can show good behavior and good choices and you could retrieve points in return that were added to your profile. As a result, within a department, you would have a leadership board with a champion on top. In turn, others were stimulate to become a winner themselves through this exemplar good behavior. This provided nice incentives to work on proper choices and behavior.

4. **What are your recommendations towards applying gamification to cyber security awareness trainings?**

Content should be relevant and the impact should be shown; this relates to my answers on the previous questions. Next, on a business context, it is important to realize up front before you gamify something in what way you are going to assess what you want to achieve with it. How does success look like? How can you measure the current state? What is the state after gamification? This is important because I do not think that gamification is a measure that you can use for everything. I think gamification is very good to stimulate positive behavior and making people aware. But when you want to make someone aware and there is urgency or when the message has 'een andere lading', then other approaches might be more suitable. In other words, gamification might be conflicting due to its emphasis on fun or playful. So when alertness, being on the edge or acts are required, gamification might not be appropriate.

**Framework introduction**

5. **What are your first impressions of the framework?**

It makes sense, for example the objectives make sense. I wonder if the business targets are the same as learning objectives. I would be interested how the business and learning objectives are connected to the other checkmarks in the other steps. In my opinion, it is very important to have the business and learning objectives implemented solidly into everything that you do in the gamification process. Next, I think from the objectives a set of requirements, user stories, storylines, or flows can be derived. I miss this in your framework, but it might be just a first impression.

*This framework is to aid people in applying gamification to existing cyber security awareness trainings. It visualizes a four phased approach consisting of eight steps.*

6. **How does this information affect your impression of the framework?**

From my experience it is extremely difficult to make objectives measurable. Therefore I think that the evaluate phase needs more coloring in; for example take objectives as red thread to base the evaluation on. This is besides the user experiences and how the gamified environment came across. In other words, something can be fun and the experiences can be positive, but the gamification should also still achieve goals. So; there should be a harder connection.

7. **To what extent do you recognize these phases and steps (practical experience)?**

I recognize some of the checkmarks in the different steps as considerations that I took in different projects, but not as complete and connected as this framework so I think that is very helpful. I never started with gamification from scratch, there was always already a concept, so there are different starting points if I look at this framework. I think it is very interesting to have this entire thing laid out because it could help in selection processes or in determining gamification types.

8. **How can this phased approach be improved according to your expertise?**

Still my main point is in connecting objectives to the different steps, maybe in detailing the (functional/nonfunctional) requirements from this. Next in the evaluation phase; how do you measure success related to the objectives? Another idea is to make the content less listed, for example, are all terms equally important? So maybe you can chunk up or sort elements. Next, I have a mental framing when reading your terms, but I might be misinterpreting them. So for me, either provide 'naslagwerk' or frame me a little bit with an example or with compartmented steps/terms. This first option is a rather closed variant, whereas the other is more open. The balance is in providing information about the terms or limiting creativity. As a side note; I believe that you might still have successful gamification, even when design is rubbish.

9. **What do you think the arrows represent?**

I think these represent an iteration or a loop back where you evaluate and where you might enhance the elements that you have evaluated. These can relate to the objectives, or the context, or the design and gameplay elements.

*Red flag(s) feedback loop: return to design phases. Ok feedback loop: regular checkups; e.g. objectives.*

10. **Do you agree with these feedback loops? (Do you think there should be other feedback loops?)**

I suggest that you put also text to these loops and make the symbols more standing out. These loops are an example that I would not leave to the imagination of the one using this framework. I believe that the green arrow is worse, but green is good in my mind, so maybe change the color. Blue arrow represents the ongoing cycle so to reuse the gamification if there is a change in objectives or stakeholders. In general; feedback loops make sense, but how do you measure when you go back. So; not the metrics per se, because they are very situational, but the type of metrics.

11. **What do you think of the contents of the steps?**

In addition to the previous answers; you really describe it on a metalevel, you do not mention anything about content. This content is freely for the user of the framework to fill in. You only grab the attention towards which elements require attention or are required for success.

**12. How can the contents of these steps be improved according to your expertise?**

Deepening the content of these steps; make them less widely interpretable.

**13. What two remarks or recommendations do you have regarding this framework?**

Illustrate what is between build and evaluate. For example, after building there will be some testing; is that the evaluate phase or do you keep on evaluating it when it is in production. For me, the green arrow, I can imagine that that arrow comes from the build step, so before the gamification is actually in production. The blue arrow is more when the gamification is in production. So maybe you can illustrate this in a different way to visualize the two different types of evaluation. In practice; when something is in production and you met the green arrow how it is stated now; the production will stop. Finally, I am still looking for the context, so either in text or in legend or in examples next to the terms.

**14. Can I contact you if I have further questions?**

Yes.

### Interview (3)

1. **How are you involved in the topic of cyber security awareness?**

I am one of the subject matter experts on awareness. I have developed, implemented and participated in various programs with large clients. I am one of the leads on the subject in the team.

2. **What are your experiences with gamification?**

I came upon it as a solution to make the content more engaging. My most important experience is the escape room I developed in which I gamified cyber security awareness. Next, I have a brother who makes games, which might help during such projects.

3. **What are your experiences with the application of gamification in the context of cyber security awareness?**

Yeah, the escape room is also a good example here. Next, I have experienced it myself, for example a gamified introduction quiz concerning all proper ways of handling yourself. Everybody was really into it, joining as teams and such, other than the standard mostly boring quizzes.

4. **What are your recommendations towards applying gamification to cyber security awareness trainings?**

Think how your game is useful for your purpose; the game aligns and fit with that purpose. I would not recommend making everything a quiz. It is about trying to combine elements. Do remember that somebody has to do it and that it has to be fun. In other words it is a balancing act; educating people and make it in a fun way so they will not be bored. I noticed some examples of gamified cyber security awareness contexts that were informative but on the entertainment level they have to compete with something like candy crush. So; when I want to play a game I go for the latter because that is made to let me play. In other words; don't try to compete with that on that level; make sure the gamification fits the purpose. There are some drawback in the escape room from which you can learn, for example the scalability, transportation, hardware. But, the escape room is good for the purpose. Besides, it creates an event, an experience, it is not the same as downloading an app.

**Framework introduction**

5. **What are your first impressions of the framework?**

I miss execute somewhere, but that is a small comment. Next, I suppose there is an explanation of the terms somewhere. In my opinion it can be either 4 or 12 steps, but overall it makes perfectly sense.

*This framework is to aid people in applying gamification to existing cyber security awareness trainings. It visualizes a four phased approach consisting of eight steps.*

6. **How does this information affect your impression of the framework?**

How do you deal with the fact that content might not be available. For example, there is additional content necessary in order for the gamification to work. Is there a moment for this to add content? But if you only consider gamification of existing content than this is fine as it is. Just note that when your gamification does not work for your content is not right, considerations of this might be needed. For example adjust content, add more or skip some.

7. **To what extent do you recognize these phases and steps (practical experience)?**

I would say the blueprint, design, evaluation phase make sense. Otherwise I need to know a little more about the definition you are using.

8. **How can this phased approach be improved according to your expertise?**

I think this provides a nice way to start. I suggest you can keep on improving it when this necessarily. For example when adapting it to local needs or something. It is not written in stone; it is a framework, so it might also be 5 or 12 steps, but I think it is fine.

9. **What do you think the arrows represent?**

Feedback. But maybe I can elaborate on this when I know a little more about these arrows.

*Red flag(s) feedback loop: return to design phases. Ok feedback loop: regular checkups; e.g. objectives.*

10. **Do you agree with these feedback loops? (Do you think there should be other feedback loops?)**

I would visualize them differently, and maybe mention it in the arrow. For example from evaluate to a textbox called objectives and this arrow should be both ways. I think the green arrow is a smaller scale check; does my design works how it is supposed to work? In other words, this arrow is to check if your sails are in the right position. The blue arrow is to check if you are still on the right track. So; this arrow is to check if you still sail in the right direction to reach your goals. Overall; I think these feedback loops make sense.

**11. What do you think of the contents of the steps?**

When regarding the order of the resources and structure steps; I think this needs consideration. For example, when your resources are big, then you are very free in deciding on the entire structure of the gamification. So; structure is subordinate to resources. Next, when you base your structure on the work of others, this might not align with your resources and might not be good or appropriate for the situation in general. I suggest to look at resources first, what is allowed, then structure. This order sounds more inclusive. But; there might not be a right or wrong answer here.

**12. How can the contents of these steps be improved according to your expertise?**

Learning objectives and CSA topics could stem from business objectives. Currently, these terms look equal in the framework, but I think business objectives are the foundation. Maybe security strategy can be incorporated also and link it to business targets. I think learning objectives are somewhat more general so maybe security learning objectives is more appropriate, or keep them general and at the same level as other objectives. Suggestion: first business objectives, under it you write security strategy, under that you write CSA topics and under or next to that, learning objectives. Overall I read the terms as considerations how it is visualized now, but I like to see how these terms cohere. If you know the coherence between these terms, you can make improvements or prioritize elements. Next, for example regarding the capacities and behavior, I really think it is important to have such a 'current status' checkmark. Lastly, there should be requirements somewhere because they influence your resources and your design.

**13. What two remarks or recommendations do you have regarding this framework?**

I think I already mentioned the most important ones. Next, the considerations of the client are important; for example when scalability is required. For scalability and in general, e-learnings are the standard, it is easy to measure how many people you reached. But still; they are no good, nobody truly participates in them and therefore they are limited in their effectiveness. Gamification is the option to make is more fun so I think you can truly reach more people when something is not boring. In the end, when gamification is applied successfully, it makes people forget that they are learning. I think this is the ultimate goal.

**14. Can I contact you if I have further questions?**

Yes.

# Appendix C Basic Instructions of Gamified Training

## Rules of the game

Use your brain! Teamwork, good communication, creativity, logic and attention for detail are also very important.

### Preparation

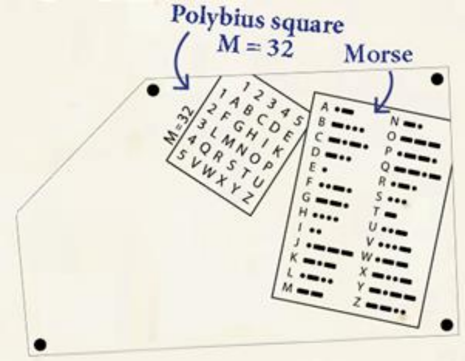
Make sure everyone has pen and paper ready; **never** write on the provided items.

### Aim of the game

The challenge has 3 parts. In each part, you must find a code consisting of *4 keys* that you enter into the Chrono Decoder. Find 3 correct codes within 60 minutes to win the game.

### The game

**Never** open an envelope unless you are specifically indicated to do so. Read the introduction, take envelope part 1 and read the instructions. Then switch on the Chrono Decoder by sliding the button on the bottom to 'on' and press START. The clock will start counting down exactly 60 minutes and the game has begun! The players proceed to check all the provided materials. Search for clues, codes, and (parts of) puzzles and work as a team.

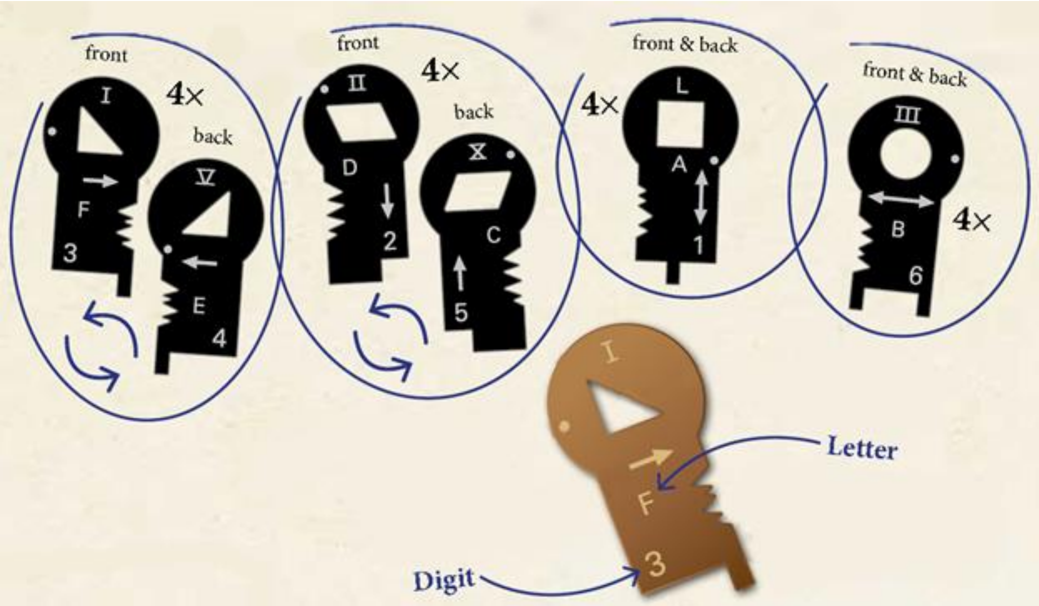


### Chrono decoder (CD)

During the game, you will occasionally see the text **CD**. This means that you must convert something using 1 of the decoder systems on the side of the Chrono Decoder. Only the *two* ciphers as displayed in the picture on the right are relevant for this game.

### Keys

The game includes 16 keys. These keys have 6 different key sides, each stating different information corresponding with the codes you will find during the game. The other keys are exact copies. Examine the keys before starting the game. You will only be needing the letters and digits in this game.



### Entering a code

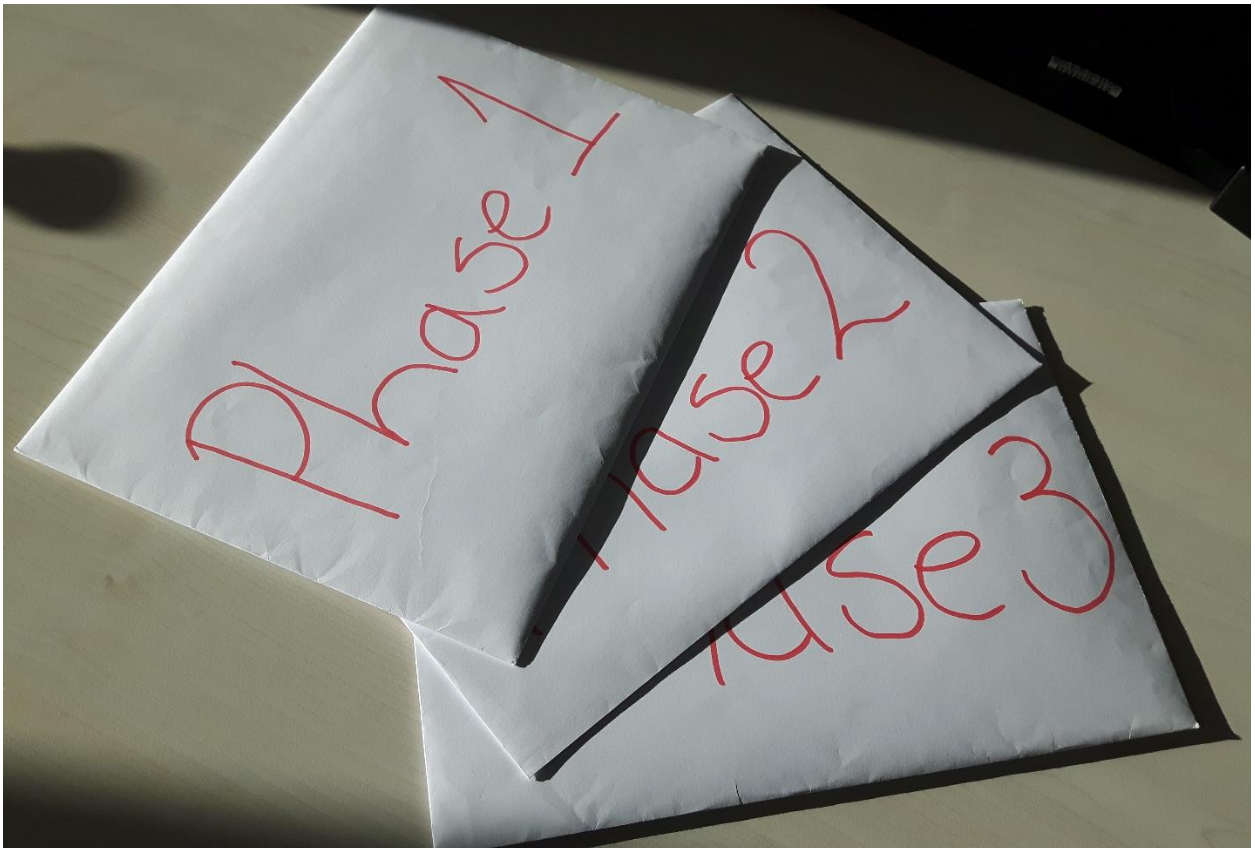
Once you find a code, place the 4 keys from left to right into the Chrono Decoder. If the code entered is incorrect, you'll hear an 'error' sound and 1 minute will be deducted from the remaining time. Try to find the right code again. You cannot continue to the next part until this code has been cracked. If the code is correct, you'll hear a 'confirmation' sound and you can open the next part of the adventure and proceed to decipher the next code. Remove the keys from the Chrono Decoder after entering a code.

### Hints

Occasionally you will hear a 'beep-beep' sound to indicate that you can take one hint card to ask the game master for a hint. You can opt not to use it (yet). You have 8 hints in total for this game.

### Winning

If you have entered 3 correct codes within 60 minutes, you'll hear 'victory' music, the time will stop and you have won the game. If you were unsuccessful in finding all correct codes within 60 minutes you will hear the 'losing' sound and the time will start counting up. You can still proceed to find the code(s) and the decoder will work the same way it did before.
Good luck!



## Appendix D Gamified Training

In this appendix, the texts accompanying the three different parts of the training are provided along with the introduction to the training and the certificate that would be provided to every participant.

### Introduction

### Cyber: a war next

It is a typical day at the office, 15.00 on the clock. Bob is happy with his new position as a manager at the telecom company MCLT. The company has recently developed a new low-cost solution for providing fast internet. This solution is one of a kind and very promising as a competitive advantage.

Eve is a loyal former employee of Lecomté, a big competitor of MCLT. She overheard rumors of MCLT's innovation and worries about the effects of it on her former employer. Currently, Eve is starting to look into some new hobbies and stumbled upon the trending topic of cyber. Eve spots a win-win opportunity; learning some cyber basics and putting them into practice by trying to retrieve information about MCLT's innovation. Besides, what if she could sell the retrieved information and make some money on the side?

In this scenario, you will help Eve. Your ultimate goal is to get access to secret company information surrounding MCLT's recent innovation and sell it on the Deep Web. You have only <u>one hour</u> for this three-phased challenge. When you're ready you can start the 3 phased challenge by turning the <u>Chrono Decoder (CD)</u> on and pressing the red start button.

## Part 1

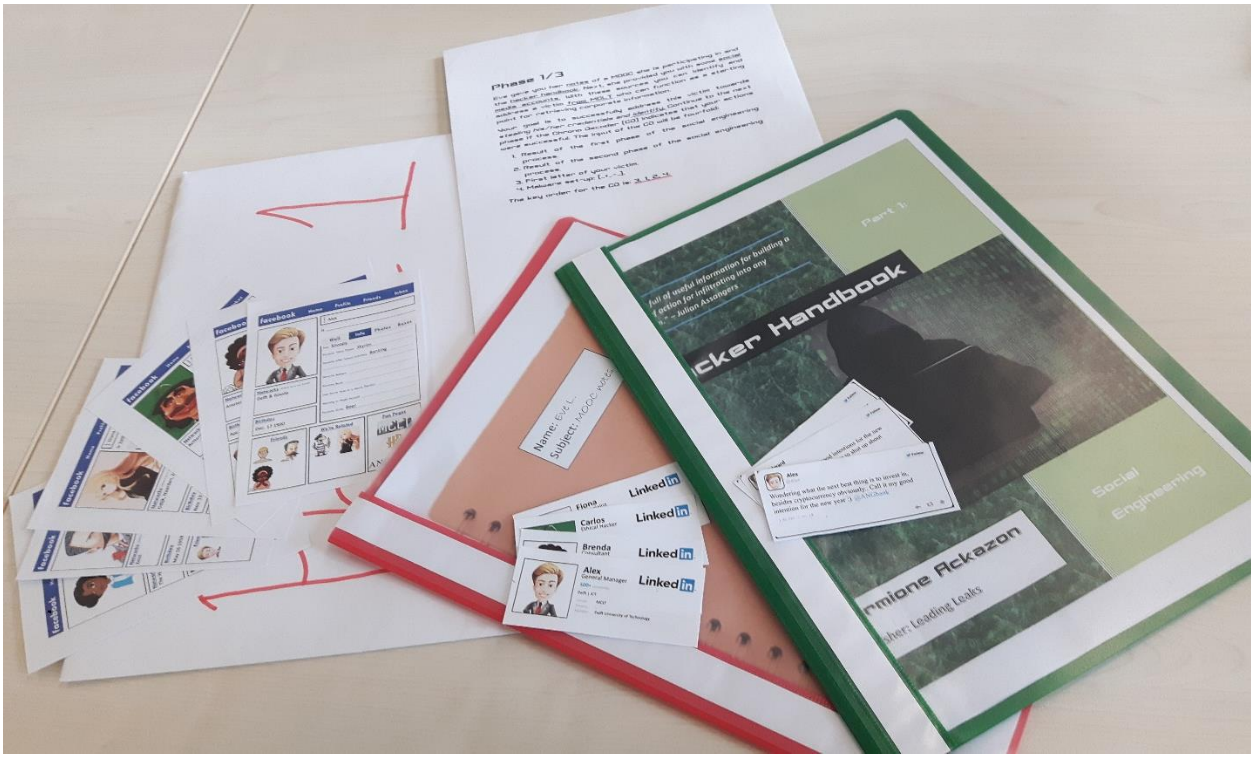
Phase 1/3

Eve gave you her notes of a MOOC she is participating in and the hacker handbook. Next, she provided you with some social media accounts. With these sources you can identify and address a victim from MCLT who can function as a starting point for retrieving corporate information.

Your goal is to successfully address this victim towards *stealing his/her credentials and identity*. Continue to the next phase if the Chrono Decoder (CD) indicates that your actions were successful. The input of the CD will be fourfold:

1. Result of the first phase of the social engineering process.
2. Result of the second phase of the social engineering process.
3. First letter of your victim.
4. Malware set-up: (..+..-..).

The key order for the CD is: 3, 1, 2, 4.



## Part 2

### Phase 2/3

The email with iOS malware sent to Alex concerning a secret banking announcement was successful. You can now access his private email inbox and identify your final target.

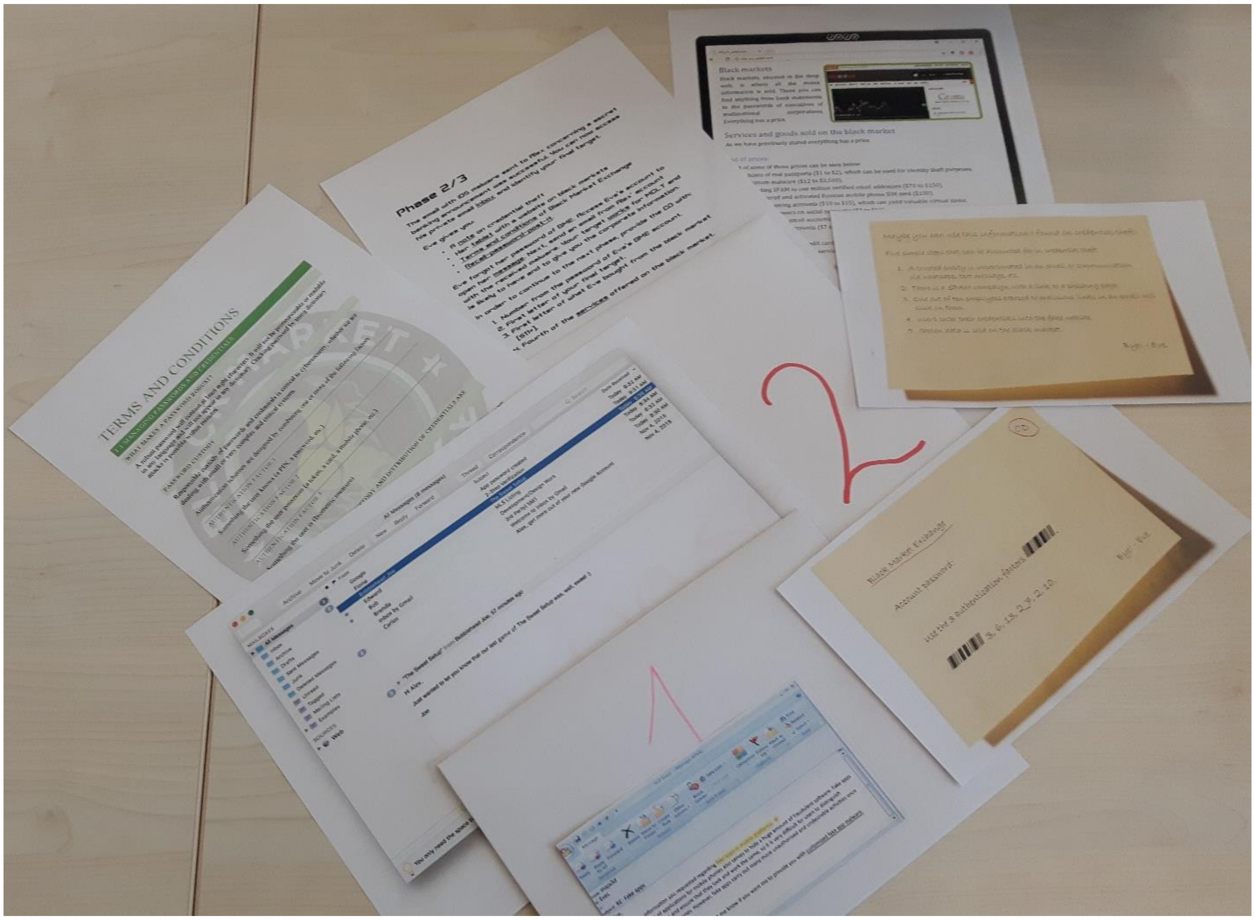
Eve gives you:

- A note on credential theft
- Her tablet with a website on black markets
- Terms and conditions of Black Market Exchange
- Recall-password-post-it.

Eve forgot her password of BME. Access Eve's account to open her message. Next, send an email from Alex' account with the received malware. Your target works for MCLT and is likely to have and to give you the corporate information.

In order to continue to the next phase, provide the CD with:

1. Number from the password of Eve's BME account.
2. First letter of your final target.
3. First letter of what Eve bought from the black market ($11+).
4. Fourth of the services offered on the black market



## Part 3

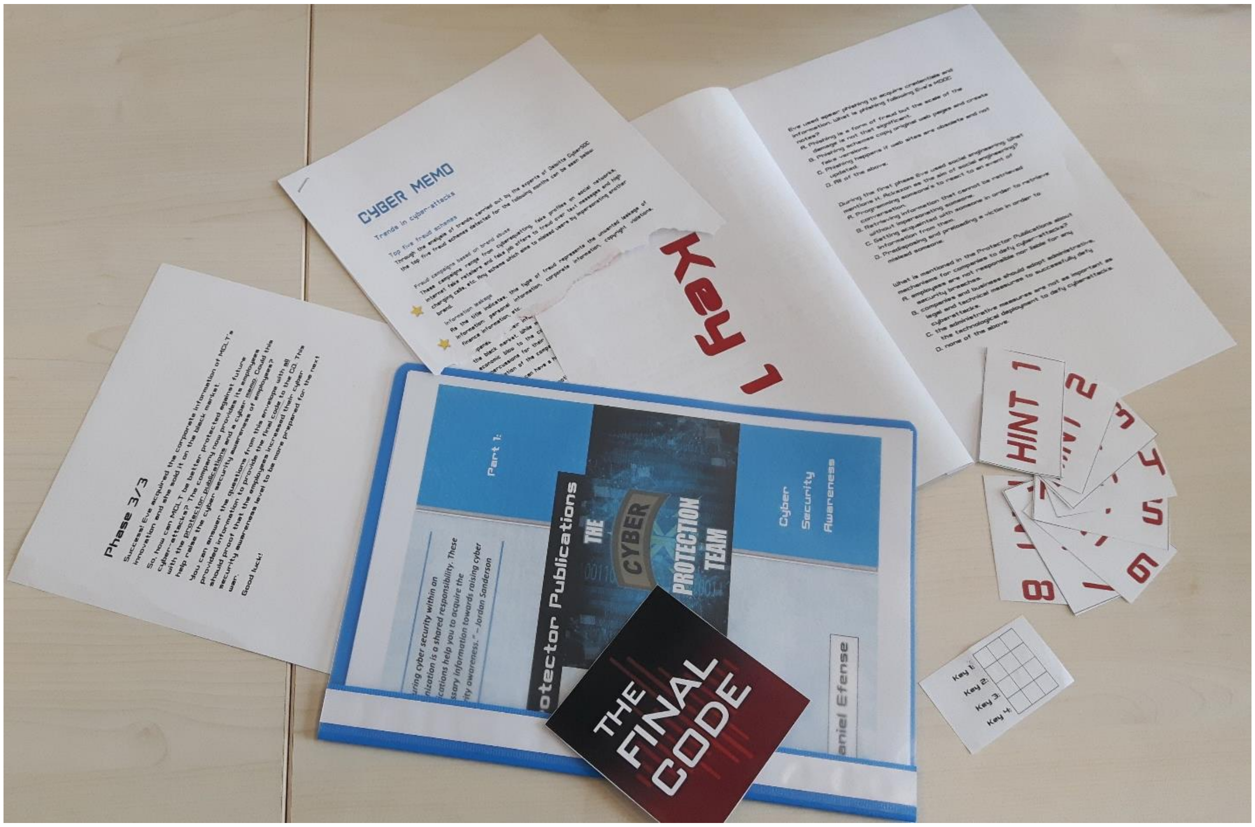
### Phase 3/3

Success! Eve acquired the corporate information of MCLT's innovation and she sold it on the black market.

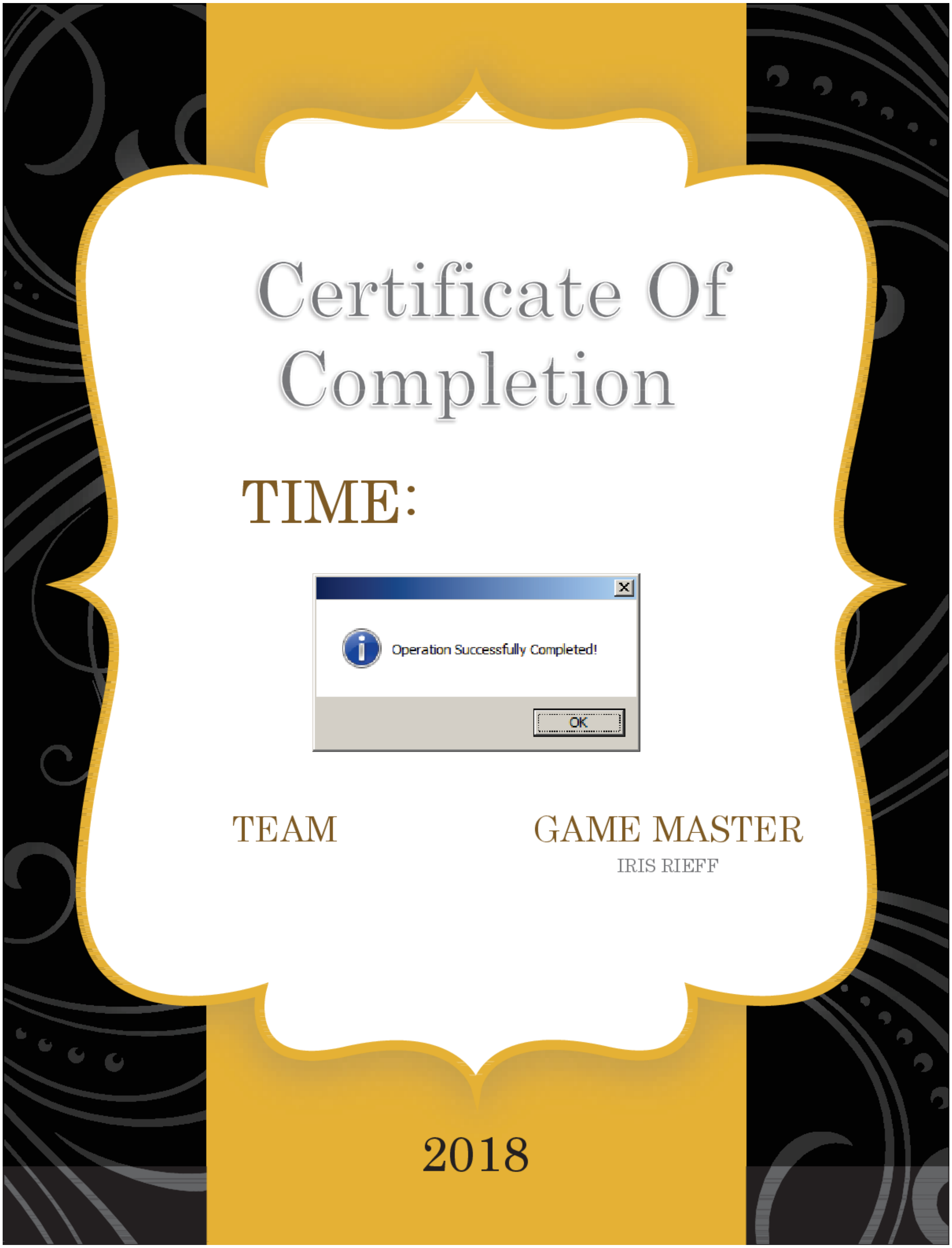
So, how can MCLT be better protected against future cyber-attacks? The company now provides its employees with the protector publications and a cyber memo. Could this help raise the cyber security awareness of employees?

You can answer the questions from this envelope with all provided information to provide the final code to the CD. This should proof that the employees increased their cyber security awareness level to be more prepared for the next war.

Good luck!



## Certificate



Certificate Of Completion

TIME:

Operation Successfully Completed!

TEAM

GAME MASTER

IRIS RIEFF

2018

# Appendix E Questionnaires

## Questionnaire Cyber Security Awareness Training (Pre-Training)

This questionnaire was developed to collect your feedback on your expectations and experiences with cyber security awareness and this cyber security awareness training. Please take a few minutes to answer the questions below. You will not be assessed based on this questionnaire. The anonymous results of this questionnaire will only be used for the purpose of improving future trainings.

Name:

**On a scale of 1 to 5, how would you rank your cyber security awareness?**
*Very little* 1 2 3 4 5 *Very much*

**What experiences do you have regarding cyber security awareness trainings?**

______________________________________________

______________________________________________

**What do you expect of this cyber security awareness training?**

______________________________________________

______________________________________________

**What topics do you expect to be touched upon in this training?**

______________________________________________

______________________________________________

Attitude can be described as a feeling or opinion about something. It is a state of readiness that will impact an individual's response to any situation. Attitudes have an important impact on one's judgment of the world around him or her.

**On a scale of 1 to 5, how would you rank your <u>attitude</u> regarding cyber security?**
*Very little* 1 2 3 4 5 *Very much*

**On a scale of 1 to 5, how would you rank your <u>knowledge</u> regarding cyber security?**
*Very little* 1 2 3 4 5 *Very much*

**On a scale of 1 to 5, how would you rank your <u>skills</u> regarding cyber security? E.g. backups, managing passwords.**
*Very little* 1 2 3 4 5 *Very much*

**On a scale of 1 to 5, how would you rank your <u>actions</u> regarding cyber security? E.g. locking your laptop**
*Very little* 1 2 3 4 5 *Very much*

**What additional comments, suggestions, feedback do you have?**

______________________________________________

______________________________________________

Thank you for your participation and feedback!

## Questionnaire Cyber Security Awareness Training (Post-Training)

This questionnaire was developed to collect your feedback on your expectations and experiences with cyber security awareness and this cyber security awareness training. Please take a few minutes to answer the questions below. You will not be assessed based on this questionnaire. The anonymous results of this questionnaire will only be used for the purpose of improving future trainings.

Name:

**On a scale of 1 to 5, how much did the training affect your cyber security awareness?**
*Very little* 1 2 3 4 5 *Very much*

**On a scale of 1 to 5, how much did the training match your expectations?**
*Very little* 1 2 3 4 5 *Very much*

**What differed according to your expectations of the training?**

**What would you consider the 3 key takeaways of this training?**

**What would you consider the 3 strengths of this training?**

**What would you consider the 3 aspects of this training that could be adjusted to improve its effectiveness?**

**On a scale of 1 to 5, how much did or will the training affect your <u>attitude</u> regarding cyber security?**
*Very little* 1 2 3 4 5 *Very much*

**On a scale of 1 to 5, how much did or will the training affect your <u>knowledge</u> regarding cyber security?**
*Very little* 1 2 3 4 5 *Very much*

**On a scale of 1 to 5, how much did or will the training affect your <u>skills</u> regarding cyber security?**
*Very little* 1 2 3 4 5 *Very much*

**On a scale of 1 to 5, how much did or will the training affect your <u>actions</u> regarding cyber security?**
*Very little* 1 2 3 4 5 *Very much*

**On a scale of 1 to 5, how much did the training encouraged your participation during the training?**
*Very little* 1 2 3 4 5 *Very much*

**On a scale of 1 to 5, how much did the training encouraged your interaction during the training?**
*Very little* 1 2 3 4 5 *Very much*

**Would you recommend this training to your co-workers?**

**What additional comments, suggestions, feedback do you have?**

Thank you for your participation and feedback!

## Quantitative results of the questionnaires

### *Existing training*

| Pre-training | 1-5 | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| CSA | 5 | 4.5 | 4 | 4 | 3 | 3 | 5 | 4 |
| attitude | 5 | 5 | 5 | 4 | 3 | 4 | 3 | 4 |
| knowledge | 5 | 4 | 2 | 3 | 3 | 2 | 4 | 4 |
| skills | 4 | 4 | 3 | 3 | 3 | 3 | 5 | 4 |
| actions | 4 | 5 | 4 | 4 | 3 | 3 | 5 | 4 |

| Post-training | 1-5 | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| CSA | 2 | 1 | 2 | 3 | 4 | 4 | 1 | 3 |
| attitude | 3 | 1 | 1 | 3 | 3 | 4 | 1 | 2 |
| knowledge | 2 | 1 | 2 | 3 | 4 | 4 | 1 | 3 |
| skills | 2 | 1 | 2 | 3 | 4 | 3 | 1 | 2 |
| actions | 1 | 1 | 2 | 3 | 3 | 3 | 1 | 2 |
| expectations | 1 | 2 | 3 | 4 | 4 | 4 | 2 | 5 |
| participation | 1 | 3 | 5 | 4 | 3 | 3 | 1 | 3 |
| interaction | 1 | 3 | 2 | 3 | 3 | 4 | 1 | 2 |
| recommend | ~ | n | y | y | y | y | n | ~ |

### *Gamified training*

| Pre-training | 1-5 | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| CSA | 4 | 4 | 4 | 4 | 4 | 4 | 3 | 4 |
| attitude | 4 | 4 | 4 | 4 | 5 | 4 | 3 | 4 |
| knowledge | 4 | 3.5 | 4 | 4 | 4 | 3 | 3 | 3 |
| skills | 4 | 3.5 | 2 | 4 | 4 | 4 | 4 | 4 |
| actions | 5 | 4.5 | 3 | 4 | 5 | 3 | 4 | 4 |

| Post-training | 1-5 | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| CSA | 3.5 | 4 | 2 | 1 | 2 | 2 | 4 | 4 |
| attitude | 4 | 4 | 1 | 2 | 2 | 2 | 4 | 3 |
| knowledge | 4 | 4 | 1 | 1 | 2 | 2 | 3 | 4 |
| skills | 3 | 4 | 2 | 1 | 1 | 2 | 2 | 3 |
| actions | 3 | 4 | 2 | 1 | 3 | 2 | 3 | 3 |
| expectations | 4 | 4 | 1 | 2 | 2 | 4 | 3 | 3 |
| participation | 5 | 5 | 2 | 1 | 5 | 4 | 4 | 5 |
| interaction | 5 | 5 | 4 | 1 | 5 | 4 | 5 | 4 |
| recommend | y | y | n | n | y | y | y | y |