GHOST: An Evaluated Competence Developing Game for Cybersecurity Awareness Training

Johannes A. König and Martin R. Wolf
Lab for IT Organization and Management
Aachen University of Applied Sciences
Aachen, Germany
email: koenig@fh-aachen.de, m.wolf@fh-aachen.de

***Abstract*—To train end users how to interact with digital systems is indispensable to ensure a strong computer security. 'Competence Developing Game'-based approaches are particularly suitable for this purpose because of their motivation- and simulation- aspects. In this paper the Competence Developing Game 'GHOST' for cybersecurity awareness trainings and its underlying patterns are described. Accordingly, requirements for an 'Competence Developing Game' based training are discussed. Based on these requirements it is shown how a game can fulfill these requirements. A supplementary game interaction design and a corresponding evaluation study is shown. The combination of training requirements and interaction design is used to create a 'Competence Developing Game' -based training concept. A part of these concept is implemented into a playable prototype that serves around one hour of play respectively training time. This prototype is used to perform an evaluation of the game and training aspects of the awareness training. Thereby, the quality of the game aspect and the effectiveness of the training aspect are shown.**

Keywords-Cybersecurity; Awareness; CDG; Serious Game; tablet game; business simulation; evaluation.

I. INTRODUCTION

The use of digital systems is crucial in modern companies and one effort of digitization is to use these digital systems more efficiently. Through these efforts, more and more analog processes are no longer available. By that, nowadays almost all relevant records are stored in databases or on cloud based file servers. Accordingly, the analog data management will be reduced to minimum, if that has not already happened.

Of course, a well-functioning digital working environment is required to ensure that the data are always available. If data are accessible everywhere and always for employees, then assailants are able to use these infrastructure, too. This issue is getting worse because nowadays, in modern digitalized systems, employees are owners of the keys necessary for data access. Consequently, it is no longer necessary for an assailant to attack the IT-infrastructure (IT = Information technology) or the IT-department. He can focus his attack directly on the data-using persons, e.g., with fishing-mails, social attacks, manipulated flash drives, etc. Despite this issue, this kind of always available data management is indispensable for modern companies.

An "Competence Developing Game"-concept (CDG) to train non-IT employs was presented by König and Wolf [1] in a shorter version of these paper on the ACHI 2018 conference. In that paper, however, it has remained at the concept level, a prototype was not presented. Supplementary to the old paper, in this contribution it is shown how the CDG prototype exactly looks like. That includes all prototype quests with their serious and entertaining aspects. Further, based on the prototype, an empirical study is presented. The study is used to evaluate the serious and the entertainment aspects of the CDG.

Regardless of the chosen approach, it is essential to train non-IT personnel how to avoid cybersecurity risks arising within their daily digitalized work [2]. Already today, employees are often the biggest threat in the cybersecurity chain [3]. To offer an effective cybersecurity awareness training, it is important to establish a continuous training cycle to establish a long term behavior change **(**req. **7** (see Section II)**)**. It should be noted that too many topics in too short time increase the risk to overwhelm the exercisers which is also a reason for a long training cycle. Basically, a successful cybersecurity awareness training has to solve two tasks. On one hand, it has to attract the attention of the participants for a defined time period. On the other hand it has to convey the training content as efficiently as possible. Unfortunately, most of today's trainings solutions show weaknesses in dealing with both aspects. A very suitable solutions to address both aspects is the use of interactive computer-based training methods **(**req. 6 (see Section II)**)** [2]. The use of gaming concepts in serious situations provides the possibility to transfer the motivation of a gaming situation into a serious learning context. In addition, games provide an environment which allows to choose risky or intentional wrong strategies just to figure out what will happen. Generally, there are three major kinds of games with a serious approach: Serious Games, Business Simulation/Games and the approach of Gamification. Further, there are different gradations of, e.g., serious games, which are not consistently defined [4].

However, instead of questioning 'What defines a particular game kind?' König and Wolf suggest focussing on the question 'What characteristics of which game kind are well suited for a specific application' [5]. For this, they provide the umbrella term CDG that encompasses all 'serious' game types (digital and analog):

'A Competence Developing Game (CDG) is a game that has the primary purpose to teach [how to use] knowledge, skills and personal, social and/or methodological abilities, in work or study situations and in professional and personal development of the game player, by retaining the motivation of a gaming situation' [4] (Note: The 'how to use' was accidently missing in the original source).

Accordingly, this paper examines what features a digital CDG must have in order to enable a cybersecurity awareness training for (German) business users. Further, it shows a specific CDG-design, in which these features are adressed. The CDG is called GHOST: Gamified Hacking Offence Simulation-based Training. In addition, a prototype will be introduced that contains a sample of the game ideas. Further, using this prototype an empiric evaluation study will be performed, analyzed and interpreted to prove the game's concepts. In detail, this paper is structured as follows:

In Section II, the target audience is determined in more detail, to understand their preferences and requirements. Section III addresses these requirements to determine a suitable CDG game kind. In Section IV, it is explained, how a game interaction interface design for a huge audience group like, 'business users', could look like. In addition, in Section V, a study that examines game interaction systems is briefly presented. Section VI describes the CDG GHOST which results from all previous considerations. In Section VII a prototype of the GHOST game and a corresponding evaluation study is presented. In addition, in Section VIII the study results are shown and interpreted. Finally, Section IX offers a conclusion and an overview about future work and use.

II. FINDING REQUIREMENTS BY UNDERSTANDING THE AUDIENCE

A study in German enterprises determined that the three most common reasons for employee related trainings are: the development of employee skills, increasing employee motivation and job satisfaction, and strengthening the employee-company relation (req. 1). The study also determined the obstacles that inhibit employee trainings. The identified top-two reasons not to train although there is a need are: no time available to dispense employees (43.8%) and missing internal capacity to organize a training (42.6%) [6]. A second study in German companies identified training costs and also the time issue as main reasons not to train employees. The three most common training methods are learning at the place of work (46%), external courses (28%) and in-house courses (<28%) [7].

In the case of learning at the place of work, the time an employee needs to be dispensed is limited to the actual duration of the training, because there is no traveling time (obstacle: no dispense time available) (req. 2.a.). The absence of traveling time is linked to the absence of traveling costs (obstacle: training costs) (req. 2.c.). By that, the organizational complexity of the training is also reduced, as employees must be covered shorter, and they are more easily accessible in crisis situations, etc. (obstacle: organizational capacity) (req. 2.b.). Accordingly, in the case of a continuous training cycle, as needed for a cybersecurity awareness training and therefore for GHOST, learning at the place of work seems particularly advantageous. These considerations clarify why learning at the place of work is the most popular training method and therefore it should be the method of choice for GHOST (req. 2).

In addition to these employer-focused considerations, the CDG GHOST is after all played by employees. As explained in Section I, more or less every employee who uses digital systems for work reasons should participate in a cybersecurity awareness training. By that, the target audience is broad (req. 3). Since the GHOST-Research-Project is granted by a German ministry (Federal Ministry of Education and Research), the German employee sector was considered in first place. According to a report by the Federal Institute for Vocational Education and Training, the average German trainee is 19.7 years old. The report shows the first grouping called "16-year-olds and younger". The average age of all employees was 43 years in 2016, with a relatively balanced distribution between women (~ 47%) and men (~ 53%) [8]. In summary, it can be stated that the vast majority of the target group is > = 16 years and <67 years old, the average age is 43, and women and men are similarly distributed.

As already mentioned, the use of a CDG as a training instrument has the advantage that the motivation of a game situation can be transferred in a serious context. In order to use this advantage a CDG must entertain players in a fun way while keeping the serious content in focus. This aspect requires a CDG that matches the tastes and abilities of the target audience. But because of the diversified target group, it is nearly impossible to construct a CDG that fulfills the individual game taste of each subject. On the other hand, the development of many games that meet the individual taste of each player would be expensive and it would stand in opposite to the obstacle: 'costs'. Following these remarks, a CDG that addresses a broad audience always represents a compromise in game design.

To find the major common denominator of each CDG-Player the 'Pyramid Assessment Framework for 'Competence Developing Games'' ('PACDG-Framework') was studied with this objective. The PACDG-Framework represents a tool that delivers the capability to analyze different game kinds in a standardized way. To do so, the framework covers, among other things, the entire player perspective of a CDG [5], as it was proposed (also) in the well-known MDA-framework for conventional entertainment games [9]. However, the PACDG-Framework covers the CDG-Player perspective in the three steps: "Experience", "Aftereffect" and "Impact". The last two steps refer to the same idea: A CDG should lead to competence acquisition, where the competences should help to solve at least one real life problem (req. 4). The step "Experience" is all about the player's claim to participate in an emphatic and positive gaming experience. In order to meet this claim, a high, entertainment game equivalent, quality must be delivered (req. 5).

Therefore, a CDG-based training that is accessible for all employees who use digital systems for work reasons should…:

Req. 1. …develop skills, increasing motivation / satisfaction, strengthening the job relation.

Req. 2. …take place at the place of work to reduce

a. time expense and release time,
b. organizational overhead and by that
c. costs.

Req. 3. …be accessible for every target group member.
Req. 4. …help to solve a real life problem.
Req. 5. …be similar in quality to an entertainment game.

Additionally a CDG for a cybersecurity awareness training should…: (see Section I)

Req. 6. …use interactive computer based training methods.
Req. 7. …occur in a continuous training cycle.

III. GAME TYPE SELECTION

As discussed in Sections I and II, the use of interactive computer-based training methods is suitable for a cybersecurity awareness training. By that, a serious game, a business simulation (supported by a computer based simulation model) or a gamified work environment could be used (fulfill req. 6). Furthermore, it is of course possible to develop a CDG in one of the named kinds with an entertainment game comparable quality (fulfill req. 5).

However, every well designed cybersecurity awareness training will match the requirements 1 and 4, too. It is because the main CDG purpose would be to lead to competence acquisition, where these competence acquisition refers to the ability to perceive possible IT-Security threats (fulfill req. 1). As IT-Security issues are a real life problem, of course, such competences would support to solve a real life problem (fulfill req. 4). Therefore, it can be assumed that a capable development team has the ability to develop a CDG from one of the named game kinds that has the potential to fulfill the requirements 1, 4, 5 and 6.

So, to choose the most suitable CDG game kind it is necessary to determine whether the requirements 2, 3 and 7 can be fulfilled.

''Gamification' is the use of game design elements in non-game contexts" [10]. As a result, for the gamification solution a deeply integration of game elements into the computer environment of the employees would be necessary. Based on such integration, e.g., correct behavior such as scanning a flash drive or locking the screen during a longer period of inactivity could be rewarded with points (fulfill req. 2a-b). This solution would enable a permanent and time neutral training without the need of learning to handle the training instrument (fulfill req. 3 and 7). However, the necessary development effort would be high (game element integration in every used program and operating system) and the privacy protection question would need clarification (not fulfill req. 2c). In addition, the extensive system intervention could have unforeseeable consequences on the IT security of the manipulated operating systems and programs. For these reasons a gamification solutions does not seem suitable for a cybersecurity awareness training.

A closed 'Business Simulation' is characterized by the participants being placed into a well-defined and prepared action situation. A model calculation (the simulation) assesses the decision effects on the game environment. Further the model communicates the success of each action to the players [11]. Since a business simulation is similar to a board game the majority of the employees should not have any problem to handle the game (fulfill req. 3). In addition, many simulation games are turn-based anyway and thus predestined for a long continuous game cycle (fulfill req. 7). The problem here is that even if it is possible to organize multiple business game session at the work (fulfill req. 2a), fixed dates have to be coordinated between different employees plus the necessary setup and dismantling of the business game have to be organized in time (not fulfill req. 2b-c). That means, a business simulation can also not fulfill all requirements.

The third alternative are 'Serious Games'. Serious Games are video games where the primary purpose is not entertainment, enjoyment or fun, which does not mean that Serious Games are not entertaining. They just have another primary purpose, in kind of an ulterior motive [12]. A video game has the advantage of being fully flexible in terms of time. Further no coordination is required between employees nor an organization of the game setup and it can also take place at work (fulfill req. 2a-c) However, it is difficult to realize a continuous training cycle without a turn-based design and such a design is not intended for Serious Games (not fulfill req. 7). But indeed it is the only approach that has the potential to fulfill requirement 2.

At this point, a CDG reveals its strength. The solution is to mix up the game kinds. Serious Games are the only game type that fulfills the requirements 2a-c, but the turn-based design of business simulations supports a continuous game cycle. Accordingly the solution is to develop a Serious Game with Business Simulation (turn-based) game mechanics (see Section VI). Therefore, only the mix out of a Serious Game and a Business Simulation has the potential to fulfill requirements 1 to 7.

Due to this design choice, the biggest problem with meeting the requirements will be requirement 3 in which a CDG is demanded that is playable for every target group member. In requirement 5, the demand for a quality which is similar to an entertainment game is formulated. It needs to be kept in mind that not all members of the target group have experience with video games. It must therefore be ensured that requirement 3 can be met without losing number 5. Therefore, it is necessary to find an interaction-interface for a high quality video game that does not require any video game experience. Section V will introduce a case study that was performed to evaluate how a game interface has to be designed to meet requirement 3 even when the game uses a 3D-Environment to fulfill requirement 5. Section IV explains the game interface development and the case study design.

IV. DEALING WITH THE GAME INTERACTION ISSUE

Germany is on of the largest video game markets in Europe with sales of 2.8 billion euros in 2015. Overall, the video game players are distributed as follows: PC / laptop 18.4 million players, smartphone 17.2 million players, console 15.6 million players, tablet 11.5 million players, handheld 8.3 million players. It should be noted that smartphones and tablets both use gaming apps, which means gaming apps with 23 million players in total have the largest player community

[13]. Accordingly to that information even in the aimed target group the amount of people who have experience with gaming apps should be higher than with other video game mediums.

In addition, it can be stated that touchscreens as used in smartphones and tablets have significantly changed the world of games in a short period of time. Modern touchscreen devices show a very intuitive interaction design that allows even children to use such a device successfully.

To explain why touchscreen devices are intuitive to such strong extend, a look at the three-layered brain model is helpful. To use a tool (in a computer context a tool means a device like a keyboard, a mouse, a game controller, etc.) humans have to make use of their neocortex. The cerebrum represents the highest layer in the brain model. In contrast, for 'touches', as needed during the use of a touchscreen device, humans only need to use the reptilian brain, which is represented in the lowest layer in the three-layered brain model [14]. Both aspects, (a) the widely use of gaming apps and (b) the intuitive aspect of modern touchscreen devices lead to the conclusion that a gaming app based CDG is the right choice for GHOST. Considering the broad target audience it is further reasonable to use a tablet based gaming app because of the larger screen size compared to a smartphone.

According to the last section, a CDG should be similar in quality to an entertainment game (req. 5). Modern gaming apps with the scope to be played over a longer period of time (as it is planned in GHOST) implement a three-dimensional, high quality looking game environment regardless of the genre (see e.g., Lara Croft Go, Lego Star Wars, Jam League, Modern Combat, Asphalt, Bothers: a tale of two sons, etc.). By that, GHOST has to be a three-dimensional tablet based CDG. On the other hand, GHOST has to be accessible for every target group member (req. 3). Thus, an appropriate game interaction system has to be found, that allows three-dimensional tablet based playing even for people who have never played a video game in their live. However, there are well established interaction systems for videogames that are also adapted for touchscreen devices.

The three most common used are 1st-Person, 3rd-Person and God view. The idea behind the 1st-Person perspective is that the player sees through the eyes of his player-character (PC) [15]. In conventional video games, the player controls the PC with mouse and keyboard [16]. Touchscreen based 1st-Person games are usually implemented in landscape mode. To control the PC the left and right thumb are used. The left thumb is used in the lower left area of the screen to control the movement of the PC. The right thumb is used in the lower right area of the screen to control the viewing direction [17].

In games that implement a 3rd-person perspective, a camera is used, which is aligned to the top of the PC to show him completely. Sometimes 3rd-person is implemented with „Trailing" option, then the camera is anchored at head height behind the PC. In classic video games, the control is similar to 1st-person games [16] the same applies to the touch screen control.

A God View perspective, also referred to by the terms 'overhead', 'top down' and 'God Eye', provides a perspective in which the game map is shown from above. Usually, the control is realized with the mouse [15]. Touchscreen-based God View games are often implemented by touching directly on the device. In such case the 'touch' on the device is equivalent to a mouse click. Additionally, manipulations of the camera perspective are done by the usual multi-touch gestures (e.g., two-finger zoom). Consequently, any 3D gaming interaction system known from the Computer/Laptop can be adapted for touch screen based games.

It has to be noted that the 1st-person and 3rd-person solution only replace mouse and keyboard through two equivalent virtual generated tools. By that, according to Schell [14], neocortex participation is still needed and whereby the advantage of a touchscreen solution is not exploited. Only the 'God View' interaction systems provide a solution that's natively transforms touch into interaction. As a result, this kind of game interaction should be manageable for inexperienced players and therefore is the right solutions for a touchscreen based CDG and GHOST.

However, this question cannot be clarified for the intended target audience based on the state of scientific research. There is a lack of empirical research that investigates the suitability of existing touch screen-based control and camera tracking paradigms for 3D serious games. However, since a well-functioning interaction system is elemental for the CDG success, a corresponding study has been carried out that will be briefly discussed in the next section.

V. INTERACTION SYSTEM FOR A TOUCHSCREEN BASED CDG

In the following different interaction systems are discussed and the study results are presented.

A. Discussion of possible interaction systems

The main objective of the study is to investigate wheatear it is possible to find an interaction-interface for a high quality tablet based video games that does not require any video game experience. Such an interaction-interface would connect requirements 3 and 5 that seem as if they exclude each other. The presence of such an interface would open the possibility to develop a cybersecurity awareness training that fulfills all seven requirements in the first place.

From a theoretical point of view, a game that responds as intuitive as possible on touch screen input should be advantageous for the players. As shown in the last section even the 'God View' interaction system relies on not intuitive multi-touch gestures for camera control. For that reason, a new interaction system for the GHOST prototype was designed.

These 'optimized' called interaction system provides the PC control via finger touch. The PC automatically moves to the location of the map where the map was touched. Even the interaction with game objects or non-player characters (NPC) works this way. If a player, e.g., touches a game object his PC will automatically move to the point next to the object. After arriving at this point an interaction dialog opens automatically. To remove the maybe not intuitive camera control the whole game map is divided in different camera zones (partly multiple zones in one room). Each zone provides its own static camera perspective. If the player controls his avatar from one camera zone to another, the camera angle

changes automatically. The player is not aware of where the zone boundaries are, the camera angle change just happens. To help the CDG-Player's orientation, there is also a second 'optimized+' called interaction system where the camera change from one position to the next one appears in a smooth move. Additionally, to the three mentioned interactions systems (1st-Person, 3rd-Person, God View) both versions were examined in a blind study. For this purpose, a small game was designed where the participant had to find six game objects or NPCs to interact with. At the beginning of the test a participant is set in a game environment with six rooms and two corridors. The participant does not get any map because the study also refers to the orientation ability. Finally, the time needed to complete the interaction tasks was measured.

A total of five mini games (demo versions) were developed:

- Demo1: 1st-Person
- Demo2: 3rd-Person
- Demo3: God View
- Demo4: optimized+
- Demo5: optimized

Deviating from the previous explanation of 3rd-Person interaction-systems the 3rd-Person PC control was changed. Usually the PC is controlled with the left and right thumb as in a 1st-Person tablet game.

Indeed, the interaction system in Demo2 uses a touch based PC movement control as in the 'optimized' demo versions. In addition, camera rotation was enabled by integrating a two-finger-rotate gesture for camera rotation. The classic two thumb control is still used in Demo1. Figures 1 to 4 are screenshots made of each demo version, respectively.

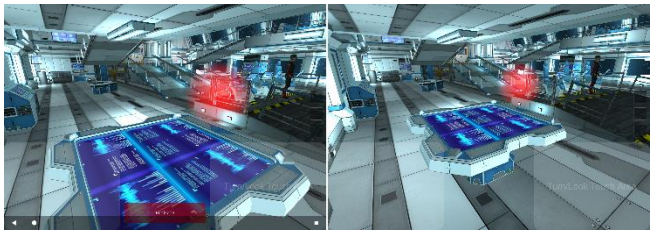

Figure 1. 1st-Person interaction system with dynamic appearing 'activate'-button for object interaction (Demo1).

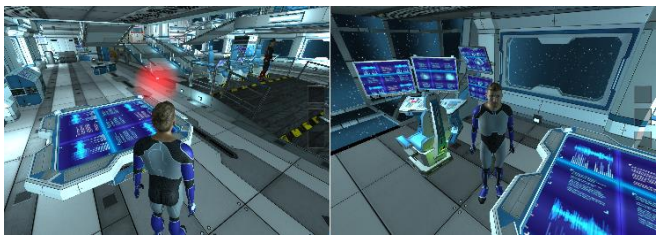

Figure 2. 3rd-Person interaction system before and after two-finger-rotate (Demo2).

Figure 3. Good-View before and after gesture based camera rotation (Demo3).

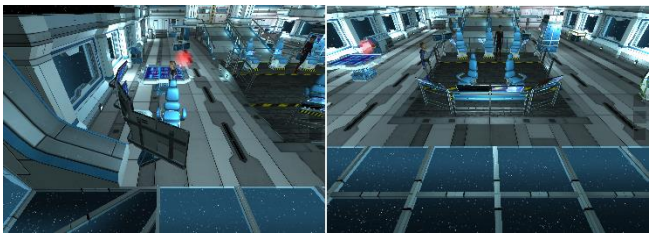

Figure 4. Adjacent camera zones in the optimized(+) interaction system (Demo4&5).

B. *Summary of Study Results*

TABLE I. SUBJECT DISTRIBUTION

	subject distribution				
	Demo1	***Demo2***	***Demo3***	***Demo4***	***Demo5***
age<=37	7	7	7	7	6
age>37	6	6	6	6	6
$\bar{x}$ age	39	38	40	41	41
SD age	17	16	16	15	15
n woman	6	6	6	6	6
n men	7	7	7	7	6
n	13	13	13	13	12

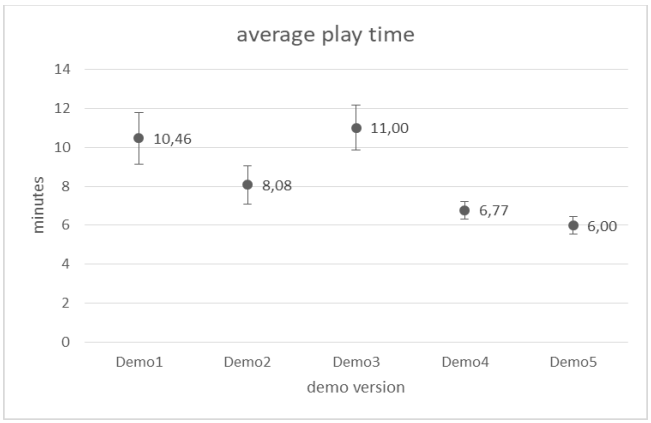

Figure 5. Average play time and 95% confidence interval.

In total 64 participants participated in the study. Table I provides information about the exact distribution of the test subjects to the individual demo versions.

An ANOVA was calculated and, by that, proved that the playtime differences are statistically significant ($\alpha = .05$; $F_{(4,59)} = 4{,}26$; $p < 0{,}0011$) . Figure 5 shows the average playtime for each demo version. It can be seen, that the playing time of the demo versions 4 and 5 are the shortest ones. As a result, the assumption that an intuitive interaction system simplifies the access to the game can be confirmed. By that, the 'optimized' or 'optimized+' interaction systems are the most suitable solutions for the GHOST-Prototype. Moreover, the results show that there are performance differences between the groups <=37 and >37 and that demo version 4 and 5 minimize these differences.

VI. GHOST: A CDG BASED CYBERSECURITY AWARENESS TRAINING

Following the remarks of this paper, GHOST is a turn-based, tablet-based, serious game like, Competence Developing Game, which provides a cybersecurity awareness training for end users in companies. Furthermore, in GHOST a new intuitive interaction systems was implemented. By that, it has the potential to fulfill the seven requirements which were derived in section two.

Whether GHOST meets these requirements depends on the game design. First of all the game design tracks two aspects. It creates the space to experience which personal actions are positive respectively negative for the cybersecurity. Second, it demonstrates which and why IT-department activities are necessary and meaningful. By that, it allows the end user to notice missing activities in his/her company and in addition it will increase the employee's acceptance for such activities.

In case of a cybersecurity training too many topics in a short time period increase the risk to overwhelm the exercisers [2]. Therefore, in the beginning each game round treats only one serious topic. The IT risks are hidden between other tasks and rarely occur, as in reality. In order to evaluate which serious content should find its way into the GHOST CDG, Annex 'A' of ISO 27001 was analyzed (ISO/IEC 27001: Information technology – Security techniques – Information security management systems – requirements, see [18]). In Table II, the serious topic of each game round is presented.

The idea behind GHOST's game design is to minimize the organizational effort. By a trick, GHOST still provides player the illusion of playing together. Every GHOST training is designed for 8 players in two groups at the same time. The training consists of 16 units (game rounds) in total. However, each round gets a specific time period in which the round is active and ready for play. In this period each player can choose the moment to play the round individually. At the end of the time period the GHOST-System calculates, based on each individual result in a group, a common group result which is the starting point for the next round. If, e.g., a player misses to participate in one round the whole group result will be weakened. This kind of game design uses the business simulation advantages like group motivation and the enforcing of a specific continuous training cycle without the disadvantages of complicated appointment organization. Nevertheless, GHOST allows even real multiplayer experience. The Round 7&8 as 15&16 require all 8 players to participate the training at the same time. Each group has to be in one physical room, the merging of the groups takes place via internet. These real multiplayer rounds serve as highlights of the complete training cycle. However, since two multiplayer rounds are played at one appointment, accordingly only two appointments must be arranged. As a result GHOST provides 16 play rounds and only requires the coordination of two appointments, which results in a huge reduction of the organizational effort compared to business simulations. Table II shows the assignment between serious content and game rounds.

As already mentioned, the serious content in GHOST is hidden between other tasks. To assure a simple knowledge transfer between the game environment and the real world it seems to be obvious to build an office environment inside the game. Accordingly, the player would solve every day work tasks inside the game world to come across serious content from time to time. This would result in a game that simulates an office for a game player whose position is currently an office, means playing-office in the office.

TABLE II. GAME ROUNDS

Round	***Serious topic***
1	Screen lock
2	Handling of foreign flash drives
3	Phishing-Mails
4	Backups
5	Mobile Devices (especially Smartphones)
6	Websites, software installation, own IT infrastructure
7&8 (MP)	Passwords, Information encoding, Emergency response, Environmental Security, Backups
9	Access rights
10	Environmental Security, safe workplace
11	Virus prevention, Keylogger, Work delegation
12	Network Devices, Audits,
13	Log files, Access Right Management
14	Quiz Round
15&16 (MP)	Flash drive, Information encoding, Phishing-Mails, Malware, Passwords, Emergency response

MP = Multiplayer

This would most likely ruin the fun aspect of the game, what would gamble away the main advantage of a CDG, the transfer of the motivation of a game situation to a serious context. For this reason, the game was moved 50 years into the future. The players find themselves in a science fiction scenario on a space ship named GHOST. They experience a journey of sixteen laps (one lap one round) and figure out quickly that someone tries to sabotage the mission by infiltrating the ship's computer systems.

As a crew member each player has to handle a lot of day-to-day tasks, which are intentionally similar to 2018 tasks in a

normal office. Nevertheless, a player has to be constantly on guard while interacting with the computer systems or other aspects in his environment. The assailant could start the next cyber-attack in any moment, with any strategy.

VII. PROTOTYPE FOR EVALUATION

As shown in Section II, the awareness training should fulfill at least seven requirements to match employer and employee expectations. Most of them can be fulfilled through design decisions described in this paper: A GHOST training can take place at the place of work to reduce the time expense. Since an extensive preparation is not needed the organizational overhead is reduced. This helps to reduce the training costs (req. 2a-c). Because of its sophisticated empirical evaluated (see Section V) interaction system even employees without any game experience can participate the training (req. 3). In addition, this interaction system helps GHOST to have an entertainment game look and feel (req. 5). The turn-based, business game inspired, game design allows further a continuous training cycle, that is made possible with a computer-based training (req. 6 and 7). Moreover, the social significance of - and the increased attacks on- IT systems leave no doubt on the real-life relevance of the underlying problem (req. 4). Therefore, on to this point only requirement 1 is left unmentioned. Requirement 1 demands a CDG to help an employee to develop skills, to increase his motivation and satisfaction and to strengthen the job relation. The last both aspects of requirement 1 can presumably only be evaluated when the GHOST CDG is completely developed (as described in Table II) and used in practice. But the first aspect of requirement 1 -to develop skills- can be evaluated with a prototype. Therefore, a prototype was developed that follows the principles shown in this paper (for an overview see Section VI). To provide a game situation to the participants with proper length to gain an intense impression the prototype should cover around one hour of gaming. Accordingly, to develop just one game round would not be purposeful. Instead four serious topics: “Screen lock”, “Handling of foreign flash drives”, “Network Devices” and “Passwords” were combined to one large gaming round that is implemented for evaluation reasons only.

In the beginning of the prototype an introduction video is presented to the participants. The video covers the control elements of the game and explains them. The whole interaction system is equal to the optimized+ interaction system as shown before. The camera moves automatically in a smooth way and for the game objects interaction the participant in every case needs a one finger touch to start interaction.

A. Storyline overview

During the gameplay the participant finds out that he is on a space ship called GHOST on a mission to find a new discovered high energy element: Industrium. Overall, the participant has to pass eight quests. He deals with the sabotage of the crew's mission. In the beginning, the participant is presented with the conundrum of what to do with an unfamiliar flash drive prompting an investigation by the chief of security into its origins. This is the first of several attacks that are made on the ship's security. As the game progresses, the crew becomes more nervous and the participant must assist in improving the ship's security. However, all efforts are too late as just after industrium collection is concluded the main systems of the ship suddenly shut down. The chief engineer explains that the systems responsible for keeping them alive and creating fuel from the harvested industrium are failing due to the disturbance. The participant is tasked with finding the devices that are causing the disturbance and restarting the system. Once he has finished this task, the crew is saved and prepares for a leap through space.

B. Game play and serious content

Quest 1 gameplay: The participant must activate the ships systems and he must find the ghost-drive of the quartermaster (a device that looks like a flash-drive). In doing so the participant has to find his way through the ship to find a computer console that is marked with an arrow. After that, the ships lights are activated, and the participant will find the ghost-drive nearby. In the end of the quest the participant is told to keep the found ghost-drive because he needs one for his next task anyway.

Quest 1 serious content: The ghost-drive is infected with a virus (what the participant does not know about). From the moment the participant finds the drive he has the possibility to visit the security chief to get the problem fixed. (Serious goal: Flash-Drive security awareness) (see Figure 5)

Quest 2 gameplay: The participant gets the task to collect status reports from five crew members who are in the rear sections of the ship. The crew members will transfer their reports to his ghost-drive. At the quest end the participant will merge the reports by using his terminal and sent them to the captain (only a few clicks needed).

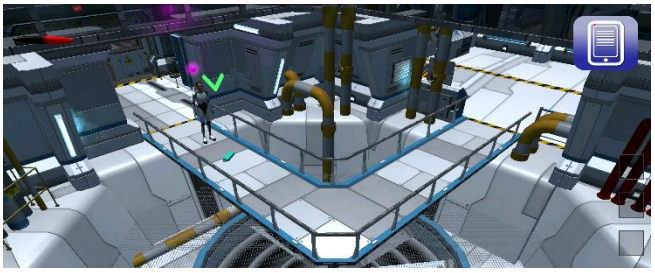

Figure 5. Finding the lost ghost-drive after activating the ship systems (cropped)

Quest 2 serious content: The participant still has the opportunity to find and fix the virus problem by visiting the security chef. When the participant speaks to one of the five crew members and if his drive is still infected he can choose if he wants to do “something else” or if he gives his ghost-drive to the person he is speaking with. If the participant infects a crew member's computer, the security chef will arrive in seconds, detect the problem, explain the problem and hand over a ghost-drive that is safe to use. The negative consequences are that the report is lost and that every other

crew member mentions the incident later in quest 2. However, close to the quest end and after the participant sends the merged report away he has two options to leave the terminal: The more obvious option is to touch on “leave the terminal”. This is equal to leave a PC unlocked. Second, the participant can touch the “Show shutdown menu” Button that reveals the “lock” Button for leaving the terminal in a safe way. (Serious goals: Flash-Drive security awareness)

Quest 3 gameplay: The participant is requested to the bridge. On the bridge the participant and the captain have a small talk about the ship systems and the merged report.

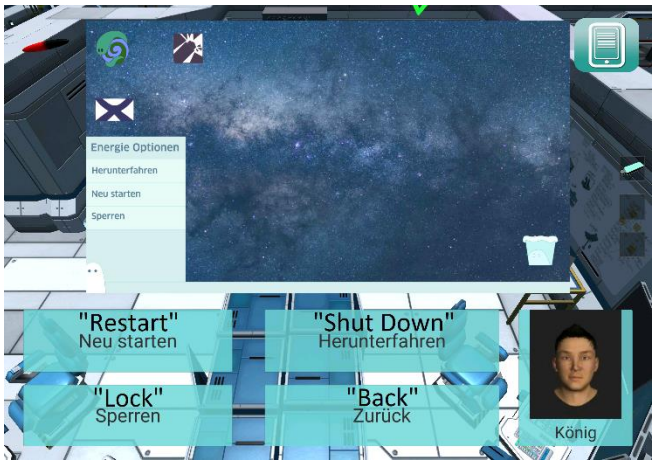

Figure 6. Options after touching the “Show shutdown menu” button (Button translation inserted)

Quest 3 serious content: During the chat the camera suddenly moves onto the main screen of the bridge. Depending on whether the player locked his screen in Quest 2 or not there is a different email-like message on the screen. If he forgot to lock his screen the participant is addressed directly by his name and the mail is sent from his terminal. But if he locked his screen in Quest 2 the message is addressed to a crew member and sent from the crew member's terminal. In both cases the captain points out that someone made a joke and that it is important to lock the screen always. (Serious goal: more frequent screen locking) (see Figure 6)

Quest 4 gameplay: The participant will be requested to the security chef. They chat about the infected ghost-drive and the security chef points out that he needs help to generate new passwords that are good to remember.

Quest 4 serious content: The password generation is wrapped in a mini-game. During the game, the participant has to shot on eight words that will be the long enough to be a good base for the password generation. If the participant shoots a short word he loses one of the already collected long words. However, after the collection of words the player modifies the words to passwords. For that, he selects a character he wants to change or add (e.g., a 1 for an i, etc.) and tries to shoot down the wished character. As he makes the changes, he sees a constantly changing display indicating how secure the password currently is. By that, the participant gets a feel for what makes a password secure. (Serious goal: teach how to build a safe password) (see Figure 7).

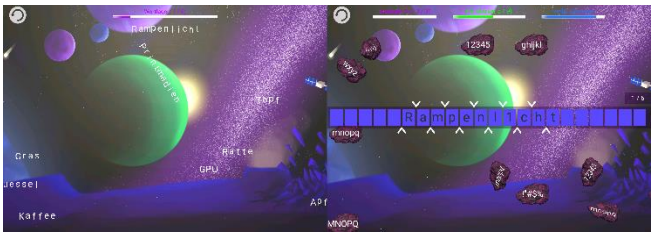

Figure 7. Mini-Game for the password generation. Left: shoot long words; right: modify words to passwords

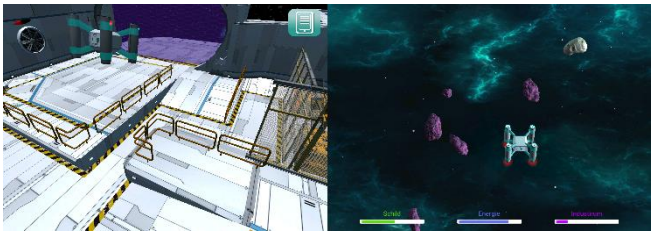

Figure 8. Mini-Game for the industrium collection. Left: animated drone start; right: industrium collection

Quest 5 gameplay: The participant gets a call that he has to check the current industrium research reports that are send as a message to his terminal.

Quest 5 serious content: After using his terminal the participant has to remember to lock his screen comparable to quest 2. If he remembers to lock his screen he gets a positive feedback from the security chef after a while. If he forgets to lock the screen he gets an equivalent negative feedback. (Serious goal: more frequent screen locking)

Quest 6 gameplay: The participant has to collect industrium with a remote-controlled drone. The drone-flight is implemented as a mini game. The participant controls the drone with his finger. He has to hit the pink asteroids for collecting industrium while avoiding the other ones (see Figure 8).

Quest 6 serious content: none.

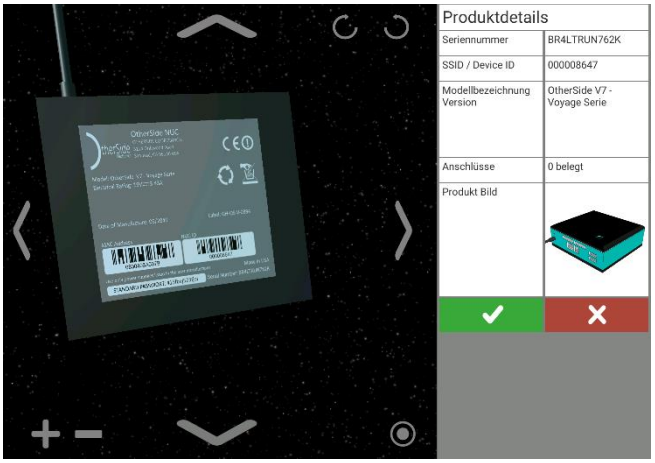

Figure 9. Mini-Game: “Network-Devices”

Quest 7 gameplay: There is a shipside system failure and it is not possible to reactivate the ship's systems. The participant has to help to identify if there are any corrupt devices on the ship. His search area is the communication room and the mess. In the end of the quest the participant is able to reactivate the systems in the same way as in quest 1.

Quest 7 serious content: The player has to check devices that are similar to network devices like network switches or repeaters. The checking is implemented as a mini game where the player compares a device on the ship with the manual (e.g., number of free ports, picture, serial number, etc.). The player has to decide if the device is safe or not. When he decided to report a device, he has to choose which aspect is corrupted. (Serious goal: Create awareness that new network devices could leak the security chain) (see Figure 9).

Figure 10. Debriefing supported by drawings (current topic on screenshot: screen lock)

Quest 8 gameplay: The quartermaster informs the participant, that his leap capsule is ready. After entering the capsule, the prototype finalizes.

Quest 8 serious content: Before the end a debriefing is shown. The debriefing picks up all serious topics and explains them one last time. The debriefing presentation is supported by drawings (Serious goal: deepening and transfer) (see Figure 10).

C. Experimental procedure

Each participant playing the prototype is supported by a test leader. The test leader is allowed to offer help to the participant whereby the amount of help is strictly regulated through the test design. After playing the prototype the participant has to fill out a questionnaire. In addition, approximately two months after the prototype-based training the participant gets a second short questionnaire via email. The first questionnaire contains three objects of investigation: "game experience", "prototype review" and "competence growth". The second questionnaire is only about "competence growth".

To measure the "game experience" the core module of the "The Game Experience Questionnaire" is used. The core module assesses the game experience separated in seven components [19]. The items of the questionnaire are translated to the German language enabling the participants to use their native language.

To receive a standardized game review from the participants a cross section of the work from Vohwinkel is used. Vohwinkel presents a well evaluated questionnaire for standardized game reviews [20]. He takes a variety of usability and game work into account and reorganizes them to a full-scale measuring instrument for commercial video games.

As part of the research project it is not possible to measure the "competence growth" in a real-life work situation of the participants. Instead the participants are asked three times after a self-assessment. First, for each of the four serious aspects they are asked how they handled the aspect before they participated to the prototype-based training. In the end of the long questionnaire they are asked again with a changed focus. Now they should assess how they plan to act in the future. Then, in the questionnaire that the participants received after approximately two months, they are asked how they actually acted in the last months. In total, this creates an overall picture of the self-assessed competence situation. The self-assessment questions are formulated as follows, each adapted to the position in the questionnaire/s:

- I locked my screen when leaving my place of work
- If I recognized new IT-Devices on my place of work I was thinking about whether it is necessary to report them to somebody.
- Before using a flash-drive I was thinking about if it is safe.
- I knew exactly how to generate an easy to remember and safe password.

As shown in the interaction system study there are differences in the play times between the groups "age<=37" and "age>37". Other play time relevant factors were not identified. It was shown that the interaction systems optimized and optimized+ are able to reduce the play time differences. To further reduce these play time differences to a minimum an interactive map is added to the prototype. In addition, the participant gets navigational help through the test leader if necessary. In later implementations this kind of guiding should be made automatically by the game itself.

However, one evaluation goal is to discover how differently the play performance and the game impression between the age groups still are. So, the described aspects of investigation are evaluated for each age group separately. Because there is approximately one year between the both empirical studies the age groups for this study are defined as: "age<=38" and "age>38".

VIII. EVALUATION

In this section the game experience and the competence growth are discussed.

A. Game experience & game review

Overall 31 participants take part in the study and completed 1,777 minutes of play time. The follow-up

questionnaire after two months got 14 responses. Table III shows the distribution of participants and Figure 11 shows an evaluation example.

TABLE III. SUBJECT DISTRIBUTION

	Distribution
Age<=38	19
Age>38	12
$\bar{x}$ *age*	35.7
SD age	15.3
n woman	9
n men	22
n	31

Figure 11. Evaluation

The participants evaluated the game experience and reviewed the game on the same five-point scale (1 to 5). During this analysis the averaged answers are interpreted as school marks in the following way:

- [>=1.0 “E” <1.8] (worst grade),
- [>=1.8 “D” <2.6],
- [>=2.6 “C” <3.4],
- [>=3.4 “B” <4.2],
- [>=4.2 “A” <=5] (best grade)

On average the participants of both age groups assess the game experience with an B (3.5). Thereby, only the game experience “challenge” got a bad rating (D). One possible explanation is a too low level of difficulty. Nevertheless, the data points out that both age groups had a similar positive game experience with little weaknesses only. Table IV shows the results of the seven components of the measured game experiences in both age groups.

Beyond the game experience evaluation, the participants reviewed the prototype using an adapted measuring instrument for commercial video games. Again, both age groups reviewed in a very similar way by giving an B mostly. On detail, the participants who correspond to the group “Age>38” rated minimal better. Table V shows the results in detail.

TABLE IV. GAME EXPERIENCE

	Age <= 38		**Age >38**	
Component	$\bar{x}$	***mark***	$\bar{x}$	***mark***
Competence	3.6	B	3.8	B
Sensory and Imaginative Immersion	3.0	C	3.2	C
Flow	3.2	C	3.0	C
Tension/ Annoyance	1.6 (4.4)	A	1,3 (4.7)	A
Challenge	2.2	D	1.9	D
Negative affect	1.9 (4.1)	B	1.7 (4.3)	A
Positive affect	3.9	B	3.7	B
Average	3.5	B	3.5	B

see [19]

TABLE V. PROTOTYPE REVIEW

	Age <= 38		**Age >38**	
Component	$\bar{x}$	***mark***	$\bar{x}$	***mark***
Graphics / Camera / Control	3.7	B	4.2	B
Narration / Avatar / NPCs	3.7	B	3.7	B
Help / easy game learning	3.9	B	4.1	B
Traceability / Game-Goals	4.1	B	4.3	A
Average	3.9	B	4.1	B

see [20]

In addition, the play time of each participant was measured. The mean playing time of all participants was 57.4 minutes. Thereby, the mean playing time difference between the both age groups was only about 5 minutes. The group “age<=38” needed an average of 55.4 minutes to play the prototype while the other group “age>38” needed with 60.4 minutes a little more time. Figure 12 represents a scatter plot for the variables age and play time. A relationship between age and play time is visible. A Pearson's correlation was calculated with a result of 0.30, so a light correlation was detected. With a p-value of .285 in the present sample the correlation is not statistically significant. However, a five-minute play time difference has no impact on the practical usability of the concept.

The interpretation of the presented data indicates that the combination between interaction system and game design minimizes the differences between the age groups so far that these are no longer significant. This can be seen in all the three presented evaluation aspects. Further it can be determined that the participants evaluated the prototype’s gaming aspects in a positive way. This impression is strengthened through a further item in the questionnaire. The participants were directly asked about their overall impression and rated the prototype in mean with 7.7 out of 10 points (B). Accordingly, the differentiate review and the overall impression of the prototype are consistent and both positive.

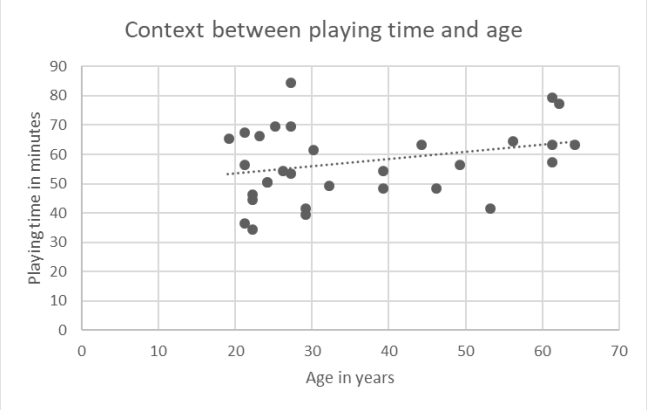

Figure 12. Scatter plot: Age->Playing time

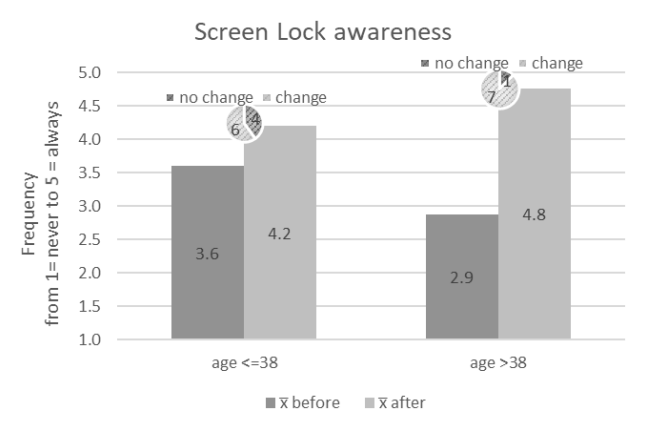

Figure 13. Screen Lock

B. Competence growth

In the following the growing of the participant's competences for each of the four serious aspects is evaluated. Thereby, only records allowing a competence growth are used. That means if a participant stated that he always locked his screen or that he perfectly knew how to generate a password even before he participated on the prototype-based training his record regarding the specific serious content is not used.

For the measurement of the three serious topics "Screen lock", "Handling of foreign flash drives" and "Network Devices" frequencies were queried (5-Point-Scale). According to the scale the mean results are interpreted in the following way:

- [>=1.0 "Never" <1.8] (worst grade),
- [>=1.8 "Rarely" <2.6],
- [>=2.6 "Occasionally" <3.4],
- [>=3.4 "Often" <4.2],
- [>=4.2 "Always" <=5] (best grade)

Figure 13 shows the results of the participants self-assessment regarding the serious content "Screen lock". Before participating in the prototype usage, the group "age<=38" in mean stated to often lock the screen (3.6) ($\bar{x}$ before). After the training participation the average frequency value was 4.2 (often) ($\bar{x}$ after) whereby 6 of 10 people improved their competences. The group "age>38" chose an average frequency of occasionally (2.9) before participating in the training. After the training they stated that they are planning to lock their screens in future always (4.9). Overall, 7 of 8 participants were able to increase their performance. Summarized the measurements for both groups show satisfactory results after participating the prototype training. It is noticeable, that the group with less previous competences could leap higher, which results in a similar competence level between both groups.

The follow-up questionnaire (after two month) contained 6 relevant records for the younger and 3 records for the older group. Overall, when asked how frequent they have locked their screen since prototype testing, the younger group shows two deviations in the size of: once -1 and once -2. That results in comparison to $\bar{x}_a$ ($\bar{x}_a = \bar{x}$ after) in a mean loss of -0.03 ($\bar{x}_{a+} - \bar{x}_a$) (Note: The differences are calculated precise with 15 digits). The records of the older group contained one difference of -1, which results in a mean loss of -0.08. For the present sample this leads to the conclusion that the prototype has a long-lasting aftereffect regarding the serious content "screen lock". The deviations can be neglected because of their low severity. Table VI gives an overview about the follow-up survey.

TABLE VI. SCREEN LOCK FOLLOW UP SURVEY

Group	$\bar{x}_{a+}$	$\bar{x}_{a+} - \bar{x}_a$	Absolute change		AVG change
			-1	-2	
age<=38	4.17	-0.03	1	1	-0.5
age>38	4.67	-0.08	1	-	-0.3

$\bar{x}_{a+}$ = mean frequency in the relevant follow up records

Figure 14 shows the results of the "Flash Drives" assessment. The members of the group "age<=38" stated that they occasionally (2.4) think about whether the use of a flash-drive is safe. After the training, the measured frequency-value grew into the "often" area (3.8). A total of 14 participants had the chance to increase their competence and 11 of them did so. The average of the group "age>38" was 3.5 (often) before the training. After participating in the training, the group stated to think about flash-drive security always (4.5) in the future. Overall, 6 of 8 participants were able to change their awareness. However, both groups achieved a change, where in this case the change for the younger group is more pronounced. It seems, that the development-potential depends on the individual foreknowledge and not on the group membership.

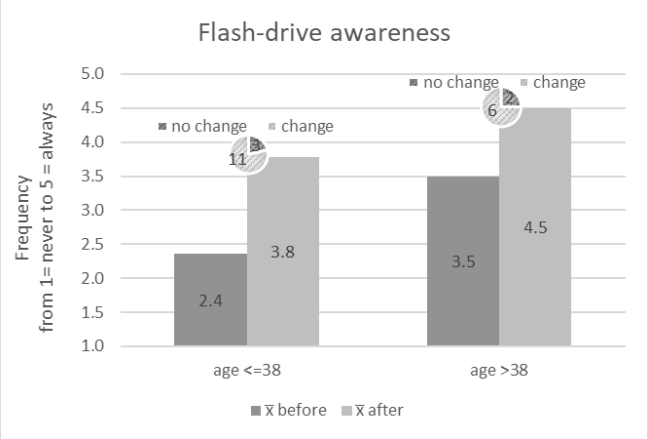

Figure 14. Flash-drive

The follow-up survey results in 8 relevant records for the younger and 4 records for the older group. The group "age<=38" shows 5 differences: three times -3, once -2 and once +1 which results in a mean loss of -0.29 compared to $\bar{x}\ after$. The other group points 3 differences: once -1, once -2 and once +1. This results in a mean loss of -0.50. By that, for the present sample, the deviation can be neglected again. The aftereffect is long-lasting too. It is noticeable, that two participants have changed their behavior more than planned. A possible explanation are exchanges with colleagues or deepening thoughts in the aftermath of the training. This emphasizes that the training's serious topics remain in the consciousness of the subjects even beyond the training. The data are shown in Table VII.

TABLE VII. FLASH-DRIVE FOLLOW UP SURVEY

Group	$\bar{x}_{a+}$	$\bar{x}_{a+} - \bar{x}_a$	Absolute change			AVG change
			-1	*-2*	*+1*	
age<=38	3.5	-0.29	3	1	1	-0.5
age>38	4.0	-0.50	1	1	1	-0.3

Figure 15 shows the data related to the "Network devices" topic. The data indicates, that the competences before the training were very low. In total the group "age<=38" contains 15 relevant records while the group "age>38" contains 8. The mean data of the younger participants shows that they were thinking rarely (1.9) about whether it could be necessary to report new devices. With a value of 1.8 (rarely) the results of the older participants are similar. Accordingly, a large competence increase was achieved through the training. Both groups stated that in future they will think always (4.5 and 4.9) about whether new IT-devices are authorized or not. Moreover, all 23 relevant participants achieved a competence growth. By that, the assumption potential of development depending on the individual foreknowledge and not on the group membership seems to be confirmed. The GHOST-based Training works out for the whole target audience.

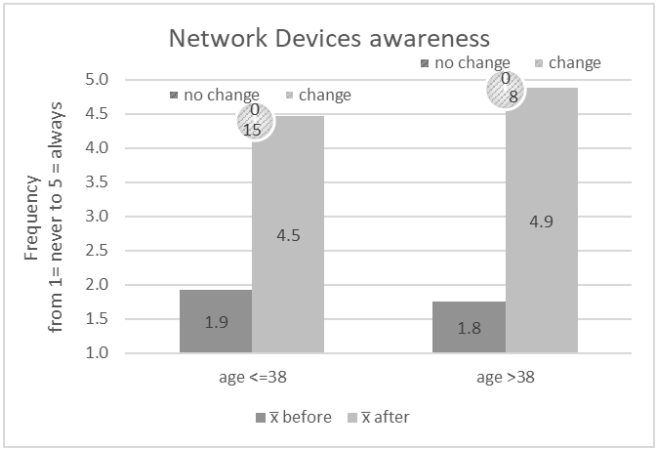

Figure 15. Network Devices

At the follow-up survey, 12 relevant records were recorded. Again, only small differences were found. The group "age<=38" shows 8 relevant records whereby 5 records show deviations. The mean difference is -0.22. In the other group 4 records were registered whereby 2 of them show differences. Overall, the average frequency in the group "age>38" dropped by -0.38. Therefore, for the present data, the deviation can be neglected again. A data overview is presented in Table VIII.

TABLE VIII. NETWIRK DEVICES FOLLOW UP SURVEY

Group	$\bar{x}_{a+}$	$\bar{x}_{a+} - \bar{x}_a$	Absolute change				AVG change
			-1	*-2*	*-3*	*+1*	
age<=38	4.25	-0.22	1	1	1	2	-0.5
age>38	4..5	-0.38	2	-	-	-	-0.5

Based on the assumption that the importance of secure passwords is common sense the password aspect of the prototype is not a classic awareness training. Rather the focus is to teach how to create a safe and simple to remember password. As shown in Section VII, the password mini-game represents an exception in the game design. Also, the mini-game is controllable with one finger, its game mechanic includes action elements that require a quick gameplay. By that it is exploratory checked whether the older age group is able to participate on CDGs that require an action gameplay.

Therefore, the participants were asked to self-assess their ability to generate safe and easy to use passwords. A 4-Point-Scale was used (from strongly disagree to strongly agree). According to the scale, the ability to generate passwords are interpreted in the following way:

- [>=1.0 "D" <1.75] (no ability),
- [>=1.75 "C" <2.5],
- [>=2.5 "B" <3.25],
- [>=3.25 "A" <4.0], (fully capable)

Figure 16 shows the evaluation results regarding the password generation. It is noticeable that the ability before training to generate passwords was already strong. Only 7 participants of the Group "age<=38" and 4 participants of the

group "age>38" had the option to strengthen their ability. This shows how well known the password security topic is especially to the older participants. Maybe another sub-topic of the password theme (e.g., sharing passwords or multiple using of password) would had been more useful for this evaluation to measure more results in the older group. However, for the participants that are 38 or younger the results shown that the measured mean ability to generate safe passwords starts within the B (3.0) area. After the prototype participation it growths into the A (3.9) area. Moreover, 6 of 7 participants were able to achieve a development. The group "age>38" starts within the B (2.5) area and ends within the A (3.5) area but only the half (2 of 4) of the participants improved through the training the other half showed no change. That may indicate that the needed quick game-play required to solve the password mini game overwarm a part of the participants in that group. But because there are only 4 relevant records in this sample that kind of assumption cannot be proved with this study. A further investigation is needed. Regardless to that, it could be shown that a calm-gameplay works out to convey serious content to the whole target audience.

An evaluation of the follow-up survey is not made because of a lack of data.

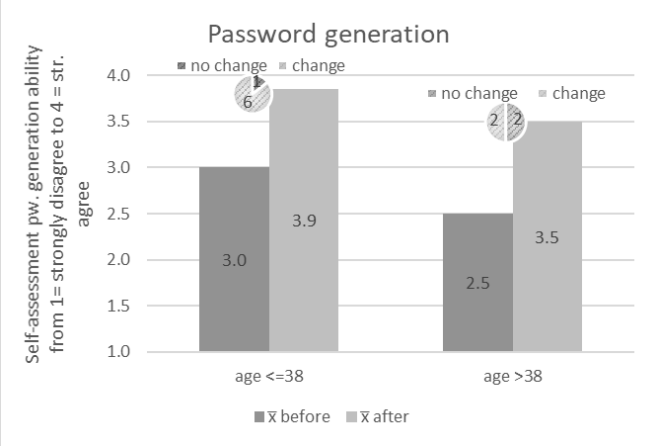

Figure 16. Passwords

To determine whether the measured awareness (Screen Lock, Flash-drive, Network Devices) or ability (Password generation) changes statistically significant t-tests are performed. It is assumed that the training increases the awareness or ability. Therefore, one-tailed t-tests for dependent samples were calculated. An overview of the training effects and the corresponding t-test results are shown in Table IX. The results show that with a $\alpha = .05$ the changes are statistically significant. There was only one exception found. The group "Age>38" shows no statistic significant change regarding the password generation topic. A possible explanation can be found in two aspects. First, only the password mini-game requires a quick gameplay because of its action-based game mechanics. Second, there were only four participants in that group that had the possibility to improve their ability to generate passwords. Therefore, it is not possible to select which of these both aspects were the crucial one by studying the data. Nevertheless, the test leaders pointed out that they noticed many participants of the older group having trouble playing the password mini game. Such a subjective impression was not reported for any of the other training sections.

TABLE IX. OVERVIEW OF THE TRAINING EFFECTS

	Age<=38			***Age>38***		
	x̄ before	**x̄ after**	**p-value**	**x̄ before**	**x̄ after**	**p-value**
Screen Lock	3.6	4.2	.003	2.9	4.8	.001
Flash-drive	2.4	3.8	.0004	3.5	4.5	.004
Network Devices	1.9	4.5	<.0001	1.8	4.9	.0002
Password	3.0	3.9	.0005	2.5	3.5	.09

IX. CONCLUSION

GHOST is a new approach to perform a cybersecurity awareness training for end users in companies. It was shown how the serious game content was systematically developed out of the well-known ISO 27001 and it was also elaborated what kind of requirements a cybersecurity awareness training should fulfill. Further it was shown that the majority of the resulting seven requirements could be fulfilled through an adequate game design. A GHOST training can take place at the place of work to reduce the time expense. Since an extensive preparation is not needed the organizational overhead is reduced. Both aspects also reduce the training costs (req. 2a-c). The turn-based, business game inspired game design allows further a continuous training cycle, that is made possible with a computer-based training (req. 6 and 7). Moreover, the social significance of - and the increased attacks on- IT systems leave no doubt on the real-life relevance of the underlying problem (req. 4).

The requirements 1, 3 and 5 needed a further investigation. Requirement 5 asks for a game quality that is similar to entertainment games. It is shown that nowadays even mobile entertainment games have a sophisticated game environment often represented as a three-dimensional game world. Requirement 3 asks to make the training accessible for every target group member. To fulfill these both requirements a new kind of interaction design for three-dimensional tablet games is developed and evaluated through an empirical study.

Requirement 1 asks amongst other things for a training that helps the participants to develop specific skills. To prove this aspect a prototype that includes the four serious topics Screen Lock, Flash-drive, Network Devices and Password is implemented. The prototype is designed to fulfill the awareness training requirements that are introduced in this paper. By that, the prototype is suitable for an evaluation of the GHOST concept. An appropriate evaluation was performed through an empiric study. The results indicate that the GHOST prototype leads to a grown cybersecurity awareness and at the same time is enjoyable. Thereby, it can be shown that the postulated requirements and the proposed

implementation leads to a productive Competence Developing Game for the Cybersecurity Awareness Training.

Future research could evaluate to what extend the GHOST concept is usable for CDGs for other serios topic. To considerate CDGs for related topics in first, could be a meaningful approach. In this context, it is planned to examine the usefulness of the GHOST concept for digitalization education as a next step. Additionally, the implementation of the whole 16 game round CDG in a commercial context is intended.

REFERENCES

[1] J. A. König, M. R. Wolf, "Cybersecurity Awareness Training provided by the Competence Developing Game GHOST", ACHI 2018, pp. 81-87, 2018.

[2] A. Nagarajan, J. M. Allbeck, A. Sood and T. L. Janssen, "Exploring game design for cybersecurity training", Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), IEEE International Conference, pp. 256-262, 2012.

[3] S. Culp, "Cyber Risk: People Are Often The Weakest Link In The Security Chain", Forbes, [Online]. Available: https://www.forbes.com/sites/steveculp/2016/05/10/cyber-risk-people-are-often-the-weakest-link-in-the-security-chain, Last access: 13.11.2017, 2016.

[4] J. A. König and M. R. Wolf, "A New Definition of Competence Developing Games," ACHI 2016, pp. 95-97, 2016.

[5] J. A. König and M. R. Wolf, "The Pyramid Assessment Framework for 'Competence Developing Games'", HCI International, pp. 232-237, 2016.

[6] S. Seyda and Werner, "IW Continuous Vocational Training Survey 2014 - Companies Show In-creased Committed and Invest more in Enhancing their Employees' Skills", Cologne Institute for Economic Research, 2014.

[7] Gesellschaft für Innovationsforschung und Beratung mbH., "Empirical monitoring to the qualification situation in the German economy" (original foreign title: "Empiriegestütztes Monitoring zur Qualifizierungssituation in der deutschen Wirtschaft"), Berlin: Federal Ministry for Economics Affairs and Energy, 2014.

[8] BIBB, "Data Expose to the Vocational Training Report 2017 – Information and analysis in on the development of vocational training" (original foreign title: „Datenreport zum Berufsbildungsbericht 2017 - Informationen und Analysen zur Entwicklung der beruflichen Bildung"), Federal Institute for Vocational Education and Training, 2017.

[9] R. Hunicke, M. Leblanc and R. Zubek, "MDA: a formal approach to game design and game research" In: Proceedings of the Challenges in Games AI Workshop, Nineteenth National Conference of Artificial Intelligence, 2004.

[10] S. Deterding, D. Dixon, R. Khaled and L. Nacke, "From game design elements to gamefulness: defining "gamification"", Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments. Finland: ACM, pp. 9-15, 2011.

[11] U. Blötz, "Business Games and Serious Games in Vocational Training" (original foreign title: "Planspiele und Serious Games in der beruflichen Bildung"), Bertelsmann, 2015.

[12] D. Michael and S. Chen, "Serious Games: Games That Educate, Train, and Inform," Thomson Course Technology PTR, 2005.

[13] GTAI, "The Gaming Industry in Germany", Berlin: Germany Trade and Invest, supported by Federal Ministery for Economics Affairs and Energy, 2016.

[14] J. Schell, "The Art of Game Design – A Book of Lenses", 2. Edition, mitp, 2016.

[15] L. N. Taylor, "Video games: perspective, point-of-view, and immersion", Master Thesis - University of Florida, 2002.

[16] D. A. Bowman, E. Kruijff, J. J. LaViola Jr. and I. Poupyrev, "3D User interfaces: Theory and Practise", Addison Wesley, USA, 2005.

[17] T. Hynninen, "First-Person Shooter Controls on Touchscreen Devices: a Heuristic Evaluation of Three Games on the iPod Touch", Master Thesis - University of Tampere, department of Computer Sciences, 2012.

[18] ISO/IEC 27001:2013 - Annex A, information technology - Security techniques - Information security management systems – Requirements, 2013.

[19] W. A. IJsselsteijn, Y. A. W. de Kort, K. Poels, "The Game Experience Questionnaire", Eindhoven Univversity of Technology, 2013.

[20] K. Vohwinkel, "Playability: Evaluation of computer and video games" (original foreign title: "Playability: Evaluierung von Computer- und Videospielen"), Thesis, University of Cologne, 2010.