CySecEscape 2.0—A Virtual Escape Room To Raise Cybersecurity Awareness

Emanuel Löffler[1], Bettina Schneider[2], Petra Maria Asprion[3], Trupti Zanwar[4]
[1-4] *University of Applied Sciences and Arts Northwestern Switzerland FHNW*
emanuel.loeffler@fhnw.ch, bettina.schneider@fhnw.ch,
petra.asprion@fhnw.ch, trupti.zanwar@students.fhnw.ch

Abstract

An increasing number of small and medium-sized enterprises (SMEs) use the Internet to support and grow businesses. The application of new technologies comes with inherent risks of ever-changing cyberspace and increasing cybercrime. Previous research has shown that the human factor remains the core element in the cybersecurity chain. Therefore, it is paramount that employees receive effective training to acquire a security mindset. This study puts forward previous research that resulted in a portable escape room game to raise cybersecurity awareness. The purpose of the study is to elaborate the transformation of the physical game into a virtual learning experience to increase flexibility in times such as the Covid-19 lockdown. As main method, we applied the design science framework of Hevner et al. As main result, the research elaborates the design of the developed artifact—a virtual prototype of the escape room game addressing the cybersecurity challenges of SMEs. For the evaluation of the prototype, empirical data was collected in qualitative and quantitative form. As main conclusions, we have observed that a physical escape room can be transformed into a virtual setting with little means without sacrificing player immersion. A limitation was identified in teaching targeted social engineering attacks.

Keywords: *Cybersecurity Awareness, Escape Room Game, Small and Medium-sized Enterprises, Design Science Research;*

1 Introduction

The rise of digitalization has significantly influenced how companies and their stakeholders interact, as it enables virtual business to be conducted over the Internet with no physical space to set up, and no assets to own or store. However, these promising opportunities are associated with novel risks such as cyber threats and cybercrime. Concerning large companies, the importance of cybersecurity has been recognized and resources are being mobilized to implement formal methods that promote awareness and adaptation of cybersecurity processes in their workforce [1]. Small and medium-sized enterprises (SMEs)—although representing the backbone of economies around the world—struggle with significantly tighter resource constraints, while facing similar cyber threats. According to recent surveys, the proportion of small firms reporting one or more incidents is at 41% [2], and lack of employee awareness remains the number one cause for security incidents [3]. Therefore, employee trainings are key for mitigating the risks posed by cyberspace. A sound awareness program ensures that people understand the organization's policies, their

responsibilities in the field of cybersecurity as well as the proper use and protection of organizational assets.

Several interactive training approaches have been designed in recent years, of which a very promising one is the escape room technique. Escape rooms are typically designed for recreational purposes, in which players face real-world simulated challenges as a team [4]. The usage of the escape room technique is growing for corporate training along with its recreational value [5].

This study addresses the cybersecurity awareness challenges of SMEs using this new training approach. The objective is to develop and evaluate a prototype to train employees in cybersecurity. The study is based on existing research results from a physical cybersecurity escape room that is played in the office environment of SMEs [6]. Facing the Covid-19 pandemic, escape rooms relying on physical presence in one room turned out to be a bottleneck. Prompt adaptation to the "new normal" was required and led our research team to transform our existing physical game into a virtual escape room variant.

Our hypotheses for this paper are as follows:

- *Adaptability:* A physical escape room setting can be transformed into a virtual experience with few adaptations to the original concept. However, we make the assumption that a virtual setting needs more intentional distractions (decoys) because virtual objects do not allow creative interaction in the same way physical objects do. Participants in an online setting might address puzzles more directly.
- *Immersion:* In comparison to physical setups, a virtual escape room environment might be less immersive.
- *Memory:* Increased flexibility and standardization of the game through virtualization eases scaling and presumably fosters follow-up discussions between colleagues on how they solved the game, giving an advantage in memorizing through repetition.

The remainder of the paper is structured as follows: Section 2.1 elaborates the Design Science Research methodology applied. Section 2.2 describes design guidelines for escape rooms from the literature and provides an overview of existing cybersecurity escape rooms. To embed the study in its environment, cybersecurity-related challenges of SMEs are outlined in Section 2.3. At the core of this research, in Section 3, the next revision—a virtual escape room game—is presented. In Section 4, the evaluation results of the virtual prototype are described and discussed. The paper closes with an outlook on areas for further research.

2 Methodology and previous work

2.1 Design science research as methodological framework

As a methodological approach, the Design Science Research (DSR) guidelines were applied [7]. According to Hevner et al. [8], DSR must lead to an artifact, which could be a construct, model, method, or an instantiation. This was considered suitable for our research, which aims to yield a learning approach as a cybersecurity escape room. The DSR approach is moreover very appropriate as it aligns research processes with real-world problems, and as it helps integrating business with technical aspects. A first version—a physical, portable game called *CySecEscape 1.0*—was derived from the existing knowledge base and the SMEs' environment in Switzerland. The prototype was improved based on the evaluation obtained by game executions and feedback rounds with SME employees. The results were published in the 2020 Future of Education Conference [6]. In this paper, we focus on a second version of the prototype. Due to the Covid-19 pandemic hitting Europe in 2020, the application of a cybersecurity escape room demanding physical presence has become a bottleneck. The second design cycle thus elaborates the transformation and enhancement

of *CySecEscape 1.0* into a virtual learning experience, called *CySecEscape 2.0*. Figure 1 shows how the research framework was adapted.

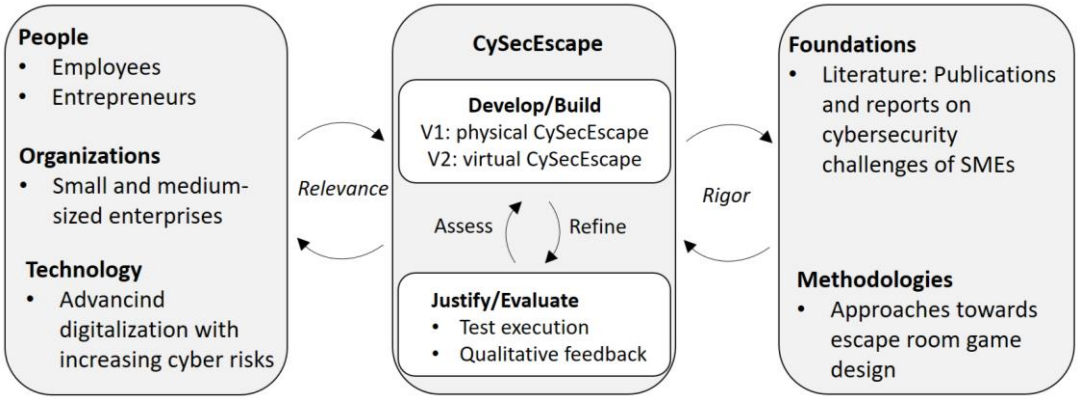

Figure 1. *Hevner et al. framework adopted to the study*

As shown in the right box of Figure 1, the knowledge base is relevant for the rigor cycle. In a literature review, the design of escape rooms was analyzed and existing escape rooms in the field of cybersecurity were identified. The left box of Figure 1 is the environment, represented by SMEs in Switzerland and composes the relevance cycle. Based on recent publications, cybersecurity-related challenges of SMEs were collected.

Two design loops are present, whereas the first resulted in the already existing and published *CySecEscape 1.0*, the second design loop is the core of this study and resulted in *CySecEscape 2.0*—a virtual escape room to raise cybersecurity awareness in SMEs. When evaluating the developed artifact, empirical data was collected by testing the game with selected SME representatives and full-time as well as part-time students. Two test rounds with SME-employees were conducted in groups of two with physical presence of a moderator documenting their interaction and questions and giving advice when needed. In this setting, a computer was provided for ideal playing conditions, leading to very positive feedback. In the student test rounds, learners were provided with a web link to play the prototype on their own devices during a remote lecture setting. Here, positive feedback prevailed as well. Nevertheless, more difficulties interacting with the interface were reported, which can be explained by the absence of a physically present moderator. Remote players were more prone to explore alternative solutions through inspecting the game source code, where a "hidden path" of playing was in place (see also 3.1.).

2.2 Escape room design and existing cybersecurity escape rooms

In the escape room game setup, participants form a team attempting to solve puzzles with the help of clues and strategies to escape from a confined area in a given time span [5]. Escape room challenges involve activities demanding close coordination and teamwork such as situational awareness, task division and specialization, communication, leadership, as well as critical and lateral thinking [5]. During these immersive experiences, the individuals take the avatar of the in-game characters and feel very connected to the situation at hand. Several approaches to design an escape room can be found (e.g., [9][10]). The design framework by Clarke et al. [11] was chosen to guide this study. It incorporates following elements [6]:

1. *Participants:* When designing an escape room, it is important to put the player at the center. Therefore, the first crucial step is to analyze and understand the needs of the individuals who will experience the game. Classifying the participants into categories helps in deciding the structure, difficulty level, duration and scale (group size) of the game.

2. *Objectives:* Second, it is important to think about and agree on the expected game outcome to ensure that the experience is suitably set up. In addition to classic learning objectives, as a game designer, one needs to consider other soft objectives such as team bonding and coordination, problem-solving and communication skills the participants will develop during the game.
3. *Theme:* The theme is definitely the core of any escape room. The narrative provides the context and justifies the challenges that the players have to master. Themes that are typically chosen are detective mysteries, prison breaks, kidnapper escapes, or spy/espionage games.
4. *Puzzles:* Puzzles connected to the theme build the backbone of the game [10]. The variety of puzzles used in escape rooms is large and ranges from riddles, word puzzles to tasks that require good teamwork, hand-eye coordination or an ability to think outside the box. Puzzles can be used in combination with one another to build a meta puzzle, that is, the solutions from the different puzzles are connected to find the final answer, which provides the solution to escape the room [10]. These so-called paths to arrange puzzles can be a) linear: participants progress sequentially and the solution of the first puzzle leads to the clue for solving the next puzzle; b) open: participants can progress/work in any order. Nevertheless, the final puzzle to escape the room can only be tackled when all other puzzles are resolved; c) multi-linear: a series of linear paths can be played in parallel, whereas intersections and different ending points are possible [10].
5. *Location and equipment:* In this very practical element, it is important to make sure that all features and locations are smoothly integrated into the given theme.
6. *Evaluation:* Evaluating the game experience and refining it continually is the final component of the escape room design framework. The evaluation is closely tied with the objectives defined at the beginning of the design process [12].

Even though escape rooms targeted towards cybersecurity are a new phenomenon, several games already exist. Some are embedded in a university or school context (e.g., [13] [14]); others focus on the corporate world [15]. In addition, mobile and physical game versions playable in a truck are available (e.g., [16][17]).

Besides physical escape rooms, variations such as a tabletop escape room game used by the Virginia State Corporation Commission have evolved [18]. In addition, virtual escape room games in the field of cybersecurity have been developed. Examples stem from commercial providers specialized in cybersecurity offering their virtual experiences as paid service (e.g., [19][20] and more background on virtual escape room games in Section 3.1). The *CySecEscape 1.0* developed by our research team was designed as a physical, portable escape room that can be played in any office environment [6], thereby addressing the special challenges of SMEs in Switzerland summarized in the following section. The virtual *CySecEscape 2.0* elaborated in this paper, also targets small enterprises: The SME-rooted story-line of misconduct in a high-trust environment was adapted from the physical *CySecEscape 1.0.* The puzzles revolve around an unmanaged IT-infrastructure—a case which is less common in larger enterprises.

2.3 Cybersecurity-related challenges of SMEs and implications

As listed in Table 1, SMEs face particular challenges when it comes to cybersecurity.

Table 1. *Cybersecurity challenges of SMEs.*

Criteria	***Description***
Executive awareness	A recent Swiss cybersecurity survey [21] revealed that only a small proportion (11%) of SME executives expect to fall victim to a cyberattack causing their company to be out of service for at least one day. This shows that risk awareness is low.
Resources	Although increasingly faced with the same cybersecurity risks as larger companies, SMEs are confronted with tighter resource constraints. As an example, only 9% of Swiss SMEs invested in additional IT security measures during the first wave of Covid-19 [21].
Responsibility	Within SMEs, responsibility for setting IT security strategy and priorities is dispersed. Therefore, the ability to have effective leadership in the IT security function is missing in many SMEs [22].
Workforce skills	More in-house expertise is imperative in SMEs to strengthen their cybersecurity postures. However, according to a study of Ponemon LLC [22], less than one third of the participating small businesses rated their ability to mitigate cyber-threats as highly effective.
Technology	Since many SMEs utilize third-party vendors to carry out tasks that allow them to grow and scale within their budget, the risk of weak passwords, ineffective mobile device policies, and misunderstanding cybersecurity threats can quickly compromise the entire organization [6].

As implications from the specific situation of SMEs, the escape room designed by our research team considers the following aspects:

Targeted theme: In order to enhance the credibility of the game, the theme relates very closely to the professional life of SME employees. For this reason, the theme selected is investigating financial fraud and finding an absconding rogue employee in a SME.

Time and costs: The pure playing time of the game has to be limited. In the first design loop (physical *CySecEscape 1.0*), it was set to 40 minutes framed by a quick briefing and debriefing session. This way, the participants can predict the time investment very well. In the second design loop (virtual *CySecEscape 2.0*), time is more flexible with game executions now more independent of a game proctor or host. Nevertheless, the time is still foreseen to be limited to 40 min in order to create the sense of urgency, which is a typical element of escape rooms. Briefing and debriefing will also be part of *CySecEscape 2.0* as a virtual introduction and ending sequence. In a related manner, costs are low, possibly zero, disregarding employee working hours, which come into play in each of the settings.

Flexibility: A portable escape room (fitting in a cabin size suitcase) has been designed for the *CySecEscape 1.0*. All the puzzles designed are created using readily available props such as keys, number lock, plants, laptop (carrying preconfigured email inbox, social media account, Microsoft Excel files) and mobiles. The virtual setup is designed to run inside any modern web-browser on a suitable screen, starting from tablet sizes.

Small group size: In the physical escape room, a minimum of two and a maximum of four participants can effectively play the game as a team. In the virtual scenario (*CySecEscape 2.0*), the game can be played individually or by very small teams.

The special feature of this study and prototype is the focus on the real-world SME life and challenges. Moreover, as virtual variant, location is no issue. Nevertheless, the game is set up in a virtual office environment of a typical SME, therefore being both flexible and ensuring a good level of immersion into a real-world context.

3 Results

Readers interested in more details on the design of the physical *CySecEscape 1.0* are referred to our existing publication [6], where we describe the SME-focused game development including the design elements, the topics and puzzles, as well as the game flow. The following sections are dedicated to the next revision, the virtual *CySecEscape 2.0*.

3.1 Design decisions for the virtual escape room

Our research team, when transforming the existing physical escape room into a virtual experience, made the following design decisions.

Virtualization: The Covid-19 pandemic fundamentally changed public life in general and the way SMEs could work and interact. One of the most common changes in all industries was a sharp rise in remote work due to increased risks of infection. In cases where employees were not equipped with mobile devices from their employers, private devices became part of the working tools. Our initial design of playing the escape room directly at the SME offices thus had to be altered and needed to reflect the necessity of "physical distancing". However, with homes and private devices introduced to SME environments, the need for cybersecurity awareness has even increased and calls for alternative means of education. Thus, we decided to invest our resources in the transformation of the physical cybersecurity escape room into a virtual artifact. The game should become playable in a web-browser with basic modern functionality (HTML5+CSS3, Javascript) rendering it sustainable through independence from a specific platform. This way, it could serve both as a self-contained game and as a teaser module for our physical setup once it can be applied again. Most of our physical escape room content was easily transported into a virtual setting. Game props are now represented as graphics in a graphical environment.

Story design: The original story had to be altered in minor ways. As an example, a simulated social engineering phone call had to be removed. In exchange, a turn of events was added to the end of the existing storyline to include the issue of identity theft and impersonation, which has become a pertinent issue during the pandemic, where personal interaction for reassurance of valid identities in communication has become very difficult.

Visual and interactive design: In a first development phase, we decided to sketch the visual design (see Appendix), giving it a similar comic-style approach to the one used in *CySecEsape 1.0* to introduce the storyline (this video remains part of the virtual game). The players are presented with a visualization of an office desk with several objects that can be enlarged through clicking/tapping (e.g., wall calendar), that can be manipulated (e.g., opening a drawer), or that lead to puzzles (e.g., guessing the locker combination). A number of decoys were placed in the game, making the environment more immersive and solutions less obvious. The complexity of the game can be adjusted through these decoys. In addition to the intended game flow, a "hidden path" is available that engages players with advanced IT knowledge that may try to inspect the game source code. Strategically placed comments in the code address the players and build the foundation of discussing real-world options of compromising a computer (e.g., retrieving a password from the source code demonstrates the need for secure password storage through hashing). Both paths (original and "hidden") can be played individually or in sessions with two players sharing a screen.

Supervision and support: With a physical setup, the host can step in and support the players whenever they appear to need help. This aid is common in physical escape room setups. Thus, our virtual design needed an adequate replacement. To observe player interaction with the game without host intervention, a small sample of observed test rounds was arranged under strict Covid-19 security measures. With the eventual decoupling of game instructor and player in mind, we ran two test rounds with two participants each and the game developer in a room. After these test rounds, minor changes were made to the user

interface, removing the most common misconceptions observed. A larger round of tests with three online classes of students was run successfully without personal observation and without the need for human intervention.

Development approach: Escape rooms and related riddles have existed as a motif in various video game settings for a long time. It can be assumed that escape rooms in fact originated from the virtual medium [23]. Ancestors to be named are text adventures such as the 1988 game Behind Closed Doors leading to the genre of graphical Point-and-Click games that encompass the famous escape room series by Japanese developer Toshimitsu Tagaki. He started with Crimson Room in 2004, where players found themselves locked in a three-dimensional room without any clues on why they were locked in or how to escape, leaving them to find objects that later formed parts of the larger puzzle [24][25]. Crimson Room, one of the most successful browser games of its time, was based on the proprietary platform Adobe Flash, which has been discontinued by Adobe. We assumed that, even though Crimson Room can still be found online, without the availability of Flash it cannot be run easily anymore on a modern computer. Even though the case of Adobe Flash went in another direction and with the Open Source Software Ruffle (https://www.ruffle.rs), there is now a modern way of running Flash, the risk of time rendering a program obsolete due to external dependencies remained. Learning from this, we have chosen a minimalistic approach based on open standards, utilizing only HTML+CSS and JavaScript without additional Frameworks or a server backend. This shall ensure the possibility to run the game on all modern and future platforms with the capability of displaying web content and even without the need for a remote server.

Testing phase: For a better insight into the playing experience, two test runs in presence of a game host were conducted. Three more test rounds were included into an online lecture at the FHNW School of Business in Basel, Switzerland. Here, the students were asked to give standardized feedback through a survey tool and to elaborate their experience in the virtual classroom.

3.2 The CySecEscape2.0 prototype

The setup of the developed virtual escape room is summarized in Figure 2.

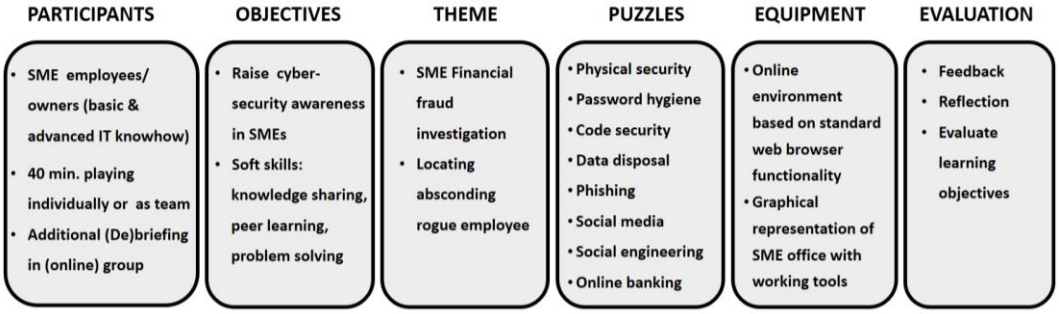

Figure 2. *CySecEscape 2.0 prototype design*

Participants: The escape room addresses SME owners and employees with basic IT knowledge as the main target group. As a new feature, the *CySecEscape 2.0* additionally targets advanced players that are able to investigate the game source code ("hidden path"). Even though time management is more flexible, similar to the initial physical game, the virtual game is foreseen to be limited to 40 min maximum playing time. Whereas the physical escape room was not intended to be used as single player, the virtual version can be executed individually or by a team of two players sharing a screen. The briefing and debriefing still is designed as a group activity.

Objectives: While the overall objective is to raise awareness of cybersecurity, the participants in particular learn the key elements of physical and cyber-security and their applicability in practice. Additionally, soft skills, such as problem solving, are strengthened.

Even in cases where the game is played individually, the group (de)briefing enables knowledge sharing, and peer learning. Team building, which was an objective of the physical *CySecEscape 1.0*, was not regarded as core of the virtual experience. Nevertheless, two people joining forces might still perceive improved team spirit in the context of their shared online adventure.

Theme: The theme revolves around the investigation of financial fraud in a SME and aims at finding an absconding rogue employee. The players seek to save the SME by stopping the online bank transfer carried out by a criminal employee. Participants must find clues left by the fugitive employee and link them together to stop the bank transaction. In addition, the *CySecEscape 2.0* enhanced the storyline to account for identity theft. This extension aims to provide an unexpected turn towards the very end of the game experience.

Puzzles: The puzzles listed in Table 2 are arranged to form a multi-linear puzzle path.

Table 2. *Virtual CySecEscape 2.0—Awareness topics and related puzzles.*

Awareness topic	***Puzzle***
Physical security	Unclean desk contains hints about login credentials.
Password hygiene	Easy-to-guess password.
Source code security	Source code evaluation (“hidden path”).
Information disposal	Bank account data in trash.
Securing sensitive digital data	Password reuse on sensitive file.
Public oversharing/identity theft	The missing employee is found through social media, then turns out to be impersonated.
Phishing and online banking	Phishing mail causes loss of access to bank account (game ends).

Equipment: The newly developed escape room is embedded in a virtual environment visualizing an SME office as described in Section 3.1. The virtual location is supplemented with props such as the office desk, a closet, some plants, or a paper shredder.

Evaluation: To assess the usability and applicability of the game, a questionnaire is used to obtain feedback from the participants. As part of the debriefing, the learning outcomes and goals are reflected in the group and feedback is gathered.

4 Evaluation of the prototype and discussion

As outlined in Section 3.1 under “Supervision and support”, two types of evaluation were conducted: Two small-scale on-premises runs and three medium-scale runs with online-classrooms. Below, these runs will be summarized and followed by a reflection of our hypotheses that were introduced in Section 1.

To receive an early feedback for our developed prototype, four participants tested parts of the game at an early stage of the game development (first three awareness topics from Table 2). In teams of two people the players worked on one shared screen. Conducting the game extract had a duration of 15 minutes. During the test phases, the experiment leader who was present in the same location as the players documented the strategic approaches.

The players were encouraged to “think out loud”, making a qualitative evaluation of thought processes possible (see e.g., [26] on the application of the think-aloud method for usability testing). Most prominently, the following observations were made:

1. The interface design choice proved to be intuitive; there were no questions asked on how to interact with the virtual environment. However, during the tests, the participants were frequently confused by the availability of interactive vs. non-interactive objects included in the game front-end.

2. The immediate approach of both observed teams was to look for the birthdate of the suspect employee's son, displaying a common expectation on how to solve the puzzle. Thus, the approach of re-building this prop from the physical *CySecEscape 1.0* into a decoy proved itself suitable.
3. The availability of non-essential elements such as some pictures on the wall created the necessary degree of difficulty for the game. The players would discuss these findings and tried to turn them into login credentials. With help of such elements, the difficulty of the game can be finely adjusted.
4. As two players shared a screen to conduct the game, it was interesting to observe that the participants equally engaged in the game despite only one player being able to control the environment.

Furthermore, three test runs were conducted in context of an undergraduate IT-Security course at the FHNW School of Business in Basel, Switzerland. Due to the classes being taught online, an evaluation of the players' behavior during the game was not possible. However, discussions after the test gave insights to the students' interaction with the game. In this more professional setting, a considerable number of students had chosen the approach of inspecting the source code of the game and thereby discovering the hidden message to participants on this path of solution. This introduced the possibility of circumventing login procedures by technical means in a real-world scenario and thus allowed for a technically advanced discussion of cybersecurity measures (encryption of hard drives and password hashing). Hereby, the game addresses different levels of expertise at once.

Evaluation sheets of the game experience were filled in after both the offline and online sessions, based on a questionnaire that was developed in the first design cycle. Table 3 summarizes the participants' rating showing that the *CySecEscape 2.0* prototype was overall reaching positive feedback.

Table 3. *Evaluation of playing experience.*

Rating	***Total (n=81)***	***Percent***
Terrible	1	1
Not good	3	4
Ok	27	33
Good	34	42
Great	4	5
No answer	12	15

In Section 1, hypotheses on "Adaptability" of the game scenario into a virtual setting, on "Immersion" and on "Memory" in this virtual setup were devised. In regard to these hypotheses, we have come to the following conclusions:

Adaptability: The transformation of a physical escape room into a virtual experience was largely straightforward, confirming our hypothesis that a physical escape room setting can be transformed into a virtual experience with few adaptations to the original concept. Few changes needed to be made to the story or its elements in the first phase of the game. Solutions for features in the following phases have already been identified: For instance, a virtual desktop environment will be simulated utilizing HTML+CSS and JavaScript, thus facilitating all digital puzzles from our first design loop. However, some limitations became apparent. Specifically, person-to-person interactive scenarios remain difficult to reproduce within the scope of our game development approach. Most prominently, the simulation of a social engineering telephone call cannot be implemented in the same personalized manner as in our first design loop, where a real, personal call attempted to extract information from the players.

The implementation of decoy elements in the game environment had a positive impact on user interaction and led them to reason about various solutions before finding the right one. Yet, caution in the design of decoys is of importance, as players tended to become frustrated if objects were entirely non-interactive.

Immersion: During the screen-based game, the players did not lose focus or talk about things unrelated to the game, showing a high level of immersion. The limited time frame during our test runs might have also contributed by generating a stronger sense of urgency. Under the given testing conditions, the assumption of a lower immersion in screen-based settings was not confirmed.

Memory: Discussions among the participants were sparked, showing a general interest in discussing the game after playing. In a SME context, this effect may lead to the cybersecurity-related conversations expected in our hypothesis, where those who played the game may pass their knowledge on through storytelling and hence improve memorization through repetition.

5 Outlook

As a next step, further development to improve the virtual *CySecEscape 2.0* will be necessary. As an example, embedding personalized photos of dedicated SME workplaces instead of the comic-like workplace will be tested with the aim to increase the sense of affiliation to the visualized location. In addition, the test cycles revealed that for a larger rollout, a hint system with increasingly explicit hints should be included in the game. This way, "offline" interventions with a game proctor during game execution—that risk reducing immersion into the virtual setting—should be minimized.

In our future research, we plan to conduct additional evaluation of both physical and virtual escape room approaches in SME contexts. This will allow for further comparative results that will potentially lead to improvements or enhancements of the games. In particular, we intend to use the learning approaches for a large international research project aiming to raise the cybersecurity and privacy of small enterprises throughout Europe. This H2020 initiative, called GEIGER (https://project.cyber-geiger.eu/) will build a community of certified "Security Defenders" and an innovate learning approach, such as our escape room game, could serve as a building block towards building a cybersecurity awareness.

Appendix

The following screenshot provides an impression of the comic-like office environment used for the *CySecEscape 2.0* initial testing.

The storyline of the *CySecEscape* game can be viewed as a video via https://tube.switch.ch/videos/9a148409

References

[1] Kessler & Co Inc, *Cyber Risk Survey Report 2019. Cyber Risk from a Swiss Perspective*, 2019. Accessed on: Oct 2, 2020. [Online]. Available: https://www.kessler.ch/fileadmin/09_PDFs/KS_Cyber _Report_2019_EN.pdf

[2] Hiscox SA, *Hiscox Cyber Readiness Report 2020*, 2020. Accessed on: Oct 2, 2020. [Online]. Available: https://www.hiscox.de/cyber-readiness-report-2020/

[3] ISACA, *State of Cybersecurity 2019, Part 2: Current Trend in Attacks, Awareness and Governance*, 2019. Accessed on: Oct 2, 2020. [Online]. Available: https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whpsc192

[4] N. Scott, "Creating Engaging Escape Rooms for the Classroom", *Childhood Education*, vol. 94, no. 1, pp. 44–49, 2018. https://doi.org/10.1080/00094056.2018.1420363

[5] H. Warmelink, I. Mayer, J. Weber, B. Heijligers, M. Haggis, E. Peters, and M. Louwerse. "AMELIO: Evaluating the Team-building Potential of a Mixed Reality Escape Room Game", *CHI PLAY '17 Extended Abstracts: Extended Abstracts Publication of the Annual Symposium on Computer-Human Interaction in Play*, New York, Association for Computing Machinery, pp. 111-123, 2017. https://doi.org/10.1145/3130859.3131436

[6] B. Schneider, and T. Zanwar, "CySecEscape – Escape Room Technique to Raise Cybersecurity Awareness in SMEs.", The Future of Education International Conference, edited by Pixel, 2020.

[7] A.R. Hevner and S. Chatterjee, "Design Research in Information Systems", in *Design Research in Information Systems. Integrated Series in Information Systems*, vol 22. Springer, Boston, MA. https://doi.org/10.1007/978-1-4419-5653-8_2

[8] A.R. Hevner, S.T. March, J. Park, and S. Ram, “Design Science in Information Systems Research.” *MIS Quarterly*, vol. 28, no. 1, pp. 75–105, 2004. https://doi.org/10.2307/25148625
[9] M. Wiemker, E. Errol, and C. Adam, *Escape Room Games: ‘Can You Transform an Unpleasant Situation into a Pleasant One?,’* 2015. Accessed on: Oct 2, 2020. [Online]. Available: https://thecodex.ca/wp-content/uploads/2016/08/00511Wiemker-et-al-Paper-Escape-Room-Games.pdf.
[10] O. Heikkinen and J. Shumeyko, *Designing an escape room with the Experience Pyramid model*, Published thesis, 2016. Accessed on: Oct 2, 2020. [Online]. Available: https://www.theseus.fi/handle/10024/112798.
[11] S. J. Clarke, D. J. Peel, S. Arnab, L. Morini, H. Keegan, and O. Wood, “EscapED: A Framework for Creating Educational Escape Rooms and Interactive Games to For Higher/Further Education”, *International Journal of Serious Games*, vol. 4, no. 3, pp. 73–86, 2017. https://doi.org/10.17083/ijsg.v4i3.180
[12] S. Arnab and S. Clarke, “Towards a Trans-Disciplinary Methodology for a Game-Based Intervention Development Process: Towards a Trans-Disciplinary Methodology.” *British Journal of Educational Technology*, vol. 48, no. 2, pp. 279–312, 2017. https://doi.org/10.1111/bjet.12377
[13] L. Ludwig, *Cybersecurity Awareness Escape Rooms – Join the Fun!*, Activity at Security Professionals Conference, 2019. Accessed on: Oct 2, 2020. [Online].
[14] SUPSI, *Hack the Internet. Escape room developed by the Laboratorio tecnologie e media in educazione Dipartimento formazione e apprendimento, SUPSI, Switzerland*, 2019. Accessed on: Oct 2, 2020. [Online]. Available: http://www.school-break.eu/wp-content/uploads/2019/09/HackingTheInternet_TeacherGuide.pdf
[15] S. Jagmetti, *Hack The Hacker – It’s on!*, 2018. Accessed on: Oct 2, 2020. [Online]. Available: https://www.switch.ch/de/stories/escape-room-hack-the-hacker/
[16] Secticity, *Cyber Security Truck.* Accessed on: Oct 2, 2020. [Online]. Available: https://sectricity.com/en/security-awareness-en/cyber-security-escape-room/.
[17] Infosecure, *Race against the clock to gain security awareness and escape before the bang*. Accessed on: Oct 2, 2020. [Online]. Available: https://www.infosequre.com/security-awareness-escape-room
[18] C. Wood, *A Virginia agency built an escape room for cybersecurity training*. Accessed on: Oct 5, 2020. [Online]. Available: https://statescoop.com/a-virginia-agency-built-an-escape-room-for-cybersecurity-training/
[19] Triple Cyberness, *Cyber Security Awareness Training*. Accessed on: Oct 5, 2020. [Online]. Available: https://www.triplecyberness.com/home
[20] EMT, *Online Cyber Security Escape Rooms*. Accessed on: Oct 5, 2020. [Online]. Available: https://www.emtdist.com/products/layer-8-security/online-cyber-security-escape-rooms/
[21] M.K. Peter, A. Hölzli, A.W. Kaelin, K. Mändli Lerch, P. Vifian, and N. Wettstein, *Digitalisierung, Home-Office und Cyber-Sicherheit in KMU. Ein Beitrag zum Verständnis und zur Stärkung von Schweizer KMU mit 4 – 49 Mitarbeitenden im Umfeld von Corona (COVID-19)*, 2020. Accessed on: Feb 17, 2021. [Online]. Available: https://kmu-transformation.ch/wp/wp-content/uploads/2020/12/Digitalisierung-Home-Office-Cyber-Sicherheit-KMU-2020-12.pdf
[22] Ponemon Institute, *2018 State of Cybersecurity in Small & Medium Size Businesses*, 2018. Accessed on: Oct 2, 2020. [Online]. Available: https://www.keepersecurity.com/assets/pdf/Keeper-2018-Ponemon-Report.pdf
[23] J. Risler, “Escape Room Challenge: Does Your Team Have What it Takes?”, *Security Magazine*, Feb 2020. Accessed on: Oct 5, 2020. [Online]. Available: https://www.securitymagazine.com/articles/91794-escape-room-challenge-does-your-team-have-what-it-takes.
[24] E. Kroski, *Escape Rooms and Other Immersive Experiences in the Library*. American Library Association, 2018.
[25] K. Penttilä, “History of Escape Games. Examined through Real-Life-and Digital Precursors and the Production of Spygame”, Published Thesis, 2018. Accessed on: Oct 5, 2020. [Online]. Available: https://www.utupub.fi/bitstream/handle/10024/145879/History_of_Escape_Games_ProGradu_Katriina_Penttil%C3%A4.pdf.
[26] S. McDonald, H. M. Edwards, and T. Zhao. "Exploring think-alouds in usability testing: An international survey." *IEEE Transactions on Professional Communication*, vol. 55, no. 1, pp. 2–19, 2012. https://doi.org/10.1109/TPC.2011.2182569