CySecEscape – Escape Room Technique to Raise Cybersecurity Awareness in SMEs

Bettina Schneider[1], Trupti Zanwar[2]

University of Applied Sciences and Arts Northwestern Switzerland FHNW, Switzerland[1,2]

Abstract

With the evolution of information technology, more and more small and medium-sized enterprises (SMEs) are using technology to support and grow businesses. With the prevalence of the internet, SMEs are constantly evaluating and adapting new technologies such as software as a service, cloud computing, or the internet of things. All these new opportunities are coming with inherent risks of ever-changing cyberspace and overgrowing cybercrime. SMEs are soft targets for cybercriminals and the need for controls is evidenced by accumulating fraud incidents, identity thefts, denial of service attacks and illicit accesses or breaches of data over the last few years. This limits the ability of SMEs to innovate and gain business advantage. Previous research has shown that the human factor remains the weakest link in the cybersecurity chain, so it is paramount to make sure the employees receive effective training to embrace a security mindset. This study focuses on developing a prototype of a portable escape room to raise cybersecurity awareness in SMEs. Evaluation highlights that the escape room method is a worthy instrument.

Keywords: *cyber security awareness, escape room technique, small and medium-sized enterprises*

1. Introduction

Digitalization has fundamentally influenced the way companies and their stakeholders interact with each other, making it possible to conduct virtual business over the internet without setting up physical premises as well as owning or storing goods. These promising opportunities are associated with risks such as data breaches or cybercrime. Small and medium-sized enterprises (SMEs) that build the backbone of economies around the world are facing serious challenges related to cybersecurity as described in Table 1.

Table 1: SME Cybersecurity Challenges Based on [1]

Resources	Although cybersecurity risks for larger companies as well as SMEs are similar, SMEs are confronted with tighter resource constraints that make it difficult to invest in cyber security measures.
Expertise	To strengthen their cybersecurity postures, SMEs need more in-house expertise. However, understanding of how to protect the company against cyber-attacks is reported to be lacking.
Responsibility	Responsibility for determining cybersecurity priorities is dispersed throughout SMEs. Therefore, the ability to have effective leadership in the cybersecurity function is missing in many SMEs.
Technology	Many SMEs use third party providers to support their processes. While this allows them to grow and scale within their budget, there is a risk of misjudging the remaining cybersecurity threats, which can quickly affect the entire organization.

A considerable number of incidents in SMEs are due to negligent employees [1]. Therefore, awareness trainings are key for mitigating the risk. Several interactive training approaches have emerged in recent years. One very promising is the escape room technique. This study addresses the cybersecurity awareness challenges of SMEs using this approach.

2. Escape Room Technique

In escape room games, participants form a team to solve puzzles with the help of clues and strategies with the aim to escape from a confined area in a given time span. 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 [2]. During these

immersive experiences, the individuals take the avatar of in-game characters and feel very connected to the situation at hand. For designing an escape room, the framework of [3] and recommendations of [4] suggest to consider following elements:

Participants: Analysing and understanding the needs of the people who will experience the game is a crucial first step. Identifying the participant type helps in deciding the structure, difficulty level, duration as well as scale (group size).
Objectives: It is important to be clear about the concrete objectives and outcomes to be achieved through the game in order to shape the experience accordingly. In addition, game designers should include soft skills such as team building and coordination, problem solving and communication skills as a goal of personal development for the participants.
Theme: At the core of any escape room, a theme conveys the narrative, provides a context and justifies the challenges the participants must experience. Some popular themes are detective mysteries, prison breaks, escape the kidnapper or spy/espionage games. The theme forms the foundation for subsequent elements.
Puzzles: Puzzles such as word riddles, physical exercises, and tasks requiring teamwork, hand-eye coordination or the ability to think outside the box, constitute the backbone of the game. It is possible to combine the puzzles into a meta-puzzle, i.e. the individual solutions are linked together to find the final answer needed to escape the room. These so-called 'paths' can be a) **linear** (a puzzle leads sequentially to the clue for solving the following one), b) **open** (working on puzzles is possible in any order to arrive at the final solution), c) **multi-linear** (several linear paths towards a final solution can be played simultaneously, with intersections and different ends possible).
Location & Equipment: Very practically, all physical features have to be smoothly integrated into the game. The environment, in which the experience takes place, needs to be safe and pleasant.
Evaluation: Evaluating and constantly refining the escape room is an important task helping to reach the intended objectives.

Although a new phenomenon, there are several cybersecurity escape rooms for corporate purposes, including mobile versions that can be played in a truck, e.g. [5], [6]. The originality of this study and the prototype is its focus on the challenges faced by SMEs and the associated creation of a portable game. Being played directly in the SMEs' own office, it is flexible and ensures a high degree of identification with the reality of work.

3. CySecEscape – Portable Escape Room for SMEs

To meet the SME needs, the 'CySecEscape' prototype considers following aspects:

- **Targeted theme:** To enhance immersion, the theme relates closely to the professional life of SME employees. It revolves around investigating financial fraud and finding an absconding rogue employee.
- **Time & costs**: The pure playing time is limited to 40 minutes framed by a quick briefing and debriefing session. This way, the participants can predict the time investment very well. In addition, costs should be controlled to make the game an attractive proposition for SMEs.
- **Flexibility**: The designed game is portable (fitting in a cabin-size suitcase). All the puzzles rely on easy-to-obtain requisites such as keys, plants, and a laptop.
- **Small scaling**: A minimum of two and a maximum of four participants can effectively play the developed game.

Figure 1 summarizes the features of 'CySecEscape':

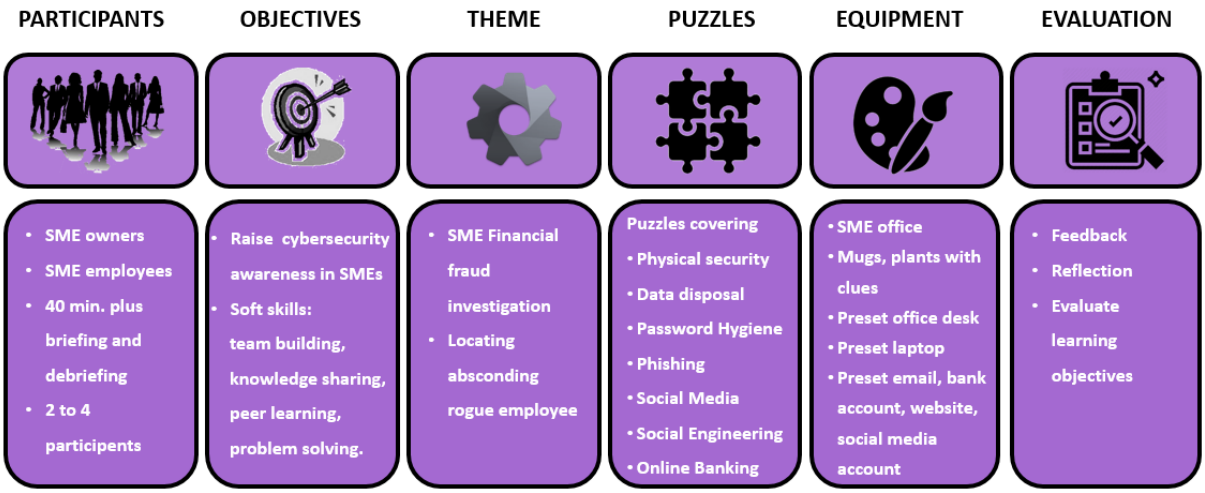

Figure 1: Prototype Applying the Approach of [3]

Participants: The escape room addresses SME owners and employees. Their particular challenges in the area of cybersecurity were analysed as a prerequisite for understanding the target group.
Objectives: While the overall objective is to raise cybersecurity awareness, the participants should in particular become familiar with the key elements of physical and cybersecurity and their applicability in practice. Additionally, soft skills such as problem solving and peer learning are encouraged. A literature review and expert interviews resulted in relevant topics the game intends to improve (Table 2).

Table 2: Topics and Puzzles

Topic	Puzzle
Physical Security	Players experience effects resulting from not having a clean desk, e.g. when a key for a cupboard is easily accessible or a smartphone is left on the desk.
Information Disposal	During the game, participants get the clue to the bank contract number from half shredded and not well-disposed bank statement.
Password Hygiene	As an example, players experience the effects when passwords are easy to guess (i.e., using name of child and year of birth whereas this information is placed openly on photos and mugs on the office desk).
Securing Sensitive Digital Data	The puzzles address unprotected Excel files containing critical business data and the use of the same password for multiple critical business applications, including mailbox and social media accounts.
Public Oversharing	By posting too much information publicly in social media, the location of the criminal employee can be discovered in the course of the game.
Phishing & Online Banking	A phishing email in the mailbox hinders access to online banking.
Social Engineering	The game simulates a telephone call placed by a person pretending to be a bank employee trying to obtain a password.
Remark: wide variety of topics concerning specific SME situations like WiFi security, software updates, procedures around access/ways of working in critical business applications can be covered by adapting the puzzles.	

Theme: The game deals with financial fraud in a SME committed by an in-house employee. The players seek to save the SME by stopping the online bank transfer carried out by the criminal. Participants must find clues left by the fugitive employee and link them together to stop the bank transactions. Figure 2 shows the game flow covering the phases with related activities and media.

Activity	Context Setting	Initial Investigation (Team Building)	Connecting the clues	Stopping the crime
Medium	Letter / Video	Physical work + Puzzle	Online activity	Online activity
	Phase 1 (5')	Phase 2 (10')	Phase 3 (15')	Phase 4 (10')

Figure 2: Game Flow

Puzzles: The puzzles listed in Table 2 serve as core of the game, forming a multi-linear path.
Equipment & Location: Commonly available props such as the office desk, some plants, or a paper shredder are used to play the game at the SME location.
Evaluation: A developed questionnaire helps to get the participants' feedback on the usability and applicability of the game and to assess the learning objectives. Moreover, the game master observes the performance and effectiveness of the participating groups in order to provide an overview of the current state of knowledge during the debriefing and to suggest further measures.

Four groups comprising twelve employees from different sectors and with varying levels of cybersecurity expertise formally tested the prototype. The usability was rated as 'very good' with a score of 4.46 out of 5 points. In terms of usability, the participants appreciated the captivating theme, the puzzles on key topics, the portability, the short duration, and the limited budget required for the game. Further feedback from the players showed that the developed prototype is a highly instructive, immersive, entertaining and engaging team building activity.
The game master's observations revealed several areas, in which the groups did not know the concepts and learned them from the fellow players. Especially the awareness of phishing is a topic where all groups failed to discover the trap.

4. Conclusions and Future Research

Overall, it can be concluded that the escape room method is a worthy instrument to increase cybersecurity awareness in SMEs. In future, it will be critical to evaluate the long lasting effects of the training to ensure the objective being met.
The current version of the game is designed for small group sizes. The puzzles are very interactive and require the attention of the game master. This allows for a very intense experience. However, it turned out to be a limiting factor that it is difficult to run multiple instances of the game in different rooms in parallel.
With the SMEs being resource constrained, one more area to be explored is how 'CySecEscape' can be embedded in a wider context (e.g., training-as-a-service offering). Altogether, there is good amount of potential in game-based learning methods like escape rooms, and their applicability in enterprise awareness trainings should be expanded further.

References

[1] Ponemone Institute "2018 State of Cybersecurity in Small & Medium Size Businesses", https://www.keepersecurity.com/assets/pdf/Keeper-2018-Ponemon-Report.pdf, 2018.
[2] Warmelink, H., Mayer, I., Weber, J., Heijligers, B., Haggis, M., Peters, E., Louwerse, M. "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, 2017, 111-123.
[3] Clarke, S. J., Peel, D. J., Arnab, S., Morini, L., Keegan, H., Wood, O. “EscapED: A Framework for Creating Educational Escape Rooms and Interactive Games to For Higher/Further Education”, International Journal of Serious Games, 4(3), 2017, 73-86.
[4] Heikkinen, O.; Shumeyko, J. “Designing an escape room with the Experience Pyramid model”, https://www.theseus.fi/handle/10024/112798, 2016.
[5] Sectricity. “Cyber Security Escape Van”, https://sectricity.com/en/security-awareness-en/cyber-security-escape-van/, 2020.
[6] riske & jorns GmbH. “The Honeypot”, https://www.awareness-escape-truck.de/, 2020.