Journal of Cybersecurity Education, Research and Practice

Volume 2022 | Number 1 Article 5

2021

A Serious Game For Social Engineering Awareness Creation

Fabian Muhly
School of Criminal Sciences, University of Lausanne, Switzerland, fabian.muhly@unil.ch

Philipp Leo
Cyber Risk Expert, Leo & Muhly Cyber Advisory, leo@leomuhly.com

Stefano Caneppele
School of Criminal Sciences, University of Lausanne, Switzerland, stefano.caneppele@unil.ch

A Serious Game For Social Engineering Awareness Creation

Abstract

Social engineering is a method used by offenders to deceive their targets utilizing rationales of human psychology. Offenders aim to exploit information and use them for intelligence purposes or financial gains. Generating resilience against these malicious methods is still challenging. Literature shows that serious gaming learning approaches are used more frequently to instill lasting retention effects. Serious games are interactive, experiential learning approaches that impart knowledge about rationales and concepts in a way that fosters retention. In three samples and totally 97 participants the study at hand evaluated a social engineering serious game for participants' involvement and instruction compliance during the game. Field observations and unstructured interviews were used to collect data on participants' engagement, satisfaction and compliance with game master instructions. The findings show that there are potentials in changing the game material and its process to foster these dimensions and make it more useful as an instructional instrument for social engineering awareness creation.

Keywords

Serious Gaming; Social Engineering; Human Factor; Information Security; Experiential Learning; Field Observation; Business and Management Environment

INTRODUCTION

The method of social engineering (SE) was initially defined as an instrument of politics to steer future social change and societal behavior (Popper, 1966). Nowadays, however, SE is rather connected to the exploitation of the human factor in cybercrime and defined as deceiving targets using psychological manipulation techniques (Rusch, 1999; Mouton, 2016; Bullée, 2017). Proofpoint (2019), in their *Human Factor Report*, highlight that almost 99% of cybercrime incidents that were surveyed among their global customer base in 2018 had exploited the human factor for the attack. Even for advocates of the human security dimension, this number seems to be somewhat propagandistically high. However, in a study that lasted for five years, researchers were physically penetrating the security systems of 1,000 banks, using human psychology to steal confidential data about customers. They were successful in 96.3% of the cases (Robinson, 2008). Verizon's (2021) most recent *Data Breach Investigations Report* also states that the majority of data breaches involve a human element. The 2020 Twitter hack also showed the dimension that social engineering attacks (SEAs) can have. Three cybercriminals used SE to hack around 130 Twitter accounts belonging to various politicians and celebrities for monetary gain (United States Department of Justice [DoJ], 2020). But SEAs not only pose risks to banks, politicians, and celebrities they also pose severe security threats to critical infrastructures, the organizations controlling them (Green et al., 2015; Ghafir et al., 2018), and basically to anybody with information that can be exploited by offenders for a financial gain or espionage purposes. It is therefore needless to say that approaches to the detection of and the protection against SE menaces are beneficial for ordinary people in their private lives, as well as for organizations in the public or private sector to keep critical information safe.

A promising approach for the education of people about the concepts and threats of SE is serious gaming (SG). Serious games are interactive, experiential learning tools that educate people about a specific topic in an entertaining way. The current study used an SG approach to evaluate participants' involvement and instruction compliance in three field observations. The findings of those observations were used to improve the game's administration and process before testing the approach experimentally in future research as a tool for reducing people's proneness to fall for SE.

The remaining paper is structured as follows: The following section reviews the origin of the SG vein in more detail, addressing its application in different domains and as a tool for SE awareness creation. Section 3 presents the purpose of the research. Section 4 describes the game's components and the gaming process used in the study. Sections 5 and 6 present the research data and method, as well as the corresponding results. In sections 7 and 8, the results are discussed and concluded before section 9 presents the limitations of the study and the aspirations for future research on the presented approach.

LITERATURE REVIEW

Serious games and SG are relatively new concepts, with serious games being perceived as *games that do not have entertainment, enjoyment, or fun as their primary purpose* (Michael & Chen, 2005, p. 21). Similarly, Vermillion (2017, p. 1) describes SG as being used *for purposes beyond entertainment*. This definition is widely accepted and is therefore the most current designation within the evolution of the definition of the term (Djaouti et al., 2011). According to Djaouti et al. (2011), these definitions have all been derived from Sawyer and Rejeski (2002) who, with their white paper, paved the way to the current understanding of applying SG with technology for training and education. Further, the authors made a decisive contribution to the SG industry by inventing the Serious Game Initiative and serious gaming conferences such as the Serious Gaming Summit or Games for Health (Djaouti et al., 2011). The original heritage of the SG definition and the term's first usage dates to the 1970s. In his book *Serious Games*, Clark Abt (1970) describes the use of games for training and educational purposes and how decision makers of different domains in industry, government, education, and personal relations can be trained through those games (Abt Associates, 2020). Nowadays, serious games are commonly perceived to be virtual computer games and assumed to be limited to the digital sphere (Zyda, 2005; Rudman, 2019). Abt's (1970) definition, however, is rather open and does not relate to technology:

> *Games may be played seriously or casually. We are concerned with serious games in the sense that these games have an explicit and carefully thought-out educational purpose and are not intended to be played primarily for amusement. This does not mean that serious games are not, or should not be, entertaining.* (Abt, 1970 p. 9)

The fact that serious games nowadays are commonly digital does not mean that SG is meant to be purely digital. A serious game presented by Jansiewicz (1973) for educating students about the mechanisms of United States politics provides a good reason why SG should not be seen as purely digital. Games that are played by incorporating human interactions are better suited to teach complex matters (Linehan et al., 2009; Jansiewicz, 2020). Moreover, interactive, experiential learning methods are ideally suited to assist participants in understanding implicit and subtle concepts, such as deception (Arcos & Lahnemann, 2019). Using an offline serious game as an interactive, experiential learning method to confront participants with the deceptive rationales of SE is therefore reasonable.

A Selective Review of Serious Gaming Application Domains

Serious games are applied in a broad range of domains, such as military, education, health care, communications, and politics (Djaouti et al., 2011). The first reported SG applications refer to the training of decision makers in industry, government, or education (Abt, 1970). Abt created different games, digital and nondigital, that were used by schools to educate pupils or by the military to train officers in Cold War simulations (Djaouti et al., 2011). Since then, the fields of application have widened and releases of serious games have accelerated (Djaouti et al., 2011). The continuous improvement in digital or virtual computer capabilities has contributed to this increase as well. The domains in which SG could be applied are almost limitless according to Abt's definition because such games are being built for educational and training purposes, fostering informed decision-making. The scope of application is open to almost every domain or industry where knowledge and awareness creation are needed to support people's understanding of principles, processes, and rationales. Scholars have used gaming to research human behavior in emergency scenarios and disaster communication, anti-terrorism training, engineering and information systems, health care, the military, environmental contexts, and policing contexts as well as to research the effect of gaming approaches in cybersecurity trainings. Table 1 provides a selective overview of literature from those domains with their respective academic contributors who either applied or discussed an SG approach as an educational experiential learning tool. The selection was made based on a contribution's relevance to the discussed topic and the academic fields of the authors. There are highlighted authors who contributed more than one study. However, only the initial, most relevant study from a given author or group of authors was chosen to keep the selection concise.

Table 1. *Selected domains of SG application in the academic literature*

Domain	Academic Contributors
Disaster Communication	Haferkamp, 2011; Almeida et al., 2017
Anti-terrorism Training	Bruzzone, 2009; Sormani, 2016
Engineering and Information Systems	Vermillion et al., 2017; Kwak et al., 2019
Military	Garris et al., 2002; Zyda, 2005; Yildirim, 2010
Policing	BinSubaih, 2005; Bosse & Gerritsen, 2017; Sorace et al., 2018; Akhgar et al., 2019
Cybersecurity	Sheng et al., 2007; Cone et al., 2007; Newbould & Furnell, 2009; Arachchilage, 2013; Denning et al., 2013; Olanrewaju & Zakaria, 2015; Hendrix & Sherbaz, 2016; Beckers & Pape, 2016; Aladawy et al., 2018; Chothia et al., 2018; Frey et al., 2018; Goeke et al., 2019; Hart et al., 2020

Serious Gaming and Social Engineering

Serious games for SE are identified among other industrial or commercial training programs as solutions for cybersecurity (Aldawood & Skinner, 2019). The following paragraphs highlight foundational approaches that invented or further developed such gamified approaches. They present innovative means of instruction for the topic under discussion and different degrees of content of the SE rationales.

Anti-Phishing Phil

An early and seminal example of a gamified approach that tries to raise awareness for malicious SE techniques among players is the game Anti-phishing Phil (Sheng et al., 2007) developed at Carnegie Mellon University. It is an online game that teaches players ways to identify phishing attacks. The researchers tested its effectiveness by evaluating a player's ability to spot fraudulent websites compared to the abilities of study participants who did not play the game. The researchers recruited 42 participants on campus who were split into three study groups. Although phishing is a very prevalent type of SE attack, it is only one attack vector in the malicious repertoire of social engineers.

Playing Safe

Another early gamified approach that made use of SG for awareness creation of SE threats was undertaken by Newbould and Furnell (2009). With a digital board game, they informed and educated players about the dangers of different SEA techniques. The authors performed a prototype test game with 21 players. Based on the players' self-evaluated level of awareness, the authors argue that the game helped to increase awareness of SE.

Social Engineering Awareness Game

In another approach, Olanrewaju and Zakaria (2015) tested their Social Engineering Awareness Game to see whether it improved information security awareness in a controlled laboratory experiment with 20 students. The game was conducted in a paper-based and prototype digital-based form. The players had to complete three levels during the game. A quiz section asked questions about SE. In a second step, players had to match pictures with definitions in a memory card game, and in a third step, real-life applications were tested. The researchers compared the performance of the paper-based game participants with that of the prototype digital-based game participants. Based on players' subjective perceptions, they conclude that the prototype game seems to be beneficial for SE awareness creation. Similar to the game of Newbould and Furnell (2009), however, their game also lacks the component of being interactive on the human level. Still, it is worth noting that SE is a concept of psychological manipulation and entails forms of direct or indirect human interaction.

A Serious Game for Eliciting Social Engineering Security Requirements

Beckers and Pape (2016) describe the invention of a tabletop serious game for SE awareness creation. They validated the approach in practical experiments with 27 university employees, with 3 to 4 players per experiment. The players took on the role of the social engineer and had to apply psychological principles of influence in combination with a suitable SEA technique to formulate an attack based on the playing cards they have drawn from the respective card deck (psychological influences and attack techniques). Those cards are then used to come up with a suitable SEA applied on a target person selected from a pool of different characters presented in a fictitious corporate environment. The fictitious corporate environment consists of an environment map, representing the corporate floor, and shows the offices of the fictitious target persons. The target persons are described using different attributes and skills, therefore leaving room to conduct different kinds of SEAs.

The suitability of the formulated attack is mutually evaluated by the players. The advantage of this approach is the active examination of the SE rationales and principles in a reflective and socially interactive way. A disadvantage of this offline tabletop approach is its scalability. Aladawy et al. (2018) and Goeke et al. (2019) developed an online version of the game and changed the player perspective from being a social engineer to being a SEA defender to train players' resistance against persuasion. Being put into a defending position correlates better with real-world scenarios (generally, most people would rather face situations where they must defend against SEAs than be an attacker themselves). However, research confirms that increased understanding and awareness creation about criminal processes and techniques can be obtained from putting someone into the criminal's perspective (Wright & Bennett, 1990; Jacques & Bonomo, 2017).

A game that simulates SEAs will create awareness at the player's level, but it will also generate insights on creative SEA techniques invented by the players that could be prevented in future real-life situations. Thus, the game could be preventive through awareness creation and by preventively addressing future SEAs. Similar thoughts apply to the pedagogical layout of the game. Physical social interaction and the exchange of ideas during a tabletop game with a role-playing character provides valuable experiences to the players. Such a game can contribute positively to awareness creation, as well as to the knowledge creation process (Linehan et al., 2009; Jansiewicz, 2020). Offline role-playing games foster creativity and social skills (Karwowski & Soszynski, 2008; Chung, 2013; Dyson et al., 2015; Spinelli, 2018). SE is based on the exploitation of psychological triggers to manipulate victims. The means by which social engineers can manipulate the victims are therefore only limited by their creativity.

RISIKO

Most recently, Hart et al. (2020) further developed the approach of Beckers and Pape (2016). The researchers created a tabletop game that incorporates a more general view of aspects of cybersecurity and a larger variety of attack types. Hence, in their opinion, their game is educational and entails more than SE-related aspects. They proposed a tabletop game for increasing cybersecurity awareness among people in organizations without a technical background. The researchers evaluated the game in four experiments with a total of 54 participants, of whom 29 were students or recent graduates. Using a post-activity questionnaire, they asked participants about the perceived ease of use of the game, perceived usefulness of the game, and their intention to use any lessons learned.

SG approaches that specifically focus on SE rationales and concepts are rare. Different scholars have provided approaches that look only at single attack vectors of SEAs; have mostly applied the approaches in an academic, nonprofessional setting; and have often used online approaches without the possibility of direct human interaction. A tabletop offline gaming approach, however, seems to be reasonable to convey knowledge and rationales that are based on human psychology. Being put in front of a screen externalizes the human component and makes it more intangible again. We, therefore, find it reasonable and beneficial to use an offline tabletop game that lets players directly interact with each other and learn about rationales that are based on social interactions. The SG approach that is used in the study at hand resembled that of Beckers and Pape (2016) because it is a full offline SG tabletop approach, is socially interactive, and specifically focuses on SE.

RESEARCH PURPOSE

The current study explores the application of an SG approach as described in the previous section. The purpose of this study is to observe participants' game involvement and instruction compliance and to derive administrative and procedural improvement potentials before testing the game's effectiveness as an experiential learning tool experimentally in further studies. Moreover, the study seeks to broaden the research field by specifically focusing on a business environment. Prior research, as mentioned in section 2.2, applied such approaches only to a very limited extent in professional settings. The discovery of practical implications for the applicability of an SG approach for SE in the business environment provides added value. Thus, the research objectives that were assessed by this study are as follows:

1. *Observe participants' involvement with the game throughout the playing process.*

The first objective of this study was to observe participant engagement throughout the game and whether the game content as well as the game procedure catches their attention.

2. *Observe and evaluate participants' compliance with the instructions given by the game masters and game material.*

A second goal of this study was to observe specifically the compliance of players with the instructions given by the game masters and the game material, as these are the direct connecting points in conveying the topic and the rationales of SE to the players.

3. *Observe other relevant findings that could be identified throughout the events.*

We wanted to leave room in our research approach to insights that evolve in the course of an interactive SG approach that are beyond the primary focus but would improve the quality of this instructional approach. Based on the research objectives, the research questions that were subject to this study are as follows:

RQ1: Are there game improvement potentials?

With *improvement potentials* we mean any change in the administrative or procedural design of the game that would help to foster participants' engagement, satisfaction, and interpersonal interactions during the game. Prior research suggests that specific introductory material might assist players from a broader background in more easily engaging with the rationales and purpose of the game (Beckers & Pape, 2016). Moreover, interpersonal interaction is a key element of the SG approach (Beckers & Pape, 2016; Hart al., 2020). Sample sizes that are significantly larger than those in the aforementioned studies might expose improvement potentials in the dimension of interpersonal interaction.

RQ2: Do game masters take on an essential role for participants' performance and their instruction compliance during the game?

Prior research has shown that the role of the game master is relevant to the overall success of a game. Hart et al. (2020) state that game masters have *a focal role* in engaging the participants and making the game fun. Game masters motivate players, guide the game process, and ensure the procedural sequence of the game (Beckers & Pape, 2016). Facts that qualify for an investigation of the role of the game master are also addressed in the study at hand.

GAME DESCRIPTION

The following section provides an overview of the game process and its components as it was applied in the three samples. The approach resembled the one taken by Beckers and Pape (2016).

Game Process

We have chosen to start the game with a short 5-to-10-minute introduction presentation about the topic of SE, as well as about the purpose and rationales of the game, as done by Beckers and Pape (2016). The game then starts and lasts for one or two iterations. The game is led by one game master per game table, and each game table consists of three to four teams with two to three players per team. In each iteration, the teams must create a suitable SEA based on the given game material. It consists of a situation plan for a fictitious company (office); a set of fictitious employee profiles, where each employee is characterized by position, computers skills, and strengths and weaknesses; and an attack plan sheet that guides the players through the process. Additionally, the game set consists of two stacks of cards. One set covers the principles of influence of social psychology, which are the foundation of SE deception techniques for building trust. The second set incorporates different SE attack vectors. Every card from either stack has a precise description. This process helps players familiarize themselves with the concept of SE.

After an initial familiarization phase of about 10 minutes with the situation plan and the fictitious employees, each team draws three cards from both of the stacks. The teams now receive their attack plan sheets where they have to formulate a reasonable SEA, and they will again have about 10 minutes available. The aim is to formulate an attack that applies a reasonable combination of a compliance principle with an attack vector on a suitable target person to exploit a formulated target asset, for instance, access to the CEO's office or access to specific financial information. Based on the cards they have drawn, there will be more or less suitable attack options that they will have to evaluate themselves. In the next phase, the teams will present their formulated attacks to the other teams at the game table. For the presentation, each team is allotted around 5–7 minutes. Each presenting team is evaluated by the other (evaluating) teams based on a predefined point scale. The evaluating teams have the ability to propose attack improvements to gain bonus points. Thus, the point rating acts as a proofing instrument, showing whether the concepts have been understood, correctly. Once this is completed, another iteration can be played. The team that accumulates the most points over the two rounds will be the winner of the game. Although winning is not the sole purpose of the game, its playful character is meant to engage participants with the concepts.

Game Components

The game material generally consists of a fictitious corporate situation plan, a description of the different target persons (employees), an attack plan sheet, and two stacks of playing cards (see also annex B).

Fictitious corporate situation plan: First, the game contains a fictitious corporate situation plan. In the setting at hand, the situation plan reflects an office environment. The situation plan also accounts for the fact that SE attacks can be executed physically by the means of person-to-person contact or digitally by using technological means.

Target persons: A second crucial component is the set of fictitious target persons. Each person is characterized by a different corporate function and personal characteristics, strengths and weaknesses, interests, and computer skills. The game is meant to help participants understand the characteristics of the fictitious target persons that could be exploited in SEAs.

Attack plan sheet: The attack plan sheet guides the players through the game process. It provides the participants help on how to structure their attack and how to use the game material. Moreover, the attack plan sheet entails examples for each component to foster the familiarization process.

Compliance principles cards: The concept of SE is based on psychological principles of persuasion or influence to deceive targeted persons and make them comply with a request. Those compliance principles can be authority, reciprocity, or social proof, for example (Cialdini, 2021). The playing cards are meant to help the participants understand the different ways that the cards could be used in SE, such that participants can better detect and protect themselves against targeted attacks.

Attack vector cards: Additionally, there are attack vector playing cards. It is important for the participants to understand that SE attacks can take on various forms, for instance, phishing or tailgating. This knowledge will help participants better detect SE attacks and protect themselves against them.

DATA AND METHODOLOGY

The current study was conducted using a qualitative research approach that included field observations and unstructured field interviews. It was intended to produce ethnographic knowledge about the behaviors and social interactions of the participants during the game. Field observations are well suited for drawing conclusions about specific conditions and behaviors in a natural setting (Maxfield & Babbie, 2017). As Hochstetler and Copes (2016) say, qualitative research provides context to the topics under investigation. Field observations provide the opportunity to generate depth and free-flowing participant responses.

The researchers' positions took on different forms in the study. They were either full participants administering the game as a game master or were full participant observers. Either position had its benefits and limits. Whereas the full participant position provided the researchers the opportunity to interact with the participants and collect firsthand insights, there was a risk that immediate involvement would influence the researchers' assessment of participants' behaviors and perceptions. The position as a full participant observer was better suited to avoid selective perception from the researchers, but it also limited the researchers' direct interaction with the participants. To balance the benefits and limits of those stances, the researchers took on positions that complemented each other in all observations such that both positions were filled in either of the observations. We used the SG approach of Beckers and Pape (2016) to assess the research objectives and research questions. However, in contrast to aforementioned researchers, our approach was administered by game masters who were each in control of a game table with three to four teams and two to three players per team and table. Each of the teams was asked to create a SEA based on the information and game material provided by the game master. The game material consisted of an attack plan sheet that helps the players to navigate through the game, a floor plan of a fictitious company with fictitious employees as target persons, a description sheet that characterizes the target persons, and SE deception principle and SE attack vector playing cards. At the end of a game iteration, the teams mutually evaluated each other's SEAs and in doing so further fostered their reflection on and understanding of the subject in an interactive way. Additionally, game masters were provided a game master instruction cheat sheet in advance of a game (see annex B for an exemplary extract of the game material and game structure, as well as the game master cheat sheet).

Data and Data Collection

Between December 2019 and February 2020, we observed a heterogenous group of 97 professionals in three independent observations. The sample population consisted of practitioners of various industries and professions. The participants represented different Swiss companies or Swiss affiliates of international companies from the telecommunications, technology, and energy industry from Swiss and international advisory firms, law and cybersecurity firms, and information technology (IT) apprentices of a Swiss governmental defense organization. Overall, the sample population reflected a pronounced degree of heterogeneity in terms of the sectors, industries, professions, and life and professional experiences represented. Participants were between 16 and 20 years old for IT apprentices and up to around 55 years old for senior professionals. The gender ratio was 11 female to 86 male participants; they were consultants, finance or marketing specialists, lawyers, key account managers, and management personnel. The sample was recruited by using the researchers' professional networks, pursuing a purposive sampling path of opportunity. Table 2 provides a summary of the sample characteristics.

Table 2. *Summary of general sample characteristics*

Sample	Date	Place	Sector	Industry	Sample Size
1	05.12.2019	Zürich, CH	Private	Consumer electronics, telecommunications, and crisis management	9
2	05.12.2019	Zürich, CH	Private	Telecommunications, advisory, technology, energy, law, and cybersecurity	83
3	13.02.2020	Bern, CH	Public	Defense	5

Each sample was exposed to the game independently, at different times and places, to collect the data. The observations were conducted in a workshop-style format on the premises of the respective host organization. The observations lasted for two hours in samples 1 and 2 with one game iteration. The observation in sample 3 lasted for four hours because in sample 3, the researchers decided to conduct a two-iterations game to study the effects that two iterations would have on the considerations stated in the objectives. Sample 1 and sample 2 were conducted in the afternoon, whereas sample 3 was a full morning workshop with a 15-minute break between the iterations. Each of the observations took place in a climatized room with conference tables and chairs organized for the grouping of three to four teams per table and two to four participants per team. Sample 3 was organized into three teams with two participants per team, but one participant had to leave the game during the second iteration due to an urgent professional obligation. For sample 2, the researchers were assisted by voluntary game masters who were briefed on the game and their task as game masters in advance of the observation.

The data produced were collected and recorded through note-taking during the games and by transcribing the content of the unstructured interviews to a Microsoft Excel data bank after the respective observations. The interviews did not follow a predefined structure but were discussions between the researchers and individual participants about their experiences and perception of the game. The researchers nevertheless asked all interviewees about their evaluation of the game's attractiveness and possible improvement proposals for the game. Besides that, free-flowing comments from the interviewees were collected. Note-taking took place through both the researchers and the participants. Whereas the researchers took notes to directly record anything that related to the research objectives, the participants took notes with respect to the game proceedings on the provided attack plan sheets (see annex B) that were collected by the researchers from the teams after the game's conclusion. The sheets were used to record additional data and insights for the research objectives while representing

a standardized reporting tool across the samples. All collected data were recorded in a Microsoft Excel data bank for each sample, with a structure presented in annex A.

Method of Analysis

Data were collected by the means of observing participant behavior, gathering feedback through unstructured interviews, and recording the respective data through note-taking. Additionally, the attack plan sheets that had to be filled out by each team in each sample of the game proceedings were collected. In a deductive process, familiarization with and a first screening of the collected data was performed. Deductive coding processes are categorized by analyzing data with respect to a predefined list of codes (Miles et al., 2013). The predefined categories of interest in the study at hand referred to the research objectives presented earlier and related to participants' game involvement, their instruction compliance, and other relevant findings. Data were allocated in the predefined categories afterward. Moreover, categorizing patterns of data aided in the further identification and coding of subthemes. To illustrate the findings, we present a table of the categories, the identified coded subthemes, and relevant examples (see table 3 in the results section). Further, we have used verbatim quotations from the unstructured interviews to present response categories with the number of an interviewee and the interviewee's industry mentioned in brackets (e.g., (20; defense)). Each theme was analyzed to gain a deeper understanding of participants' perceptions of the game and gaming behaviors to help answer the research questions.

RESULTS

The findings indicate that there are several procedural and content-related improvement potentials to make the approach more participant centric and knowledge conveying so that the game can be a promising instructional tool for SE awareness creation. Table 3 hereafter illustrates the structure of the derived findings.

The analysis of the data shows that there are specific themes that appeared repeatedly among the participants in either the observations or the unstructured interviews that would be categorizable under either of the three research objectives. The coded subthemes have been presented because they represent in a good way what was important for the research, namely whether the observations and unstructured interviews would expose improvement potentials concerning the level of engagement, satisfaction, and interaction among the participants and their compliance with instructions during the game.

Table 3. *Categories of interest, coded subthemes, and examples*

Category	Subtheme	Example
Game involvement	Game material	Familiarization ease, language, game material usage, and improvement proposals
	Teamwork	Within and among teams, directive, authoritative, and cooperative
	Active participation	Discussion intensity, voluntary comments, and call for participation
	Understanding rationales	Poorly completed attack plan sheets, messy SEA creation, and usefulness of compliance principles
	Environmental factors	Room appropriateness, population size, noise, time constraint, and team grouping
Instruction compliance	Game material	Game material usage in way of order and attack plan sheet completion
	Game master ability	Participants asked for clarifications, discussions out of context, and lack of introduction and control
	Presentation of attack	Explaining the situation and used methods, conveying rationales, and attack improvement proposals
Other findings	Deviant behavior and thoughts	Theft of game material and pronounced deviant considerations
	Information overload	Not using game material properly, poorly completed attack plan sheets, and attack plan improvement proposals being too demanding in one iteration

Game Involvement

It appeared that participants' involvement with the game differed within the samples and among the samples. Based on the researchers' observations and the feedback gathered from the participants, several findings have been derived. In particular, there are some suggestions to improve the game proceedings and the game material. Interviewees mentioned the following:

This was an interesting and educational event. One suggestion for the game from my side would be an introduction sheet at the beginning of the game to better familiarize the participants with the game's rationale. Moreover, a sociogram that captures exploitable social relationships among the target persons could be a nice extension. (2; crisis management)

In my opinion, a more profound introductory presentation would have been beneficial for a general familiarization with the topic. (5; telecommunications)

The game should be digitized to scale it and make it more accessible. (12; advisory)

The game was really fun, and we could administer it in our company as well. The only problem I had was with the game material, as I am not perfectly fluent in English. (19; energy provider)

The sociocultural behavior of participants within their teams, among teams, and toward the game masters was observed to be heterogenous as was the overall demography of the population in each sample. When there was a diverse demography in terms of gender, age, education, profession, and extent of professional experience, participants with a higher education and participants who seemed to be more open and extraverted dominated the discussions within the teams and among the teams. When the demographic distribution among the participants was rather homogenous, a compliant and cooperative working style within the teams and a more directive, authoritarian working style with less cooperation but a high degree of competitiveness was observed among the teams. Although professional and life experiences seemed to be linked positively with active participation, once younger participants were invited to participate, they provided valuable feedback for the researchers in terms of personal involvement:

This game was fun and educational. I guess, I learned more in this half day than in the last couple of months in vocational school. (20; defense)

Oh, we already have a break? I did not recognize the time passing by. (21; defense)

Another important factor for the effectiveness of the approach is participants' involvement with the underlying rationales. The analysis of the teams' attack plan sheets and the data collected from each team's attack presentation suggest that participants' understanding of the basic principles underlying this SE approach should be guided:

The case study and the presentation of the social engineering principles really helped me to better grasp the game's rationales. (11; technology provider)

Another participant's feedback does, however, show that an introductory presentation is no guarantee for the comprehensibilty and the conveyance of the game's underlying principles and rationales:

I did not find the compliance principle cards of psychological manipulation helpful and would abandon them from the game. (24; defense)

For a freer-flowing attack formulation without a scientifically proven framework of psychological principles, this request would be feasible. Psychological principles of interpersonal influence are, however, fundamental for SEAs and therefore should be well integrated within a game that intends to convey awareness about SE rationales.

Lastly, the analysis of the data hints at the fact that specific environmental factors play an important role in participants' involvement with the game. In two of the three samples, the population sizes ranged within 5–9 participants, which was administratively easier to handle than a population size of 83. But this somewhat opposing study condition also revealed limitations to the operability of the approach. An increasing population size not only requires more game masters but also asks for specific logistic prerequisites, such as room size or room climatization for the participants to stay focused. If such conditions are not met, participants may get distracted and annoyed by noises, heat, or a lack of space, which would negatively impact their involvement with the game:

The tight seating and grouping of game tables was not that comfortable, as it was hard to always get what the others at the table were saying with the noise behind my back. (11; technology provider)

The room was almost too small, as it has become too noisy. (13; advisory)

Instruction Compliance

Based on the collected data, the findings suggest that participants enjoyed the game but sometimes had trouble with following the game instructions. The attack plan sheets to be filled out provided a unified measure among each sample and team to review participants' compliance to the overall instruction of using the game material to create a reasonable SEA, respecting the components and rationales of SE. It was intended that participants would familiarize themselves with the concepts and rationales and think through their SEA approach by filling out the sheet. The attack plan sheet contained specific examples per each step and acted as a guide for the participants. In total, we have analyzed 27 attack plan sheets for the participants' instruction compliance in filling them out as demanded. The findings show that most of the teams sporadically completed the sheets in note form and that others did not even complete them:

I did not see any use in completing the attack plan sheet. We rather enjoyed discussing the things. (7; telecommunications)

Although discussing the rationales and principles of the game with the team members is an essential part of the familiarization and awareness creation process, it is vital to follow the structure of the attack plan that replicates the underlying procedural principles of SE. If these structures are not respected, the game reflects an interactive and fun event with discussions about the topic but does not get down to the point that SEAs are accurately planned, as well as precisely and purposefully executed. Building on this, another focal finding in terms of participants' instruction compliance refers to the game master's ability. Discussions out of context, participants asking for clarification, or a game master who was too passive were signs of an ineffectively administered game table. The game master's primary role is to explain to the participants the game material, the goal of the game, and the information they need to process and to effectively guide participants through the structure of the game. In this sense, it was observed that not all game masters possessed this authoritative but permissive nature to effectively guide the participants through the framework of the game while leaving room for nourishing discussions:

Although I generally liked the game, it was not perfectly administered and the introduction to the game material could have been more extensive. (15; technology provider)

I liked the approach, but it was a lot of information, and it would have been beneficial if the game master more strictly guided through the process. (17; telecommunications)

Lastly, a good overall indication of whether the participants stuck to the instructions were the SEA presentations of the teams at the end of each game iteration. In samples 1 and 3, the researchers witnessed all the presentations personally while in sample 2, the researchers listened to random samples of SEA presentations and also asked the respective game masters about how participants put the instructions into practice. The findings were that most participants grasped the essential idea of the game and its instructions but struggled with the detailed implementation of the rationales and structure of a SEA. The analysis of the attack plan sheets mentioned above supports this finding. Some presentations indeed showcased detailed considerations but not in terms of an in-depth application of SE principles, and not many of the attack plan sheets reflected this either.

Other Findings

The analysis of the data revealed two other important findings besides those that can be directly allocated to either the participant involvement or the instruction compliance category. First, deviant tendencies were observed and recorded for two of the three samples. In sample 2, the game revealed a deviant behavior by one of the participants who purposefully took the property of the researchers. Similarly, in sample 3, one participant exposed deviant thoughts during the game that were unsettling and an expression of a well-thought-through plan rather than the correct application of the game's rationales and principles. During the proceedings of the game, the researchers asked the participants how they were doing with their brainstorming and whether they had already come up with an idea for an attack. One participant answered as follows:

Yes, we could poison the assistant's cat, such that she has to go to the doctor's, and we can take advantage of her not being present in the office…Then we would smash the windows in the office to gather access to her office…These are things I already made up when I was 14 years old…(24; defense)

Second, the analysis of the data revealed that the gaming approach contains a large amount of information to be processed by the participants. Time constraints and a one-iteration game structure seemed to particularly impact participants' satisfaction with and receptivity to the game:

I enjoyed the game and could imagine replicating it in our company. However, I would propose to have different levels of complexity and more time available, as it were a lot of information to be processed. (17; telecommunications)

The game was educational and fun. I wished to have had more time available to play a second iteration. (10; cybersecurity)

DISCUSSION

To the best of our knowledge, this is the first study in criminology that applied SG for SE and looked for improvement potentials to make the serious game more effective as an educational tool based on field observations. However, there have been studies outside criminology that used a similar approach. Beckers and Pape (2016) performed experiments to test the effectiveness of an SG approach for SE awareness creation and further developed the approach to create an online version of the game (Aladawy et al., 2018; Goeke et al., 2019). The initial approach, however, was not further evaluated for improvement potentials. We think that the results of the three field observations support the view that the interactive and interpersonal character of an offline tabletop game approach is well suited to foster knowledge and awareness of the creation process among the participants and that several game improvements are possible to enhance this process. Hart et al. (2020) used an offline tabletop SG approach for

cybersecurity awareness and education for people with no technical background. Although their approach does not specifically focus on SE and features other content in terms of game material, the administrative design resembles the one used in this research study. In accordance with our findings, they conclude that the game master takes on a *focal role in stimulating active learning* and thus fosters the degree of participant involvement with the game. For the overall improvement of the approach in terms of participant involvement, instruction compliance, and consistent pedagogical quality, the importance of the game master should not be underestimated.

Analysis

Based on the findings, we derived two improvement dimensions: the game material and the game process. Each dimension can be improved in the following areas: the briefing, the level of complexity, and other. Eventually, we propose the following adaptions for the game. First, to increase participants' involvement and instruction compliance, it is essential that players are briefed more thoroughly. In the game, we followed the approach of Beckers and Pape (2016), who gave a short introduction to their game. Obviously, this practice is not sufficient. We therefore see a need to prepare the players better at the beginning of the game. This will be achieved by conducting a stimulating SE introductory presentation and by providing an introductory sheet at the beginning of the game. Moreover, game masters need to be more comprehensively briefed because we can confirm that they play a *focal role* in the game (Hart et al., 2020). Second, it seems to be beneficial for the awareness creation process and for the reduction of information overload to apply an increasing level of complexity by adding different levels of difficulty during the game process. This implies that, ideally, the game process should encompass more than one iteration, and in the second iteration, players will be provided a sociogram of the target persons as an additional layer of difficulty. Further, they will only be given the ability to propose attack improvements during the mutual evaluation phase in the second iteration. Table 4 summarizes the key improvements discovered during the field observations.

Table 4. *Summary of key improvement potential applications for the serious game*

Dimension/Area	Briefing	Complexity Level	Other
Game Material	Provision of introductory sheet	Provision of sociogram for target persons in second iteration	
Game Process	Stimulating introductory presentation	Two iterations approach. Mutual attack improvement proposals only in second iteration.	Comprehensive training of game masters

LIMITATIONS AND FUTURE RESEARCH

The study at hand evaluated the participants' engagement and satisfaction with SG for SE awareness creation in a business environment. The study was a pilot project that seized the opportunity to conduct observations in the business environment, which is hard to achieve and an added value. It provided the opportunity to apply the game in a naturalistic setting in the field and to gather practical knowledge about its purpose, which is to help organizations increase SE awareness among their employees. Although we properly prepared and executed the study, there are methodological limits given the fact that the study was set up in a very short period. We were supposed to implement the insights from this study in the methodological setup of further observations in the field during 2020/2021 with organizations that had confirmed their cooperation for it. Unfortunately, due to the COVID-19 pandemic, these field studies have not taken place so far. We, nevertheless, decided to publish the study at hand because we are convinced that the study bears valuable and shareable results.

The outcome of the study at hand will be used for the improvement of the respective SG approach. It will be applied as an operational framework in a randomized controlled trial research design that tests the serious game's effectiveness as an educational tool to reduce participants' proneness to fall for SE's influencing techniques. Simultaneously, the research design aims to control for personality differences and different methods of instruction.

Further, we will pursue aspirations to adapt the game's content, in particular the target person descriptions and the corporate environment sheet, to a version appropriate for educating intelligence officers. Based on feedback received from the intelligence community, we see a potential to tailor the game to the needs of educating intelligence personnel about the power of social psychology in influencing situations.

Moreover, even though offline interactive educational tools might be the purest form of social interaction, they are not suited for pandemics, as COVID-19 has taught us. The authors therefore aspire to create a technology-assisted gaming approach. However, we still believe that social interaction during such a game is key for the process of SE awareness creation.

CONCLUSION

This article presented an evaluation of an SG approach as an interactive, experiential learning tool for SE awareness creation. Through three field observations with a total of 97 participants, insights on possible improvements for the applied SG approach were derived. Besides pure sociodynamic observations, it was possible to identify valuable insights on how to adapt the layout and the administration of the serious game to make it more accessible, less generic, and

hopefully, effective in raising awareness among the participants about the rationales and techniques of SE. Moreover, in two of the three samples, the researchers observed deviant behavior and thoughts. However, this observation does not mean that those people tend to be criminals outside the game setting. Still, this specific observation was nevertheless unsettling to the researchers and thus was worth reporting on. Generally, we have learned that research in the business environment bears challenges that should be respected in the methodological setup. We, nevertheless, gathered valuable insights for future studies. This study does not provide insights on the SG approach's ability in improving responses to SEA. But it does add value to the **ABC** of cybersecurity. The observations and participant feedbacks that were collected during the study do not only help to improve the gaming approach, but they also showed that it is a reasonable approach to create **A**wareness for SE. Whether it can help change people's **B**ehavior in real-life SE situations and create a SE resilient **C**ulture is yet to be tested.

This game was fun and educational. I guess, I learned more in this half day than in the last couple of months in vocational school. (20; defense) Although this statement is subjective and should be treated carefully and neither reflects the quality of the school nor of the serious game, it nevertheless indicates that the SG approach was impressive, was fun, involved the participants in the game, and made people aware about SE threats and rationales.

DISCLOSURE STATEMENT

No potential conflict of interest was reported by the authors.

NOTES

REFERENCES

Abt Associates (2020). Biography of Clark C. Abt. Retrieved January 6, 2020, from https://www.abtassociates.com/who-we-are/our-people/clark-c-abt-phd.

Abt, C.C. (1970). Serious Games. University Press of America.

Akhgar, B., Redhead, A., Davey, S., & Saunders, J. (2019). Introduction: Serious Games for Law Enforcement Agencies. In: Akhgar B. (eds) Serious Games for Enhancing Law Enforcement Agencies. Security Informatics and Law Enforcement. Springer, Cham.

Aladawy, D., Beckers, K., & Pape, S. (2018). PERSUADED: Fighting Social Engineering Attacks with a Serious Game. In: Furnell S., Mouratidis H., Pernul G. (eds) Trust, Privacy and Security in Digital Business. TrustBus 2018. Lecture Notes in Computer Science, vol 11033. Springer, Cham.

Aldawood, H., & Skinner, G. (2019). A Taxonomy for Social Engineering Attacks via Personal Devices. International Journal of Computer Applications (0975 – 8887) Volume 178 – No. 50, September 2019.

Almeida, J. E., Rossetti, R. J. F., Jacob, J. T. P. N., Faria, B. M., & Leça Coelho, A. (2017). Serious games for the human behaviour analysis in emergency evacuation scenario. Cluster Computing, 20(1), 707-720.

Arachchilage, N.A.G., & Love, S. (2013). A game design framework for avoiding phishing attacks. Computers in Human Behavior, 29(3):706{714.

Arcos, R., & Lahnemann, W.J. (2019). The Art of Intelligence. More Simulations, Exercises and Games. Security and Professional Intelligence Education Series (SPIES). Series Editor: Jan Goldman. The Rowman & Littlefield Publishing Group, Inc.

Barber, R. (2001). Social engineering: A People Problem? Network Security, 2001, Vol.2001(7), pp.9-11.

Beckers, K., & Pape, S. (2016). A Serious Game for Eliciting Social Engineering Security Requirements. 2016 IEEE 24th International Requirements Engineering Conference (RE), Beijing, 2016, pp. 16-25.

BinSubaih, A., Maddock, S., & Romano, D.M. (2005). Comparing the use of a tabletop and a collaborative desktop virtual environment for training police officers to deal with traffic accidents: Case study. International Conference on Engineering Education, July 25–29th, Gliwice, Poland, Volume 2, pp. 94–100.

Bosse, T., & Gerritsen, C. (2017). Towards Serious Gaming for Communication Training - A Pilot Study With Police Academy Students. Paper presented at the 8th International Conference on Intelligent Technologies for Interactive Entertainment, Utrecht, the Netherlands, 28–30 June 2016.

Bruzzone, A., Tremori, A., & Massei, M. (2009). Serious games for training and education on defense against terrorism. Italy: Defense Technical Information Center.

Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P.H. (2017). On the anatomy of social engineering attacks - A literature-based dissection of successful attacks. Journal of Investigative Psychology and Offender Profiling, 2018, pp.urn:issn:1544-4759.

Chothia, T., Paiu, S. I., & Oultram, M. (2018). Phishing attacks: Learning by doing. In 2018 {USENIX} Workshop on Advances in Security Education ({ASE} 18).

Chung, T.S. (2013). Table-top role playing game and creativity. Thinking Skills and Creativity, 8 (2013), pp. 56-71.

Cialdini, R.B. (2021). Influence, New and Expanded: The Psychology of Persuasion. Harper Business; Expanded ed. Edition (4. Mai 2021).

Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A Video Game for Cyber Security Training and Awareness. Computers & Security, 26(1): 63–72.

Denning, T., Lerner, A., Shostack, A., Kohno, T. (2013). Control-Alt-Hack: The design and evaluation of a card game for computer security awareness and education. Proceedings of the ACM Conference on Computer and Communications Security. 915-928. 10.1145/2508859.2516753.

Djaouti, D., Alvarez, J., Jessel, J. P., & Rampnoux, O. (2011). Origins of serious games. Serious games and edutainment applications (pp. 25–43). London: Springer.

DoJ (2020). Three Individuals Charged For Alleged Roles In Twitter Hack. United States Department of Justice, DoJ, 31st July 2020. https://www.justice.gov/usao-ndca/pr/three-individuals-charged-alleged-roles-twitter-hack.

Dyson, S.B., Chang, Y.-L., Chen, H.-C., Hsiung, H.-Y., Tseng, C.-C., & Chang, J.-H. (2015). The effect of tabletop role-playing games on the creative potential and emotional creativity of Taiwanese college students. Thinking Skills and Creativity 19 (2016) 88–96.

Frey, S., Rashid, A., Anthonysamy, P., Pinto-Albuquerque, M., & Naqvi, S. A. (2019). The Good, the Bad and the Ugly: A Study of Security Decisions in a Cyber-Physical Systems Game. *IEEE Transactions on Software Engineering*, *45*(5), 521-536. [8194898]. https://doi.org/10.1109/TSE.2017.2782813

Garris, R., Ahlers, R. & Driskell, J. E. (2002). Games, Motivation and Learning. Research and Practice Model. In: Simulation & Gaming, 33. Jg., H. 4: Newbury Park (USA): Sage Publications, S. 441-467.

Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., Jabbar, S. & Baker, T. (2018). Security threats to critical infrastructure: the human factor. The Journal of Supercomputing, 74(10), pp.4986-5002.

Goeke, L., Quintanar, A., Beckers K., & Pape, S. (2019). PROTECT - An Easy Configurable Serious Game to Train Employees Against Social Engineering Attacks. Conference: Computer Security - ESORICS 2019 International Workshops, MSTEC 2019, Luxemburg, September 26-27, 2019.

Green, B., Prince, D., Busby, J. & Hutchison, D. (2015). The impact of social engineering on Industrial Control System security. In Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy (pp. 23-29).

Haferkamp, N., Kraemer N.C., Linehan C., & Schembri, M. (2011). Training disaster communication by means of serious games in virtual environments. Entertainment Computing 2 (2011) 81–88.

Hart, S., Margheri, A., Paci, F., Sassone, V. (2020). Riskio: A Serious Game for Cyber Security Awareness and Education. Computers & Security 95 (2020) 101827.

Hendrix, M., Al-Sherbaz, A., & Bloom, V. (2016). Game Based Cyber Security Training: are Serious Games suitable for cyber security training? International Journal of Serious Games. 3(1).

Hochstetler A. & Copes H. (2016). Qualitative Criminology's Contributions to Theory. In: The Handbook of Criminological Theory, First Edition. Edited by Alex R. Piquero. 2016 John Wiley & Sons, Inc. Published 2016 by John Wiley & Sons, Inc.

Jacques, S., & Bonomo, E. (2017). Learning from the Offenders' Perspective on Crime Prevention. In: LeClerc B., Savona E. (eds) Crime Prevention in the 21st Century. Springer, Cham.

Jansiewicz, D. R. (1973). The New Alexandria Simulation: A Serious Game of State and Local Politics. Canfield Press.

Jansiewicz, D. R. (2020). The Game of Politics - Frequently Asked Questions. Retrieved January 6, 2020, from: http://gameofpolitics.com/f__a__q_.htm.

Karwowski, M., & Soszynski, M. (2008). How to develop creative imagination? Assumptions, aims and effectiveness of role play training in creativity (RPTC). Thinking Skills and Creativity, 3 (2008), pp. 163-171.

Kwak, D.-H., Ma, X., Polites, G., Srite, M., Hightower, R., et al. (2019). Cross-Level Moderation of Team Cohesion in Individuals' Utilitarian and Hedonic Information Processing: Evidence in the Context of Team-Based Gamified Training. Journal of the Association for Information Systems; Atlanta.

Linehan, C., Lawson, S., & Doughty, M. (2009). Tabletop Prototyping of Serious Games for 'Soft Skills' Training. Coventry, UK: 2009 Conference in games and virtual worlds for serious applications.

Maxfield, M., & Babbie, E. (2017). Research Methods for Criminal Justice and Criminology 8th Edition. Wadsworth Publishing.

Michael, D., & Chen, S. (2005). Serious Games: Games That Educate, Train, and Inform (1er ed.). Course Technology PTR.

Miles, M. B., Huberman, A. M., & Saldana, J. (2013). Qualitative data analysis: A methods sourcebook. Thousand Oaks, CA: SAGE Publications, Incorporated.

Mouton, F., Leenen, L., & Venter, H.S. (2016). Social Engineering Attack Examples, Templates and Scenarios. Computers & Security, Jun 2016, Vol.59, p.186.

Newbould, M., & Furnell, S. (2009). Playing Safe: A Prototype Game For Raising Awareness of Social Engineering. Proceedings of the 7th Australian Information Security Management Conference.

Olanrewaju, A.-S. T., & Zakaria, N.H. (2015). Social Engineering Awareness Game (SEAG): An Empirical Evaluation Of Using Game Towards Improving Information Security Awareness. Proceedings of the 5th International Conference on Computing and Informatics, ICOCI 2015 11-13 August 2015 Istanbul, Turkey.

Popper, K.R. (1966). The Open Society and Its Enemies. (Princeton University Press, Princeton, New Jersey, fifth edition, 1966).

Proofpoint, Inc. (PFPT) (2019). Human Factor Report 2019. Retrieved December 16, 2021, from: https://www.proofpoint.com/us/newsroom/press-releases/proofpoints-annual-human-factor-report-details-top-cybercriminal-trends-more.

Redpath, S. M., Keane, A., Andrén, H., Baynham-Herd, Z., Bunnefeld, N., Duthie, A. B., & Travers, H. (2018). Games as Tools to Address Conservation Conflicts. Trends in ecology & evolution, 33(6), 415-426.

Robinson, J. (2008, September 9). Researchers dupe banks with heists without holdups. Arizona Republic, p. D5.

Rudman, S.A. (2019). Serious games to study the influence of wildlife devaluation strategies on hunter behaviour. A thesis submitted to the Victoria University of Wellington in fulfilment of the requirements for the degree of Master of Science. Victoria University of Wellington, 2019.

Rusch, J. (1999). The Social Engineering of Internet Fraud. United States Justice Department – Proceedings of the 1999 Internet Society Conference.

Russell, C.K. (2005). A taxonomy of serious games for education in the healthcare professions. In Proceedings of NMC Online Conference on Educational Gaming.

Sawyer, B., & Rejeski, D. (2002). Serious Games: Improving Public Policy Through Game-based Learning and Simulation. Woodrow Wilson International Center for Scholars.

Sheng, S., Magnien, B,, Kumaraguru, P., Acquisti, A., Cranor, L., Hong, J. and Nunge. E. (2007). "Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish", in Proceedings of the 2007 Symposium On Usable Privacy and Security, Pittsburgh, PA, 18-20 July 2007.

Sorace, S., Quercia, E., La Mattina, E., Charalampos, Z. Patrikakis, L., Bacon, G., & Mackinnon, L. (2018). Serious Games: An Attractive Approach to Improve Awareness. Community-Oriented Policing and Technological Innovations.

Sormani, R., Soldatos, J., Vassilaras, S., Kioumourtzis, G., Leventakis, G., Giordani, I., et al. (2016). A serious game empowering the prediction of potential terrorist actions. Journal of Policing, Intelligence and Counter Terrorism, 11(1), 30.

Spinelli, L. (2018). Tabletop Role-Playing Games and Social Skills in Young Adults. Honors College Theses. 192.

Stapleton, A. (2005). Game issue report. Korea IT Industry Promotion Agency, Serial No. 25.

Verizon Communications Inc. (2021). DBIR 2021 Data Breach Investigations Report. Retrieved December 16, 2021, from: https://www.verizon.com/business/resources/reports/dbir/.

Vermillion, S. D., Malak, R. J., Smallman, R., Becker, B., Sferra, M., & Fields, S. (2017). An investigation on using serious gaming to study human decision-making in engineering contexts. Design Science, 3.

Wright, R., & Bennett, T. (1990). Exploring the Offender's Perspective: Observing and Interviewing Criminals. In: Kempf K.L. (eds) Measurement Issues in Criminology. Springer, New York, NY.

Zyda, M (2005). From Visual Simulation to Virtual Reality to Games. Computer, September 2005, pp. 25–32.

Yildirim, S. (2010). Serious game design for military training. In Games: Design and Research Conference, Volda University College (pp. 3-4).

APPENDIX

A: Structure of Data Collection Reporting

Serious Gaming Data Reporting	
Research Method:	
Researcher's involvement:	
Sampling method:	
Data Collection/Recording:	
Sample No.:	
Organization:	
Date:	
Time:	
Location:	
Duration:	
Room:	
Room conditions:	
Paid/unpaid:	
Researcher's involvement:	
Game extent:	
Table administration:	
Preceding SE presentation:	
Pre-/post-questionnaire:	
Language (game material):	
Language game:	
Game masters No.:	
Game Master Training:	
GM Training administration:	
Sample size:	
Population details	
Male-Female ratio:	
Age range:	
Population industries:	
Population professions:	
Population behaviour:	
Socio-cultural behaviour:	
Population feedbacks:	
Criminal behaviour/intentions:	
Citations of feedbacks:	
Other observations/final remarks:	
Other Remarks	

B: Serious Game Proceedings Structure and Game Material Excerpts

Social Engineering War Gaming: Game Play

1. Draw Cards
   a. Each team draws one card from the set COMPLIANCE PRINCIPLES. The card deck contains the human behavioral patterns
   b. Each team draws three cards from the set of ATTACK VECTORS. The card deck contains attack techniques.
2. Brainstorming Phase

   The teams take the role of the attacking social engineers and prepare a sophisticated attack with the combination of the following factors. The teams have ten minutes to prepare their attacks in writing.

   a. COMPLIANCE PRINCIPLE

      The card drawn with the COMPLIANCE PRINCIPLE forms the foundation of the attack preparation and must be implemented as precisely as possible. For example:

      « DECEPTION is at the heart of innumerable fraud scenarios. Things and people are often not what they seem. People are easily tricked, even when they think they are being cautious. Social Engineers take advantage of the fact that most victims go along with their expectations of what will happen in any given situation. »

   b. ATTACK VECTOR

      One of the three ATTACK VECTORS drawn must be selected and scheduled for the attack. For example:

      « PRETEXTING is the type of social engineering attack which is targeted and involves inventing a scenario to gather information from an unsuspecting user. The social engineers research about the target and collects enough information to use it for manipulation or impersonation. For this attack to be successful, a solid pretext is necessary. The key things research, information gathering and planning results in building a solid pretext and a successful attack. »

   c. Attacker

      The team has to decide whether the attacker is an insider or an outsider of the organization. An insider is a known member of the organization who has already established trust. An outsider is new to the organization and has to establish trust to its employees. For example:

      « The social engineer is an outside attacker. »

   d. Targeted Person

      A person from the corporate team has to be selected for the attack. For example:

      « MIA is the assistant to the CEO. To support him, she has access to almost everything. She does ok with computers but is bothered by the many security precautions in the company. »

   e. Targeted Asset

      A realistic information goal can be freely defined. For example:

      « The goal is to read the current email traffic of the CEO. »

   f. Context

      An outline of the situation shall be described as initial situation for the attack. For example:

      « MIA always leaves her office door and computer unlocked. The cleaning guy takes it very seriously when cleaning the offices. »

   g. Attack

      The planned attack is to be described. For example:

      « A social engineer can just enter her office pretending to be a new cleaning guy, so he can just enter and send an email using her computer and open an attachment with a trojan. »

3. Attack Phase
   a. The active team presents its attack to the group.
   b. Each attack consists of all factors of the brainstorming phase.
   c. The given factors are to be explained and the factors chosen are to be explained.
   d. After a team has proposed an attack it is initialized and cannot be changed anymore.
4. Discussion
   a. At this point, the group discusses whether the proposed attack is feasible or brings arguments why this could be unrealistic.
   b. If the proposed attack is not plausible, the turn ends immediately.
   c. Finally, the group has to make the choice on how many points are granted.
   d. In addition, the other teams can also propose improved versions of an attack and gain points.
   e. All attacks have to be documented.
5. Points

   The following points can be gained per round:

   a. COMPLIANCE PRINCIPLE

2 Points	Perfect match
1 Point	Somewhat a match
0 Point	No match

   b. ATTACK VECTOR

1 Point	Perfect match
0 Point	No match

   c. Attacker

2 Point	Inside attacker
1 Points	Outside attacker

   d. Targeted Person, Targeted Asset, Context and Attack as one consistent whole

2 Points	Feasible
1 Point	Somewhat a match
0 Point	No match, the turn ends immediately with zero points for the attacking team

   e. Attack Improvement by other teams

2 Points	Major improvement
1 Point	Minor improvement
0 Point	No improvement

6. Iteration
   a. The next team proposes an attack in the same fashion explained above.
   b. If several rounds are played, the cards are shuffled after each round and the teams pick up new cards.
   c. The brainstorming phase may be shortened at the discretion of the teams.
   d. The team with the most points wins.

GAME-MASTER INSTRUCTIONS

Sequence	Action	Responsibility	Duration
1)	**Introduction statement**	**comment**	
2)	**Allocate players at table into teams à 2-3 persons**	**moderation**	
3)	**Distribute game material per team (max. 4 teams per table)** 1 x Floor plan 1 x  1 x Target person description *Explain structure of description* 1 x 	**distribute**	**3-4 Min.**
4)	**INFORMATION-Phase - Teams acquaint themselves with game material**	**time keeping & moderation**	**10 Min.**
5)	**Distribution of play cards Compliance Principles (3x) und Attack Vectors (3x) per team 1 x Attack plan per Team** 3 x Compliance Principles  3 X Attack Vectors  1 x Attack plan (to be filled-out) 	**distribute**	**2-3 Min.**
6)	**BRAINSTORMING- Phase - Preparation of SEA & filling-out attack plan**	**time keeping & moderation**	**12 Min.**
7)	**Explain procedure of mutual evaluation phase** - every teams presents ist SEA and is evaluated by the other teams	**comment**	**1-2 Min.**
8)	**PRESENATATION & DISCUSSION of SEA per team** - Moderation of evaluation phase - Documentation of allocated score per team on scorecard  - Bonus points available for attack improvement proposals - Ask for compliance with point distribution	**time keeping & moderation**	**7 Min. per Team**
9)	**Evaluation of winner team** Count points on scorecard 	**evaluation of scorecard**	**1-2 Min.**
10)	**Announce winner team**	**moderation**	**1 Min.**
11)	**Collect game material and hand back to Fabian or Philipp**	**collect**	

Compliance Principles cards

The concept of Social Engineering is based on psychological principles of persuasion to gain trust and to deceive targeted persons. Those Compliance Principles can be authority, reciprocity or social proof, for example (Cialdini, 1984). In this regard, it is important for the participants to understand the different means of using those Compliance Principles in Social Engineering Attacks, such that participants can better detect and protect themselves against targeted attacks. Therefore, one step in the course of the game is to draw cards from the Compliance Principles stack and to familiarise with the specific persuasion tactic.

Attack Vector cards

Additionally, participants are requested to draw cards from the stack "Attack Vectors". As Social Engineering Attacks can take on various forms, it is therefore important for the participants to understand the different forms, in order to detect Social Engineering Attacks and to protect themselves against them. The purpose of the Attack Vector cards is therefore to familiarise the participants with the varying techniques and to understand the effect of combining an Attack Vector with a persuasion technique.

Target persons

The third component of the game consists of a set of fictious target persons, each with different functions and personal characteristics. It is the intention of the game to match the drawn Compliance Principle in combination with an Attack Vector and apply it to a targeted person that is most appropriate to be deceived by the attack technique. In this regard, participants are required to think through the characteristics of the specific attack techniques and how they can be applied on the characteristics of the targeted fictious persons. It is the purpose of the game that participants understand the rationale behind Social Engineering applied in different situations, such that they are more likely to detect such attacks at an early stage and prevent crimes from happening. Fictious target persons can be invented independently based on the environment the participants are acting in. In an educational setting, fictious target persons can be pupils or students, whereas in the course of the application of the game in a corporate environment fictious target persons will be employees.

Attack Plan

Compliance Principle	*Example: «Deception is at the heart of innumerable fraud scenarios. Things and people are often not what they seem. People are easily tricked, even when they think they are being cautious. Social Engineers take advantage of the fact that most victims go along with their expectations of what will happen in any given situation.»* *Notes:*	10 Points
Attack Vector	*Example: «Pretexting is the type of social engineering attack which is targeted and involves inventing a scenario to gather information from an unsuspecting user. The social engineers research about the target and collects enough information to use it for manipulation or impersonation. For this attack to be successful, a solid pretext is necessary. The key things research, information gathering and planning results in building a solid pretext and a successful attack.»* *Notes:*	10 Points
Targeted Person	*Example: «Olivia is the assistant to the CEO. To support him, she has access to almost everything. She does ok with computers but is bothered by the many security precautions in the company.»* *Notes:*	30 Points
Targeted Asset	*Example: «The goal is to read the current email traffic of the CEO.»* *Notes:*	
Context	*Example: «Olivia always leaves her office door and computer unlocked. The cleaning guy takes it very seriously when cleaning the offices.»* *Notes:*	
Attack	*Example: «A social engineer can just enter her office pretending to be a new cleaning guy, so he can just enter and send an email using her computer and open an attachment with a trojan.»* *Notes:*