Systematic Scenario Creation for Serious Security-Awareness Games

Vera Hazilov[1] and Sebastian Pape[2,3]✉[0000−0002−0893−7856]

[1] Intero Operations & Services GmbH (INOS), Munich, Germany
[2] sebastian.pape@m-chair.de
Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt, Germany
[3] Social Engineering Academy GmbH, Frankfurt, Germany

Abstract. While social engineering is still a recent threat, many organisations only address it by using traditional trainings, penetration tests, standardized security awareness campaigns or serious games. Existing research has shown that methods for raising employees' awareness are more effective if adjusted to their target audience. For that purpose, we propose the creation of specific scenarios for serious games by considering specifics of the respective organisation. Based on the work of Faily and Flechais [11], who created personas utilizing grounded theory, we demonstrate how to develop a specific scenario for HATCH [4], a serious game on social engineering. Our method for adapting a scenario of a serious game on social engineering resulted in a realistic scenario and thus was effective. Since the method is also very time-consuming, we propose future work to investigate if the effort can be reduced.

Keywords: serious game · security awareness · personas · scenario creation

1 Introduction

Social engineering is older than the electronic age itself and is still a part of our life. The European Network and Information Security Agency, ENISA, defines social engineering as a technique that exploits human weaknesses and aims to manipulate people into breaking normal security procedures [21]. In most cases, maliciously motivated attackers aim to gain access to their victims' commercial, financial, sensitive or private information in order to use it against them or cause harm otherwise [2]. Social engineering's key elements are deception, exploitation and use of psychological tricks. Social engineering attacks represent a threat to individuals and organisations and often lead to some kind of financial losses.

However, most organisations have difficulties addressing this issue adequately. According to Kevin Mitnick – a former hacker who now works as an IT security consultant, most companies rather purchase heavily standardized security products, such as firewalls or intrusion detection systems, than considering potential threats of social engineering attacks [19]. Mitnick criticizes this approach and argues that technology-based products simply create an illusion of security however, leave organisations disarmed towards attacks that are directed towards their employees. Peltier [22] supports this argument and states that technology-based countermeasures should be applied whenever possible. However, he also claims that no hardware or software is able to protect an organization fully against social engineering attacks. In addition to that, social engineering is highly interdisciplinary, however most defense strategies are advised by IT security experts who rather have a background in information systems than psychology [26, 27].

Traditional trainings mainly focus on transfer of knowledge and often do not address employees' attitude towards security or raise their awareness sufficiently. While knowledge is a prerequisite to counter social engineering attacks, a successful defense also requires a sufficient security-aware culture among staff [1], which represents a challenge for many organisations. Mainly because security policies are often in a bad shape and rather inform employees about what not to do than providing any guidance about desired behaviour and outcomes. Penetration tests are attached to a lot of obligations and legal burdens that need to be resolved beforehand. They can demotivate employees, who as a consequence might give up on defending social engineering attacks at all, and usually can not be repeated regularly, because employees become aware of penetration testers [9]. Security awareness campaigns often fail because they evoke negative feelings such as anxiety, fear or stress and are therefore often ineffective. In addition to that, individuals generally dislike following advice or instructions because it is associated with losing control. Lastly, awareness campaigns often provide only information about risks, are often not engaging, interesting and entertaining enough and therefore fail to change individuals' behavior [3]. However, serious games are more entertaining and engaging than traditional forms of learning and can influence individuals' behavior due to their use of pedagogy and game-based learning principles, such as motivation, cognitive apprenticeship and constructivism [10]. They have demonstrated a potential in industrial education and training disciplines [23, 25] if respective organizations care for players' privacy and working atmosphere [16], do not use gaming data for appraisal or selection purposes and clearly communicate this to the employees [17]. Abawajy's observations [1], that trainings can be greatly enhanced through interactive content, support this statement and make serious games a strong candidate for overcoming issues of traditional training methods.

However, not only for security awareness campaigns, but also for serious games it is important to address the target audience as specific as possible. Therefore, in this paper, we aim to adjust a serious game to a specific target group by adapting it accordingly. For that purpose we chose the serious game HATCH [5] and developed a new scenario for one of its variants in order to be suitable for consulting companies. This approach tackles that problem, that although many serious games for IT security exist, it is still hard to find a accurately fitting serious game for a specific organisation or scenario.

2 Background and Related Work

This work is based on two concepts, personas and HATCH. Personas represent a popular technique that is often used in user-centered design in order to create services, products or software [24]. HATCH is a serious game on social engineering, for which we have developed a scenario as proof of concept. However, hardly any specific properties of the game were used, so it should be possible to generalise the results and develop scenarios for related games.

2.1 Personas

By definition, personas are imaginary however, realistic descriptions of stakeholders or future users of a service or product, who have names, jobs, feelings, goals, certain needs and requirements [11]. The concept was firstly introduced by Cooper [7] in 1999. Cooper argues that developers need to consider future users' needs, goals and wishes, instead of designing products for 'elastic users'. The latter term represents highly standardized descriptions of users, which are unrealistic and in many cases rather represent developers' own needs. According to Cooper, the use of elastic users therefore leads to products, which only partly satisfy real users' needs.

In 2011, Faily and Flechais [11] introduced a method for developing personas that is based on grounded theory. The latter is a "[. . .] systematic, yet flexible guideline for collecting and analyzing qualitative data" [6]. Faily and Flechais [11] collected necessary data through interviews, each of them lasting approximately an hour. All interviews have been transcribed and subjects to a grounded theory analysis using ATLAS.ti, a qualitative data analysis and research tool. The process of developing personas included three steps [11]: the first step includes reading all interview transcripts, identifying relevant text passages, assigning appropriate phrases (codes) to them and formulating them as propositions. The propositions are later summarized and as a result represent most significant concepts developed personas need to explore. As next, appropriate propositions are selected and stated as potential characteristic of a persona. The final step of this approach involves selecting relevant characteristics and writing a persona narrative. Faily and Flechais [11] used their approach successfully to derive accurate archetypes of their respective user communities (personas) from around 300 quotations and 90 thematic concepts.

2.2 HATCH

Hack and Trick Capricious Humans (HATCH) is a physical (tabletop) serious game on social engineering [4, 5]. The game is available in two versions, a real life scenario and a generic version. Each version of the game pursues a slightly different objective: The real life scenario is aiming to derive social engineering security requirements of a company or one of its departments. Therefore, a real environment is modelled and players attack their colleagues in order to identify real attack vectors. The generic version of the game aims to raise the players' awareness for social engineering threats and educate them on detecting this kind of attacks. In order to not unnecessarily expose and blame colleagues during a training session, it is based on a virtual scenario with personas as attack victims [16]. The scenario consists of a layout of a medium-sized office and ten employees as personas, printed on cards that contain fictional descriptions of them: their names, role within the organization, familiarization with computers and their attitude towards security and privacy [5].

In both versions two deck of cards are used (psychological principles and social engineering attacks). When playing the game, each player draws one psychological principle card and three social engineering attack cards and reads the respective descriptions. Psychological principle cards state and describe human behaviors or patterns that are often exploited by social engineers, as for example: 'Distraction - While you distract your victims by whatever retains their interests, you can do anything to them'. On the other hand, the social engineering cards name and define some of the most common social engineering attacks, for example dumpster diving, which is 'the act of analyzing documents and other things in a garbage bin of an organization to reveal sensitive information'. Each player has then the task to choose a victim[4] which fits to the psychological principle card and elaborate an attack by using one of the social engineering attack cards which matches victim and psychological principle best.

Players take turns to reveal their cards and describe the social engineering attack they came up with. Other players discuss the proposed attack and award points for attack's feasibility and viability and rate if it is compliant with descriptions of this player's cards. The total score of each player is calculated by the end of the group rating and the player with the highest score wins the game. At the end of the game, all players briefly reflect on proposed social engineering attacks and derive potential security threats.

Beckers and Pape [4] showed that that the real life scenario was helpful to increase the security awareness of employees [5] and in the elicitation of context-specific attacks by utilizing the domain knowledge of the players and their observations and knowledge about daily work and processes.

3 Methodology

The data that was used to develop a consulting services scenario for HATCH was collected through expert interviews, which have proven to be of good practical value [18]. The interviews were executed as semi-structured interviews based on the interview guide described in Sect. 3.1. Section 3.2 describes the interviewees and Sect. 3.3 the subsequent coding and qualitative analysis.

3.1 Interview Guide

Meuser and Nagel [18] emphasize the importance of using an interview guide. In particular for semi-structured interviews they serve two purposed. On the one

[4] depending on the version either a colleague or a persona

hand, they help the interviewer to not get lost in irrelevant topics and focus on the goal of the interview [12]. On the other hand, they help the interviewer to organize and structure the interviews and adapt them to knowledge gained in previous interviews [20].

The interview guide was constructed taking following aspects into consideration:

- the appropriate number of questions – although a large number of questions might provide deeper insights, too many questions can also extend the interview to an inefficient level. In alignment the suggestion from Gläser and Laudel [13] to limit the number of questions to approximately fifteen, the derived interview guide consists of seventeen questions.
- appropriate format of questions – asked questions can be noted as fully formulated sentences which provides stability or stated vaguely which increases interviewer's flexibility to react ad hoc [13]
- appropriate content of questions, which means that asked questions can be based on existing theories, publications or interviewer's own experience or knowledge [12].

The interview guide was tested within two one-hour interview sessions. At the end of each session, interviewed experts were asked to provide feedback regarding the guide's length, format and content. The initial interview guide was adopted during the process based on received feedback: an explanation of this work's main objective and approach was added to the introduction section. The interview guide's second section was extended by a definition of the term social engineering for the purposes of general introduction. All remaining sections stayed unchanged and aim to uncover this industry's specifics, assets, communication channels, their physical location as well as existing roles, skills and attitudes towards security and privacy. Table 1 gives a brief overview of the interview guide's structure.

3.2 Interview Implementation and Participants

All nine expert interviews were conducted in January and February 2017 and lasted between 35 minutes and 61 minutes (cf. Tab. 2). All interviews were conducted in German –the experts' native language in order not to obstruct experts' thinking ability and allow them to provide complex and comprehensive answers. Most interviews were conducted face-to-face, only interview seven and eight were recorded over the phone. None of the participants received any printed information, such as handouts or printouts, before or during the interview in order to avoid any distraction. However, before the interviews, participants were informed about the study's approach and goal and asked for consent as indicated in Tab. 1. Table 2 presents an overview of all participants, their role, professional experience, corresponding business unit and the interview's duration.

Due to difficulties of cold calling professional consultants and requesting their help for creating a serious game scenario, all participating interviewees were approached based on existing contacts. Furthermore, none of the approached

Table 1: Interview Guide

# Section	Content
1 Introduction	• Greeting and opening • Statement of classification • Declaration of consent • Introduction to the research's approach and main goal
2 Social Engineering	• General understanding • Definition • Previous experience with SE attacks
3 Industry's Specifics	• General understanding • Associations • Characteristics
4 Assets & Location	• Company's assets and employees • Asset's location
5 Roles & Tasks	• Specific roles • Responsibilities and tasks
6 Communication Channels	• Company's communication channels • Management process • Access rights • Relevant content
7 Personas	• Skills • Knowledge • Attitude towards security and privacy

employees of a 'client company' were willing to participate, since they were afraid of revealing sensitive information which could potentially lead to a social engineering attack. However, we do not think that this was a major drawback, since the developed scenario aimed to focus on consulting companies.As a consequence, all interviewed experts have in common that they are employed by a large consulting/auditing firm, however differ in their roles, business units, gender, age and level of professional experience. The experts' selection was done in order to introduce a certain level of variety, however contain a strong focus at the same time: We expected that a more unified selection of participants would have resulted in a highly specific scenario, while a too diverse selection of experts may have yielded unfocused results.

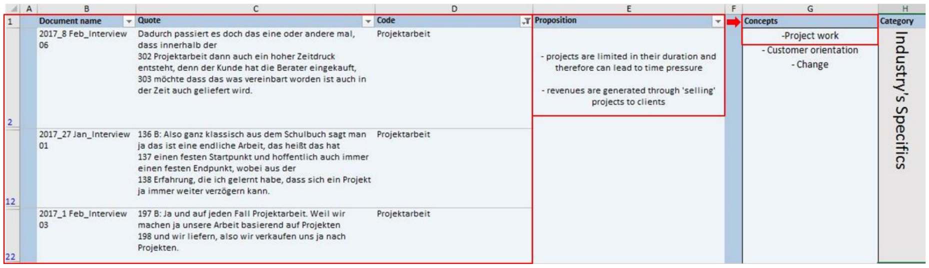
3.3 Data Analysis

All interviews were audio recorded, transcribed literally[5], and all transcripts were imported into MAXQDA, a professional software for qualitative text analysis, and coded in chronological order. The applied process of coding consisted of two

[5] pauses and certain sounds were neglected such as 'huh' etc.

Table 2: Participants Overview

#	Role	Experience	Business Unit	Duration
1	Consultant	1-3 years	Management Consulting	61 min
2	Consultant	1-3 years	Risk Consulting	54 min
3	Consultant	6+ years	Technology Consulting	55 min
4	Consultant	3-6 years	Technology Consulting	35 min
5	Assistant	1-3 years	Management Consulting	37 min
6	IT	1-3 years	Technology Consulting	60 min
7	Consultant	3-6 years	Technology Consulting	35 min
8	Consultant	6+ years	Technology Consulting	59 min
9	Consultant	6+ years	Technology Consulting	46 min



1	Document name	Quote	Code	Proposition	Concepts	Category
2	2017_8 Feb_Interview 06	Dadurch passiert es doch das eine oder andere mal, dass innerhalb der 302 Projektarbeit dann auch ein hoher Zeitdruck entsteht, denn der Kunde hat die Berater eingekauft, 303 möchte dass das was vereinbart worden ist auch in der Zeit auch geliefert wird.	Projektarbeit	- projects are limited in their duration and therefore can lead to time pressure - revenues are generated through 'selling' projects to clients	-Project work - Customer orientation - Change	Industry's Specifics
12	2017_27 Jan_Interview 01	136 B: Also ganz klassisch aus dem Schulbuch sagt man ja das ist eine endliche Arbeit, das heißt das hat 137 einen festen Startpunkt und hoffentlich auch immer einen festen Endpunkt, wobei aus der 138 Erfahrung, die ich gelernt habe, dass sich ein Projekt ja immer weiter verzögern kann.	Projektarbeit			
22	2017_1 Feb_Interview 03	197 B: Ja und auf jeden Fall Projektarbeit. Weil wir machen ja unsere Arbeit basierend auf Projekten 198 und wir liefern, also wir verkaufen uns ja nach Projekten.	Projektarbeit			

Fig. 1: Process of Axial Coding

rounds, open and axial coding. While open coding is the process of reading textual data line-by-line, identifying certain phenomena within it and attaching adequate phrases (e. g. codes) to it, axial coding represents the process of examining previously assigned codes, identifying certain relationships among them and summarizing them into concepts and categories [8]. This work's coding process is illustrated in Fig. 1.

The illustration above shows a fraction of all text passages that have been assigned with the code 'project work' and later formulated into propositions 'projects are limited in their duration and therefore can lead to time pressure' and 'revenues are generated through selling projects to clients'. All relevant propositions were later summarized to the concept 'project work' and assigned to the category 'industry's specifics'. Following this approach, 110 pages of interview transcripts were assigned with 509 codes.

3.4 Development of the Scenario

Since we took HATCH for granted, as it already existed before, we do not describe its development, however focus on the creation of a new scenario. Figure 2 illustrates the steps of the scenario development.

In the previous sections, we have already described the interview, transcript and coding phases (stage 1 to 3). Following Faily and Flechais' method [11] for developing personas, we developed propositions from codes (stage 4), such as ‘more consultants are hired for project than clients’, ‘with the exception of client’s assistants, consultants are generally younger’ and ’generally, the consulting team consists of 4 to 5 people’. These propositions were summarized, assigned to concepts and categorized (stage 5). For example, previous propositions were assigned to the concepts ’role’ and ’age’ and categorized as ’personas’. Altogether 21 concepts were sorted into five categories, which represent the main components of the consulting services scenario for HATCH. Those categories are: industry’s specifics, assets, communication channels, location and personas. The first four of them represent a consulting firm’s working environment, while the last embodies personas’ characteristics.

As the last step, appropriate propositions were selected and stated as potential characteristics of a persona to write persona narratives and develop the scenario (stage 6). For this purpose, all personas-related concepts and propositions were reviewed again, in order to identify most valuable and meaningful insights, and later embodied into future personas. For example, the propositions from the concepts ’roles’ and ’age’ lead to the decision of having more consulting personas (4) than personas of the client company (3). Furthermore, with the exception of the client’s assistant, all consulting personas are younger than personas of the client. In the same manner, propositions were used to develop professional consultants’ working environment and surroundings.

3.5 Evaluation

Note that this work focuses on creating a new scenario in order to adapt an existing game called HATCH, which has already been evaluated [4, 5]. Therefore, we did not evaluate the game, its rules and elements itself, however rather focused on evaluating the consulting services scenario.

The developed consulting services scenario for HATCH was evaluated by five players and within two sessions: the first session was conducted on 30th of March 2017 and lasted roughly one hundred minutes, while the second session took place on March 31st, 2017 and continued approximately two hours. One moderator was present at both sessions and all players had an IT background, were employed by an auditing/consulting firm. None of the players was involved in the previous interview sessions.

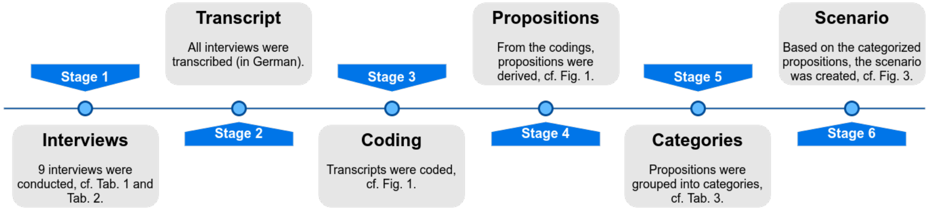

Stage 1
Interviews
9 interviews were conducted, cf. Tab. 1 and Tab. 2.
Transcript
All interviews were transcribed (in German).
Stage 2
Stage 3
Coding
Transcripts were coded, cf. Fig. 1.
Propositions
From the codings, propositions were derived, cf. Fig. 1.
Stage 4
Stage 5
Categories
Propositions were grouped into categories, cf. Tab. 3.
Scenario
Based on the categorized propositions, the scenario was created, cf. Fig. 3.
Stage 6

Fig. 2: Overview of Scenario Creation Process

Table 3: Derived Scenario Related Categories and Concepts

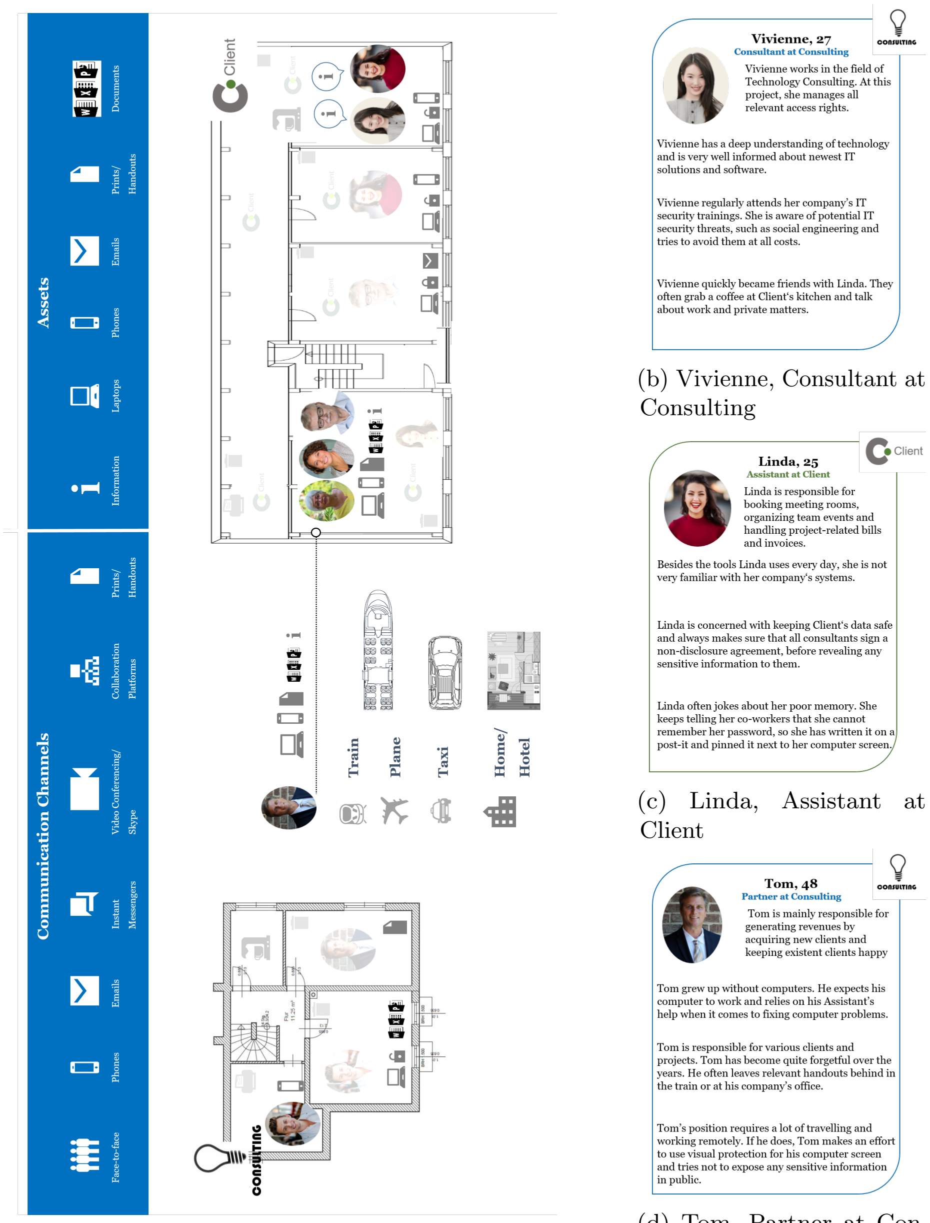
# Category	Concept
1 Industry's Specifics	• Project work • Customer orientation • Change
2 Assets	• Information (sensitive, project-related, private) • Laptops • Phones • Emails • Prints, handouts • Documents (office)
3 Communication Channels	• Face-to-face • Phone calls • Emails • Video conferences • Collaboration platforms • Prints, Handouts
4 Location	• Client's office • Remote locations
5 Personas	• Age • Roles and tasks • Skills and knowledge • Attitude towards security and privacy

4 Results

With the process described in the previous section, we derived five relevant categories with altogether 21 concepts as shown in Tab. 3. The industry's specifics, consultants' assets, communication channels and location are incorporated within the scenario, which represents working environment and surroundings of professional consultants. These companies' assets and communication channels are pictured at the top of the scenario, since their location might vary a lot between companies and we aimed to avoid a too strict mapping to an individual or a certain location (cf. Fig. 3a). The results from the personas category were used to create different persona cards as shown in Fig. 3b to Fig. 3d.

4.1 Scenario

Besides the layout of both companies, called Consulting and Client, the scenario represents this industry's characteristics and includes several personas, which are described in the next section. As illustrated in Fig. 3a, consulting firms use a number of communication channels, such as face-to-face interaction, phones, emails, instant messengers, video conferencing tools or Skype, collaboration platforms, prints, handouts and posses assets that are mostly focused around



(a) Scenario

Vivienne, 27
Consultant at Consulting

Vivienne works in the field of Technology Consulting. At this project, she manages all relevant access rights.

Vivienne has a deep understanding of technology and is very well informed about newest IT solutions and software.

Vivienne regularly attends her company's IT security trainings. She is aware of potential IT security threats, such as social engineering and tries to avoid them at all costs.

Vivienne quickly became friends with Linda. They often grab a coffee at Client's kitchen and talk about work and private matters.

(b) Vivienne, Consultant at Consulting

Linda, 25
Assistant at Client

Linda is responsible for booking meeting rooms, organizing team events and handling project-related bills and invoices.

Besides the tools Linda uses every day, she is not very familiar with her company's systems.

Linda is concerned with keeping Client's data safe and always makes sure that all consultants sign a non-disclosure agreement, before revealing any sensitive information to them.

Linda often jokes about her poor memory. She keeps telling her co-workers that she cannot remember her password, so she has written it on a post-it and pinned it next to her computer screen.

(c) Linda, Assistant at Client

Tom, 48
Partner at Consulting

Tom is mainly responsible for generating revenues by acquiring new clients and keeping existent clients happy

Tom grew up without computers. He expects his computer to work and relies on his Assistant's help when it comes to fixing computer problems.

Tom is responsible for various clients and projects. Tom has become quite forgetful over the years. He often leaves relevant handouts behind in the train or at his company's office.

Tom's position requires a lot of travelling and working remotely. If he does, Tom makes an effort to use visual protection for his computer screen and tries not to expose any sensitive information in public.

(d) Tom, Partner at Consulting

Fig. 3: Scenario and Personas "Consulting Company"

information: laptops, phones, emails, prints or handouts and Word, Excel or PowerPoint documents.

The most important characteristic of consulting firms is project-based work. Firms within this industry generate revenues by selling their services in form of projects,which are mostly executed at their customers' office. Therefore, consultants are required to travel a lot and work from various locations e.g. their own or client's office, public transportation, hotel rooms or from home. Therefore, the presented scenario pictures various locations, including layouts of two offices, which contain several elements and details. Consulting's office is placed on the left, it has a kitchen and several rooms, while the Client's office is on the right.

4.2 Personas

The scenario also contains seven personas, which are fictional descriptions of workers that are employed by the consulting company or the organisation that hired them. All personas include information such as an employee name, age, occupied role, tasks, attitude towards security/privacy and personality traits. Players will get cards with the description of the personas as shown in Fig. 3b to Fig. 3d. We also provide a more schematic presentation in Tab. 4. Since both can not describe the interactions, the remainder of this section describes the developed personas and their interactions in more detail.

Vivienne and Linda are working on the same project, but for different companies: Vivienne is a 27-year-old technology consultant and works for 'Consulting', a large auditing and consulting firm. Linda is 25 years old and has recently started her job at Client, a company that hired Vivienne's organization for a limited period. Linda works as an assistant and is therefore responsible for booking meeting rooms, organizing team events and handling all project-related bills and invoices. Vivienne, on the other hand, is responsible for managing and assigning access rights to project-related communication platforms. She also has a deeper understanding of technology, while Linda is only familiar with tools and systems she uses every day. Both women have a similar attitude towards IT security and privacy and are concerned with keeping their company's data safe. Therefore, Linda always makes sure that all consultants sign a non-disclosure agreement, while Vivienne regularly attends IT security trainings to get informed about potential IT security threats and risks. Both women are very social and became friends very quickly. As a consultant, Vivienne has strong communication skills and is comfortable with starting conversations with strangers. Linda, on the other hand, is friendly, tends to trust her co-workers and is very forgetful.

Niko is 21 years old, studies business informatics at a university and is an intern at Consulting. Niko works for Tom, a partner at Consulting, and is responsible for preparing presentations, printing relevant handouts and uploading documents for his boss. Niko loves computer games, currently learns how to program and is very ambitious. He wants to get everything right and on time, which often stresses him out. Whenever Niko is stressed, he tends to leave his computer unlocked and forgets to shred Tom's documents that often include sensitive information. As an intern, Niko is not required to travel and works form Consulting's office. Tom is often gone and Niko gets bored easily. In that case, he socializes with other interns and loves to chat about Tom's projects.

Table 4: Developed Personas with a Description of Their (T)asks, (S)kills, (A)ttitude towards security and (P)ersonality

	Vivienne, 27, Consultant at Consulting
(T)	works in the field of Technology Consulting, manages relevant access rights at this project
(S)	has a deep understanding of technology, well informed about newest IT solutions and software
(A)	attends her company's IT security training regularly, aware of potential IT security threats, such as social engineering, tries to avoid potential security threats at all costs
(P)	communicative and open minded, quickly became friends with Linda, often grabs a coffee at Client‘s kitchen to catch up with Linda
	Linda, 25, Assistant at Client
(T)	responsible for booking meeting rooms, organizing team events and handling project-related bills and invoices
(S)	familiar with tools she uses every day, not very familiar with any other of her company‘s systems
(A)	concerned with keeping her company's data safe, ensures all consultants sign a non-disclosure agreement
(P)	forgetful,trustworthy towards her co-workers, tells her co-workers that she cannot remember her password
	Barbara, 44, Project Lead at Consulting
(T)	plans, coordinates and controls the project at Client, responsible for informing the sponsor of the project about its current state
(S)	has 16+ years of experience
(A)	has a project lead, she has access to every room at Client's office, concerned with keeping any client or project-relevant data safe
(P)	required to travel a lot, spends four days a week on a project at her client's office, works from home or at her company's office on Fridays
	Hans, 56, Head of IT at Client
(T)	ensures Client's systems run smoothly, updates security features, checks if access rights are assigned correctly
(S)	knows his company's systems very well
(A)	IT security has the highest priority, spends hours getting informed about potential IT risks and how they can be prevented
(P)	passionate about his job, launched an anti-social engineering campaign at Client, informs his colleagues about adequate security behavior
	Tom, 48, Partner at Consulting
(T)	responsible for generating revenues by acquiring new clients, makes sure existent clients are happy, supervises various clients and projects
(S)	grew up without computers, expects his computer to work, relies on his assistant's help when it comes to fixing computer problems
(A)	tries not to expose any sensitive information in public or while working remotely, makes an effort to use visual protection for his computer screen
(P)	forgetful, often leaves relevant handouts behind, travels a lot due to his position
	Gabriele, 64, Project Sponsor at Client
(T)	responsible for allocating resources efficiently, ensures projects are executed on time
(S)	familiar with the tools she uses a lot, not very familiar with the tools she doesn't use regularly
(A)	careful about revealing her company's information to any of the consultants
(P)	not very trusting towards consultants, often has a hard time understanding their recommendations
	Niko, 21, Intern at Consulting
(T)	responsible for preparing presentations, printing handouts and uploading relevant documents online
(S)	studies business informatics, has a good understanding of IT due to his studies at a university, is learning how to program
(A)	not aware of potential IT security threats, not very concerned with revealing sensitive data or information
(P)	new to the consulting industry, ambitious and therefore often stressed and forgetful

Tom has been with the company for more than eighteen years and is 48 years old. As a partner at Client, he is responsible for generating revenues by acquiring new projects and clients and making sure that existing clients are happy, which requires him to travel a lot. He just left his office and is currently on his way to Client. Over the last couple of years, Tom has become forgetful and started to leave printed documents behind. Tom often works remotely and always tries to get as much work done as possible. He often participates in conference calls with his colleague Barbara and employees of Client, Hans and Gabriele. Barbara is 44, has more than 16 years of professional experience and works at Consulting as a project lead. She takes her role very seriously and is responsible for planning, coordinating and reporting this project's current status to Gabriele. Barbara is concerned with keeping any client or project-relevant data safe and, like most professional consultants, spends four days a week at Client's office. On Fridays, she either works from home or her company's office.

Gabriele is 64 years old and the CFO of Client. She is responsible for allocating her company's resources efficiently and ensures that all projects are executed on time. Due to her background in finance, Gabriele knows everything about Client's financial IT tools and systems. However, she is not very familiar with any other tools at Client. She is also very cautious about revealing her company's information to any of the consultants, especially after she started working with Hans. Hans is 56 years old and Client's Head of IT. He has dedicated his life to his department and makes sure that all systems run smoothly and Client's security features are up to date at all times. Hans knows all of his company's systems very well and often checks if all access rights were assigned correctly. IT security has the highest priority for Hans, he spends hours researching potential IT threats and how they can be prevented. He has just launched an anti-social engineering campaign at Client and uses every chance to inform his colleagues about adequate security behavior.

Today, Vivienne is not required to take part in this meeting. She often works from Client's kitchen and grabs a coffee with Linda. The two have been getting along great. Linda is always excited to catch up with Vivienne, grab a cup of coffee and have a chat about work and personal matters.

5 Evaluation

In this section, we describe the evaluation process of the scenario. It was used to evaluate our methodology's outcome, since the quality of the developed scenario and personas is the main goal of the proposed method.

The evaluation sessions were structured as follows: the participants of the session were introduced to this work's main goal, the development of a consulting services scenario for HATCH, and shown a video about social engineering in order to clarify the term social engineering, its key elements and techniques. Subsequently, any emerged questions were answered and all participants were introduced to HATCH, the game's rules, scoring sheet, scenario and personas. Next, HATCH was played according to its rules, ensuring that each player at least takes three turns. At the end of each session, all participants were first briefly asked about the game itself to prevent that a misunderstanding of the elements and rules of HATCH would influence scenario's evaluation. We then asked the players to evaluate the scenario, particularly in regards to its comprehension, completeness and closeness to reality. The provided feedback was audio recorded and subsequently analyzed.

We did not aim to evaluate HATCH's rules, game elements or mechanics and wanted to ensure that the participants of the evaluation session are not distracted from the consulting services scenario. Therefore, HATCH was not elaborated any further after the participants claimed that its rules and key elements were clear and easy to understand.

In regards to HATCH's scenario, all participants agreed and stated that the represented consulting services scenario and personas are intuitive[6], easy to understand[7] and very realistic[8]. When asked for an extension of the scenario, participants suggested that the presented scenario could be extended by additional personas. While participants of the first evaluation round suggested to include an office administrator or a receptionists, members of the second session argued for adding an external service provider such as security or a cleaning personnel[9]

6 Discussion

In this section, we first discuss the results of the evaluation, followed by considerations how the presented approach can be applied in future scenarios. At the end of this section, we discuss limitations of our research.

6.1 Scenario

Reflecting the feedback of the evaluation session, it is necessary to discuss if the created consulting services scenario should be extended by additional personas, such as an office administrator, receptionist, cleaning or security personnel. On the one hand, additional personas could potentially enrich the scenario and make the serious security-awareness game more engaging and fun. On the other hand, too many personas within the scenario increase its level of complexity, make the game more difficult to play, since players need more time to go through the persona descriptions.

[6] [ES1: 1:38] "The description of the different people is very intuitive and very simply [...] modeled, also because of the figure. You could recognise it [...] very clearly."

[7] [ES2: 2:46] "Persons were described clearly and very realistic. I am able to imagine exactly how the person might be in real life, because these different types of people really exist."

[8] [ES1: 5:35] "The scenario was definitely realistic and also the [...] markers are intuitive.“

[9] [ES2: 04:10] "if I am an outsider and I somehow sneak into the office, I still have to pass some [...] security guard or receptionist, that is still an upstream step, which should also be considered, I think."

Therefore, firstly we recommend including a justified and reasonable number of personas within a scenario. For example, a guard and a cleaner both represent employees of an external service provider over whom the two companies have only limited authority. Including these personas within the scenario might not contribute too much to raising employees' awareness, however will likely result in requests for establishing a security policy for externals (if not already in place). However, if they are included, it might be a reasonable trade-off to only include one or the other.

Secondly, we suggest summarizing similar roles, tasks, skill sets and attitudes towards security or privacy in one persona wherever possible.For example, receptionists and office administrators perform very similar tasks, such as handling incoming calls, arranging meetings, planning events, organizing meeting rooms and handling invoices and expenses, and therefore might resemble in their daily tasks and IT skills. However, it is also very likely that administrators/receptionists of different companies differ in their attitudes towards privacy and security. Considering all arguments, for the next version, we would extend the presented scenario by two additional personas: an administrator/receptionist who is employed by each of the respective companies, Consulting and Client.

As our study was done in 2017, we also considered the changes within the consulting industry, for example that the number of female consultants has increased [15], which is already at a reasonable level within our scenario.

6.2 Methodology

The feedback of the evaluation sessions also allows a second conclusion: the applied method for creating a scenario for a serious security-awareness game was successful, since all participants agreed that the scenario and its personas are intuitive, easy to understand and very realistic. However, since the applied method is very time-consuming and requires a lot of effort, it only makes sense under certain circumstances. One use case is, if the respective company plans to play the game on a regular basis or with a large number of players. Another use case of the derived scenario is, while being specific being generic enough to be used by other organization within the same industry (here: consulting).

6.3 Threats to Validity and Limitations

All participating interviewees were approached based on existing contacts, which could lead to a selection bias. The latter was a consequence that trials to attract 'external' consultants for interviews without payment failed, since we did not have any funding. However, the participating interviewees still had diverse properties such as position, age, gender, etc. Furthermore, it could be argued that only nine interviews were conducted. However, even within nine interviews, we could observe some satiation manifesting in a repetition of answers and similar views and statements of the experts. In the same manner, since there is no clear definition of the term 'expert' in this context, one could question our sampling. However, according to the definition of Meuser and Nagel [18], experts are individuals who carry specific knowledge, emphasizing with the term 'specific' that the knowledge should not reflect everyday knowledge or common sense. Thus, despite experts were chosen purely based on the judgement of this work's authors, since they all work in an consulting company, they share specific knowledge about day-to-day work and processes, and therefore can be considered as experts and appropriate participants for our study.

In addition to that, it could be argued that this work's findings are not reliable, since the interview and coding process (open and axial coding), was done in two different languages: Interviews and open coding was done in German, all propositions were later summarized in English. However, we still assume that executing the interviews in the interviewees' native language is beneficial for the outcome and the translation at the end does not harm the result.

Furthermore, received answers during interviews and evaluation sessions might be subject to response biases, since we can not rule out that interviewed participants answered what they assumed the interviewer wants to hear or is socially acceptable. We tried to address that by not using any triggering terms and did not push for a response, allowing the interviewees a way out by not answering the questions.

6.4 Future Work

We suggest further validation of our method and its results to investigate if it can be transferred to another organization or domain. Additionally, we suggest to investigate if in the same manner or with which changes, a scenario and personas could be derived for a similar serious games on social engineering.

Additionally, we think that as future work it should be evaluated if the effort can be reduced, for example by conducting less or shorter expert interviews. In addition to that, we believe that the process of deriving an interview guide can be shortened and based on the interview guide presented in this paper, since all questions are directed towards the game's key elements, which are the industry's specifics, assets, communication channels, location and existing personas.

Hill et al. [14] showed that the use of multiple photos (of males and females) for a single persona to avoid gender stereotypes did not reduce project designers' engagement with the personas. Thus, another interesting question, far beyond the scope of this work, is if the use of multiple photos for a single persona would change players' engagement with HATCH's personas.

7 Conclusion

In this paper, we added to addressing the problem that many firms do not address social engineering security threats adequately or only apply ineffective defense mechanisms, such as traditional trainings, penetration tests or standardized security awareness campaigns or serious games. We proposed to create specific scenarios considering the the organisation's specifics and based on the work of Faily and Flechais [11] proposed a method to develop a new scenario for HATCH.

The result of our research is that our method for adapting a serious game on social engineering was effective, since all participants of the evaluation sessions agreed that the derived scenario and its personas are realistic. However, the proposed method is also very time-consuming, requires a lot of effort and only makes sense if the scenario can be used several times by an organization or can be transferred to another, similar organization. We propose future work to investigate if the effort can be reduced.

Acknowledgements

This work was supported by European Union's Horizon 2020 research and innovation program from the project CyberSec4Europe (grant agreement number: 830929) and from the project THREAT-ARREST (grant agreement number: 786890). We are grateful for image services of Pixabay, Pexels and Unsplash.

Bibliography

[1] Abawajy, J.: User preference of cyber security awareness delivery methods. Behaviour & Information Technology 33(3), 237–248 (2014)

[2] Alexander, M.: Methods for understanding and reducing social engineering attacks. SANS Inst. 1, 1–32 (2016), https://www.sans.org/reading-room/whitepapers/critical/methods-understand-ing-reducing-social-engineering-attacks-36972

[3] Bada, M., Sasse, A.M., Nurse, J.R.C.: Cyber security awareness campaigns: Why do they fail to change behaviour? CoRR abs/1901.02672 (2019), http://arxiv.org/abs/1901.02672

[4] Beckers, K., Pape, S.: A serious game for eliciting social engineering security requirements. In: Proceedings of the 24th IEEE International Conference on Requirements Engineering. RE '16, IEEE Computer Society (2016)

[5] Beckers, K., Pape, S., Fries, V.: HATCH: Hack and trick capricious humans – a serious game on social engineering. In: Proceedings of the 2016 British HCI Conference, Bournemouth, United Kingdom, July 11-15, 2016 (2016)

[6] Charmaz, K.: Constructing grounded theory. sage (2014)

[7] Cooper, A.: The inmates are running the asylum. indianapolis, ia: Sams. Macmillan (1999)

[8] Corbin, J., Strauss, A.: Basics of qualitative research: Techniques and procedures for developing grounded theory. Sage publications (2014)

[9] Dimkov, T., Van Cleeff, A., Pieters, W., Hartel, P.: Two methodologies for physical penetration testing using social engineering. In: Proceedings of the 26th annual computer security applications conference. pp. 399–408 (2010)

[10] Donovan, L., Lead, P.: The use of serious games in the corporate sector. A State of the Art Report. Learnovate Centre (December 2012) (2012)

[11] Faily, S., Flechais, I.: Persona cases: a technique for grounding personas. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. pp. 2267–2270 (2011)

[12] Flick, U.: An introduction to qualitative research. Sage (2014)

[13] Gläser, J., Laudel, G.: Experteninterviews und qualitative Inhaltsanalyse: als Instrumente rekonstruierender Untersuchungen. Springer-Verlag (2009)

[14] Hill, C.G., Haag, M., Oleson, A., Mendez, C., Marsden, N., Sarma, A., Burnett, M.: Gender-inclusiveness personas vs. stereotyping: Can we have it both ways? In: Proceedings of the 2017 chi conference on human factors in computing systems. pp. 6658–6671 (2017)

[15] Huang, J., Krivkovich, A., Starikova, I., Yee, L., Zanoschi, D.: Women in the workplace 2019. McKinsey & Company and LeanIn.Org, https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Gender%20Equality/Women%20in%20the%20Workplace%202019/Women-in-the-workplace-2019.pdf (2019)

[16] Kipker, D.K., Pape, S., Wojak, S., Beckers, K.: Juristische bewertung eines social-engineering-abwehr trainings. In: Rudel, S., Lechner, U. (eds.) State of the Art: IT-Sicherheit für Kritische Infrastrukturen, pp. 112–115. Universität der Bundeswehr, Neubiberg (2018), https://www.itskritis.de/_uploads/user/IT-Sicherheit%20Kritische%20Infrastrukturen%E2%80%93screen.pdf#page=112

[17] Malheiros, M., Jennett, C., Seager, W., Sasse, M.A.: Trusting to learn: Trust and privacy issues in serious games. In: International Conference on Trust and Trustworthy Computing. pp. 116–130. Springer (2011)

[18] Meuser, M., Nagel, U.: The expert interview and changes in knowledge production. In: Interviewing experts, pp. 17–42. Springer (2009)

[19] Mitnick, K.D., Simon, W.L.: The art of deception: Controlling the human element of security. John Wiley & Sons (2003)

[20] Naderer, G., Balzer, E., Batinic, B., Bauer, F., Blank, R., David, J.: Qualitative Marktforschung in Theorie und Praxis. Springer (2007)

[21] Papadaki, M., Furnell, S., Dodge, R.: Social engineering: Exploiting the weakest links. European Network & Information Security Agency (ENISA), Heraklion, Crete (2008)

[22] Peltier, T.R.: Social engineering: Concepts and solutions. Information Security Journal 15(5), 13 (2006)

[23] Petridis, P., Hadjicosta, K., Guang Shi, V., Dunwell, I., Baines, T., Bigdeli, A., F Bustinza, O., Uren, V.: State of the art in business games. International Journal of Serious Games 2(1) (2015)

[24] Pruitt, J., Adlin, T.: The persona lifecycle: keeping people in mind throughout product design. Elsevier (2010)

[25] Riedel, J.C., Hauge, J.B.: State of the art of serious games for business and industry. In: 2011 17th International Conference on Concurrent Enterprising. pp. 1–8. IEEE (2011)

[26] Schaab, P., Beckers, K., Pape, S.: A systematic gap analysis of social engineering defence mechanisms considering social psychology. In: 10th International Symposium on Human Aspects of Information Security & Assurance, HAISA 2016 ,Frankfurt, Germany, July 19-21, 2016, Proceedings. (2016)

[27] Schaab, P., Beckers, K., Pape, S.: Social engineering defence mechanisms and counteracting training strategies. Information and Computer Security 25(2), 206–222 (2017)